

Deployment Guide

This guide is for system and network engineers who [plan](#), [install](#) and [configure](#) Verba solutions.

With the Verba Recording System you have selected a flexible, software-only solution that you can deploy and configure in many ways to fit your requirements.

Step 1 - Planning your system

When you design your system you have to make decisions about how you will deploy your system.

- [Integrations](#)
- [Select a deployment architecture](#)
- [Server sizing and requirements](#)
- [Size your disks](#)
- [SQL Server requirements](#)
- [Network requirements](#)
- [Virtualization](#)
- [Silent Monitoring](#)
- [Data models](#)

[Step 2 - Installing your system](#)

[Step 3 - Configuring your system](#)

The Verba Recording System needs configuration both in your network and in the system itself.

Design

When you design your system you have to make decisions about how you will deploy your system.

Integrations

- [Microsoft Teams](#)
 - [Microsoft Teams voice, video and screen share recording](#)
 - [Microsoft Teams chat and channel archiving](#)
 - [Microsoft Teams Recording Failover and Load-balancing Design](#)
- [Microsoft Skype for Business](#)
- [Cisco](#)
 - [Cisco network based recording](#)
 - [Capturing Cisco Jabber File Transfer](#)
 - [Passive call recording for Cisco UC 320 and UC 500](#)
 - [Cisco silent monitoring](#)
 - [Cisco phones with central call recording support](#)
- [Avaya](#)
- [Symphony](#)
- [Zoom](#)
- [BT IP Trade](#)
- [BT ITS](#)
- [IPC Unigy](#)
- [Cloud9](#)
- [Speakerbus](#)
- [Genesys](#)
- [Passive, extension side call recording](#)
- [Passive, trunk-side call recording](#)
- [Dial-in audio and video call recorder](#)
- [Screen capture](#)
- [SMS capturing for mobile networks](#)

Select a deployment architecture

- [Single server architecture](#)
- [Multi site architecture](#)
- [Desktop deployment](#)
- [Redundancy options](#)
- [Multi server architectures with load balancing and failover](#)

Server sizing and requirements

- [Media Recorder sizing for voice, video, screen - application share recording](#)
- [Ethical Wall and IM Recording server requirements](#)

Size your disks

- [Understanding RAID](#)
- [Storage requirements](#)

SQL Server requirements

Network requirements

- [IPv6 support](#)

Virtualization

- [VMware](#)
- [Microsoft Hyper-V](#)
- [Co-residency with virtualized Cisco UC applications](#)
- [Co-residency on Cisco SRE modules](#)

Silent Monitoring

Data models

Integrations

The system offers several integration options for recording, capturing, or importing conversation data. This article provides the list of supported integrations and the links to the detailed description of each.

Category	Platform	Technology	Modalities	More information	
Unified Communications	Cisco UCM (CUCM)	Network-based, JTAPI	Voice, Desktop Screen	Cisco	
	Cisco UBE (CUBE)	SIPREC	Voice, Video, Desktop Screen	Cisco	
	Cisco Voice Gateway	XCC	Voice, Desktop Screen	Cisco	
	Cisco IM&P	IM&P Compliance API	Chat, Attachment		
	Cisco	Proxy-based	Voice, Video, Screen /Application Share ¹ , Desktop Screen	Cisco	
	Cisco Webex Teams	Import	Chat, Attachment	Cisco Webex Teams	
	Microsoft Skype for Business	Proxy-based, Import	Voice, Video, Screen /Application Share, Chat, Attachment, Polls, Q&A, Whiteboard, Desktop Screen	Microsoft Skype for Business	
	Microsoft Teams		Bot	Voice, Video, Screen /Application Share, Desktop Screen	Microsoft Teams
			Webhook / Export API	Chat, Attachment	Microsoft Teams
	Avaya CM	DMCC multiple registrations	Voice, Desktop Screen	Avaya	
Avaya ESBC	SIPREC	Voice, Video, Screen /Application Share ¹ , Desktop Screen			

	BroadSoft BroadWorks	SIPREC	Voice, Video, Screen /Application Share ¹ , Desktop Screen	
	Oracle/ACME Packet SBC	SIPREC	Voice, Video, Screen /Application Share ¹ , Desktop Screen	
	MetaSwitch Perimeta SBC	SIPREC	Voice, Video, Screen /Application Share ¹ , Desktop Screen	
	SIP/SCCP compatible	Network port mirroring	Voice, Video, Screen /Application Share ¹ , Desktop Screen	
	SIP compatible	Dial-in and dial-out recorder	Voice, Video, Screen /Application Share ¹ , Desktop Screen	
	Symphony	SIPREC, Import	Voice, Screen /Application Share, Chat, Attachment, Desktop Screen	Symphony
	Bloomberg Chat	Import	Chat, Attachment	Bloomberg Instant Messages
	RingCentral	Import	Voice	RingCentral
	Huawei	SIP-based forking	Voice, Desktop Screen	
	Tango Networks	SIP-based forking	Voice, Desktop Screen	
Contact Center	Genesys PureEngage	SIP-based forking, CTI	Voice, Desktop Screen	Genesys
	Cisco UCCE	Network-based, JTAPI, CTI	Voice, Desktop Screen	Cisco UCCX Integration
	Cisco UCCX	Network-based, JTAPI, CTI	Voice, Desktop Screen	Cisco UCCE Integration

	Luware LUCS	Proxy-based	Voice, Video, Screen /Application Share, Desktop Screen	
	Luware Nimbus	Bot	Voice, Video, Screen /Application Share, Desktop Screen	
Trader Voice	BT ITS	IPSI, ITSLink	Voice	BT ITS
	BT IP Trade	Recorder API	Voice	BT IP Trade
	IPC Unigy	SIP, CTI	Voice	IPC Unigy
	Speakerbus	RTP, iCDS	Voice	Speakerbus
	Cloud9	Import	Voice	Cloud9
Mobile	Truphone	SIP-based forking	Voice, Desktop Screen	
	Centile	Import	Voice	
	O2	Import	Voice	O2
	Vodafone	Import	Voice	Vodafone
	Singtel	SIPREC	Voice	
	SMS	SMPP	SMS	SMS capturing for mobile networks
Radio	Analogue	Synology TAP card	Voice	
	Bosch Telex	RTP streaming	Voice	
	Generic RTP streaming	-	Voice	

¹ SIP/BFCP based screen and application share recording is supported, mixed into video call recording, not available as a separate recording

Microsoft Teams

- [Overview](#)
 - [Microsoft Teams recording features](#)
 - [Voice, video, and screen/application window share recording](#)
 - [Chat and channel archiving](#)
 - [Version support](#)
- [Deploying Microsoft Teams recording and archiving](#)

Overview

Microsoft Teams recording features

- Voice, video, screen/application window share recording, and chat and channel archiving
- Integration with the official Microsoft Teams Compliance Recording API and Graph API
- Support for load balancing and failover
- Supports all types of Teams endpoints and devices

Voice, video, and screen/application window share recording

- Bot based integration, where the Teams platform is able to automatically invite the recorder bot into P2P calls or meetings for the configured users
- Support for Azure cloud and hybrid deployments
- Fail-close configuration option (in case of recorder failure, the recorded user cannot join the call)
- Supports always-on, selective, and on-demand recording
- Supports all call scenarios where the recorded user is a participant
- Built-in announcement and notification (provided by the Teams platform)
- For more information, see [Microsoft Teams voice, video and screen share recording](#)

Chat and channel archiving

- Multiple integration options:
 - Event/webhook, DLP API based integration, where the Teams platform sends all updates once the recorder subscribes
 - Export API based integration, where the system can query and download messages and attachments for configured users (chats) and teams (channels)
- Support for on-prem, cloud, and hybrid deployments
- Supports always-on recording mode only
- Supports all instant message scenarios, teams, channels, P2P, and meeting chats
- Support for attachments
- Supports all formatting options, emojis, giphys, stickers, and other apps
- **Limitation: labeling and case rules are not supported**
- For more information, see [Microsoft Teams chat and channel archiving](#)

Version support

Switch Name & Model	Microsoft Teams
---------------------	-----------------

Supported Microsoft Teams Versions for voice, video, and screen /application window share recording	<p>Voice, video, and screen/application window share recording (Compliance Recording) are available to all:</p> <ul style="list-style-type: none"> • Microsoft 365 A3/A5/E3/E5/Business Premium and • Office 365 A3/A5/E3/E5 users • with no additional consumption charge. <p>For more information, see https://docs.microsoft.com/en-us/microsoftteams/teams-recording-policy</p>
Supported Microsoft Teams Versions for chats and channel archiving	<p>Chat and channel archiving requires one of the following user licenses for bot Webhook/DLP and Export API deployments for all archived users:</p> <ul style="list-style-type: none"> • Office 365 A5/E5 • Microsoft 365 A5/E5 • Microsoft 365 Information Protection and Governance • Office 365 Advanced Compliance <p>For more information, see https://docs.microsoft.com/en-us/office365/servicedescriptions/microsoft-365-service-descriptions/microsoft-365-tenantlevel-services-licensing-guidance/microsoft-365-security-compliance-licensing-guidance#microsoft-graph-apis-for-teams-data-loss-prevention-dlp-and-for-teams-export</p> <p>In addition to the user license requirements above, the owner of the application registration must define the licensing model for the deployment. Model A is required for Security and Compliance (S+C) and general usage scenarios. The licensing model is configurable in the VFC system.</p> <p>For more information about seeded capacity and consumption fees, see https://docs.microsoft.com/en-us/graph/teams-licenses.</p>
Supported Endpoint / DeviceTypes	<p>All</p>

If you are on a different version, contact your Microsoft representative for more information.

Deploying Microsoft Teams recording and archiving

For more information about deploying Microsoft Teams voice, video and screen/application window share recording, see [Microsoft Teams voice, video and screen share recording](#).

For more information about deploying Microsoft Teams chat and channel archiving, see [Microsoft Teams chat and channel archiving](#)

Microsoft Teams voice, video and screen share recording

- [Deploying Microsoft Teams voice, video and screen share recording](#)
 - [Server sizing](#)
 - [Load-balancing and Failover](#)
 - [Preparation](#)
 - [Installation](#)
 - [Configuration](#)
- [Microsoft Teams metadata for voice, video and screen & application share recordings](#)

Deploying Microsoft Teams voice, video and screen share recording

The following section contains all the necessary steps for setting up a Microsoft Teams recording infrastructure.

Server sizing

According to the Microsoft requirements, the Microsoft Teams Bot service must run on an Azure Virtual Machine. Requirements for the Recording Server role, which will host the Verba Microsoft Teams Bot service and the Unified Call Recorder service are:

- Azure Compute Unit (ACU) should be 200 or higher and 1:1 ratio for vCPU: Core
<https://docs.microsoft.com/en-us/azure/virtual-machines/acu>
- We recommend using the Dv2 series virtual machines, Standard_D3_v2 or above
<https://docs.microsoft.com/en-us/azure/virtual-machines/dv2-dsv2-series#dv2-series>
- ILPIP (Instance Level Public IP Address) for the Recording Servers
Private IP addresses are not recommended by Microsoft, due to potential performance limitation caused by the Azure NAT, although will work
- For resilient and/or high volume configurations, multiple virtual machines (running the Recording Server role) have to be deployed. In order to distribute the load across multiple Verba Microsoft Teams Bot services, an **Azure Application Gateway** has to be deployed in front of the VMs.
<https://docs.microsoft.com/en-us/azure/application-gateway/overview>

Due to performance limitations in the Microsoft Local Media SDK, the Recording Server sizing for Microsoft Teams recording is different from other integrations. The following table summarizes the server sizing for Microsoft Teams recording:

Modality	per vCPU
Voice	50
Voice and Screen & Application Share Up to x1 1080p stream / call	30
Voice and Video Up to x4 360p video streams / call	15

The values indicate the number of maximum simultaneous calls for the specified modalities per vCPU.

Testing was done with mixed audio on Azure D3v2 (4 cores), D4v2 (8 cores), and D5v2 (16 cores) virtual machines.

For requirements for other components and server roles, see [Server sizing and requirements](#)

Load-balancing and Failover

Large deployments may require multiple VMs and other Azure components.

For the failover and load-balancing options for voice, video, and screen/application window share recording, see:

[Microsoft Teams Recording Failover and Load-balancing Design](#)

Preparation

The Microsoft Teams integration requires additional prerequisites and configuration on Azure and O365, see [Configuring Microsoft Teams Recording](#) for more information.

Make sure that all the required prerequisites are installed on each server prior to the installation.

- [Prerequisites](#)
- [Installing the required prerequisites](#)

For guidance on configuring the necessary firewall port, visit [Firewall configuration for Microsoft Teams recording deployments](#)

Installation

The following articles contain all the steps for installing the various server roles:

- [Installing a Verba Single Server solution](#)
- [Installing a Verba Media Repository](#)
- [Installing a Verba Recording Server](#)

Configuration

For the configuration guide for voice / video / screen share recording, see [Configuring Microsoft Teams Recording](#).

Microsoft Teams metadata for voice, video and screen & application share recordings

The system captures the following metadata specific to Microsoft Teams voice/video/screen recordings.

Metadata Field	Description	Template	Available
Start Date	Start date of the conversation	Standard	Yes
Start Time	Start time on the conversation	Standard	Yes
End Date	End date of the conversation	Standard	Yes
End Time	End time of the conversation	Standard	Yes
Duration	Length of the conversation	Standard	Yes
User	Name of the recorded user	Standard	Yes

From	Phone number, Button name, User name	Standard	Yes
From Info	User / contact name	Standard	Yes
To	Phone number, Button name, User name	Standard	Yes
To Info	User / contact name	Standard	Yes
Direction	Direction of the call from the system perspective requires configuring internal number/domain patterns	Standard	Yes
Direction (User)	Direction of the call from the recorded user perspective	Standard	Yes
From (Verba)	Name of the Verba user associated with the calling party	Standard	Yes
To (Verba)	Name of the Verba user associated with the called party	Standard	Yes
Location	Hostname of the recording server	Standard	Yes
End Cause	Normal, Hold, Transfer, Conference, Device Change, From Terminated, To Terminated	Standard	Yes
Audio Codec	Audio codec of the recorded streams	Standard	Yes
Video codec	Video codec of the recorded streams	Standard	Yes
Platform Call ID	Unique conversation identifier received from the recorded platform	Standard	Yes
Silence Ratio	Ratio of silence in the conversation	Standard	Yes
Talkover Ratio	Talkover ratio of the conversation	Standard	Yes
Longest Silence	Length of the longest silence present in the conversation	Standard	Yes
User ID / Agent ID	Azure AD Object ID for the recorded user	Standard	Yes
From Device	Device ID of the calling party	Standard	No
To Device	Device ID of the called party	Standard	No
Dialed Number	Original dialed number	Standard	No
From IP	Defaults to 127.0.0.1 as the IP address of the devices are not available	Standard	Yes
To IP	Defaults to 127.0.0.1 as the IP address of the devices are not available	Standard	Yes
From Proxy IP	IP address of the proxy server associated with the caller party	Standard	No
To Proxy IP	IP address of the proxy server associated with the called party	Standard	No
Source Platform	Microsoft Teams	Standard	Yes
Conversation Type	Voice, Video, Screen Share	Standard	Yes
Forward Reason	Forward reason for the conversation (e.g. forwarded, transferred, team call, delegated, etc.)	Standard	No
Recording failed	Indicates if the recording has failed and the metadata was imported during CDR reconciliation	Standard	No
Media Length	Length of the media file related to the conversation in hh:mm:ss format	Standard	Yes
Media Error	Shows the media processing errors during recording	Standard	Yes
Voice Quality	Overall voice quality check score for the conversation	Standard	Yes
Record Type	Standard	Standard	Yes
2N Source	In case of duplicate (2N) recording, records are marked as primary or secondary	Standard	No
Meeting Subject	Subject of the recorded meeting	Microsoft Teams	Yes
Meeting Organizer ID	Azure AD Object ID of the recorded meeting organizer	Microsoft Teams	Yes

Meeting Organizer Name	Name of the recorded meeting organizer	Microsoft Teams	Yes
Compliance Policy	Name of the compliance policy configured in Microsoft Teams for the recorded user which triggered the recording of the call or meeting	Microsoft Teams	Yes

Microsoft Teams chat and channel archiving

Overview

Microsoft provides 2 set of Graph APIs to archive chat and channel messages for Microsoft Teams. The Verba system supports both integrations. The following table provides a comparison of the 2 integration options.

	Feature	Webhook/DLP API
Capture	Internal chat (peer-to-peer and group) messages and files	Supported
	External chat (peer-to-peer and group) messages and files	Supported Files can only be archived if the chat is started by an i
	Internal channel messages and files	Supported
	Internal meeting messages and files	Supported
	External meeting messages and files	Supported Files cannot be archived unless the meeting is hosted
	Private channel messages and files	Supported
	Channel announcement	Supported
	Replies	Supported
	Reactions	Supported
	Emoticons	Supported
	Animated GIFs, Stickers, Praises, and other rich content	Supported
	Send email to channel	Supported
	Loop components	Not supported
	OneNote	Not supported
Participant join/leave events	Supported based on periodic membership queries an is not 100% accurate all the time. VFC data is only as a	

	Selective capture	Supported for both chats and channels with limitation time (see below)
	Participant information	Chat and channel membership information is collected by querying Graph API endpoints and caching the data on the server.
	Disclaimer notification	Not supported
Architecture	Integration with Microsoft Graph APIs	<p>The Webhook/DLP API is a set of Microsoft Graph APIs that capture both chat and channel messages in a Teams tenant. The system captures messages and attachments.</p> <p>For more information, see https://docs.microsoft.com/en-us/microsoft-graph/using-webhooks.</p> <p>The system utilizes other Graph APIs to collect additional information such as group membership, etc.</p>
	Data segregation, access to regulated users' data only	Not supported, the webhook sends data for every user and the files in the file queue are encrypted automatically.
	Load balancing for Recording Director	Supported via load balancers
	Load balancing for Media Recorder	Supported via file queues
	Failover for Recording Director	Supported via load balancers
	Failover for Media Recorder	Supported by deploying standby servers
	Scalability for Recording Director	Scales by adding more servers behind a load balancer
	Scalability for Media Recorders	Scales by adding more servers
	Possible data loss scenarios	<ul style="list-style-type: none"> • Microsoft only retries sending events a few times, by deploying multiple Recording Directors behind a load balancer. • Data loss is possible if selective archiving is configured (see Participant Information for more information).
	Multi-tenancy	Supported
	Data duplication	No duplication, messages and files are stored only on the same chat or channel.
Export	Export	<p>SMTP based export only</p> <p>User/participant based or conversation/chat based export</p>

Licensing	Microsoft licensing	<p>Instant message, and attachment archiving requires c</p> <ul style="list-style-type: none"> • Office 365 A5/E5 • Microsoft 365 A5/E5 • Microsoft 365 Information Protection and Govern • Office 365 Advanced Compliance <p>For more information, see https://docs.microsoft.com/licensing-guidance#microsoft-graph-apis-for-teams-c</p> <p>In addition to the user license requirements above, th scenarios. The licensing model is configurable in the \</p> <p>For more information about seeded capacity and con</p>
Limitations	Limitations	-

Deploying Microsoft Teams chat and channel archiving

The following section contains all the necessary steps for setting up a Microsoft Teams chat and channel archiving infrastructure.

Server sizing

The IM recording architecture includes two server roles: Recording Director and Media Recorder. These roles have different sizing numbers and different factors have to be taken into account. Since the Recording Director has a small footprint compared to the Media Recorder, they are usually not separated but deployed as a single recorder.

Rule of thumb for server sizing

The following table shows the expected incoming message rates at different user numbers:

	1K Users	10K Users	100K Users
Average during the day*	1.6 msg/s	16.6 msg/s	166.6 msg/s
Low message rate**	2.7 msg/s	27.7 msg/s	277.7 msg/s
Medium message rate**	4.1 msg/s	41.6 msg/s	416.6 msg/s
High message rate**	6.9 msg/s	69.4 msg/s	694.4 msg/s

*Based on Slack usage statistics

**Based on Cisco IM/P sizing

Based on the statistics above, if the daily IM message rate has to be processed **within 8 hours**, then a **single recorder core** can handle **13K users**.

If it is enough to process the messages **within 16 hours**, then a **single recorder core** can handle **26K users**.

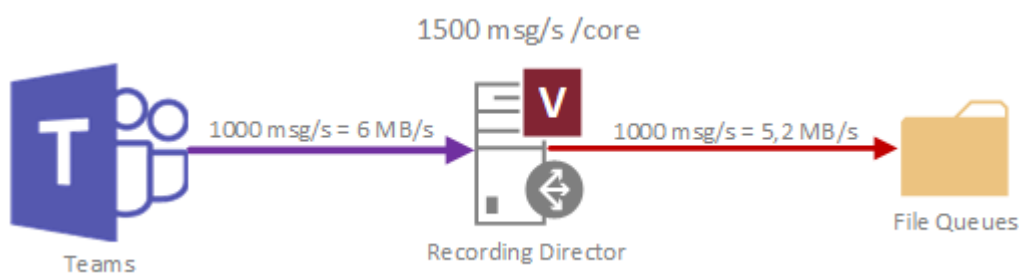
For more real-time processing during peak hours, extra CPU cores can be added:

- In the case of the real-time processing of the **low message rate**, a single CPU core can handle **8K users**.
- In the case of a **medium message rate**, a single CPU core can handle **5K users**.
- In the case of a **high message rate**, a single CPU core can handle **3K users**.

For requirements for other components and server roles, see [Server sizing and requirements](#)

For the detailed sizing guidelines of the different Recording Server components, see the paragraphs below:

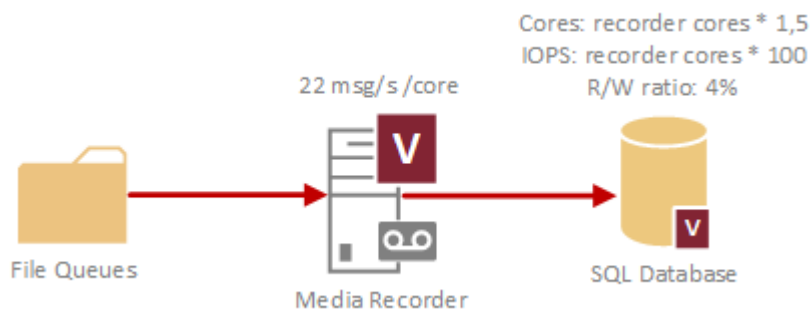
Recording Director



In the case of the Webhook/DLP API, the Recording Director component **has to be sized based on the real-time incoming load**. The minimum CPU requirement is 4 CPU cores. It can process **1500 messages every second with a single CPU core**, and 6000 messages every second with 4 cores.

In the case of higher incoming loads, the network bandwidth also has to be considered. 1000 messages per second incoming load generate 48 Mbps traffic (or 6 MB/s) between the Teams side and the Recording Director, and 42 Mbps traffic (or 5.2 MB/s) between the Recording Director and the file queue storage.

Media Recorder and SQL Server



The Media Recorder component does not have to be sized for real-time processing, since the recorded data is stored already in the file queue storage. Instead, the **Media Recorder can be sized based on the overall message count a day**. If there are more incoming messages than the real-time processing capacity of the Media Recorder(s), then the messages will be inserted into the database later, so they will be also available for search and replay through the web interface later. However, sufficient processing capacity should be provided so it can process the daily message load at least within 16 hours.

The minimum CPU requirement is 4 CPU cores. It can process **22 messages every second with a single CPU core**. In the case of multiple Media Recorder servers, all servers have to have the same number of cores.

The Recorder Director and the Media Recorder components can be co-located on the same server. In this case, the resources will be shared between them.

The **SQL Server** has to be sized based on the fully utilized CPU cores of the Media Recorder server(s). The SQL Server needs to have **one and a half times more CPU cores than the Media Recorder server(s)**. On the SQL Server physical disk, **every fully utilized Media Recorder CPU cores generate 100 IOPS**.

Load-balancing and Failover

Large deployments may require multiple VMs and other Azure components. In the case of the Webhook/DLP API, a load-balancer has to be placed in front of the Recording Servers (Recording Directors).

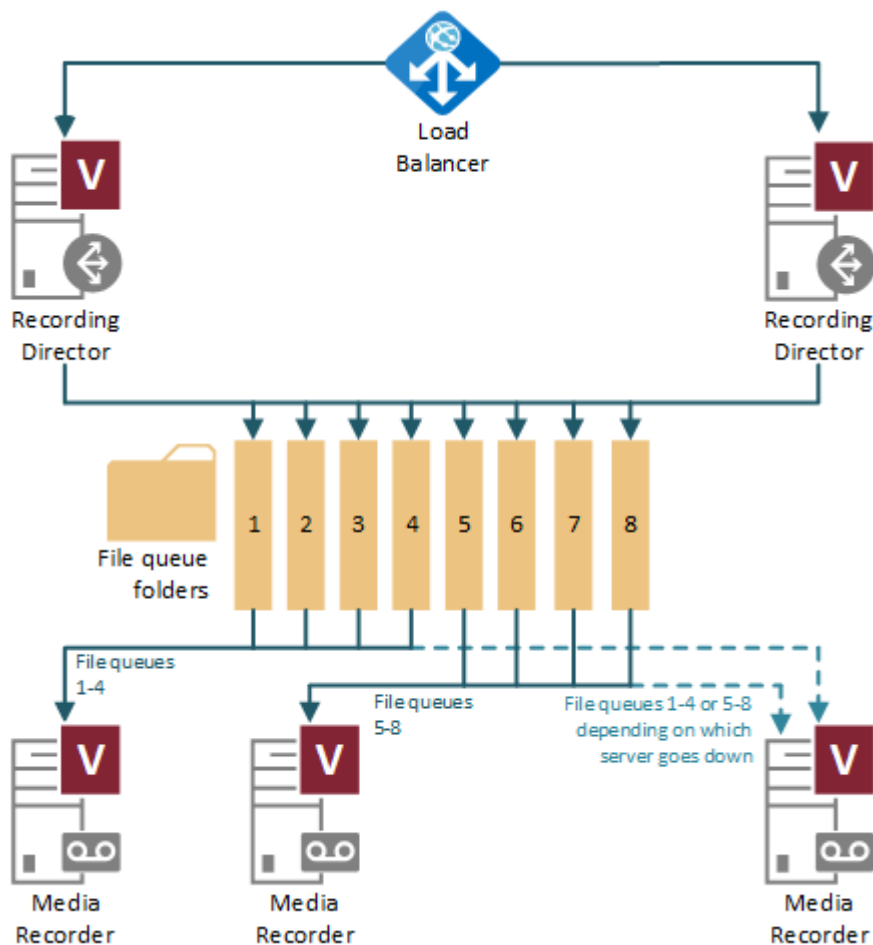
If the Recording Director and Media Recorder roles are separated, multiple Media Recorders can be deployed behind the Recording Director (s).

In the case of the Webhook/DLP API, only one of the Recording Director components is writing into the file queues at once, depending on which one receives the events from the Application Gateway. The other Recording Director(s) will be on standby.

In the case of the Export API however, the active Recording Director components divide the user list amongst each other equally, and only query the chats of their own portion of the user list. The standby Recording Director(s) will become active only if an active one goes down. In that case, it takes over the user list portion of the server that went down.

The Media Recorder component works the same way regardless of the API being used. File queues are distributed between the active Media Recorders equally. Standby Media Recorders will become active only if an active Media Recorder goes down. In that case, it takes over the file queues of the server that went down.

Highly available setup with separated server roles:



Preparation

Make sure that all the required prerequisites are installed on each server prior to the installation.

- [Prerequisites](#)
- [Installing the required prerequisites](#)

For guidance on configuring the necessary firewall port, visit [Firewall configuration for Microsoft Teams recording deployments](#)

Installation

The following articles contain all the steps for installing the various server roles:

- [Installing a Verba Single Server solution](#)
- [Installing a Verba Media Repository](#)
- [Installing a Verba Recording Server](#)

Configuration

For chat and channel archiving, see [Microsoft Teams chat and channel archiving](#).

Microsoft Teams Recording Failover and Load-balancing Design

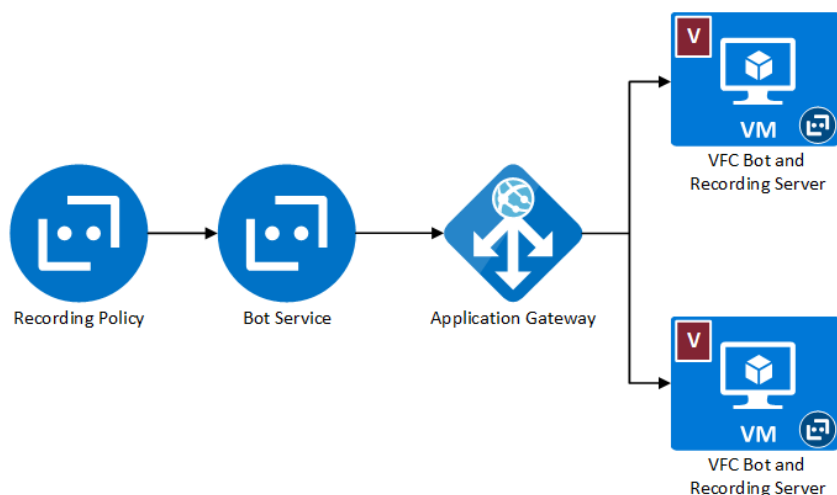
Large Microsoft Teams recording deployments can require multiple Bot and Recording Servers, and other Azure components. The following article describes the possible scenarios.

For the general overview of the Microsoft Teams recording refer to the [Microsoft Teams](#) article.

Load-balancing and Failover with Azure Application Gateway

If a single Azure VM is not enough for handling the incoming load, or it is more cost-efficient using multiple smaller VMs instead of a single large VM, then load-balancing has to be configured between the VMs. For this purpose, an Azure Application Gateway can be used. It is also capable of adding high availability to the deployment. An Application Gateway can provide N+1 (next-call) failover capability.

The following diagram shows the usage of an Application Gateway:



Geographical Routing for Global Deployments

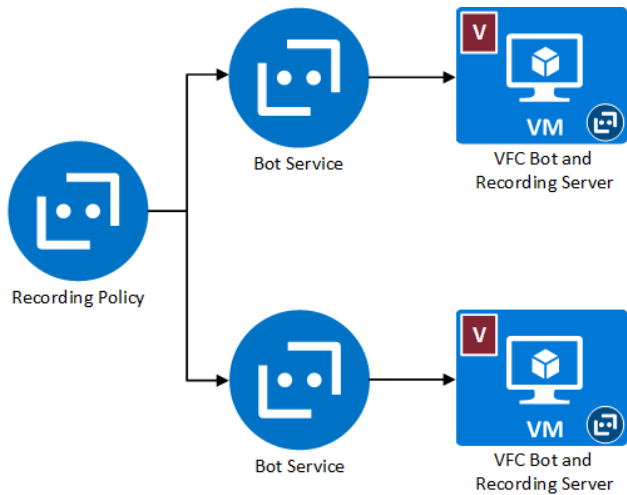
In the case of large global deployments, multiple Bot servers may be deployed in multiple geographical regions. For the geographical routing, a Traffic Manager can be used instead of the Application Gateway. The Traffic Manager can balance the load between Bot servers within the same geographical region.

2N Recording

Microsoft Teams can be configured for 2N recording also. In this case, all the components that take part in the recording have to be duplicated, and assigned to the same recording policy.

If the recording policy is set to strict mode, then the recorded Teams user will be kicked out of the call only if both bot VMs are down. If a single bot VM is still up, then the recorded Teams user can still join into calls.

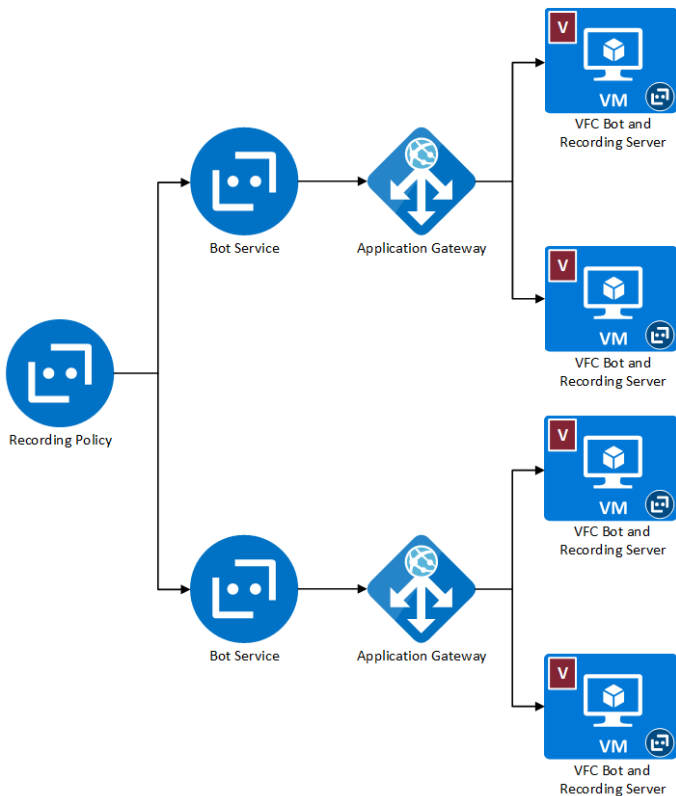
The following diagram shows the 2N recording architecture for Microsoft Teams:



2N Recording and Load-balancing

If multiple Bot and Recording Servers needed for handling the incoming load, and the 2N recording is also required, then the Application Gateway also has to be duplicated.

The following diagram shows the combination of the load-balancing and the 2N recording scenario:



Availability Sets and Availability Zones

When N+1 or 2N recording is configured, it is recommended to use Availability Sets or Availability Zones if possible. When using Availability Sets, the virtual machines are separated within the Azure datacenter, so it provides a more fail-proof functioning. On the other hand, Availability Zones physically separates the virtual machines into different zones (different datacenters) within the Azure region, so it provides even higher SLA. For more information, see [Availability options for virtual machines in Azure](#).


Microsoft Skype for Business

Overview

The Verba Recording System can record Microsoft Lync **voice calls, video calls, and instant messages** using various methods.

There are **five main components** of the Lync/SfB recording solution:

- **Verba Single Server solution:** The Verba Media Repository and the Verba Recording Server co-located on one server
- **Verba Media Repository:** Stores recordings, provides web access, storage management, security and auditing
- **Verba Recording Server:** Takes collected traffic and signaling and generates recorded calls with media and call detail records. **Contains the Verba Media Collector & Proxy role also.**
- **Verba Media Collector & Proxy:** The Media Collector component sends collected traffic to recording servers. The Proxy component proxying the calls, so they can be captured at a single point.
- **Verba SfB/Lync Front End filter plugin:** Collects the signaling and gathers the encryption keys for the media.

 **The filter plugin is necessary to be installed on all Skype / Lync Front-Ends and SBAs** because Lync communication is **encrypted**. It provides:

- **signaling information** - detailed information directly from the Lync/SfB Front-Ends
- **decryption keys** - used to decipher the media recorded from the network by the recording servers

Supported platforms

Supported Microsoft platforms:

- Microsoft Lync Server 2010
- Microsoft Lync Server 2013
- Microsoft Skype for Business

All software and physical SfB/Lync compatible endpoints are supported.

Deployment models

Depending on recording requirements different deployment models are recommended. In the Verba solution, these models can be mixed even within one recording system. The goal is the same in all situations: place recorders or traffic collectors to network locations/servers, where the media streams you want to record are passing through.

The following table summarizes the different ways the Verba Recording Servers components can be deployed.

	Media Collector & Proxy on separate servers	Media Collector installed on Mediation Servers	Recording Server with Monitor Port
No need for monitor port	YES	YES	
Call media path untouched		YES	YES
Internal calls	YES		YES 1
Inbound / Outbound calls	YES	YES	YES


Inbound / Outbound calls with media bypass	YES		YES 2
Remote / Federated calls	YES***	YES***	3
Application share	YES		3
Branch Office Survivability	YES	YES	YES
Geographical routing in large deployments	YES		

***Optionally the Media Collector component can be installed on the Edge servers. This makes possible to record federated calls also. See Recording federated calls paragraph.

¹ Requires endpoint level monitor port configuration

² Requires gateway port monitoring

³ Certain calls can be recorded by monitoring the Edge Server port(s)

 **In all scenarios the Verba SfB/Lync Filter component has to be installed on the Frontend servers.** If the Mediation role is colocated with the Frontend role, then both the Filter and the Media Collector role has to be installed on the Frontend.
For the installation guide see: [Installing the Verba Skype for Business - Lync Filter](#) or [Installing the combined Verba Lync Filter and Media Collector on a Lync server](#).

Media Collector & Proxy on separate servers

The proxy-based SfB/Lync recording environment allows Verba to record all inbound/outbound and internal calls.

Possible deployment models of Proxy-Based recording:

- **Single server solution:** All Verba services (Administration, Recorder, Proxy) are on one server.
For the installation guide see: [Installing a Verba Single Server solution](#)
- **Single server solution + Co-located Recorder and Proxy server(s):** All Verba services (Administration, Recorder) are on one server. Additional Recorder Server(s) deployed for recording high availability.
For the installation guide see: [Installing a Verba Single Server solution](#) and [Installing a Verba Recording Server](#)
- **Media Repository + Co-located Recorder and Proxy server(s):** The Verba administration/storage and the Recording server is deployed separately. For recording and proxy high availability additional Recorder Servers can be installed.
For the installation guide see: [Installing a Verba Media Repository](#) and [Installing a Verba Recording Server](#)
- **Deploy every server separately:** Best performance for proxy based recording. For high availability multiple Recorder Servers and multiple Proxy Servers can be installed.
For the installation guide see: [Installing a Verba Media Repository](#), [Installing a Verba Recording Server](#) and [Installing the Verba Media Collector and Proxy component](#)

Media Collector installed on Mediation Servers

The Mediation-based Lync recording environment allows us to record all inbound/outbound calls in our Lync system.

Possible deployment models of Mediation Based recording:

- **Single server solution + Media Collectors:** All Verba services (Administration, Recorder) are on one server. For the installation guide see: [Installing a Verba Single Server solution](#) and [Installing the Verba Media Collector and Proxy component](#)
- **Single server solution + Recorder Server(s) + Media Collectors:** All Verba services (Administration, Recorder) are on one server. Additional Recorder Server(s) deployed for recording high availability. The Media Collectors have to be installed on the Mediation servers. For the installation guide see: [Installing a Verba Single Server solution](#), [Installing a Verba Recording Server](#) and [Installing the Verba Media Collector and Proxy component](#)
- **Media Repository + Recorder Server(s) + Media Collectors:** The Verba administration/storage and the Recording server is deployed separately. For recording high availability additional Recorder Servers can be installed. The Media Collectors have to be installed on the Mediation servers. For the installation guide see: [Installing a Verba Media Repository](#), [Installing a Verba Recording Server](#) and [Installing the Verba Media Collector and Proxy component](#)

Installing the Verba Media Collector

- If your Mediation / AVMCU server(s) are co-located on your Front End(s), install the [Verba Media Collector and Lync Filter](#) role on all of them.
- For standalone Mediation servers, install the [Verba Media Collector and Proxy Server role](#) on every Mediation server.

Recording federated calls

Federated calls can be captured on the Edge servers. For this, the Media Collector and Proxy component have to be installed on all Edge servers.

For the installation guide see: [Installing the Verba Media Collector and Proxy component](#)

Recording Server with Monitor Port

The Monitor Port based recording requires network side configuration:

- [Passive, trunk-side call recording](#)
- [Passive, extension side call recording](#)

Possible deployment models of Monitor Port based recording:

- **Single Server solution:** All Verba services (Administration, Recorder) are on one server. For installation guide see: [Installing a Verba Single Server solution](#)
- **Media Repository + Recorder Server(s):** The Verba administration/storage and the Recording server is deployed separately. For the installation guide see: [Installing a Verba Media Repository](#) and [Installing a Verba Recording Server](#)



For more information about the deployment models see [Select a deployment architecture](#)

Cisco

Overview

The Verba Recording System can record Cisco **voice calls, video calls and instant messages** using various methods.

There are **five main components** of the Cisco recording solution:

- **Verba Single Server solution:** The Verba Media Repository and the Verba Recording Server co-located on one server
- **Verba Media Repository:** Stores recordings, provides web access, storage management, security, and auditing
- **Verba Recording Server:** Receives collected traffic and signaling and generates media files and call detail records. **Contains the Verba Media Collector & Proxy role as well**
- **Verba Media Collector & Proxy:** The Media Collector component sends collected traffic to recording servers. The Proxy component relays calls, so they can be captured at a single point.

Supported platforms

Verba supports all Cisco Unified Communication Manger, Unified Communication Express and IM & Presence versions.

All software and physical Cisco compatible endpoints are supported.

Deployment models

Depending on recording requirements different deployment models are recommended. In the Verba solution, these models can be mixed within one recording system deployment.

The following table summarizes the different ways the Verba Recording Servers components can be deployed.

	Verba Network-based Recording	Passive / Monitor Port Based Recording	Verba Proxy-based Recording***
No need for monitor port	YES		YES
Call path untouched	YES	YES	
Internal Audio Calls	YES ⁶	YES ¹	YES *
Inbound / Outbound Audio Calls	YES	YES ²	YES *
Video Calls		YES	YES
Encrypted Video Calls			YES
Presentation Sharing		YES ¹	YES
External / Federated calls (ExpressWay)	YES ⁷	YES ³	YES
Recording Announcements for incoming PSTN calls	YES	YES	YES
Block Calls on recording failure			YES
Load balancing	YES		YES

Mid-call failover	YES		YES
2N recording	5	YES ⁴	YES
N+1 recording	YES		YES
JTAPI Integration	YES		
CDR reconciliation	YES		

***** Verba Proxy-based Recording is recommended only in specific cases since it requires a complex custom call routing setup in the UCM!**

¹ Requires endpoint level monitor port configuration

² Requires gateway port monitoring

³ Calls can be recorded by monitoring the internal ExpressWay port(s)

⁴ Requires multiple monitor ports

⁵ Can be achieved by combining with port monitoring

⁶ Only with Built-in Bridge-based (Phone Preferred) recording mode. With Gateway based recording, only inbound and outbound PSTN calls can be recorded.

⁷ Requires ExpressWay version 8.11 or later.

* Limitations at parking scenarios

Verba Network-Based Recording


Possible deployment models of Network Based recording:

- **Single server solution:** All Verba roles (Media Repository, Recorder, Proxy) are on one server. For the installation guide see: [Installing a Verba Single Server solution](#)
- **Single server solution + Recording server(s):** All Verba roles (Media Repository, Recorder) are on one server. Additional Recording Server(s) deployed for recording high availability. For the installation guide see: [Installing a Verba Single Server solution](#) and [Installing a Verba Recording Server](#)
- **Media Repository + Recording server(s):** The Verba Media Repository and the Recording server is deployed separately. For recording high availability additional Recorder Servers can be installed. For Web Application high availability additional Media Repositories can be deployed. For the installation guide see: [Installing a Verba Media Repository](#) and [Installing a Verba Recording Server](#)

Verba Proxy-Based Recording

Possible deployment models of Proxy-Based recording:

- **Single server solution:** All Verba roles (Media Repository, Recorder, Proxy) are on one server. For the installation guide see: [Installing a Verba Single Server solution](#)
- **Deploy every role separately:** Best performance for proxy based recording. For high availability, multiple Recording Servers and multiple Proxy Servers can be installed. For the installation guide see: [Installing a Verba Media Repository](#), [Installing a Verba Recording Server](#) and [Installing the Verba Media Collector and Proxy component](#)
- **Co-locate certain roles:** Verba Roles can be selectively co-located for mid-size deployments. The possible co-locations are as follows:
 - **Media Repository and Recording Server:** This server is performing the functions of both the Media Repository and the Recording Server. For the installation guide see: [Installing a Verba Single Server solution](#)
 - **Recording Server and Proxy Server:** This server is able to relay and record calls. The communication taking place between 2 services on the same machine will reduce the network bandwidth requirements. For the installation guide see: [Installing a Verba Recording Server](#)

 The Proxy Server role is always installed when a Recording Server role is installed. After the deployment, it can optionally be turned on or off.


Passive / Monitor Port-Based Recording

The Monitor Port based recording requires network side configuration:

- [Passive, trunk-side call recording](#)
- [Passive, extension side call recording](#)

Possible deployment models of Monitor Port based recording:

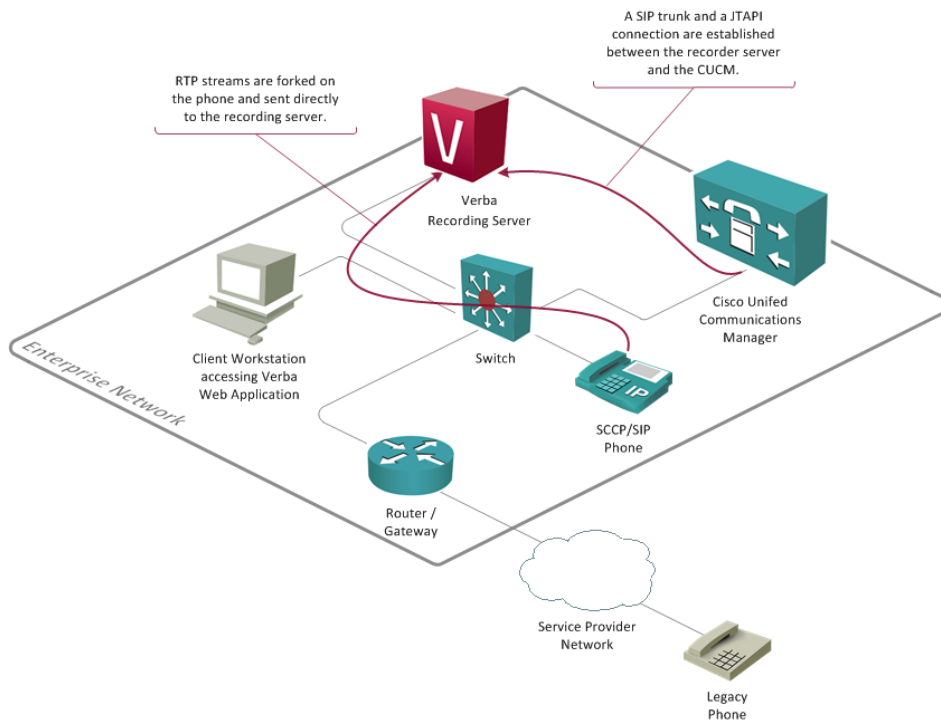
- **Single server solution:** All Verba roles (Media Repository, Recorder, Proxy) are on one server.
For the installation guide see: [Installing a Verba Single Server solution](#)
- **Single server solution + Recording server(s):** All Verba roles (Media Repository, Recorder) are on one server. Additional Recording Server(s) deployed for recording high availability.
For the installation guide see: [Installing a Verba Single Server solution](#) and [Installing a Verba Recording Server](#)
- **Media Repository + Recording server(s):** The Verba Media Repository and the Recording server is deployed separately. For recording high availability additional Recorder Servers can be installed. For Web Application high availability additional Media Repositories can be deployed.
For the installation guide see: [Installing a Verba Media Repository](#) and [Installing a Verba Recording Server](#)

 For more information about the deployment models see [Select a deployment architecture](#)

Cisco network based recording

This recording method utilizes special features of the Cisco Unified Communication Manager introduced in version 6.0. It integrates call recording and silent monitoring features into CUCM. If an extension is configured for recording (the configuration is available in the CUCM), the CUCM instructs the phone to send the RTP streams related to a given call, directly to the recording server utilizing the built-in bridge of the phone. The recording system is connected to the CUCM via a SIP trunk to capture the signaling messages. Additional call detail information is obtained by using a JTAPI interface.

You can also use this technology for **silent monitoring**, even without call recording, see [Central silent monitoring utilizing RTP forking in Cisco environment](#).



Advantages

- In a multi-site network, branches where few calls have to be recorded, the deployment of a recorder does not require a dedicated recording server for each remote site.
- Theoretically, this recorder eliminates the complexity of the switching infrastructure compared to the passive recording method, because the RTP streams are sent directly to the recording server automatically.
- Can be easily scaled by adding new recorders to the system if more capacity is required.
- Does not require extra DSP resources from the network compared to the active (conference-based) method.
- Recording tone can be generated by the phone.
- Encrypted calls can be recorded since CUCM 8.0

Considerations

- Requires additional bandwidth on the network to the recording server(s).
- Since the recording functionality is controlled by the CUCM, in case of a WAN link failure, the recording will not work at all in the branch offices (if the CUCM is in the central site).
- Cisco SRST (Survivable Remote Site Telephony) does not support native recording.
- Requires at least CUCM version 6.0.
- Does not support all phone types (check the list above)
- Requires extra capacity from the CUCM server(s) (for each recording session add 2 calls to BHCC in your dimensioning calculation).
- Only voice calls are supported.

"Almost" all Cisco phones support central recording

The Verba passive, network spanning / traffic monitoring-based recording engine technology **supports all Cisco phones**, however, the Verba central recording technology needs cooperation from software built into the Cisco phones to deliver the recording function. Not all Cisco phones support this recording mode, one requirement is the build-in-bridge technology in the phone.

Cisco maintains a detailed support matrix for RTP-forking based recording and silent monitoring: [Unified CM Recording and Silent Monitoring Supported Device Matrix](#)

You can also check the supported devices for specific CUCM versions: https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/unified/communications/system/Compatibility/CSR-Compatibility-Matrix-InteractiveHTML.html

Supported Cisco Unified Communications Manager versions: 6.x, 7.x, 8.x, 9.x,10.x, 11.x, 12.x and 14.x.

Supported Cisco IP phones (certain phones are only supported on the latest CUCM versions, please check the links above or run a report (see below) on your CUCM for the latest information):

- Cisco 6911
- Cisco 6921
- Cisco 6941
- Cisco 6945
- Cisco 6961
- Cisco 7811
- Cisco 7821
- Cisco 7832
- Cisco 7841
- Cisco 7861
- Cisco 7906
- Cisco 7911
- Cisco 7914 Sidecar
- Cisco 7915 Sidecar
- Cisco 7916 Sidecar
- Cisco CKEM Sidecar
- Cisco 7921
- Cisco 7925
- Cisco 7926
- Cisco 7931
- Cisco 7937
- Cisco 7941
- Cisco 7941G-GE
- Cisco 7942
- Cisco 7945
- Cisco 7961
- Cisco 7961G-GE
- Cisco 7962
- Cisco 7965
- Cisco 7970
- Cisco 7971
- Cisco 7975
- Cisco 7985
- Cisco 8811
- Cisco 8821
- Cisco 8831
- Cisco 8841
- Cisco 8845
- Cisco 8851
- Cisco 8861
- Cisco 8865
- Cisco 8941
- Cisco 8945

- Cisco 8961
- Cisco 9951
- Cisco 9971
- Cisco DX650
- Cisco DX70
- Cisco DX80
- Cisco IP Communicator
- Cisco Jabber for Windows
- Cisco Jabber for Mac
- Cisco Jabber for Android
- Cisco Jabber for IOS

Find out what phones are supported on your system

To find out which phones are supported on your CUCM version, use the built-in reporting tool:

Step 1 Login to **Cisco Unified Reporting** on the CUCM admin screen.

Step 2 From **System Reports** select **Unified CM Phone Feature List**.

Step 3 Select **Feature: Record**. This will list all phones capable to do RTP forking.

Encrypted call recording support matrix

Cisco Unified Communications Manager 8.0 supports the recording of encrypted calls via the RTP forking-based interface. The following table helps you to identify supported call scenarios regarding the encryption feature.

	Non-Secure Recorded Phone	Authenticated Recorded Phone	Secure Recorded Phone
Non Secure SIP trunk to the recorder	Supported	Not supported	Not supported
Encrypted SIP trunk to the recorder	Supported, but the forked RTP will not be encrypted	Not supported	Supported

Possible deployment of Cisco Central call recording with RTP forking:

- **Single server solution:** All Verba services (Administration, Recorder) are on one server. It is recommended only for a few user POC or trial deployment (10-20 users).
For the installation guide see: [Installing a Verba Single Server solution](#)
- **Media Repository + Recorder Server:** The Verba administration/storage server is deployed separately from the recorder.
For the installation guide see: [Installing a Verba Media Repository](#) and [Installing a Verba Recording Server](#)

Capturing Cisco Jabber File Transfer

AVAILABLE IN 9.1 AND LATER

The Verint Verba platform provides native support for capturing **Cisco Jabber File Transfers**.

Overview

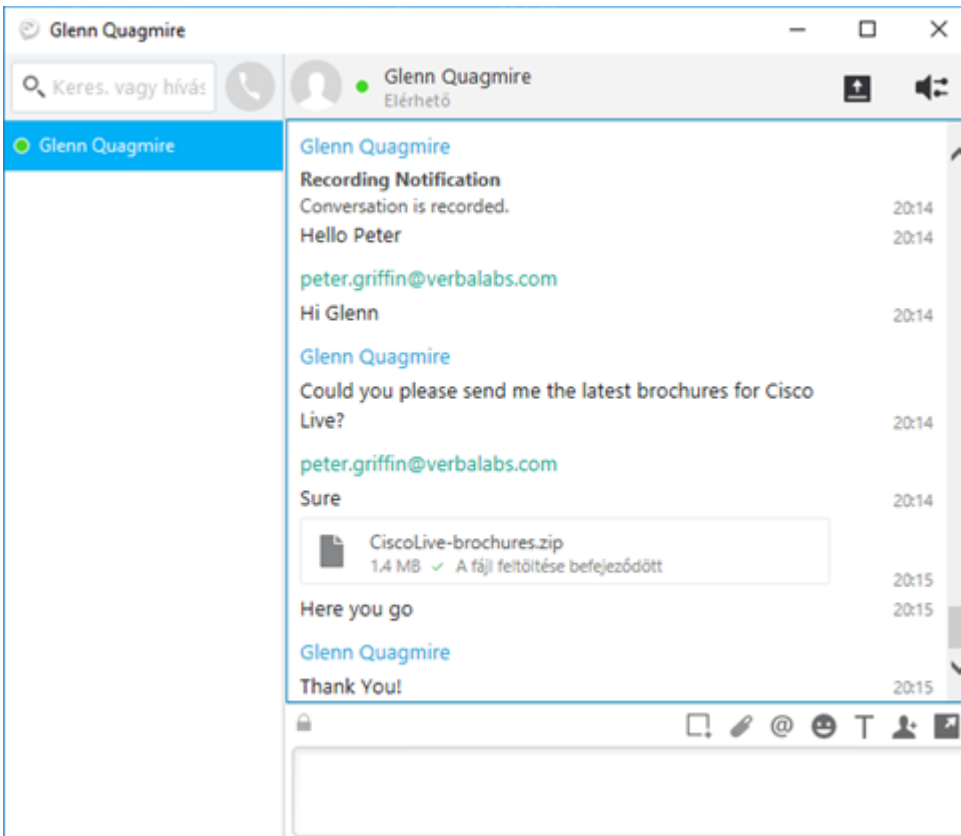
Capturing Cisco Jabber File Transfers is implemented in the **Verba Cisco Compliance Service**. In order to use the solution, a dedicated Jabber user account shall be configured. When Verba Cisco Compliance Service is configured and used, it also allows [real-time checks on file transfers for Data Loss Prevention \(DLP\)](#).

 The solution requires **Cisco IM&P Managed File Transfer**, peer-to-peer file transfer option has to be disabled.

User interface

In the Verint Verba user interface each file transfer shows up as a separate conversation. In case of group chat or persistent chat rooms, each recorded user has a unique conversation entry and a copy of the same file to allow independent enforcement of access control and retention policies (e.g. retain for one group, delete for another).

In the following screenshot there is a Cisco Jabber IM session with a file transfer in the middle:



This same session shows up in the Verint Verba search interface in the following way:

V Conversations Quality Management Workflows Communication Policies Reports Users Data System

Search

Basic Search Options

Interval: 2018.01.27 00:00 - 2018.01.27 23:59

Phone Number (From or To Party): Enter number or URL...

User: Enter user name...

Search conference participants

Label: Enter label name...

Case: --- All Conversations ---

Conversations

4 items found, displaying all items. Results per page: 20

	Start Date	Start Time	Duration	From
	Jan 27, 2018	8:15:07 PM	00:00:03	peter.griffin@
	Jan 27, 2018	8:15:07 PM	00:00:03	peter.griffin@
	Jan 27, 2018	8:14:22 PM	00:01:19	glenn.quagr
	Jan 27, 2018	8:14:22 PM	00:01:19	glenn.quagr

4 items found, displaying all items. Results per page: 20

Conversation View

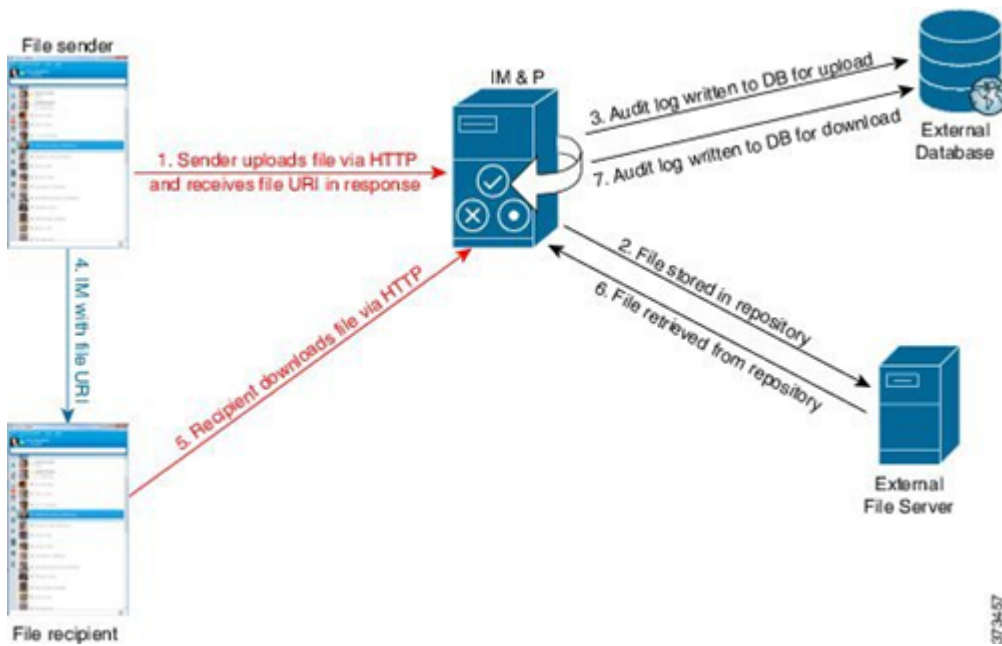
Instant Messaging

Export options: Excel | RTF | PDF

From	Message	To	Timestamp
	Hello Peter		8:14:22 PM
	Hi Glenn		8:14:29 PM
	Could you please send me the latest brochures for Cisco Live?		8:14:53 PM
	Sure		8:14:58 PM
	File sent: CiscoLive-brochures.zip (1388 kB)		8:15:07 PM
	Here you go		8:15:09 PM
	Thank You!		8:15:15 PM

About Cisco IM&P Managed File Transfer

The following diagram shows standard flows in a Cisco IM&P Managed File Transfer:

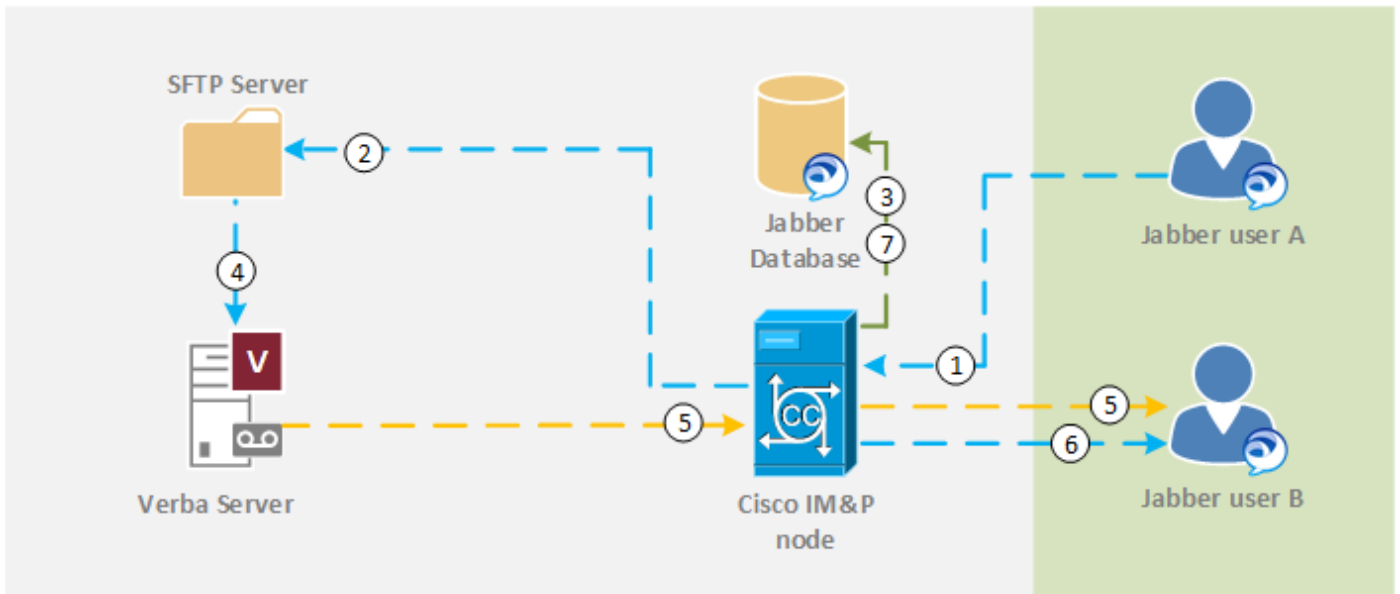


1. The sender's client uploads the file via HTTP, and the server responds with a URI for the file.
2. The file is stored in the repository on the file server.
3. An entry is written to the external database log table to record the upload.
4. The sender's client sends an IM to the recipient; the IM includes the URI of the file.
5. The recipient's client requests the file via HTTP.

After reading the file from the repository (6) and recording the download in the log table (7), the file is downloaded to the recipient.

Learn more at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/im_presence/configAdminGuide/11_5_1/CUP0_BK_CE08159C_00_config-admin-guide-imp-1151/CUP0_BK_CE08159C_00_config-admin-guide-imp-1151_chapter_01011.html

The following diagram shows how the above flow plays-out in the Verint Verba solution:



File transfer **XMPP**

Flow: Cisco IM&P File Transfer Capture

1. User A initiates a File Transfer to User B
2. The IM&P node uploads the file to the External File Server (SFTP server)
3. An audit log entry of the file upload event is created in the database
4. The Verba Server downloads the file from the SFTP Server and creates a record in the Verba database
5. The Verba Server sends a URL pointing to the file on storage to User B
6. User B clicks on the URL in the message and downloads the file
7. An audit log entry of the file download event is created in the Jabber database

Passive call recording for Cisco UC 320 and UC 500

Passive call recording for Cisco UC 320 and UC 500 series

Verba support recording on the **Cisco Unified Communications Manager Express based (CUCME)** IP PBX platforms, however **additional equipment is required to capture all of the voice calls**.

Here's why:

The CUCME platform does not allow you to use our central recording technologies, due to


- the **lack of support for the built-in-bridge function** of Cisco phones, which would allow you to use the Verba central recording technology
- the **lack of JTAPI support**, which would allow the Verba system to collect information about call details

Therefore the **only way to record calls on CUCME devices is passive recording**, which is based on port mirroring (SPAN in Cisco terminology).

UC320/UC500 series with CUCME platforms have limited support for SPAN, it do not allow you to create monitor sessions that include more than one network ports at a time, which makes it hard to capture the traffic of all your phones.

Solution

You can solve this situation, by **deploying an additional standard switch** between your phones and the CUCME boxes that supports SPAN sessions for multiple (even all ports) and VLANs.

-  An example for an entry level switch that supports SPAN port sessions with multiple ports is the Cisco Catalyst 2960-24TC-S Switch - approximately 500 USD at list price at your local Cisco distributor/integrator partner. There also smaller switches that support SPAN. Please contact your reseller for an up-to-date recommendation.

Read more about passive recording

-  [Passive, trunk-side call recording](#)
-  [Passive, extension side call recording](#)

Cisco silent monitoring

In Cisco Unified Communications Manager environments, the Verba Recording System has a special silent monitoring module, which allows to provide silent monitoring functionality without call recording. This allows organizations to implement silent monitoring in a very cost effective way. This special silent monitoring service is based on the RTP forking technology, introduced in CUCM 6.0.

The Verba Cisco Central Silent Monitoring Service is connected to the CUCM via JTAPI, and monitors all phones, which have to be silently monitored. The system automatically stores every call for the monitored phones until the calls are not ended (calls are available in the ongoing call list). Users with full privileges can list ongoing calls on the web interface and can start the silent monitoring. The main difference between the built-in recording service based silent monitoring and this method is that this method requires a Cisco IP phone, which is used to receive the forked RTP packets from the monitored phones. When a supervisor initiates silent monitoring for a call, the supervisor has to enter a directory number, where the system sends the silent monitoring session.

Supported Cisco environment

Supported Cisco Unified Communications Manager versions: 6.x, 7.x, 8.x

Supported Cisco IP phones (certain phones are only supported on the latest CUCM versions):

- Cisco 6911
- Cisco 6921
- Cisco 6941
- Cisco 6961
- Cisco 7906
- Cisco 7910
- Cisco 7911
- Cisco 7921
- Cisco 7925
- Cisco 7931
- Cisco 7937
- Cisco 7941
- Cisco 7941G-GE
- Cisco 7942
- Cisco 7945
- Cisco 7961
- Cisco 7961G-GE
- Cisco 7962
- Cisco 7965
- Cisco 7970
- Cisco 7971
- Cisco 7975
- Cisco 8961
- Cisco 9951
- Cisco 9971
- Cisco ATA 186
- Cisco IP Communicator
- Cisco VGC Phone

For a more detailed listing, see [Cisco phones with central call recording support](#).

To find out, which phones are supported on your CUCM version, use the built-in reporting tool:

Step 1 Login to **Cisco Unified Reporting** on CUCM admin screen.

Step 2 From **System Reports** select **Unified CM Phone Feature List**.

Step 3 Select **Feature: Record**. This will list all phones capable to do RTP forking.

Cisco phones with central call recording support

"Almost" all Cisco phones support central recording

The Verba passive, network spanning / traffic monitoring based recording engine technology **supports all Cisco phones**, however, the Verba central recording technology needs cooperation from software built into the Cisco phones to deliver the recording function. Not all Cisco phones support this recording mode, one requirement is the build-in-bridge technology in the phone.

**89xx and 99xx series support iSAC codec which isn't supported by Verba. UCM Region codec settings should disable this codec to record all the calls established by these models.*

Find out what phones are supported on your system

To find out, which phones are supported on your CUCM version, use the built-in reporting tool:

Step 1 Login to **Cisco Unified Reporting** on CUCM admin screen.

Step 2 From **System Reports** select **Unified CM Phone Feature List**.

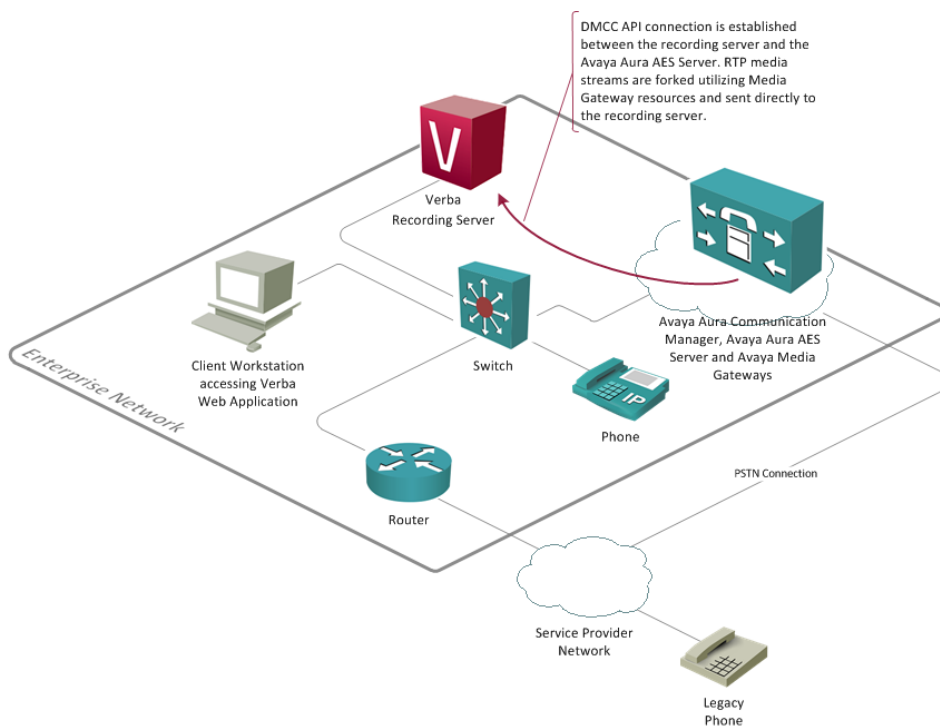
Step 3 Select **Feature: Record**. This will list all phones capable to do RTP forking.

Avaya

The Verba recording solution supports Avaya DMCC multiple registration based call recording (Avaya Aura).

Using Avaya Communication Manager release 5.0 or higher, it is possible to register up to three devices against an extension; using earlier releases, only one device can be registered.

The multiple registrations call recording method, which Verba Recording System uses takes advantage of the multiple registrations capability to register a recording device against the actual extension from which calls are to be recorded. The application simply requests listening services and CM sends a duplicated stream of all traffic from the originally provisioned extension. The forked RTP comes to the recording server from the media resource (formerly MedPro) card. The duplication request takes up a media resource, but does not require conferencing resources or timeslots compared to other recording methods.



Advantages

- Because this method does not require a standalone recording device to be added to calls, the six party limit in a call is not affected as compared to the other two recording methods (single-step-conference, service observing).
- Because the RTP is forked by the Communication Manager itself, it does not require additional TDM slots as compared to the other two typical recording methods (single-step-conference, service observing). The Multiple Registrations method consumes one additional media resource for each recording device. Additional TDM timeslots are not consumed as the recording device is not able to talk.
- Service Observing and Single conferencing both make use of standalone recording devices which are registered against extensions which have been provisioned on Communication Manager specifically for call recording purposes. Thus each recording device consumes one additional station license. Service Observing typically has a one-to-one association between target extensions and recording devices, and therefore consumes a relatively large number of station licenses. Single conferencing typically uses a pool of recording devices, and therefore potentially needs fewer station licenses, but introduces the possibility of running out of recording devices if a large number of recordings need to be made at the same time. The Multiple Registrations method used by Verba Recording System does not consume additional station licenses.

Considerations

- Requires Avaya Communication Manager 5.x or later and Avaya AES 4.2 or later.

- SIP phones can be recorded with Avaya Communication Manager 6.2 or later and Avaya AES 6.2 or later, and the Dependency Method has to be set to INDEPENDENT.
- Automatic announcement of the recording cannot be done by the recorder. An external IVR should be used.

Supported Avaya environment

- Avaya Communication Manager version: 5.0 or later
- Avaya Application Enablement Services (AES) version: 4.2 or later
- Supported phoneset types:
 - digital Avaya phones (DCP)
 - IP Avaya phones (SIP devices can be recorded from CM 6.2 and AES 6.2)

Required Avaya licenses

- Computer Telephony Adjunct Links license on the Avaya Communication Manager
- 1pc DMCC Full license for each recorded station (DMCC Basic license is enough if you already have IP_STA license for each recorded station)
- 1pc TSAPI Basic User license for each recorded device on the AES
- Optionally 1pc TSAPI Basic User license for the monitored technical hunt group (for receiving agent status information)
- Properly sized media resource card to support recording sessions (forked RTP streams)

For further information, please refer to an official Avaya representative or read the guide below:

https://www.devconnectprogram.com/site/global/products_resources/avaya_aura_application_enablement_services/support/faq/dmcc/other.gsp, drill down to What licenses are required for DMCC based Call Recording solution?

Recording approaches with Avaya Communication Manager

The following table summarizes the available recording approaches in Avaya Communication Manager environment and the available Verba support:

Recording approach	Verba support
Passive TDM trunk side recording	No
Passive IP trunk side recording	Yes, SIP only
Passive IP extension side recording	Yes, SIP only
AES: service observing	No
AES: single-step-conference	No
AES: multiple registration (RTP forking)	Yes

The well known passive IP call recording is not officially accepted by Avaya, because the signaling protocol used for Avaya devices is based on a proprietary version of H.323. The new SIP based devices can be monitored passively, but certain PBX functionality is still missing from the SIP based firmwares, so they are very rarely used. The only officially supported recording method is CTI-based recording, which means that the recording solutions must work through the Avaya AES server. On the AES server, there are different APIs:

- TSAPI
- JTAPI
- DMCC: Device, Media and Call Control API (formerly CMAPI, based on ECMA-269 Standard, used by Verba)

There are 3 different call recording approaches using the AES:

Service Observing

This method works by operating softphones and monitoring the recorded stations and invoking service observing upon recording request or automatically for each call. This way the softphones can participate in the calls, thus receive the audio. The application uses the AE Services DMCC service to register itself as a standalone recording device. The Service Observing feature is provisioned and activated on the device so that, when the target extension joins a call, the recording device is automatically added to the call. The application receives the calls aggregated RTP media stream via the recording device and records the call.

Single-step-conference

This method works by operating softphones and monitoring the recorded stations and invoking single-step-conference upon recording request or automatically for each call. In this way the softphones can participate in the calls thus receive the audio. The application uses the AE Services DMCC service to register a pool of standalone recording devices. The application uses the AE Services TSAPI service to monitor the target extension for Established Call events. Whenever the extension joins a call, an Established Call event occurs which triggers the application to use the Single conferencing method to add a recording device to the call. The application receives the calls aggregated RTP media stream via the recording device and records the call.

Multiple registration supported by Verba Recording System

Using Communication Manager release 5.0 or higher, it is possible to register up to three devices against an extension; using earlier releases, only one device can be registered. Where multiple device registration is supported, the number of DMCC devices that can be registered against an extension is determined as follows:

- If there is no physical set and no Avaya IP softphone registered at the extension, the client application can register up to three DMCC devices.
- If there is a physical set or Avaya IP softphone registered at an extension, the client application can register up to two DMCC devices.
- If a physical set and Avaya IP softphone share control of an extension, the client application can register only one DMCC device.

Possible deployment of Central call recording with RTP forking for Avaya:

- **Single server solution:** All Verba services (Administration, Recorder) are on one server. It is recommended only for a few user POC or trial deployment (10-20 users).
For the installation guide see: [Installing a Verba Single Server solution](#)
- **Media Repository + Recorder Server:** The Verba administration/storage server is deployed separately from the recorder.
For the installation guide see: [Installing a Verba Media Repository](#) and [Installing a Verba Recording Server](#)

Symphony

Overview

Symphony recording features

- Voice, screen, instant message and file recording
- Integration with the official Symphony Recording Bridge using SIPREC
- Supports always-on, selective and on-demand recording
- Supports all call scenarios where the recorded user is a participant
- Supports 2N Recording Server deployments
- Support for Media Recorder load balancing and failover
- CDR reconciliation for voice, screen recordings

Version support

Switch Name & Model	Symphony
Supported Symphony Versions	Contact Symphony
Supported Endpoint / DeviceTypes	All

Deploying Symphony recording

The following section contains the necessary steps for setting up a Symphony recording infrastructure.

Server sizing

Allocating the appropriate resources to the different servers is crucial. For guidance, see [Server sizing and requirements](#)

Preparation

The Symphony integration requires additional prerequisites and configuration in Symphony, which out of scope for this guide. Contact your Symphony representative for further information.

Make sure that all the required prerequisites are installed on each server prior to the installation.

- [Prerequisites](#)
- [Installing the required prerequisites](#)

For guidance on configuring the necessary firewall ports, visit [Firewall configuration for SIPREC recording deployments](#).

Installation

The following articles contain all the step for installing the various server roles:

- [Installing a Verba Single Server solution](#)
- [Installing a Verba Media Repository](#)
- [Installing a Verba Recording Server](#)

Configuration

The system has to be configured for Symphony in the following way:

- Recording Servers has to be configured for SIPREC recording, for more information, see [Configuring Verba for SIPREC recording](#).
- Instant message and file archiving are available through import, see [Symphony Instant Messages - Files - CDRs](#)
- CDR reconciliation is available through Symphony XML import, see [Symphony Instant Messages - Files - CDRs](#)
- Recorded users can be synchronized from Active Directory. For recorded extensions, the User Principal Name attribute has to be configured.

Symphony metadata

The system captures the following metadata specific to Symphony recordings.

Metadata Field	Description	Template	Available
Start Date	Start date of the conversation	Standard	Yes
Start Time	Start time on the conversation	Standard	Yes
End Date	End date of the conversation	Standard	Yes
End Time	End time of the conversation	Standard	Yes
Duration	Length of the conversation	Standard	Yes
User	Name of the recorded user	Standard	Yes
From	Phone number, Button name, User name	Standard	Yes
From Info	User / contact name	Standard	Yes
To	Phone number, Button name, User name	Standard	Yes
To Info	User / contact name	Standard	No
Direction	Direction of the call from the system perspective, requires configuring internal number/domain patterns	Standard	Yes
Direction (User)	Direction of the call from the recorded user perspective	Standard	Yes
From (Verba)	Name of the Verba user associated with the calling party	Standard	Yes
To (Verba)	Name of the Verba user associated with the called party	Standard	Yes
Location	Hostname of the recording server	Standard	Yes
End Cause	Normal, Hold, Transfer, Conference, Device Change, From Terminated, To Terminated	Standard	Yes
Audio Codec	Audio codec of the recorded streams	Standard	Yes
Video codec	Video codec of the recorded streams	Standard	Yes
Platform Call ID	Unique conversation identifier received from the recorded platform	Standard	Yes
Silence Ratio	Ratio of silence in the conversation	Standard	Yes
Talkover Ratio	Talkover ratio of the conversation	Standard	Yes
Longest Silence	Length of the longest silence present in the conversation	Standard	Yes
User ID / Agent ID	Symphony User ID	Standard	Yes
From Device	Device ID of the calling party	Standard	No
To Device	Device ID of the called party	Standard	No
Dialed Number	Original dialed number	Standard	No

From IP	IP address of the recording bot	Standard	Yes
To IP	IP address of the recording bot	Standard	Yes
From Proxy IP	IP address of the proxy server associated with the caller party	Standard	No
To Proxy IP	IP address of the proxy server associated with the called party	Standard	No
Source Platform	Microsoft Teams	Standard	Yes
Conversation Type	Voice, Video, Screen Share	Standard	Yes
Forward Reason	Forward reason for the conversation (e.g. forwarded, transferred, team call, delegated, etc.)	Standard	No
Recording failed	Indicates if the recording has failed and the metadata was imported during CDR reconciliation	Standard	No
Media Length	Length of the media file related to the conversation in hhh:mm:ss format	Standard	Yes
Media Error	Shows the media processing errors during recording	Standard	Yes
Voice Quality	Overall voice quality check score for the conversation	Standard	Yes
Record Type	Standard	Standard	Yes
2N Source	In case of duplicate (2N) recording, records are marked as primary or secondary	Standard	Yes

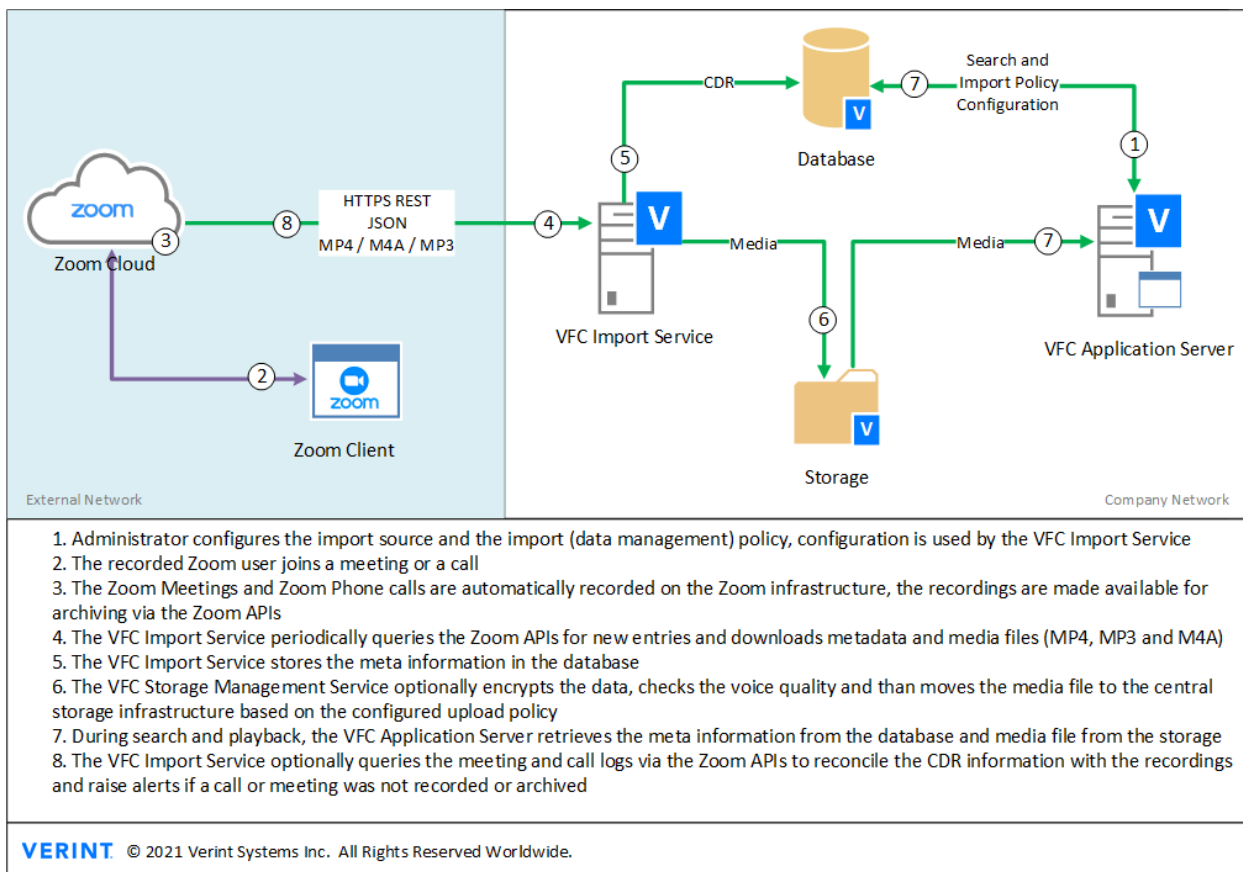
Zoom

AVAILABLE IN VERSION 9.6.13 OR LATER

- [Overview](#)
 - [Supported features](#)
 - [Known limitations and considerations](#)
 - [Version support](#)
- [Deploying Zoom recording](#)
 - [Server sizing](#)
 - [Preparation](#)
 - [Installation](#)
 - [Configuration](#)
 - [Zoom API rate limits](#)
- [Zoom Meeting metadata](#)
- [Zoom Phone metadata](#)

Overview

The Zoom integration enables you to archive recorded Zoom Meetings and Zoom Phone calls into the system. The recording takes place within the Zoom platform, and the audio and video from completed meetings and calls are downloaded from Zoom and then ingested into the system using the Zoom Meeting and/or Zoom Phone import sources.



Supported features

The Zoom integration provides the following features:

- Archiving Zoom Meetings and Zoom Phones recordings for configured users
- Integration with public Zoom APIs: <https://marketplace.zoom.us/docs/api-reference/introduction>
- Support for voice, video, and screen & application share modalities
- Unaltered download and import of media files (MP3, M4A, MP4)
- Import of meeting and phone call metadata
- CDR reconciliation with Zoom call/meeting logs to identify not recorded or archived calls
- Configurable query intervals through import policy schedule
- Multi-tenant support, the ability to configure any number of Zoom tenants as separate import sources in any environment/tenant
- Support for forward proxy based configurations

Known limitations and considerations

The Zoom integration has the following known limitations currently:

- Meetings chat archiving is not supported
- Webinars are not supported
- Video files for Meeting recordings might not match the time interval defined by the join and leave events of the recorded users. The Zoom recording process currently starts when the first recorded user joins and ends when the meeting ends. The recording system creates CDRs for each recorded user based on their join/leave events but will link the full video files to these records. Audio files are created individually for each recorded participant (individual recording has to be enabled on the Zoom side) and are not affected by this limitation.
- The APIs published by Zoom are tenant/account level APIs (not user level), which means that the API response will include information about recordings for all configured users in the tenant. The system filters the response based on the configured users and does not attempt to download recordings for users not configured in the system. When multiple systems are deployed to allow data segregation, this approach introduces some overhead as unnecessary data is downloaded (and discarded).
- Due to Zoom API rate limits and lack of filtering for specific users, large tenants might be unable to use the CDR reconciliation feature for Zoom Meetings, because the process requires to call resource-intensive APIs for every meeting in the tenant.
- Meetings hosted by external users (users outside of the customer tenant/account) can only be archived with limitations. The participant information is limited to the recorded users in the customer tenant, no external participants or non-recorded internal participants will be stored.
- Meeting recordings always include an MP4 video file (in addition to the M4A audio file) even if no camera was used or screen sharing was not enabled. The video contains a black screen with the name of the users in the center. When the recorded user is configured for voice-only recording/archiving, the system only imports the M4A audio file. If the recorded user is configured for video and/or screen share recording, the system imports the MP4 file as well and sets the modality to Screen & Application Share (regardless if video and screen share was used).
- Redundant deployments are supported but multiple servers will run independently and attempt to import the same recordings and multiply the Zoom API usage. The system will eventually import only one copy of the same call and meeting. For the same reasons, load balancing is not recommended, while supported.
- The Zoom Phone API does not support Archiving time for filtering which introduces an overhead in querying the data and the system has to query the same time interval multiple times.
- The reconciliation process for Zoom Phones only queries records where the recording_id is set.

Version support

Switch Name & Model	Zoom Meetings Zoom Phone
Supported Versions	Contact Zoom
Supported Endpoint / DeviceTypes	All

Deploying Zoom recording

The following section contains the necessary steps for setting up a Zoom recording infrastructure.

Server sizing

Allocating the appropriate resources to the different servers is crucial. For guidance, see [Server sizing and requirements](#)

For storage sizing, see the table below showing the information available for media files created by the Zoom platform:

	File Format	Codec	Size
Zoom Phone	MP3	MP3 (48 KHz, Mono, VBR)	40-75 Kbps
Zoom Meeting Audio	M4A	AAC-LC (32 KHz, Mono, CBR)	128 Kbps
Zoom Meeting Audio + Video + Screen Share	MP4	AAC-LC (32 KHz, Mono, CBR) H.264 AVC	Audio: 128 Kbps Video: entirely depends on the screen resolution, the content shared, and the variable bitrate control in Zoom. It is recommended to make test calls with the usual content and length and use it as a baseline for the calculations.

Preparation

Make sure that all the required prerequisites are installed on each server prior to the installation.

- [Prerequisites](#)
- [Installing the required prerequisites](#)

Installation

The following articles contain all the steps for installing the various server roles:

- [Installing a Verba Single Server solution](#)
- [Installing a Verba Media Repository](#)
- [Installing a Verba Recording Server](#)

Configuration

The system supports both Zoom Meeting and Zoom Phone archiving via the import service framework:

- Zoom Phone: for configuring Zoom Phone archiving, refer to [Zoom Meeting and Phone](#)
- Zoom Meeting: for configuring Zoom Meeting archiving, refer to [Zoom Meeting and Phone](#)

Zoom API rate limits

The Zoom API enforces certain limitations on the number of requests sent by an application. These rate limits can limit the number of meetings or phone calls that are imported or reconciled by the system on a daily basis. When an API limit is reached, the Zoom platform will block any subsequent API request for the API category which exceeded the published rate limit. The system will need to wait until the rate limits are reset (at 00:00 UTC every day).

For more information, see <https://marketplace.zoom.us/docs/api-reference/rate-limits>.

The following table explains the current rate limits and provides guidance on how to estimate the API usage to avoid reaching the API limits. If you are planning to deploy the integration for a large tenant/account and you believe that the rate limits will be reached, please contact Zoom about further options.

	API	Zoom API Limit (Business+)	Usage
Phone	/phone/recordings https://marketplace.zoom.us/docs/api-reference/zoom-api/phone/getphonerecordings	20 req. / second	Import
	/phone/call_logs https://marketplace.zoom.us/docs/api-reference/zoom-api/phone/accountcalllogs	40 req. / second Daily limit of 60,000 requests /day shared by heavy & resource-intensive APIs.	CDR re
Meeting	/archive_files https://marketplace.zoom.us/docs/api-reference/zoom-api/archiving/listarchivedfiles	60 req. / second	Import
	/metrics/meetings/{meetingId}/participants https://marketplace.zoom.us/docs/api-reference/zoom-api/dashboards/dashboardmeetingparticipants	20 req. / second Daily limit of 60,000 requests /day shared by heavy & resource-intensive APIs.	Both ir CDR re
	/metrics/meetings https://marketplace.zoom.us/docs/api-reference/zoom-api/dashboards/dashboardmeetings	20 req. / second Daily limit of 60,000 requests /day shared by heavy & resource-intensive APIs.	CDR re

Types of import that are subject to daily API limit:

- Zoom Phones: no
- Zoom Phones with CDR reconciliation: yes
- Zoom Meetings: yes
- Zoom Meetings with CDR reconciliation: yes

Some examples of how much volume of traffic a daily rate limit of 60 000 can safely handle when scheduling the import for every 5 minutes:

- Zoom Phones: no limit
- Zoom Phones with CDR reconciliation: 4.5 million calls daily
- Zoom Meetings: 30 000 meetings daily
- Zoom Meetings with CDR reconciliation: 29 000 meetings daily
- Zoom Meetings and Zoom Phones: combined traffic of any amount of daily calls and 30 000 meetings
- Zoom Meetings and Zoom Phones both with CDR reconciliation: combined traffic of 2.2 million daily calls and 14 500 meeting

Zoom Meeting metadata

The system captures the following metadata specific to Zoom meetings.

Metadata Field	Description	Template	Available
Start Date	Start date of the conversation	Standard	Yes
Start Time	Start time on the conversation	Standard	Yes
End Date	End date of the conversation	Standard	Yes
End Time	End time of the conversation	Standard	Yes
Duration	Length of the conversation	Standard	Yes
User	Name of the recorded user	Standard	Yes
From	Recorded User ID	Standard	Yes
From Info	Recorded user display name	Standard	Yes
To	Conference	Standard	Yes
To Info	Meeting topic	Standard	Yes
Direction	Conference	Standard	Yes
Direction (User)	Outgoing	Standard	Yes
From (Verba)	Name of the Verba user associated with the calling party	Standard	Yes
To (Verba)	Name of the Verba user associated with the called party	Standard	Yes
Location	Hostname of the recording server	Standard	Yes
End Cause	Normal, Hold, Transfer, Conference, Device Change, From Terminated, To Terminated	Standard	No
Audio Codec	Audio codec of the recorded streams	Standard	No
Video codec	Video codec of the recorded streams	Standard	No
Platform Call ID	Unique conversation identifier received from the recorded platform	Standard	Yes
Silence Ratio	Ratio of silence in the conversation	Standard	No
Talkover Ratio	Talkover ratio of the conversation	Standard	No
Longest Silence	Length of the longest silence present in the conversation	Standard	No
User ID / Agent ID	Recorded Zoom user ID	Standard	Yes
From Device	Device ID of the calling party	Standard	No
To Device	Device ID of the called party	Standard	No
Dialed Number	Original dialed number	Standard	No
From IP	IP address associated with the calling party	Standard	No
To IP	IP address associated with the called party	Standard	No
From Proxy IP	IP address of the proxy server associated with the caller party	Standard	No
To Proxy IP	IP address of the proxy server associated with the called party	Standard	No
Source	Zoom Meeting	Standard	Yes

Platform			
Conversation Type	Voice, Video, Screen & Application Share If the recorded user is configured for video and/or screen share recording, the system sets the modality to Screen & Application Share (regardless if video and screen share was used).	Standard	Yes
Forward Reason	Forward reason for the conversation (e.g. forwarded, transferred, team call, delegated, etc.)	Standard	No
Recording failed	Indicates if the recording has failed and the metadata was imported during CDR reconciliation	Standard	Yes
Media Length	Length of the media file related to the conversation in hhh:mm:ss format	Standard	No
Media Error	Shows the media processing errors during recording	Standard	No
Voice Quality	Overall voice quality check score for the conversation	Standard	Yes
Record Type	Standard	Standard	Yes
2N Source	In case of duplicate (2N) recording, records are marked as primary or secondary	Standard	No

Zoom Phone metadata

The system captures the following metadata specific to Zoom Phone recordings.

Metadata Field	Description	Template	Available
Start Date	Start date of the conversation	Standard	Yes
Start Time	Start time on the conversation	Standard	Yes
End Date	End date of the conversation	Standard	Yes
End Time	End time of the conversation	Standard	Yes
Duration	Length of the conversation	Standard	Yes
User	Name of the recorded user	Standard	Yes
From	Phone number of the calling party	Standard	Yes
From Info	Display name of the calling party	Standard	Yes
To	Phone number of the called party	Standard	Yes
To Info	Display name of the called party	Standard	Yes
Participants	Name of the participants of the call		Yes
Direction	Direction of the call from the system perspective, requires configuring internal number/domain patterns	Standard	Yes
Direction (User)	Direction of the call from the recorded user perspective	Standard	Yes
From (Verba)	Name of the Verba user associated with the calling party	Standard	Yes
To (Verba)	Name of the Verba user associated with the called party	Standard	Yes
Location	Hostname of the recording server	Standard	Yes
End Cause	Normal, Hold, Transfer, Conference, Device Change, From Terminated, To Terminated	Standard	No
Audio Codec	Audio codec of the recorded streams	Standard	No
Video codec	Video codec of the recorded streams	Standard	No

Platform Call ID	Unique conversation identifier received from the recorded platform to correlate multiple call legs	Standard	Yes
Silence Ratio	Ratio of silence in the conversation	Standard	No
Talkover Ratio	Talkover ratio of the conversation	Standard	No
Longest Silence	Length of the longest silence present in the conversation	Standard	No
User ID / Agent ID	Recorded Zoom phone extension number	Standard	Yes
From Device	Device ID of the calling party	Standard	No
To Device	Device ID of the called party	Standard	No
Dialed Number	Original dialed number	Standard	No
From IP	IP address of the recorded endpoint	Standard	No
To IP	IP address of the recorded endpoint	Standard	No
From Proxy IP	IP address of the proxy server associated with the calling party	Standard	No
To Proxy IP	IP address of the proxy server associated with the calling party	Standard	No
Source Platform	Zoom Phone	Standard	Yes
Conversation Type	Voice	Standard	Yes
Forward Reason	Forward reason for the conversation (e.g. forwarded, transferred, team call, delegated, etc.)	Standard	No
Recording failed	Indicates if the recording has failed and the metadata was imported during CDR reconciliation	Standard	Yes
Media Length	Length of the media file related to the conversation in hhh:mm:ss format	Standard	Yes
Media Error	Shows the media processing errors during recording	Standard	Yes
Voice Quality	Overall voice quality check score for the conversation	Standard	Yes
Record Type	Standard	Standard	Yes
2N Source	In case of duplicate (2N) recording, records are marked as primary or secondary	Standard	No

BT IP Trade

Overview

The integration between the Verba and IP Trade systems is based on duplication of the media stream on the turrets or TPO side. For each call, the dealer board system creates a copy of the associated inbound and outbound RTP streams. These are sent to the voice recorder server which records and archives the streams. The transmission of call detail information (CDR) and the negotiation of the RTP session parameters are performed using an XML protocol co-developed by IP Trade and Verba back in 2007. The dealer boards handle special call scenarios that require special handling on the recorder side too:

- Several calls can be active simultaneously on the dealer board, these are recorded separately
- A dealer board can register on the IP telephony infrastructure with single or multiple directory numbers, all of these are captured
- Call durations can vary from seconds up to several hours (e.g. open lines), all these are recorded as expected, with silence suppressed in long calls

BT IP Trade recording features

- Certified BT IP Trade recording solution
- 2N and N+1 recorder configurations
- Support both turret and TPO based recording
- Compatible with trader voice recording data model
- Support for VAD (voice activity detection) and media segmentation for long calls
- All types of recording mix layouts are supported
- Support for selective recoding by configuring trader IDs as recorded extensions
- Support for turret based playback

Version support

Switch Name & Model	IP Trade
Supported BT IP Trade Versions	5.2 or later
Supported Turret Types	All

If you are on a different version, contact your BT representative for more information.

Features not available

- Silent monitoring only available for Media-Only records
- Full / Always-on, Do-not-record, Never-record recording modes only (no On-demand, no Controlled)
- Desktop Screen Capture is not available
- Recoding Director and Media Recorders roles cannot be separated, no dynamic load balancing available

Deploying BT IP Trade Recording

The following section contains all the necessary steps for setting up a BT IP Trade recording infrastructure.

⚠ For BT IPTrade deployments, the Recording Director and Media Recorder roles cannot be split out to different servers. These 2 roles must run on the same Recording Server to avoid limitations around failover design inherit in the IP Trade recording protocol design. This means that the Recording Servers must be allocated across the turrets and there is no dynamic load balancing available.

Server Sizing

Allocating the appropriate resources to the different servers is crucial. For guidance, see [Server sizing and requirements](#)

Preparation

Make sure that all the required prerequisites are installed on each server prior to the installation.

- [Prerequisites](#)
- [Installing the required prerequisites](#)

For guidance on configuring the necessary firewall port, visit [Firewall configuration for BT IP Trade recording deployments](#).

Installation

The following articles contain all the step for installing the various server roles:

- [Installing a Verba Single Server solution](#)
- [Installing a Verba Media Repository](#)
- [Installing a Verba Recording Server](#)

Configuration

For configuring the Verba system for BT IP Trade recording, see [Configuring IP Trade recording](#).

BT IP Trade metadata

The system captures the following metadata specific to BT IP Trade calls when CTI messages are available. These fields are available through the standard and the IP Trade specific custom metadata template.

Metadata Field	Description	Template	Available	Turret based recording		TPO based recording	
				Available in CDR-Only record	Available in Media-Only record	Available in CDR-Only record	Available in Media-Only record
Start Date	Start date of the conversation	Standard	Yes	Yes	Yes	Yes	Yes
Start Time	Start time on the conversation	Standard	Yes	Yes	Yes	Yes	Yes
End Date	End date of the conversation	Standard	Yes	Yes	Yes	Yes	Yes
End Time	End time of the conversation	Standard	Yes	Yes	Yes	Yes	Yes
Duration	Length of the conversation	Standard	Yes	Yes	Yes	Yes	Yes

User	Name of the recorded user	Standard	Yes	Yes	Yes	Yes	No
From	Source phone number, SIP URI	Standard	Yes	Yes	No	Yes	No
From Info	Source display name	Standard	Yes	Yes	No	Yes	No
To	Destination phone number, SIP URI	Standard	Yes	Yes	No	Yes	No
To Info	Destination display name	Standard	Yes	Yes	No	Yes	No
Direction	Direction of the call from the system perspective, requires configuring internal number/domain patterns	Standard	Yes	Yes	No	Yes	No
Direction (User)	Direction of the call from the recorded user perspective	Standard	Yes	Yes	No	Yes	No
From (Verba)	Name of the Verba user associated with the calling party	Standard	Yes	Yes	Yes	Yes	No
To (Verba)	Name of the Verba user associated with the called party	Standard	Yes	Yes	Yes	Yes	No
Location	Hostname of the recording server	Standard	Yes	Yes	Yes	Yes	Yes
End Cause	Normal, Hold, Transfer, Conference, Device Change, From Terminated, To Terminated	Standard	Yes	Yes	Yes	Yes	Yes
Audio Codec	Audio codec of the recorded streams	Standard	Yes	No	Yes	No	Yes
Video codec	Video codec of the recorded streams	Standard	No	No	No	No	No
Platform Call ID	Unique conversation identifier received from the recorded platform	Standard	Yes	Yes	Yes	Yes	Yes
Silence Ratio	Ratio of silence in the conversation	Standard	No	No	No	No	No
Talkover Ratio	Talkover ratio of the conversation	Standard	No	No	No	No	No
Longest Silence	Length of the longest silence present in the conversation	Standard	No	No	No	No	No
User ID / Agent ID	Trader ID	Standard	Yes	Yes	Yes	Yes	No
From Device	Recorded turret ID	Standard	Yes	Yes	Yes	No	No
To Device	Recorded turret ID	Standard	Yes	Yes	Yes	No	No
Dialed Number	Original dialed number	Standard	No	No	No	No	No
From IP	IP address of the media source	Standard	Yes	Yes	Yes	No	Yes
To IP	IP address of the media source	Standard	Yes	Yes	Yes	No	Yes
From Proxy IP	IP address of the proxy server associated with the calling party	Standard	No	No	No	No	No
To Proxy IP	IP address of the proxy server associated with the called party	Standard	No	No	No	No	No
Source Platform	IPTrade	Standard	Yes	Yes	Yes	Yes	Yes
Conversation Type	Voice	Standard	Yes	Yes	Yes	Yes	Yes
Forward Reason	Forward reason for the conversation (e.g. forwarded, transferred, team call, delegated, etc.)	Standard	No	No	No	No	No
Recording failed	Indicates if the recording has failed and the metadata was imported during CDR reconciliation	Standard	No	No	No	No	No
Media Length	Length of the media file related to the conversation in hhh:mm:ss format	Standard	Yes	No	Yes	No	Yes
Media Error	Shows the media processing errors during recording	Standard	Yes	No	Yes	No	Yes
Voice Quality	Overall voice quality check score for the conversation	Standard	Yes	No	Yes	No	Yes
Record Type	CDR-Only, Media-Only	Standard	Yes	Yes	Yes	Yes	Yes
2N Source	In case of duplicate (2N) recording, records are marked as primary or secondary	Standard	Yes	Yes	Yes	Yes	Yes
TPO Slot	DDI slot number	IPTrade		No	No	Yes	No
Channel ID	Recording channel identifier	IPTrade		Yes	No	Yes	No

Device	Handset 1, Handset 2, Headset, Microphone 1, Microphone 2, Loudspeaker 1, Loudspeaker 2	IPTrade		Yes	Yes	No	No
Call Type	DDI, PW, Intercom	IPTrade		No	No	Yes	No
Participant Talk Mode	Marked segment while talk mode is Idle, Public or Exclusive	Marker		No	No	Yes	No

BT ITS

Overview

BT ITS recording features

- Certified BT ITS recording solution
- IPSI based recording, no TDM support
- 2N and N+1 recorder configurations
- 2N CTI resiliency deployment option
- Compatible with trader voice recording data model (only)
- Support for VAD (voice activity detection) and media segmentation for long calls
- All types of recording mix layouts are supported
- Support for TMS file and/or LDAP based configuration read

Version support

BT ITS Switch Name & Model	p31, p41, p51, p107
Supported BT ITS Switch Versions	18.5.5, 19.6.1, 19.8.1
Supported Turret Types	Netrix, Netrix R, Netrix Touchscreen
IPSI Version	3.1.7.0
ITS Link Version	5.4.3.0

If you are on a different version, contact your BT representative for more information.

Features not available

- Supports trader voice data model only
- Silent monitoring only available for Media-Only records
- No selective recording, extension / recording rule configuration is not applied, the system records everything that is configured on the BT ITS switch side
- Full / Always-on recording mode only (no On-demand, no Controlled, no Do-not-record, no Never-record)
- Desktop Screen Capture is not available
- No support for turret playback

Resiliency

The system can be deployed in various configurations to achieve resiliency. For more information, see [BT ITS recorder resiliency](#).

Configuration

For configuring the Verba system for BT ITS recording, see [Configuring BT ITS recording](#). For BT ITS related configuration, contact your BT representative.

BT ITS metadata

The system captures the following metadata specific to BT ITS calls when CTI messages are available. These fields are available through the standard and the BT ITS specific custom metadata template.

Metadata Field	Description	Template	Available	Available in CDR-Only record	Available in Media-Only record
Start Date	Start date of the conversation	Standard	Yes	Yes	Yes
Start Time	Start time on the conversation	Standard	Yes	Yes	Yes
End Date	End date of the conversation	Standard	Yes	Yes	Yes
End Time	End time of the conversation	Standard	Yes	Yes	Yes
Duration	Length of the conversation	Standard	Yes	Yes	Yes
User	Name of the recorded user	Standard	Yes	Yes	Yes when CTI is available
From	DDI Number, Line Number, Trader ID depending on the call scenario	Standard	Yes	Yes	No
From Info	DDI Label, Line Label, Trader Name depending on the call scenario	Standard	Yes	Yes	No
To	DDI Number, Line Number, Trader ID depending on the call scenario	Standard	Yes	Yes	No
To Info	DDI Label, Line Label, Trader Name depending on the call scenario	Standard	Yes	Yes	No
Direction	Direction of the call from the system perspective, requires configuring internal number/domain patterns	Standard	Yes	Yes	No
Direction (User)	Direction of the call from the recorded user perspective	Standard	Yes	Yes	No
From (Verba)	Name of the Verba user associated with the calling party	Standard	Yes	Yes	Yes when CTI is available
To (Verba)	Name of the Verba user associated with the called party	Standard	Yes	Yes	Yes when CTI is available
Location	Hostname of the recording server	Standard	Yes	Yes	Yes
End Cause	Normal, Hold, Device Change	Standard	Yes	Yes	No
Audio Codec	Audio codec of the recorded streams	Standard	Yes	No	Yes
Video codec	Video codec of the recorded streams	Standard	No	No	No
Platform Call ID	Unique conversation identifier received from the recorded platform	Standard	Yes	Yes	Yes
Silence Ratio	Ratio of silence in the conversation	Standard	No	No	No
Talkover Ratio	Talkover ratio of the conversation	Standard	No	No	No
Longest Silence	Length of the longest silence present in the conversation	Standard	No	No	No
User ID / Agent ID	Trader ID	Standard	Yes	Yes	Yes
From Device	Recorded console ID	Standard	Yes	Yes	Yes
To Device	Recorded console ID	Standard	Yes	Yes	Yes

Dialed Number	Original dialed number	Standard	No	Yes	No
From IP	IP address of the IPSI board	Standard	Yes	No	Yes
To IP	IP address of the IPSI board	Standard	Yes	No	No
From Proxy IP	IP address of the proxy server associated with the calling party	Standard	No	No	No
To Proxy IP	IP address of the proxy server associated with the called party	Standard	No	No	No
Source Platform	BT ITS	Standard	Yes	Yes	Yes
Conversation Type	Voice	Standard	Yes	Yes	Yes
Forward Reason	Forward reason for the conversation (e.g. forwarded, transferred, team call, delegated, etc.)	Standard	No	No	No
Recording failed	Indicates if the recording has failed and the metadata was imported during CDR reconciliation	Standard	Yes	No	No
Media Length	Length of the media file related to the conversation in hhh:mm:ss format	Standard	Yes	No	Yes
Media Error	Shows the media processing errors during recording	Standard	Yes	No	Yes
Voice Quality	Overall voice quality check score for the conversation	Standard	Yes	No	Yes
Record Type	CDR-Only, Media-Only	Standard	Yes	Yes	Yes
2N Source	In case of duplicate (2N) recording, records are marked as primary or secondary	Standard	Yes	Yes	Yes
Call Type	Call, Intercom, Group Intercom, Broadcast	BT ITS / IPSI		Yes	No
Device Type	Speaker, Handset, Intercom	BT ITS / IPSI		Yes	Yes
Device Instance	Identifies the device instance, e.g. Speaker 1, Speaker 2	BT ITS / IPSI		Yes	Yes
Line	Line number	BT ITS / IPSI		Yes	No
Line Name	Name of the line	BT ITS / IPSI		Yes	No
Line Type	PSTN MF, Private Wire Manual, PBX MF, ...	BT ITS / IPSI		Yes	No
Phantom DDI	Phantom Direct Dial Inward number	BT ITS / IPSI		Yes	No
Console	Turret ID	BT ITS / IPSI		Yes	Yes
Console Type	Turret model, e.g. Netrix Button	BT ITS / IPSI		Yes	Yes
Console Name	Name of the turret	BT ITS / IPSI		Yes	Yes
Vertical ID	Vertical ID	BT ITS / IPSI		Yes	Yes
Recorder Channel	Recorder Cluster ID – Recorder Trunk ID – Channel ID	BT ITS / IPSI		Yes	Yes
User Name	Name of the trader	BT ITS / IPSI		Yes	Yes
DDI	Direct Dial Inward number	BT ITS / IPSI		Yes	No
DDI Label	Direct Dial Inward label	BT ITS / IPSI		Yes	No
ELC Group Number	ELC Group Number	BT ITS / IPSI		Yes	No
Privacy	Marked segment while privacy set	Marker		Yes	No
Microphone State	Marked segment while the microphone is latched/on	Marker		Yes	No
Recording on mute	Marked segment while recording on mute is set	Marker		Yes	No

Participant Joins /Leaves	Barge in participant (trader ID) joins or leaves the call	Marker		Yes	No
---------------------------	---	--------	--	-----	----

IPC Unigy

Overview

Integration utilizes Unigy's active recording interface which consists of the following links:

- **CTI (CDR):** agent and CDR/call events
- **SIP (Audio control):** establishes recording/media channels, negotiates voice codec and SRTP crypto parameters
- **RTP/SRTP (Audio stream):** carries voice media

Recorder service at startup logs in via the CTI link and subscribes to agent and call events. When a trader agent logs in on a turret (the agent can be logged in only on one turret at the same time) the Unigy platform notifies the recorder and the recorder establishes media channels via SIP as per the recording profile configuration of the turret. When a call starts, the recorder receives a call start CTI/CDR event which refers to the related media channel. Based on this information the recorder starts recording the media and creates a database record with the CDR. When the call ends a call end CTI event is received based on which the recorder terminates the recording. At recorder startup, the recorder gets agent login and call start notification for all logged-in agent sessions and ongoing calls so can start recording from that point.

IPC Unigy recording features

- Certified IPC Unigy recording solution
- 2N and N+1 recorder configurations
- Compatible with trader voice recording data model
- Support for VAD (voice activity detection) and media segmentation for long calls
- Recording of encrypted/secure turrets when available
- All types of recording mix layouts are supported

Version support

IPC Switch Name & Model	IPC Unigy
Supported IPC Unigy Versions	1.x or later
Supported Turret Types	IQ/MAX, IQ/MAX Touch, IQ/MAX Edge (100/200) IQ/MAX Sync, IQ/MAX Omni, Pulse Enterprise, Pulse Mobile

If you are on a different version, contact your IPC representative for more information.

Features not available

- Silent monitoring only available for Media-Only records
- Full / Always-on, Do-not-record, Never-record recording modes only (no On-demand, no Controlled)
- Desktop Screen Capture is not available
- No support for turret based playback

Deploying IPC Unigy Recording

The following section contains all the necessary steps for setting up an IPC Unigy Recording infrastructure.

Server Sizing

Allocating the appropriate resources to the different servers is crucial. For guidance, see [Server sizing and requirements](#)

Preparation

Make sure that all the required prerequisites are installed on each server prior to the installation.

- [Prerequisites](#)
- [Installing the required prerequisites](#)

For guidance on configuring the necessary firewall port, visit [Firewall Configuration for IPC Unigy recording deployments](#)

Installation

The following articles contain all the step for installing the various server roles:

- [Installing a Verba Single Server solution](#)
- [Installing a Verba Media Repository](#)
- [Installing a Verba Recording Server](#)

Configuration

For configuring the system for IPC Unigy recording, see [Configuring IPC Unigy recording](#).

Resiliency

The system can be deployed in various configurations to achieve resiliency. For more information, see [IPC Unigy recorder resiliency](#).

IPC Unigy metadata

The system captures the following metadata specific to IPC Unigy calls when CTI messages are available. These fields are available through the standard and the IPC Unigy specific custom metadata template.

Metadata Field	Description	Template	Available	Available in CDR-Only records	Available in Media-Only records
Start Date	Start date of the conversation	Standard	Yes	Yes	Yes
Start Time	Start time on the conversation	Standard	Yes	Yes	Yes
End Date	End date of the conversation	Standard	Yes	Yes	Yes
End Time	End time of the conversation	Standard	Yes	Yes	Yes
Duration	Length of the conversation	Standard	Yes	Yes	Yes
User	Name of the recorded user	Standard	Yes	Yes	Yes
From	Source resource (e.g. line number)	Standard	Yes	Yes	No
From Info	Recorded trader name	Standard	Yes	Yes	No

To	Destination resource (e.g. line number)	Standard	Yes	Yes	No
To Info	Recorded trader name	Standard	Yes	Yes	No
Direction	The direction of the call from the system perspective; requires configuring internal number/domain patterns	Standard	Yes	Yes	No
Direction (User)	Direction of the call from the recorded user perspective	Standard	Yes	Yes	No
From (Verba)	Name of the Verba user associated with the calling party	Standard	Yes	Yes	Yes
To (Verba)	Name of the Verba user associated with the called party	Standard	Yes	Yes	Yes
Location	The hostname of the recording server	Standard	Yes	Yes	Yes
End Cause	Normal, Hold	Standard	Yes	Yes	Yes
Audio Codec	Audio codec of the recorded streams	Standard	Yes	No	Yes
Video codec	Video codec of the recorded streams	Standard	No	No	No
Platform Call ID	Unique conversation identifier received from the recorded platform	Standard	Yes	Yes	Yes
Silence Ratio	Ratio of silence in the conversation	Standard	No	No	No
Talkover Ratio	Talkover ratio of the conversation	Standard	No	No	No
Longest Silence	Length of the longest silence present in the conversation	Standard	No	No	No
User ID / Agent ID	Trader ID	Standard	Yes	Yes	Yes
From Device	Recorded turret/intercom ID	Standard	Yes	Yes	Yes
To Device	Recorded turret/intercom ID	Standard	Yes	Yes	Yes
Dialed Number	Original dialed number	Standard	No	No	No
From IP	IP address of the media source	Standard	Yes	Yes	Yes
To IP	IP address of the media source	Standard	Yes	Yes	Yes
From Proxy IP	IP address of the proxy server associated with the calling party	Standard	No	No	No
To Proxy IP	IP address of the proxy server associated with the called party	Standard	No	No	No
Source Platform	IPC Unigy	Standard	Yes	Yes	Yes
Conversation Type	Voice	Standard	Yes	Yes	Yes
Forward Reason	Forward reason for the conversation (e.g. forwarded, transferred, team call, delegated, etc.)	Standard	No	No	No
Recording failed	Indicates if the recording has failed and the metadata was imported during CDR reconciliation	Standard	No	No	No
Media Length	Length of the media file related to the conversation in hhh:mm:ss format	Standard	Yes	No	Yes
Media Error	Shows the media processing errors during recording	Standard	Yes	No	Yes
Voice Quality	Overall voice quality check score for the conversation	Standard	Yes	No	Yes
Record Type	CDR-Only, Media-Only	Standard	Yes	Yes	Yes

2N Source	In case of duplicate (2N) recording, records are marked as primary or secondary	Standard	Yes	Yes	Yes
Device Location	Turret location info	IPC Unigy		Yes	Yes
Audio Source	Audio source device on the turret	IPC Unigy		Yes	Yes
Line Appearance	Line appearance identifier	IPC Unigy		Yes	No
E1 Resource	E1 resource name	IPC Unigy		Yes	No
Billing Group ID	Billing group identifier	IPC Unigy		Yes	No
Session Type	Line, Turret, Speaker, Bridge, Conference, Transfer	IPC Unigy		Yes	No
Line Description	Line label	IPC Unigy		Yes	No
Push to Talk State	Marked segment while PTT is pressed	Marker		Yes	No

Cloud9

- [Overview](#)
 - [Cloud9 recording features](#)
 - [Version support](#)
- [Deploying Cloud9 recording](#)
 - [Server sizing](#)
 - [Preparation](#)
 - [Installation](#)
 - [Configuration](#)
- [Cloud9 Recording System API metadata](#)
- [Cloud9 Call Data API metadata](#)

Overview

Cloud 9 Technologies is a cloud communications service provider. They provide high-performance voice, messaging and collaboration services designed for the unique needs of distributed workgroups and teams. C9 Trader connects the institutional trading community with a voice and messaging solution designed especially for the financial markets. It provides a secure and compliant way to connect with your trading counterparties while eliminating the hassle and expense of legacy turret systems and private lines.

The C9 Trader application is able to record all calls in standard Ogg/Opus and M4A/AAC format.

There 2 integration options available for Cloud9:

- The files with related metadata (JSON) can be automatically uploaded from the C9 desktops to the Verba servers using the **Cloud9 Recording System API**, where a configured Cloud9 import source can receive, process, and archive the data. Multiple Verba serves can be deployed and used for the import. In this case, an HTTP load balancer has to be placed in front of the servers to provide load balancing and/or failover for the uploads.
- **Cloud9 Call Data API** allows downloading the recordings from the Cloud9 cloud platform and archives them in Verba. The C9 clients are initially uploading the recordings to the Cloud9 cloud platform and the Verba application is periodically checking the Call Data API for new data. C9 clients are uploading metadata and media files separately, media files are not necessarily available at the same time metadata is retrieved. The Verba system creates the CDR entry in the database after downloading the metadata record and when the media file becomes available, the record is updated in the database and the file is imported to the default media folder. An upload or move data management policy has to be configured to place the files on the storage infrastructure.

Cloud9 recording features

- Voice recording
- Integration options:
 - Cloud9 Call Data API
 - Cloud9 Recording System API
- Compatible with trader voice recording data model (Cloud9 Call Data API only)
- All types of recording mix layouts are supported
- Support for selective recoding by configuring trader IDs as recorded extensions

Version support

Switch Name & Model	Cloud9
Supported Symphony Versions	Contact Cloud9
Supported Endpoint / DeviceTypes	All

Deploying Cloud9 recording

The following section contains the necessary steps for setting up a Cloud9 recording infrastructure.

Server sizing

Allocating the appropriate resources to the different servers is crucial. For guidance, see [Server sizing and requirements](#)

Preparation

The Cloud9 integration requires additional prerequisites and configuration in Cloud9, which out of scope for this guide. Contact your Cloud9 representative for further information.

Make sure that all the required prerequisites are installed on each server prior to the installation.

- [Prerequisites](#)
- [Installing the required prerequisites](#)

Installation

The following articles contain all the step for installing the various server roles:

- [Installing a Verba Single Server solution](#)
- [Installing a Verba Media Repository](#)
- [Installing a Verba Recording Server](#)

Configuration

The system has to be configured for Cloud9 in the following way:

- Cloud9 Recording System API based integration requires configuring the related import sources and enable the Import Service on one of the Recording Servers. For more information, see [Cloud9 Recording System API](#).
- Cloud9 Call Data API based integration requires configuring the related import sources and enable the Import Service on one of the Recording Servers. For more information, see [Cloud9 Call Data API](#).
- Recorded users can be synchronized from Active Directory. To match the imported conversations to an extension (and to a user account) you need to add the Cloud9 login names as **extensions** with type **User / Agent ID**.

Cloud9 Recording System API metadata

The system captures the following metadata specific to Cloud9 recordings. These fields are available through the standard and the Cloud9 specific custom metadata template.

Metadata Field	Description	Template	Available
Start Date	Start date of the conversation	Standard	Yes
Start Time	Start time on the conversation	Standard	Yes
End Date	End date of the conversation	Standard	Yes
End Time	End time of the conversation	Standard	Yes
Duration	Length of the conversation	Standard	Yes
User	Name of the recorded user	Standard	Yes

From	Phone number, Button name, User name	Standard	Yes
From Info	User / contact name	Standard	Yes
To	Phone number, Button name, User name	Standard	Yes
To Info	User / contact name	Standard	Yes
Direction	Direction of the call from the system perspective, requires configuring internal number/domain patterns	Standard	Yes
Direction (User)	Direction of the call from the recorded user perspective	Standard	Yes
From (Verba)	Name of the Verba user associated with the calling party	Standard	Yes
To (Verba)	Name of the Verba user associated with the called party	Standard	Yes
Location	Hostname of the recording server	Standard	Yes
End Cause	Normal, Hold, Transfer, Conference, Device Change, From Terminated, To Terminated	Standard	No
Audio Codec	Audio codec of the recorded streams	Standard	No
Video codec	Video codec of the recorded streams	Standard	No
Platform Call ID	Unique conversation identifier received from the recorded platform	Standard	Yes
Silence Ratio	Ratio of silence in the conversation	Standard	No
Talkover Ratio	Talkover ratio of the conversation	Standard	No
Longest Silence	Length of the longest silence present in the conversation	Standard	No
User ID / Agent ID	Cloud9 user ID	Standard	Yes
From Device	Device ID of the calling party	Standard	No
To Device	Device ID of the called party	Standard	No
Dialed Number	Original dialed number	Standard	No
From IP	IP address associated with the calling party	Standard	No
To IP	IP address associated with the called party	Standard	No
From Proxy IP	IP address of the proxy server associated with the caller party	Standard	No
To Proxy IP	IP address of the proxy server associated with the called party	Standard	No
Source Platform	Cloud9	Standard	Yes
Conversation Type	Voice	Standard	Yes
Forward Reason	Forward reason for the conversation (e.g. forwarded, transferred, team call, delegated, etc.)	Standard	No
Recording failed	Indicates if the recording has failed and the metadata was imported during CDR reconciliation	Standard	No
Media Length	Length of the media file related to the conversation in hhh:mm:ss format	Standard	No
Media Error	Shows the media processing errors during recording	Standard	No
Voice Quality	Overall voice quality check score for the conversation	Standard	Yes
Record Type	Standard	Standard	Yes
2N Source	In case of duplicate (2N) recording, records are marked as primary or secondary	Standard	No
Firm Name	Far-end firm name	Cloud9	
Group Name	Far-end group name	Cloud9	
Group ID	Far-end group ID	Cloud9	
Device Type	Handset 1, Handset 2, Microphone	Cloud9	

Call Type	Click to Call, Ring Down, Shout Down	Cloud9	
-----------	--------------------------------------	--------	--

Cloud9 Call Data API metadata

The system captures the following metadata specific to Cloud9 recordings. These fields are available through the standard and the Cloud9 specific custom metadata template. The system can store data using both standard and trader voice specific data models.

Metadata Field	Description	Template	Available in Standard record	Available in CDR-Only record	Available in Media-Only record
Start Date	Start date of the conversation	Standard	Yes	Yes	Yes
Start Time	Start time on the conversation	Standard	Yes	Yes	Yes
End Date	End date of the conversation	Standard	Yes	Yes	Yes
End Time	End time of the conversation	Standard	Yes	Yes	Yes
Duration	Length of the conversation	Standard	Yes	Yes	Yes
User	Name of the recorded user	Standard	Yes	Yes	Yes
From	Phone number, Button ID, User name depending on the call scenario	Standard	Yes	Yes	No
From Info	Button name depending on the call scenario	Standard	Yes	Yes	No
To	Phone number, Button ID, User name depending on the call scenario	Standard	Yes	Yes	No
To Info	Button name depending on the call scenario	Standard	Yes	Yes	No
Participants	Name of the participants of the call		Yes	Yes	No
Direction	Direction of the call from the system perspective, requires configuring internal number/domain patterns	Standard	Yes	Yes	No
Direction (User)	Direction of the call from the recorded user perspective	Standard	Yes	Yes	No
From (Verba)	Name of the Verba user associated with the calling party	Standard	Yes	Yes	Yes
To (Verba)	Name of the Verba user associated with the called party	Standard	Yes	Yes	Yes
Location	Hostname of the recording server	Standard	Yes	Yes	Yes
End Cause	User Release, Auto Release, Toggle Device, User Release Transfer, Auto Release Transfer, Unspecified	Standard	Yes	Yes	No
Audio Codec	Audio codec of the recorded streams	Standard	No	No	No
Video codec	Video codec of the recorded streams	Standard	No	No	No
Platform Call ID	Unique conversation identifier received from the recorded platform to correlate multiple call legs	Standard	Yes	Yes	No
Silence Ratio	Ratio of silence in the conversation	Standard	No	No	No
Talkover Ratio	Talkover ratio of the conversation	Standard	No	No	No
Longest Silence	Length of the longest silence present in the conversation	Standard	No	No	No

User ID / Agent ID	Cloud9 user ID	Standard	Yes	Yes	Yes
From Device	Recorded console ID	Standard	No	No	No
To Device	Recorded console ID	Standard	No	No	No
Dialed Number	Original dialed number	Standard	No	No	No
From IP	IP address of the recorded endpoint	Standard	No	No	No
To IP	IP address of the recorded endpoint	Standard	No	No	No
From Proxy IP	IP address of the proxy server associated with the calling party	Standard	No	No	No
To Proxy IP	IP address of the proxy server associated with the calling party	Standard	No	No	No
Source Platform	Cloud9	Standard	Yes	Yes	Yes
Conversation Type	Voice	Standard	Yes	Yes	Yes
Forward Reason	Forward reason for the conversation (e.g. forwarded, transferred, team call, delegated, etc.)	Standard	No	No	No
Recording failed	Indicates if the recording has failed and the metadata was imported during CDR reconciliation	Standard	Yes	Yes	No
Media Length	Length of the media file related to the conversation in hhh:mm:ss format	Standard	Yes	No	Yes
Media Error	Shows the media processing errors during recording	Standard	Yes	No	Yes
Voice Quality	Overall voice quality check score for the conversation	Standard	Yes	No	Yes
Record Type	Standard, CDR-Only, Media-Only	Standard	Yes	Yes	Yes
2N Source	In case of duplicate (2N) recording, records are marked as primary or secondary	Standard	No	No	No
Technical Call ID	Unique conversation identifier received from the recorded platform	Standard	Yes	Yes	Yes
Audio Interface	The audio device used for the call: Left handset, Microphone, Right handset	Cloud9 Call Data API	Yes	Yes	No
Call Type	Shout Down, Gateway Shout Down, Ring Down, Gateway Ring Down, Dial Tone, Intercom, Large Hoot	Cloud9 Call Data API	Yes	Yes	No
Near-end Firm Name	Name of your firm (as nearEnd) as defined in Cloud9 portal	Cloud9 Call Data API	Yes	Yes	No
Far-end Firm Name	Name of the other firm (as farEnd) on the call, as defined in Cloud9 portal	Cloud9 Call Data API	Yes	Yes	No
Near-end Legal Entity	Legal Entity ID of the nearEndFirm as relevant to the call. The LEI may be set on the Group or Connection level and Cloud9 picks up the relevant LEI, based on the specific usage of the call. If not set will be Cloud9 Firm ID.	Cloud9 Call Data API	Yes	Yes	No
Far-end Legal Entity	Legal Entity ID of the farEndFirm as relevant to the call. The LEI may be set on the Group or Connection level and Cloud9 picks up the relevant LEI, based on the specific usage of the call. If not will be Cloud9 Firm ID.	Cloud9 Call Data API	Yes	Yes	No
Near-end Group Name	Name of nearEndGroup to which the connection belongs	Cloud9 Call Data API	Yes	Yes	No
Far-end Group Name	Name of farEndGroup to which the connection belongs	Cloud9 Call Data API	Yes	Yes	No

Near-end Group ID	Unique ID of the nearEndGroup to which the connection belongs	Cloud9 Call Data API	Yes	Yes	No
Far-End Group ID	Unique ID of the farEndGroup to which the connection belongs	Cloud9 Call Data API	Yes	Yes	No
Call Quality Score	Voice Quality of Service rating for the call as calculated by Cloud9	Cloud9 Call Data API	Yes	Yes	No
Connection ID	Unique ID for the Button for the user that was used for the call	Cloud9 Call Data API	Yes	Yes	No
Button Name	The name of the Button for the user that was used for the call	Cloud9 Call Data API	Yes	Yes	No
C9 Circuit Reference	The Cloud9 circuit reference ID as displayed in the portal	Cloud9 Call Data API	Yes	Yes	No
C9 Circuit ID	The internal Cloud9 circuit ID	Cloud9 Call Data API	Yes	Yes	No

Speakerbus

Overview

The Speakerbus iSeries recorder integration relies on individual iSeries devices being responsible for the transmission of audio and call event information. The solution can essentially be split into 3 distinct areas.

- **Audio:** Each iSeries device is able to transmit one or more simultaneous audio streams (VoIP) as encoded RTP (Real Time Protocol) over UDP (User Datagram Protocol). The codecs that are supported are G.711 (A-Law or μ -Law), G.729 (Annex A or Annex AB) and G.722.
- **Call Data Records (CDR):** Each iSeries device is responsible for transmitting Call Data Records (CDR) that relate to events happening on that individual device.
- **iManager Call Data Service (iCDS):** iCDS is a supervisory application that runs as a service on Microsoft Server operating systems. It acts as a multiplexer that receives CDR information from multiple iSeries devices and multiplexers the CDR information into a single stream that can be sent to multiple 3rd party devices / applications.

Speakerbus recording features

- Certified Speakerbus recording solution
- 2N recorder configurations
- Compatible with trader voice recording data model
- Support for VAD (voice activity detection) and media segmentation for long calls
- All types of recording mix layouts are supported

Version support

Speakerbus Switch Name & Model	Speakerbus
Supported Turret Types	iD808, iE801, iD712, SE 708
Supported iCDS Versions	2.1 or later

If you are on a different version, contact you Speakerbus representative for more information.

Features not available

- Silent monitoring only available for Media-Only records
- Full / Always-on, Do-not-record, Never-record recording modes only (no On-demand, no Controlled)
- Desktop Screen Capture is not available
- No support for turret based playback

Configuration

For configuring the system for Speakerbus recording, see [Configuring Speakerbus recording](#).

Speakerbus metadata

The system captures the following metadata specific to Speakerbus calls when CTI messages are available. These fields are available through the standard and the Speakerbus specific custom metadata template.

Metadata Field	Description	Template	Available	Available in CDR-Only records	Available in Media-Only records
Start Date	Start date of the conversation	Standard	Yes	Yes	Yes
Start Time	Start time on the conversation	Standard	Yes	Yes	Yes
End Date	End date of the conversation	Standard	Yes	Yes	Yes
End Time	End time of the conversation	Standard	Yes	Yes	Yes
Duration	Length of the conversation	Standard	Yes	Yes	Yes
User	Name of the recorded user	Standard	Yes	Yes	Yes
From	From address	Standard	Yes	Yes	No
From Info	From name	Standard	Yes	Yes	No
To	To address	Standard	Yes	Yes	No
To Info	To name	Standard	Yes	Yes	No
Direction	Direction of the call from the system perspective, requires configuring internal number/domain patterns	Standard	Yes	Yes	No
Direction (User)	Direction of the call from the recorded user perspective	Standard	Yes	Yes	No
From (Verba)	Name of the Verba user associated with the calling party	Standard	Yes	Yes	Yes
To (Verba)	Name of the Verba user associated with the called party	Standard	Yes	Yes	Yes
Location	Hostname of the recording server	Standard	Yes	Yes	Yes
End Cause	Normal, Hold, Transfer, Conference, Device Change	Standard	Yes	Yes	Yes
Audio Codec	Audio codec of the recorded streams	Standard	Yes	No	Yes
Video codec	Video codec of the recorded streams	Standard	No	No	No
Platform Call ID	Unique conversation identifier received from the recorded platform	Standard	Yes	Yes	Yes
Silence Ratio	Only for media-only records	Standard	No	No	No
Talkover Ratio	Only for media-only records	Standard	No	No	No
Longest Silence	Only for media-only records	Standard	No	No	No
User ID / Agent ID	Trader ID	Standard	Yes	Yes	Yes
From Device	Recorded turret ID	Standard	Yes	Yes	Yes
To Device	Recorded turret ID	Standard	Yes	Yes	Yes
Dialed Number	Original dialed number	Standard	No	No	No
From IP	IP address of the media source	Standard	Yes	Yes	Yes
To IP	IP address of the media source	Standard	Yes	Yes	Yes
From Proxy IP	IP address of the proxy server associated with the calling party	Standard	No	No	No
To Proxy IP	IP address of the proxy server associated with the called party	Standard	No	No	No
Source Platform	Speakerbus	Standard	Yes	Yes	Yes

Conversation Type	Voice	Standard	Yes	Yes	Yes
Forward Reason	Forward reason for the conversation (e.g. forwarded, transferred, team call, delegated, etc.)	Standard	No	No	No
Recording failed	Only for media-only records	Standard	No	No	No
Media Length	Only for media-only records	Standard	Yes	No	Yes
Media Error	Only for media-only records	Standard	Yes	No	Yes
Voice Quality	Only for media-only records	Standard	Yes	No	Yes
Record Type	CDR-Only, Media-Only	Standard	Yes	Yes	Yes
2N Source	In case of duplicate (2N) recording, records are marked as primary or secondary	Standard	Yes	Yes	Yes
Device	Handset 1, Handset 2, Handsfree 1, Handsfree 2, Intercom Handsfree, Bridged Handsets	Speakerbus		Yes	Yes
Conference Join/Leave	Conference join/leave events (phone number or Trader ID (display name))	Marker		Yes	No

Genesys

AVAILABLE IN VERSION 9.6.10 AND LATER

- [Overview](#)
 - [Genesys active recording features](#)
 - [Version support](#)
- [Deploying Genesys active recording](#)
 - [Preparation](#)
 - [Installation](#)
 - [Configuration](#)
 - [Genesys metadata](#)

Overview

The system supports multiple integration options with the Genesys platform:

- Genesys active recording
- Genesys CTI integration for Cisco network-based recording

This guide focuses on the Genesys active recording integration only. For more information on Genesys CTI integration with Cisco recording, see [Genesys integration for Cisco network based recording](#).

The Active Recording Ecosystem uses Media Stream Replication (MSR) for a fully Active recording solution with Dual Channel Recording. SIP sessions to the recorder provide basic call information and voice (Real-time Transport Protocol (RTP)) data. MSR is where Media Server replicates the RTPs and makes them available to the recording server. Additional events and information are provided by the T-Server part of the SIP Server. For a full overview and architecture of the Genesys Active Recording Ecosystem please refer to the following document: [Active Recording Ecosystem Overview](#)

Genesys active recording features

- Voice recording and archiving
- Integration with Genesys SIP Server for media stream recording
- Integration with Genesys T-Server for CTI / metadata
- Compatible with the advanced data model (only)
- Support for always-on recording
- Support for selective recording through selective recording rules
- Silent monitoring is not supported

Version support

Switch Name & Model	Genesys PureEngage
Supported Genesys Versions	Genesys SIP Server 8.x or later Genesys T-Server 8.x or later
Supported Endpoint / DeviceTypes	Genesys SIP endpoints

If you are on a different version, contact your Genesys representative for more information.

Deploying Genesys active recording

The following section contains all the necessary steps for setting up a Genesys active recording infrastructure.

Preparation

Make sure that all the required prerequisites are installed on each server prior to the installation.

- [Prerequisites](#)
- [Installing the required prerequisites](#)

For guidance on configuring the necessary firewall port, visit [Firewall configuration for Genesys active recording deployments](#)

Installation

The following articles contain all the step for installing the various server roles:

- [Installing a Verba Single Server solution](#)
- [Installing a Verba Media Repository](#)
- [Installing a Verba Recording Server](#)

Configuration

For the configuration guide, see [Configuring Genesys active recording](#)

Genesys metadata

The system captures the following metadata specific to Genesys recordings.

Metadata Field	Description	Template	Available	Available in CDR-Only record	Available in Media-Only record
Start Date	Start date of the conversation	Standard	Yes	Yes	Yes
Start Time	Start time on the conversation	Standard	Yes	Yes	Yes
End Date	End date of the conversation	Standard	Yes	Yes	Yes
End Time	End time of the conversation	Standard	Yes	Yes	Yes
Duration	Length of the conversation	Standard	Yes	Yes	Yes
User	Name of the recorded user	Standard	Yes	Yes	Yes
From	Directory Number, Phone Number	Standard	Yes	Yes	No
From Info	Caller party name	Standard	Yes	Yes	No
To	Directory Number, Phone Number	Standard	Yes	Yes	No
To Info	Called party name	Standard	Yes	Yes	No
Direction	Direction of the call from the system perspective, requires configuring internal number/domain patterns	Standard	Yes	Yes	No
Direction (User)	Direction of the call from the recorded user perspective	Standard	Yes	Yes	No
From (Verba)	Name of the Verba user associated with the calling party	Standard	Yes	Yes	Yes

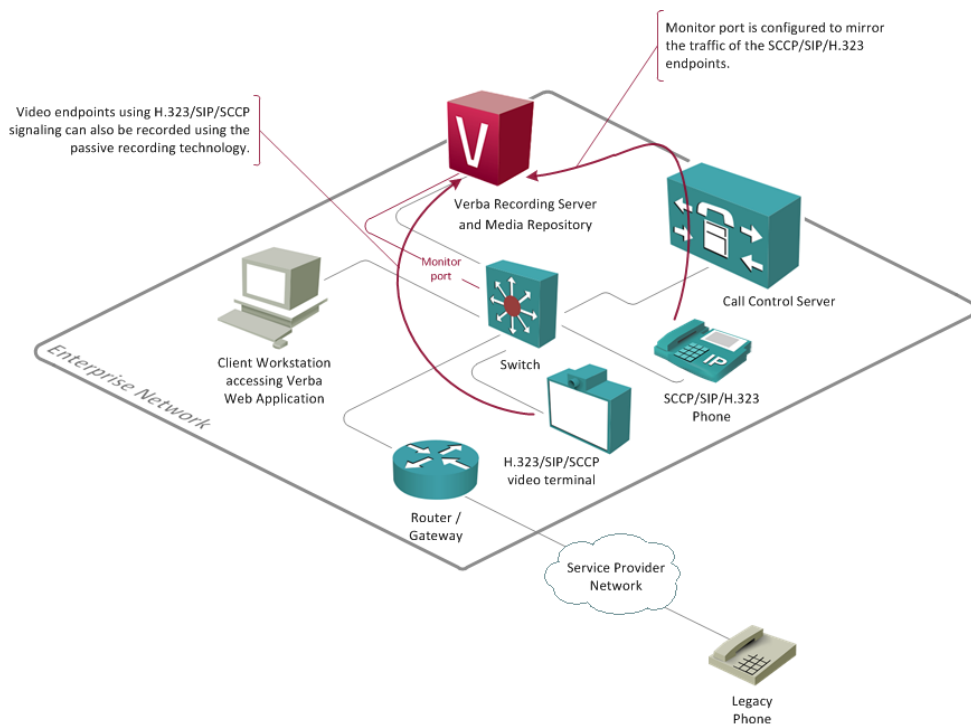
To (Verba)	Name of the Verba user associated with the called party	Standard	Yes	Yes	Yes
Location	Hostname of the recording server	Standard	Yes	Yes	Yes
End Cause	Normal, Hold, Transfer, Conference	Standard	Yes	Yes	No
Audio Codec	Audio codec of the recorded streams	Standard	Yes	Yes	No
Video codec	Video codec of the recorded streams	Standard	Yes	No	No
Platform Call ID	Unique conversation identifier received from the recorded platform	Standard	Yes	Yes	Yes
Silence Ratio	Ratio of silence in the conversation	Standard	Yes	No	Yes
Talkover Ratio	Talkover ratio of the conversation	Standard	Yes	No	Yes
Longest Silence	Length of the longest silence present in the conversation	Standard	Yes	No	Yes
User ID / Agent ID	Genesys Agent ID	Standard	Yes	Yes	No
From Device	Device ID of the calling party	Standard	No	No	No
To Device	Device ID of the called party	Standard	No	No	No
Dialed Number	Original dialed number	Standard	No	No	No
From IP	IP Address of the Genesys Server	Standard	Yes	No	Yes
To IP	IP address of the called party device	Standard	No	No	No
From Proxy IP	IP address of the proxy server associated with the caller party	Standard	No	No	No
To Proxy IP	IP address of the proxy server associated with the called party	Standard	No	No	No
Source Platform	Genesys T-Server	Standard	Yes	Yes	Yes
Conversation Type	Voice	Standard	Yes	Yes	Yes
Forward Reason	Forward reason for the conversation (e.g. forwarded, transferred, team call, delegated, etc.)	Standard	No	No	No
Recording failed	Indicates if the recording has failed and the metadata was imported during CDR reconciliation	Standard	No	No	No
Media Length	Length of the media file related to the conversation in hhh:mm:ss format	Standard	Yes	No	Yes
Media Error	Shows the media processing errors during recording	Standard	Yes	No	Yes
Voice Quality	Overall voice quality check score for the conversation	Standard	Yes	No	Yes
Record Type	CDR-Only, Media-Only	Standard	Yes	Yes	Yes
2N Source	In case of duplicate (2N) recording, records are marked as primary or secondary	Standard	Yes	Yes	Yes
ANI	Identification (the DN from which the inbound call was made)	Genesys	Yes	Yes	No
DNIS	The Directory Number Information Service (the DN to which the inbound call in question has been made)	Genesys	Yes	Yes	No
Call Type	The type of call in question	Genesys	Yes	Yes	No
This Party	The directory number of the third party in a transfer or conference call	Genesys	Yes	Yes	No

This Party Role	The role of the telephony object specified by Third Party DN in the event in question	Genesys	Yes	Yes	No
This Party Queue	The queue related to the Third Party DN	Genesys	Yes	Yes	No
This Party Trunk	The trunk group identifier related to the Third Party Queue	Genesys	Yes	Yes	No
Other Party	The directory number of the second most significant telephony object (except an ACD group or trunk group) with respect to the event in question. The application does not have to be registered to this directory number to receive the event in question.	Genesys	Yes	Yes	No
Other Party Role	The role of the telephony object specified by Other Party DN in the event in question	Genesys	Yes	Yes	No
Other Party Queue	The directory number of the second most significant ACD group with respect to the event in question	Genesys	Yes	Yes	No
Other Party Trunk	The trunk group identifier related to Other Party Queue	Genesys	Yes	Yes	No
Call UUID	Call UUID	Genesys	Yes	Yes	No
GSIP_REC_FN		Genesys	Yes	Yes	No
Agent ID	The agent identifier specified by PBX or ACD	Genesys	Yes	Yes	No
Party UUID	Party UUID	Genesys	Yes	Yes	No
Customer ID	The string containing the customer identifier through which processing of the call was initiated	Genesys	Yes	Yes	No
Propagated Call Type	Propagated Call Type	Genesys	Yes	Yes	No
Wrap Up Time	Wrap Up Time	Genesys	Yes	Yes	No

Passive, extension side call recording

The passive recording method is achieved by connecting the recorder server to a monitor port of a switch (SPAN/RSPAN port). The monitor port receives all of the traffic for each phones that need to be recorded. The recorder captures all the traffic, including the RTP media streams and the SCCP, SIP signaling messages.

Using Verba Recording System, multiple recording servers can be deployed in order to support multi-site configurations or branch office networks and/or high volume systems with or without redundancy.



Supported platforms

The following list contains all supported platforms for passive, network monitoring based recording:

Supported Platform	Supported Signaling Protocols	Supported Media Types
Cisco	SCCP SIP	Voice, Video, TelePresence
BroadSoft	SIP, SCCP	Voice
LifeSize	H.323***, SIP	Voice, Video
Polycom*	H.323***, SIP	Voice, Video
Any SCCP, SIP compliant endpoint or phone	-	Voice, Video

* For Polycom we do not support the following: Siren22 audio codec, Polycom telepresence endpoints, and all non-standard proprietary extensions.

Advantages

- Due to the nature of the passive recording method, there is no extra bandwidth or resource requirement from the network or call control servers.
- There is no connection to the call control server(s) or usage of TAPI/JTAPI. In case of call control server failure, the recording system is not affected, the recording can work continuously if survivable telephony functionality is available on the site (e.g. Cisco SRST - Survivable Remote Site Telephony). In this case, a recording server is deployed at the site.
- Because of the passive approach, the flow of the call is not affected at all.
- Can be easily deployed and maintained.
- Using Verba Recording System multi-site deployment architecture, the system can be adapted very well to a wide array of use cases.
- If high-volume traffic is recorded, the system can be scaled easily by adding new recording servers.
- All types of SCCP/SIP phones can be recorded.
- Monitor port technology is widely used approach.
- In most cases it can be easily configured and used.
- Silent monitoring can be supported natively by the recorder.
- Video and TelePresence calls can also be recorded on certain platforms.

Considerations

- In complex switching infrastructure, the monitor port configuration can be a headache.
- In a multi-site network, branches where a few calls have to be recorded, requires dedicated recording server.
- Automatic announcement of the recording cannot be done by the recorder. An external IVR or TCL script on the gateway should be involved.
- Encrypted calls cannot be recorded.

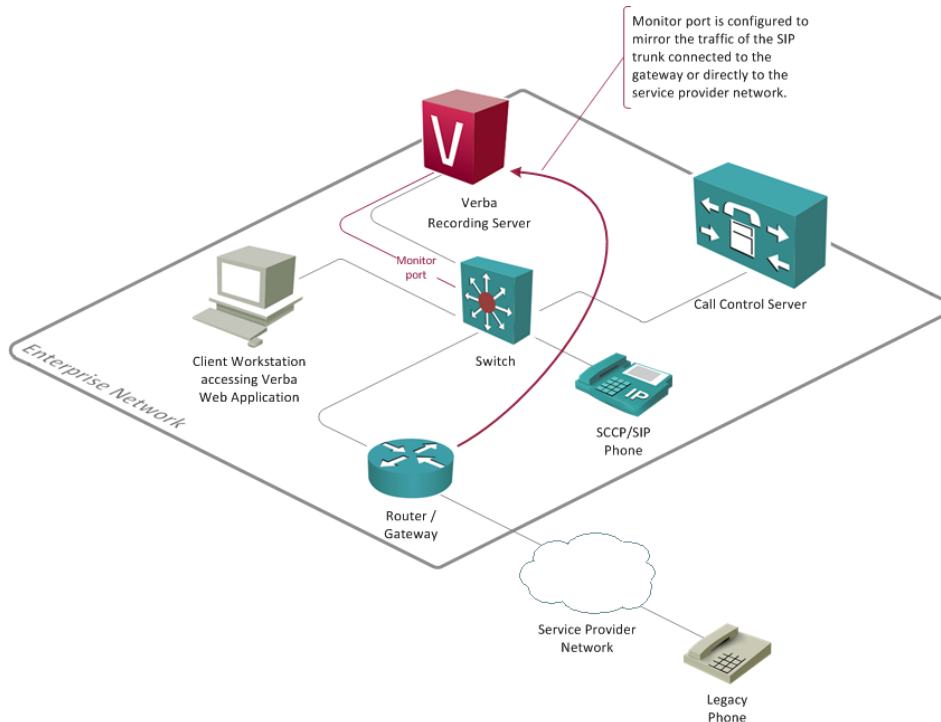
Possible deployment of passive, extension side call recording:

- **Single Server solution:** All Verba services (Administration, Recorder) are on one server.
For installation guide see: [Installing a Verba Single Server solution](#)
- **Media Repository + Recorder Server:** The Verba administration/storage and the Recording server is deployed separately.
For the installation guide see: [Installing a Verba Media Repository](#) and [Installing a Verba Recording Server](#)

Passive, trunk-side call recording

The passive recording method is achieved by connecting the recorder server to a monitor port of a switch (SPAN/RSPAN port). The monitor port receives all of the traffic for each trunk that need to be recorded. The recorder captures all the traffic, including the RTP media streams and the SIP/H.323 signaling messages. SIP/H.323 trunks usually connect the call control server with the PSTN gateways or establish a direct IP trunk connection with the service provider.

Using Verba Recording System, multiple recording servers can be deployed in order to support multi-site configurations or branch office networks and/or high volume systems with or without redundancy.



Advantages

- There is no connection to the CUCM server(s), so there is no extra capacity requirement at all.
- In case of CUCM failure, the recording system is not affected, the recording can work continuously even in SRST (Survivable Remote Site Telephony) mode (if a local recording server is deployed at the remote side).
- Because of the passive approach, the flow of the call is not affected at all.
- Can be easily deployed and maintained.
- Using Verba multi-site deployment architecture, the system can be adapted very well to fit a wide array of use cases.
- If high-volume traffic should be recorded, the system can be scaled easily.
- Monitor port technology is widely used approach. In most cases it can be easily configured and used.
- Silent monitoring can be supported natively by the recorder.
- Mobile phones can be recorded if the calls are routed through a SIP/H.323 mobile adapter (makes sense for transferred or forwarded calls only).

Considerations

- Encrypted calls cannot be recorded.
- Internal calls between IP phones cannot be recorded.
- Only SIP and H.323 trunks are supported by Verba. (MGCP is not supported)
- Automatic announcement of the recording cannot be done by the recorder itself. An external IVR should be involved.
- Directory number/extension information is usually not available.

Possible deployment of passive, trunk-side call recording:

- **Single Server solution:** All Verba services (Administration, Recorder) are on one server.
For installation guide see: [Installing a Verba Single Server solution](#)
- **Media Repository + Recorder Server:** The Verba administration/storage and the Recording server is deployed separately.
For the installation guide see: [Installing a Verba Media Repository](#) and [Installing a Verba Recording Server](#)

Dial-in audio and video call recorder

The Verba Dial-in Recorder is an **audio and video** call recording solution, where users can actively dial into various recorder lines to access the following services:

1. record a call or conference (both audio and video)
2. playback recorded calls (both audio and video)
3. listen to ongoing calls on your network (audio only)

When used for recording the dial-in recorder becomes a party of the conversation. There are two main recording situations:

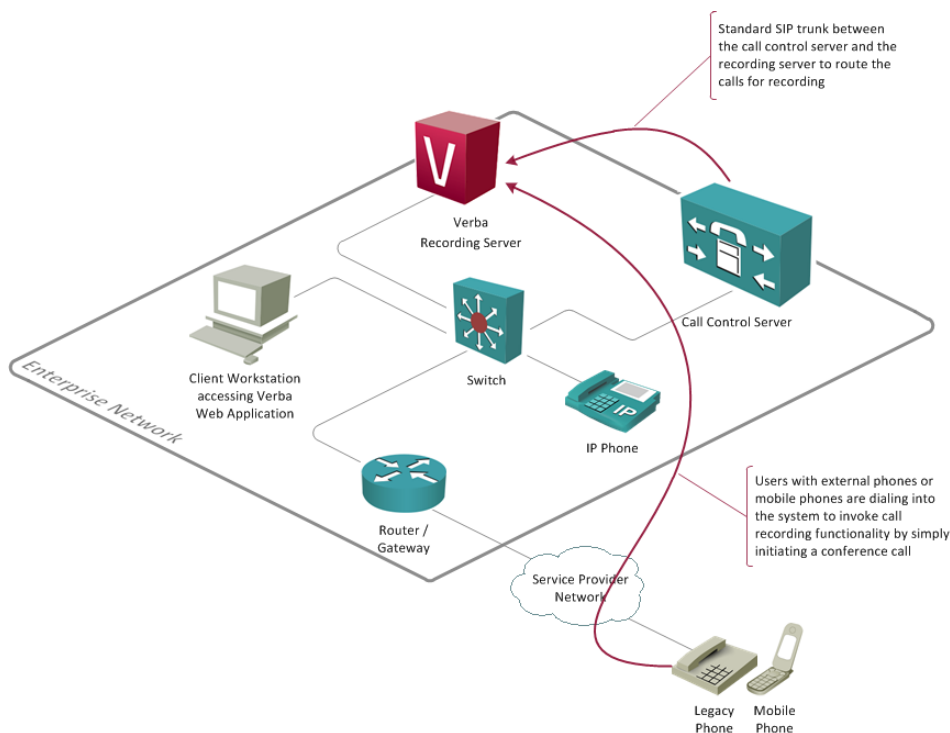
1. **dictation, note taking** - when a caller calls the line, talks and does not connect any other party
2. **conference recording** - when the caller adds the recorder to a conference call where more two or more parties are present

All recordings are stored in a central archive and are available through our web interface.

The recording lines can be **secured** using caller number detection or even PIN authentication.

Consider the following example user cases to get a better understanding of the solution:

- **Conference call** - A consultant wants to record a conference call at the customer-site where the internal recording system is not available
- **Trading** - A trader needs documentation of a deal, but she is currently out of office, where recording is not available
- **Interviews** - A journalist wants to record an interview from a mobile phone: calls the recorder and starts a three party conference to conduct an interview
- **Verbal contracts and third party verification** - A call center worker can connect the dial-in recorder into a call when the a voice contract is started



Supported audio phones

The dial-in recorder solution supports:

- **all audio endpoints** in Cisco UCM and BroadSoft BroadWorks environments are officially supported.

- most **standard SIP audio endpoints**
- all endpoints where the phone system can **route calls to the recorder through a SIP trunk** (this way the solution can record calls from analogue phones, digital phones, mobile phones and more)

Experimental H.323 support is also available.

Supported video phones

The dial-in recorder solution supports **most standard SIP video endpoints**.

In **Cisco environment** the solution supports the following endpoints:

- Cisco Unified Video Advantage associated with a Cisco Unified IP Phone 7911, 7940, 7941, 7942, 7945, 7960, 7961, 7962, 7965, 7970, 7971, or 7975, or with Cisco IP Communicator, running Skinny Client Control Protocol (SCCP)
- Cisco Unified IP Phones 9971 and 9951 with the optional USB camera attachment
- Cisco Unified IP Phones 8941 and 8945 with built-in camera
- Cisco IP Video Phone 7985
- Cisco E20 Video Phone
- Tandberg 2000 MXP, 1500 MXP, 1000 MXP, 770 MXP, 550 MXP, T-1000, and T-550 models running SCCP
- Sony PCS-1, PCS-TL30, and PCS-TL50 models running SCCP
- Cisco Unified Personal Communicator (running in softphone mode)
- Cisco Unified Client Services Framework (CSF) clients
- Cisco Unified Personal Communicator and Cisco Unified Client Services Framework (CSF) clients (running in deskphone mode) associated with a Cisco Unified IP Phone 7941, 7942, 7945, 7961, 7962, 7965, 7971, or 7975 running Skinny Client Control Protocol (SCCP)

Experimental H.323 support is also available.

Advantages

- **Record any calls** - Any phone call can be recorded; even mobile phone calls are supported.
- **Playback on phone** - Call playback on any phone device.
- **Silent monitoring on phone** - Supports silent monitoring.

Considerations

- **No automatic/compliance recording** - the conference has to be manually set up on the phone device by the user

Screen capture

Screen capturing overview

Verba Screen Capture module is an optional building block of the Verba Performance and Quality Management system. Contact center supervisors and managers are now able to monitor and evaluate agent performance by recording the content of the agent's computer desktop screen during the calls.

The lightweight screen capture agent module is installed on the agent computer and it automatically records the screen activity during the agent's calls. The recorded screen capture video files are automatically uploaded to the Verba Media Repository server, where the files are merged with the audio counterparts, providing a single, synchronized media file for playback. The upload process is configurable and it supports scheduling. As all other system components, these screen capture modules are also configured and managed centrally. Administrators can simply apply a common settings for all agent computers by a single mouse click, through a configuration profile on the web based management interface.

Screen capture features

The following lists summarize the **Verba Desktop Recorder**, that includes the Screen Capture module. This recorder is a lightweight software installed on the client PCs that need screen recording.

Recording features

- **Automatic recording mode** - Automatically starts the screen capturing process when the associated calls are started and automatically stop the recording process after the call ends.
- **Invisible mode** - The application can be configured to work completely invisible on the client PC.
- **Recording of after call wrap-up** - Screen recordings can continue for configured amount of time after the phone call is finished
- **Automatic uploads** - The screen capture video recordings are automatically uploaded and synchronized with the audio counterparts on the Media Repository server, this upload can be immediate
- **Ability to choose which screen or window should be recorded** - It is possible to choose from the following options:
 - Record Primary Screen Only
 - Record All Screens
 - Record Screen of Current In-Focus Window
 - Record Current In-Focus Window

Screen recording features

- **Lossless screen video** - Lossless, optimized video recording codec technology.
- **Low CPU utilization** - when the Verba Screen Capture Codec is used, the CPU utilization is exceptionally low on the client PCs
- **Multiple codecs** - The recordings can be stored in: **Techsmith Screen Capture Codec**: third party codec optimized for screen recording **Verba Screen Recorder Codec**: in-house compression technology highly optimized for screen recording based on latest image processing theories, **Windows Media Screen Codec**: widely supported format from mobile devices to home entertainment, built-in support for playback on Windows

Media export features

- **Flexible media export** - The recordings can be published/exported in the following formats: Windows Media, MP4 (AAC audio, H.264 video)
- **Audio-only exports** - Users can switch between the original audio and screen capture video files during playback or file download operations.

Features important for IT

- **PCI DSS compliance** - Pause/Resume recordings during calls manually or through HTTP API

- **Support ofr Desktop virtualization** - Recording Windows Terminal Server and other desktop virtualization sessions is supported
- **Multi-monitor support** - Multi-monitor recording is supported as well, it can be configured to record primary screen only or all available monitors
- **Unattended installations** - MSI based installer package with 100% unattended installation option
- **Centralized configuration** - All desktop recorders are configured centrally from one point. The call association is based on the extension - user assignment in the system configuration. The login ID of the Windows user has to match the configured login ID in the Verba Recording System.

Storage requirements

For detailed storage requirement for screen captures, see [Storage requirements](#).

SMS capturing for mobile networks

AVAILABLE IN 9.1 AND LATER

The Verint Verba platform provides native support for **SMPP (Short Message Peer-to-Peer)** to capture **SMS (Short Message Service)** text messages. SMPP is an open telecommunications industry standard protocol designed to provide a communication interface for the transfer of short message data on mobile networks.

Supported Verint Verba platform features

SMS is a core communication modality in Verint Verba, similar to chat messages.

This means all platform capabilities that apply to chat are available for SMS messages:

- SMS capture can be enabled/disabled on a per extension level
- integrated into search & replay
- standard data retention rules, encryption, signing, access control, etc. apply

Searching SMS messages

In the search interface, each message is shown as separate sessions next to phone calls and other conversations. However, when a session is loaded into [Conversation View](#), it shows related SMS history.

The screenshot displays the Verint Verba search interface. The top section shows a list of search results for SMS messages. Each row includes a search icon, a timestamp, a duration, a phone number, a service name, a contact name, and a direction (PSTN Out). The messages are as follows:

Timestamp	Duration	Phone Number	Service	Contact	Direction
Jan 23, 2018 1:39:22 PM	00:00:00	+1 800 765 4321	Banking Service	+1 212 123 4567 John Doe	PSTN Out
Jan 23, 2018 1:39:22 PM	00:00:00	+1 800 765 4321	Banking Service	+1 212 123 4567 John Doe	PSTN Out
Jan 23, 2018 1:38:39 PM	00:00:00	+1 212 123 4567	John Doe	+1 800 765 4321 Banking Service	PSTN Out
Jan 23, 2018 1:38:39 PM	00:00:00	+1 212 123 4567	John Doe	+1 800 765 4321 Banking Service	PSTN Out
Jan 23, 2018 1:37:54 PM	00:00:00	+1 800 765 4321	Banking Service	+1 212 123 4567 John Doe	PSTN Out
Jan 23, 2018 1:37:54 PM	00:00:00	+1 800 765 4321	Banking Service	+1 212 123 4567 John Doe	PSTN Out
Jan 23, 2018 1:36:47 PM	00:00:00	+1 212 123 4567	John Doe	+1 800 765 4321 Banking Service	PSTN Out

The bottom section shows the 'Conversation View' for the selected message. It displays a chat interface with a 'Message' column and a 'Timestamp' column. The messages are as follows:

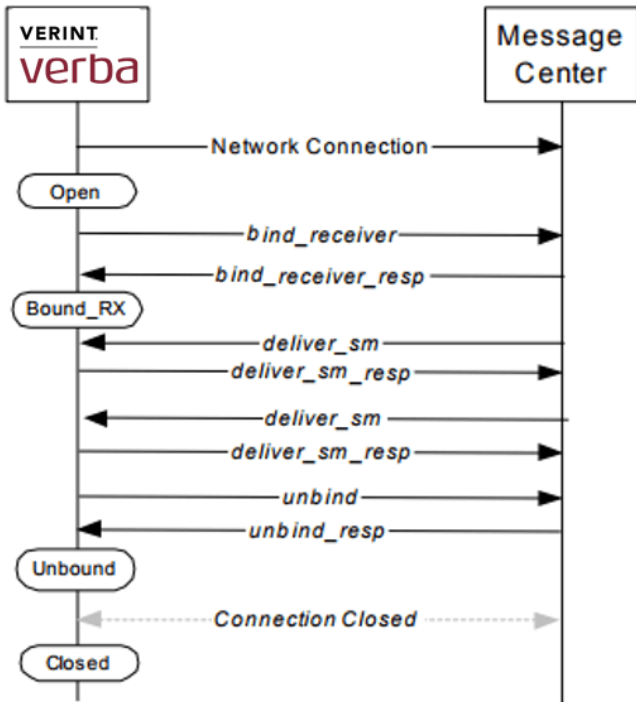
Message	Timestamp
Done!	Jan 23, 2018 01:40:31 PM
Also, you didn't make a payment to [Service] this month. Was this planned?	Jan 23, 2018 01:40:05 PM
You spent 15% more on groceries last month.	Jan 23, 2018 01:39:22 PM
Anything unusual in the past month?	Jan 23, 2018 01:38:39 PM
Your current balance is \$1,234.00	1:37:54 PM
What's my current balance?	Jan 23, 2018 01:36:47 PM

The 'Conversation Details' panel on the right shows the date range (Jan 23, 2018 1:37:54 PM - Jan 23, 2018 1:37:54 PM), the contact name (+1 800 765 4321 (Banking Service)), and the contact name (+1 212 123 4567 (John Doe)). It also includes checkboxes for 'Protected', 'Private', and 'Important'.

SMPP support

The **Verint Verba SMS Recorder service** supports SMPP v3.3, v3.4 and v5.0 in Receiver only mode. In the SMS architecture, the Verint Verba service is an External Short Message Entity (ESME). The service supports TLS and can run in both TCP server mode (provider established the connection, default) or outbind mode. For more information on SMPP v5, see <http://opensmpp.org/specs/smppv50.pdf>

The following diagram shows a typical message flow:



Operator site load balancing/failover scenarios are supported, multiple servers can run the Verint Verba SMS Recorder within the same platform.

Messages are stored in the SQL database of the platform, and in an optional transcript file on disc (*.sms).

For configuration details see the [Configuring SMS Recording](#) article.

Select a deployment architecture

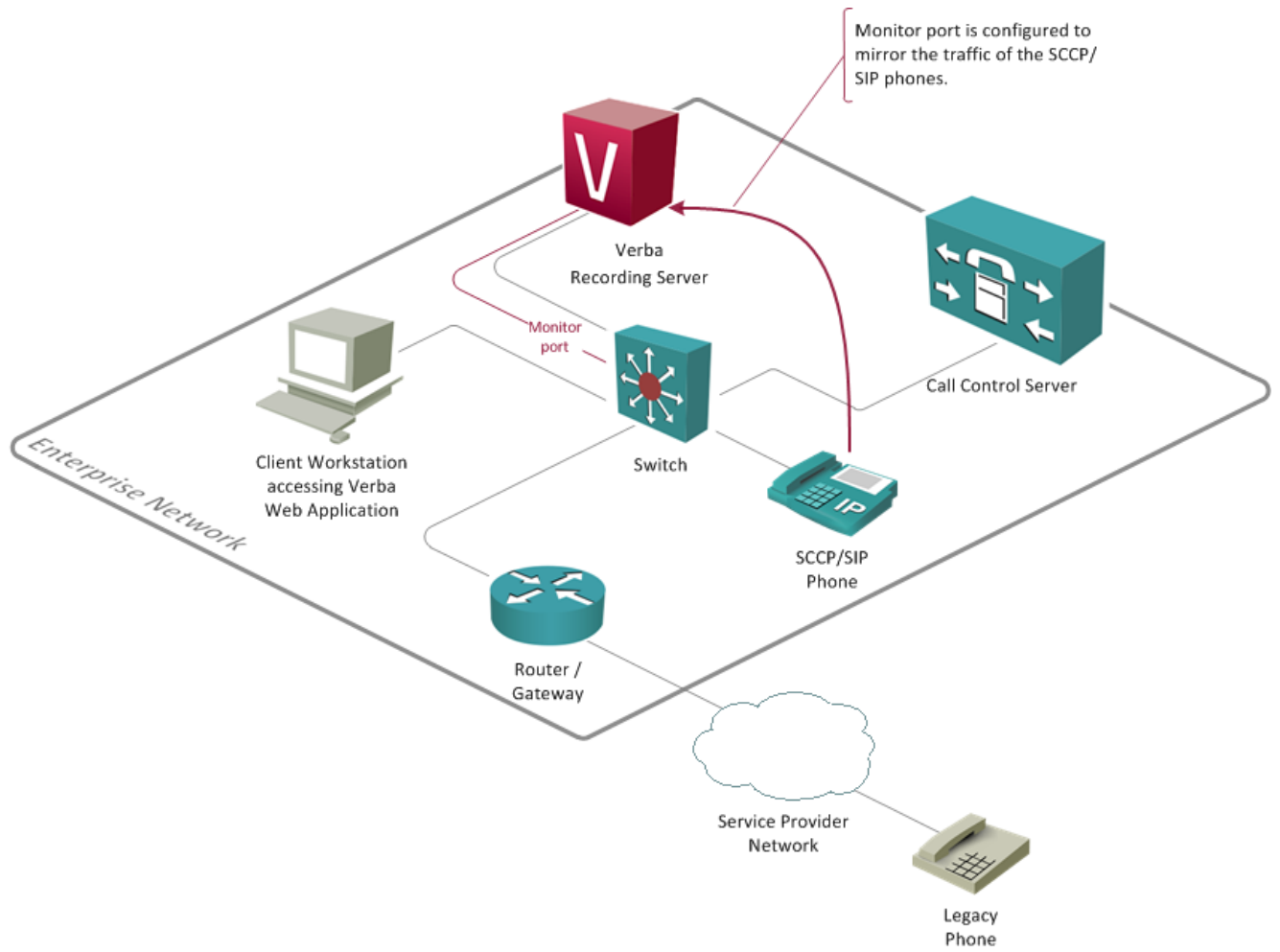
Verba offers the flexibility of various deployment options:

- [Single server architecture](#)
- [Multi server architectures with load balancing and failover](#)
- [Multi site architecture](#)
- [Verba desktop application](#)

Single server architecture

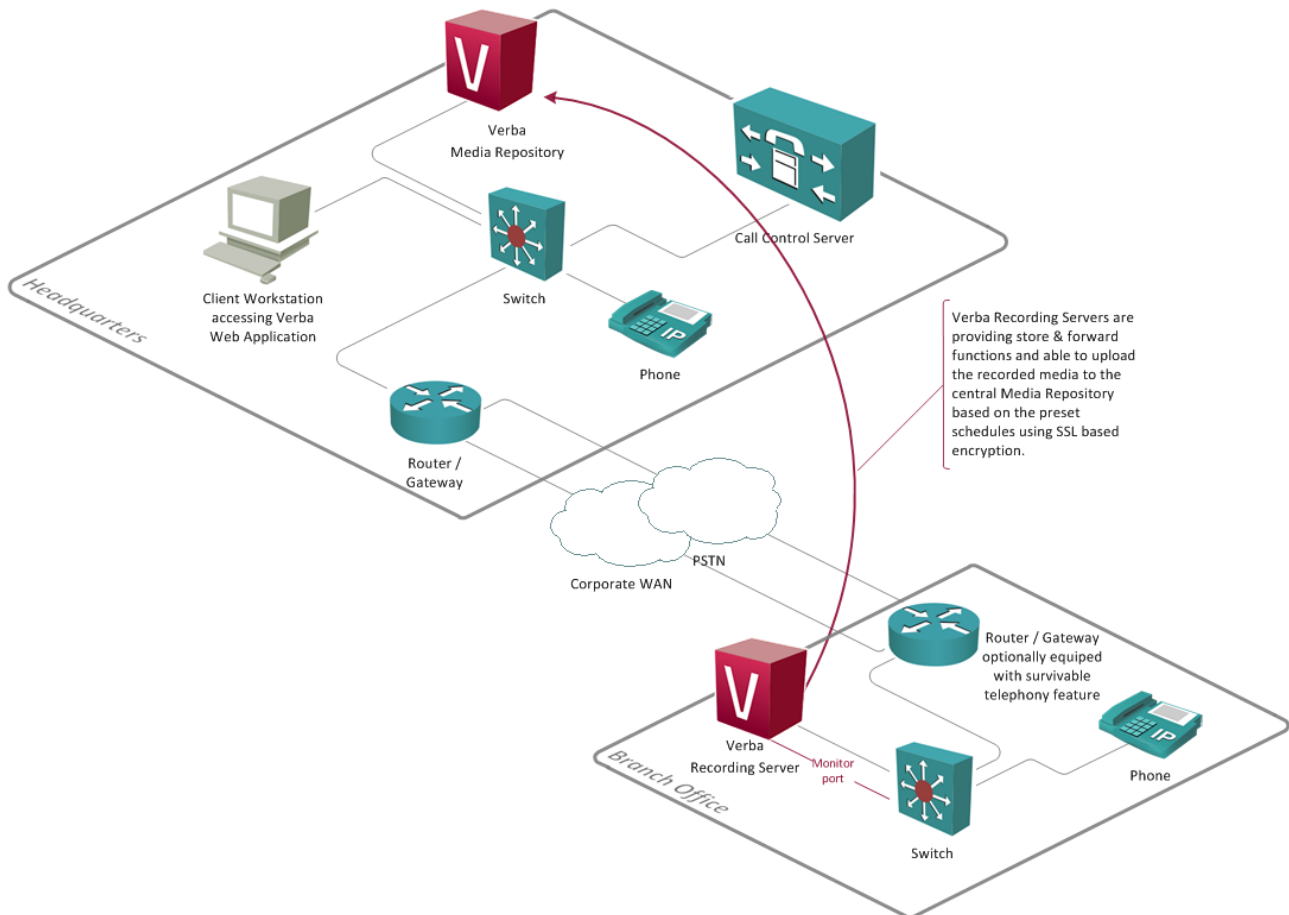
In this configuration all Verba components (Recording Server and Media Repository) are installed on the same server.

All functionality, including recording, archiving, web-based access with security, auditing and more is deployed on a single server.



Multi site architecture

In this configuration, the Verba components (Recording Server and Media Repository) are installed on separated servers. Distributing the system components can increase system capacity and adds multi-site recording functionality to the system. If more than one Recording Server is required (for multi site or increasing recording capacity), each Recording Server records the configured IP phone conversations at their site and uses the same Media Repository as a central database.



Benefits

- Fully centralized solution with distributable system components.
- Proven architecture with hundreds of reference sites all around the world.
- The remote sites or branches are running a lightweight store and forward module called the Recording Server while at the main site, the Media Repository component is installed, which provides centralized storage, playback, administration and archiving.
- Very low O&M costs due to the centralized management, storage, archiving and playback.
- WAN failure resilient since the Recording Server components is able to work without the central Media Repository and can synchronize the recorded media when the WAN link is up again. Support for Cisco Survivable Remote Site Telephony (SRST).
- Support for blade servers and VMware servers for even smaller footprint and lower total cost of ownership (TCO) and increased manageability.
- Support for video and telepresence, in addition to voice.
- Extremely flexible and scalable solution to support even hundreds of Recording Servers in a single solution.
- Secure communications and data transmission among the system components using industry standards like SSL and AES.

i Not all types of branch infrastructures are requiring the deployment of recording servers in the branches. Verba Technologies offers various other centralized recording methods, where the recorded media is automatically sent/forked to the recording server at the main site. The Verba Recording System even allows the deployment of a mixed solution, where the various

recording methods and architectures are combined in order to support the most versatile requirements of the customers.
Contact us to start discussing the best option for your system.

Desktop deployment

The Verba Desktop Recorder role/component is installed on the users' desktop computer. This component contains the Verba Screen capture module, which is responsible to record the computer screen on the desktop. The Verba Desktop Recorder component is similar to the Verba Recording Server, where the recorded files are automatically uploaded to the Media Repository server. For further information about the screen capture module, see [Screen capturing](#).

Redundancy options

Overview

There are two fundamental functions in the recording system that might need redundancy:

- **Media Repository (MR) redundancy** - this can be achieved by deploying two Media Repositories in the solution
- **Recording Server (RS) redundancy** - this can be achieved by deploying more than one Recording Servers in the solution

It is important to decide an ambition level for redundancy your organization. For some organizations recording is mission critical, but downtime is acceptable on the media repository.


Redundant deployment topologies

Multiple Media Repositories and the Recording Servers can be connected to each other in the following ways:

- **Recording Servers feeding the same Media Repository**
 - this provides RS redundancy
 - this solution is managed as one system centrally from the MR servers

You need to calculate with the fact that different recording technologies provide different redundancy possibilities:

- **passive recording**
 - provides a redundancy where all recording servers that get the same traffic all can record it at the same time
 - if one of them fails the others will still have the complete call
- **central / RTP-forking based**
 - these solutions (e.g. Cisco, Avaya, IP Trade) can send only to one recorder at a time
 - they offer failover between recorders on a per call basis
 - if one fails during a call, the last part of the call will be lost, but the next call will be recorded by another server

 Redundancy scenarios can become complex if the requirements are very strict. We recommend that you contact a Verba expert to evaluate your options.

Redundant topology example

Let's look at the following example requirements and design a redundant solution based on these:

- call recording is critical for the organisation, which works in finance sector
- calls must be stored for 7 years, calls might be provided to regulators within 5 workdays
- Cisco UCM 8.5 is deployed the customer
- 200 Cisco desktop phones users and 25 IP Trade turrets are used by the customer

Based on these requirements we make the following assumptions:

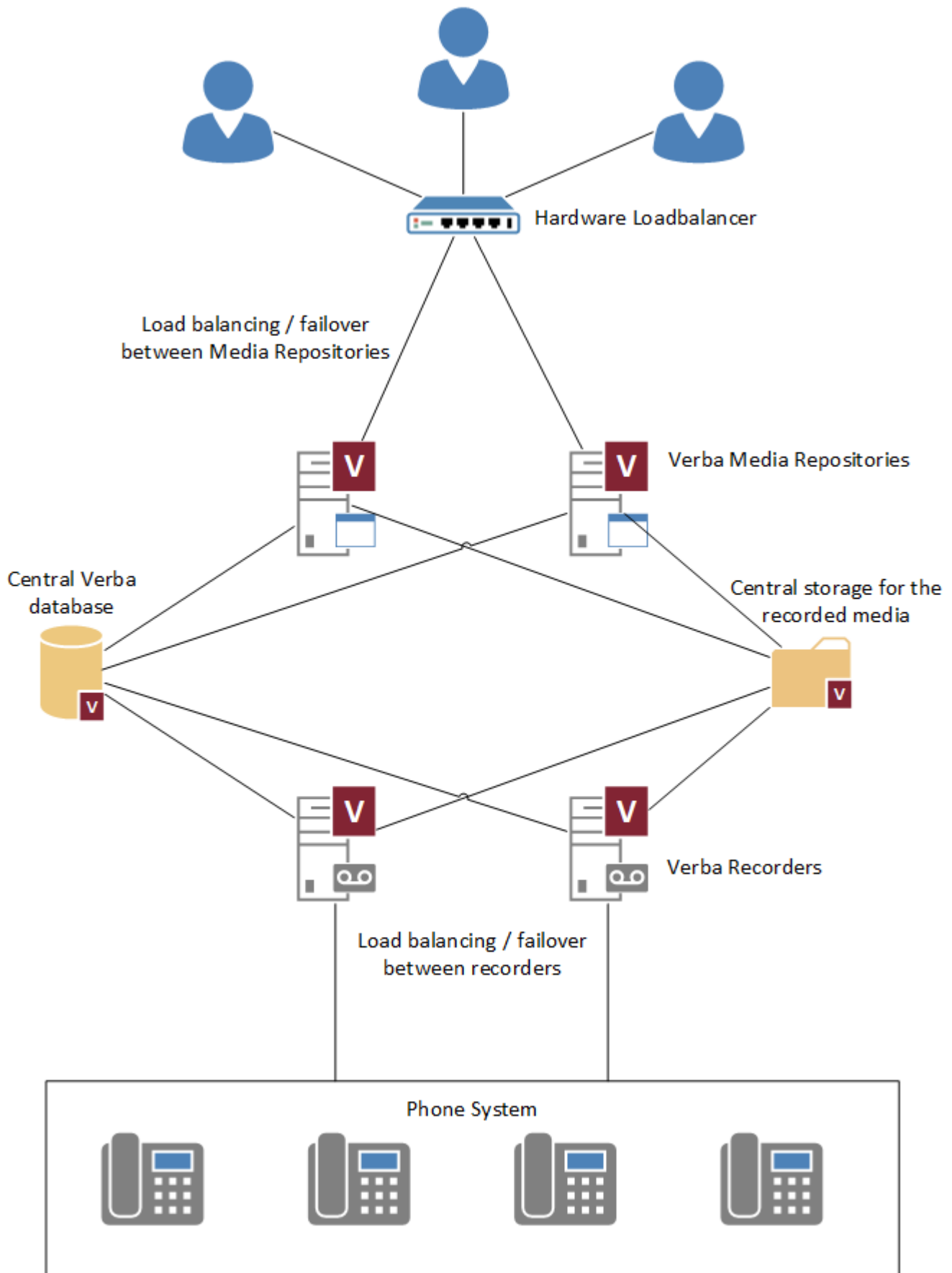
- all phones support the Cisco built-in bridge functionality (should be verified with the customer)
- multiple recording servers will be needed
- one media repository server might be enough, but long term storage is important

In this case, the following are recommended:

- use 1 Verba Media Repository server
 - virtualize the server with VMware, so it can be easily moved to other hardware when it fails (boot image might be in SAN to facilitate this)
 - mount redundant SAN volumes to the virtual server
- deploy 2 Verba Recording Servers
 - both servers can run both the Cisco and IP Trade central recording engines
 - the Cisco and IP Trade solution shall be configured with both recorders in their recording server list
 - both servers will upload to the Verba Media Repository Server (will buffer locally if the MR is not available)

Multi server architectures with load balancing and failover

In this configuration, the Verba components (Recording Server and Media Repository) are installed on separated servers and in more than one instance. Distributing and multiplicating the system components can increase system capacity and adds failover and/or load balancing capabilities. If more than one Media Repository or Recording Server is required, each server use the same central database.



Benefits

- Fully centralized solution with distributable system components.
- Very low O&M costs due to the centralized management, storage, archiving and playback.
- Extremely flexible and scalable solution to support even hundreds of servers in a single solution.
- Secure communications and data transmission among the system components using industry standards like SSL and AES.

Server sizing and requirements

This page provides information for server sizing showing detailed information about server requirements such as CPU, memory, hard disk, virtualization, operating system, etc.

Please note, that Verba does not sell server hardware, OS and database licenses.

- [Server sizing](#)
- [Server sizing for servers with co-located/mixed roles](#)
- [Desktop requirements for Verba Desktop Agent](#)
- [Desktop requirements for standard search and replay workstations](#)
- [Media Recorder sizing for voice, video, screen - application share recording](#)
- [Ethical Wall and IM Recording server requirements](#)

Server sizing

This table outlines typical server sizing and recommended hardware and software configurations:

Server Role	Recording Server (RS)	Media Repository / Application Server (MR)	Proxy Server
Server Platform	Industry standard PC servers Physical or virtual		
CPU	Intel Xeon 2.4 GHz or higher Up to 16 CPU cores or vCPUs 2 cores/vCPUs must be "reserved" for the OS, only the rest can be used for application sizing Numbers only applicable when Receive-side scaling (RSS) is enabled in the OS		
	Refer to Media Recorder sizing for voice, video, screen - application share recording When Recording Director is installed as separate servers: <ul style="list-style-type: none"> • Up to 5000 devices/endpoints (standard telephony or UC): 2 cores • Up to 1000 turrets (trader voice): 2 cores 	Up to 100 user sessions: 4 cores Up to 500 user sessions: 8 cores If SQL Server is installed on the server, additional CPU cores are required.	Skype for Business: 200 voice calls / core Cisco: 150 voice calls / core 75 video calls / core
Memory	8 GB	Up to 100 user sessions: 4 GB Up to 500 user sessions: 8 GB If SQL Server is installed on the server, additional memory is required.	4 GB
Hard disk	System partition (OS and applications): 80 GB or more Media partition: 80 GB or more, use the Storage Disk Space Calculator tool to size your hard disk capacity Always use redundant disks with RAID and have separate Media and System volumes		

Network	All server clocks must be synchronized, typically either with the domain controller or time server	
	All servers must have the latest Time Zone configuration	
	Custom time zones are not supported	
	1x Gigabit Ethernet plus 1x Gigabit Ethernet port if you use passive, port mirroring based recording	1x Gigabit Ethernet
Operating system	Microsoft Windows Server 2012 R2 Microsoft Windows Server 2016 Microsoft Windows Server 2019 Standard Edition, latest service packs installed We support the English versions of Microsoft server software	
Database	Microsoft SQL Server 2014 Microsoft SQL Server 2016 Microsoft SQL Server 2017 Microsoft SQL Server 2019 Express, Standard or Enterprise Edition, latest service packs installed Express Edition is bundled for free, recommended up to 1.000.000 calls. If the Full-Text Search feature is needed, then install SQL Server Express with Advanced Services. See SQL Server requirements for more information If you have an existing SQL Server cluster, we recommend using that for the Verba database	
Virtualization	VMware and Hyper-V are recommended, see Virtualization .	
Antivirus	Make sure your Antivirus software does not scan database, media and log folders .	
Power	Redundant Power Supply UPS recommended	

Please note the following:

- **No other apps on the server** - Verba components should be installed on dedicated servers or virtual server instances with no other applications being co-hosted on them.
- **You can contact Verba for server review** - You can contact Verba or your system integrator representative for a review before submitting orders for your server.
- **A good backup is essential** - A regular (daily) backup procedure of the Verba servers, recorded media files and database needs to be established to prevent data loss and allow disaster recovery.
- **Contact Verba for video recording planning** - For video, telepresence and agent computer screen deployments, please contact your Verba or system integrator representative.

The following documents provide additional support to size your solution:

- [Media Recorder sizing for voice, video, screen - application share recording](#)
- [Ethical Wall and IM Recording server requirements](#)

Server sizing for servers with co-located/mixed roles

The different server roles can be installed on a single server when the capacity does not exceed the limitations. When sizing the servers with co-located server roles, each role has to be sized separately and added to the overall capacity. The system allows deploying the following server roles:

Server Role	Description
Media Repository / Application Server and Recording Server (Combo)	Includes all Verba services, except the Filter services running on the Skype for Business servers
Recording Server	Includes all recording services, ethical wall capabilities, announcement
Media Repository / Application Server	Includes all central applications such as web UI, storage management, licensing, APIs, speech recognition, etc.
Media Collector and Proxy Server	Includes the media collector and proxy application
Announcement Server	Includes the announcement application
Speech Analytics Server	Includes speech recognition applications
Skype for Business Filter	Includes the applications running on the Skype For Business Front-End servers
Media Collector and Skype for Business Filter	Includes the applications running on the Skype For Business Front-End servers and the media collector and proxy application
Desktop Recorder	Includes the screen capture application running the desktop computers

A single server can have only one of the above roles.

Desktop requirements for Verba Desktop Agent

This component is installed on the PC of the agent whose screen shall be recorded during the phone calls.

Hardware and 3rd party software requirements for Verba Desktop Agent component deployment:

CPU	Intel Pentium 4 or later
Memory	4 GB
Network	10/100/1000 LAN interface card
Operating system	Microsoft Windows 7 (64 bit) Microsoft Windows 8 (64 bit) Microsoft Windows 10 (64 bit)
Display	The system can record all resolutions, color depths, multiscreen setups. The following recommendations help to dramatically lower disk space requirements of the recordings: <ul style="list-style-type: none"> • Use the minimum possible screen resolution that still fulfills software usability requirements • Use 16 bit color depth • Turn off background picture on the desktop • Use a low screen recording rate: 3 frame/sec is typically enough for a proper review

Desktop requirements for standard search and replay workstations

Hardware and 3rd party software requirements for client computers accessing the web based user interface:

Computer platform	Multimedia PC
CPU	Intel Pentium 4 or later
Memory	4 GB

Network	10/100 LAN interface card or WiFi adapter
Operating system	Microsoft Windows 7/8/10 macOS Linux
Browser	Google Chrome Microsoft Internet Explorer 11 or later Mozilla Firefox Safari Edge
Media Player	Windows Media Player 10.x or later on Windows using Internet Explorer HTML5 audio/video tag compatible browser
Display	1920x1080 resolution
Other	Sound card, speaker or headphone Monitor, keyboard, mouse

Media Recorder sizing for voice, video, screen - application share recording

- [Voice recording CPU sizing](#)
 - [Sample calculations](#)
- [Voice recording on co-located Proxy and Media Recorder server CPU sizing](#)
- [Video and Screen Share recording sizing](#)
 - [CPU sizing](#)
 - [Video recording](#)
 - [Screen Sharing recording](#)
 - [Video recording and storage devices](#)

Voice recording CPU sizing

The table below shows the supported number of simultaneous voice calls per CPU core:

- The system was tested up to 16 core servers, where 2 cores must be reserved for the OS, leaving up to 14 CPU cores for the application.
- When certain features are enabled on the Recording Servers, the capacity numbers change:
 - Encryption: when storage file encryption is enabled, capacity numbers must be decreased by 10%
 - Voice quality check: when voice quality check is enabled, capacity numbers must be decreased by 15%
- **Numbers in red** denotes default values, should be used for server sizing
- Numbers only applicable when Receive-side scaling (RSS) is enabled in the OS

Recorded Platform		Storage Codec / Network Codec		
		Silk	G.711	G.722
Skype for Business	GSM-FR (Wave)	140	250	160
	PCM (Wave)	154	275	176
	MS-ADPCM (Wave)	140	250	160
	Speex (Ogg)	92	165	106
		G.729	G.711	G.722
Cisco Network-Based Recording	GSM-FR (Wave)	120	175	113
	PCM (Wave)	132	193	124
	MS-ADPCM (Wave)	120	175	113
	Speex (Ogg)	79	116	75
		G.729	G.711 / PCM	G.722
IPTrade, IPC, Speakerbus, BT ITS ^{1 2}	GSM-FR (Wave)	207	300	195
	PCM (Wave)	228	330	215
	Speex (Ogg)	137	198	129
		G.729	G.711	G.722
Cisco Proxy and Dial-in recording, ACME Packet / Oracle, Cisco CUBE, Sonus, MetaSwitch SBCs, and other SIP/SIPREC recording	GSM-FR (Wave)	120	175	113
	PCM (Wave)	132	193	124
	MS-ADPCM (Wave)	120	175	113

	Speex (Ogg)	79	116	75
		G.729	G.711	G.722
Network port mirroring based SIP/SCCP recording	GSM-FR (Wave)	170	250	160
	PCM (Wave)	187	275	176
	MS-ADPCM (Wave)	170	250	160
	Speex (Ogg)	112	165	106
		G.729	G.711	G.722
Avaya ¹	GSM-FR (Wave)	207	300	195
	PCM (Wave)	228	330	215
	Speex (Ogg)	137	198	129

¹ Simplex stream recording, e.g recording channel mixing on turrets

² BT ITS supports PCM streams only

Sample calculations

Scenario	CPU sizing
Skype for Business recording for 1000 users	<ul style="list-style-type: none"> Skype for Business uses Silk for most call scenarios GSM-FR is the recommended storage codec To plan for the worst case, we assume 1000 simultaneous calls (duplex streams) Encryption and voice quality checks are not required CPU requirement: $1000 / 140 = 8$
Trader voice recording for 500 users	<ul style="list-style-type: none"> Trader voice platforms use G.711 simplex streams for most call scenarios GSM-FR is the recommended storage codec (recorders support VAD to filter out long silence) To plan for the worst case, we assume 4 simplex recording streams per turret (depends on the recording channel mixing configuration) Encryption and voice quality checks are both required CPU requirement: $500 \times 4 / (300 \times 0.9^* \times 0.85^{**}) = 9$ <p>* The performance multiplier of the Encryption process ** The performance multiplier of the Voice Quality Check process</p>

Voice recording on co-located Proxy and Media Recorder server CPU sizing

A standalone proxy server can handle **200 concurrent sessions per CPU core in the case of Skype for Business, and 150 in the case of Cisco**. The following table shows the sizing in the case of co-located proxy and recording services.

Recorded Platform	Storage Codec / Network Codec			
		Silk	G.711	G.722
Skype for Business	GSM-FR (Wave)	82	111	89
	PCM (Wave)	87	116	94
	MS-ADPCM (Wave)	82	111	89
	Speex (Ogg)	63	90	69

		G.729	G.711	G.722
Cisco Proxy-Based Recording	GSM-FR (Wave)	56	81	54
	PCM (Wave)	60	74	57
	MS-ADPCM (Wave)	56	70	54
	Speex (Ogg)	43	55	41

Video and Screen Share recording sizing

CPU sizing

When recording video, besides the number of recorded endpoints, the video bandwidth also has to be taken into account.

With a single CPU core, **125 Mbps** total video or screen share stream can be recorded. So with the minimum server requirements (4 cores, 2 cores considered as reserved for the OS), the system can record up to 250 Mbps video or screen share streams total.

Video recording

The bandwidth usage of the video endpoints can vary based on the device types, their configuration, and the available network bandwidth. The following table shows the bandwidths with different video resolutions when using fullscreen video call:

Video resolution and framerate	Bandwidth	
	Skype for Business	Cisco
360p @ 30 fps	300 - 800 Kbps	300 - 600 Kbps
480p @ 30 fps	400 - 1500 Kbps	600 - 800 Kbps
720p @ 30 fps	700 - 2500 Kbps	1300 - 2000 Kbps
1080p @ 30 fps	1500 - 4400 Kbps	2000 - 4000 Kbps

However, when using a smaller client window size, or the default, the video resolution changes, therefore the bandwidth as well. The following table shows the bandwidths with different client window sizes in the case of 1080p video call:

Skype for Business client window size	Average bitrate	Maximum bitrate
Default	115 Kbps	500 Kbps
Resized	600 Kbps	815 Kbps
Maximized	1730 Kbps	2770 Kbps
Full Screen	2890 Kbps	4415 Kbps

For more information, refer to the following articles:

<https://docs.microsoft.com/en-us/skypeforbusiness/plan-your-deployment/network-requirements/network-requirements>
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab12/collab12/cac.html

It is important to note, that the numbers above **have to be multiplied by two because there is always an incoming and an outgoing stream.**

Calculating with 2*2 Mbps video streams per endpoint, with a single CPU core, 31 concurrent video sessions can be recorded. Therefore, a 4-core Recording Server (2 cores considered as reserved for OS) can record 62 concurrent video sessions.

Numbers only applicable when Receive-side scaling (RSS) is enabled in the OS

Screen Sharing recording

While in the case of the Video calls the bandwidth depends on the resolution and the client window size, in the case of Screen Sharing, the bandwidth depends only on the resolution.

The following table shows the bandwidths with different resolutions, depending on the available network bandwidth:

Screen Resolution	Available network bandwidth	
	Acceptable	Optimal
1280*800	385 Kbps	1500 Kbps
1440*900	515 Kbps	2000 Kbps
1680*1050	770 Kbps	2750 Kbps
1920*1200	1000 Kbps	3500 Kbps

Acceptable bandwidth provides a decent user experience. When the optimal bandwidth is available, the screen-sharing experience will be much smoother.

Calculating with 2 Mbps screen share streams per endpoint, with a single CPU core, 62 concurrent video sessions can be recorded. Therefore, a 4-core Recording Server (2 cores considered as reserved for OS) can record 124 concurrent video sessions.

Video recording and storage devices

In the case of a high number of recorded video endpoints, the type of the storage device also has to be considered. An HDD usually has a write speed of 50-120 MB/s, while an average SSD has 200-520 MB/s, or even more in the case of high-end devices. The disk utilization for the recording shouldn't be more than 60% and the disk must provide sustained I/O performance at this rate. Numbers only applicable when Receive-side scaling (RSS) is enabled in the OS.

The following table shows some examples for maximum total video bandwidth per Recording Server:

Storage type and maximum write speed	Maximum video bandwidth at 60% disk utilization and required recorder cores	Maximum number of recorded video endpoints (calculating with 2*2,5 Mbps streams per endpoint)
HDD - 50 MB/s	240 Mbps / 2 cores	48 endpoints
HDD - 80 MB/s	384 Mbps / 4 cores	76 endpoints
HDD - 120 MB/s	576 Mbps / 5 cores	115 endpoints
SSD - 200 MB/s	960 Mbps / 8 cores	192 endpoints
SSD - 350 MB/s	1680 Mbps / 14 cores	336 endpoints

Ethical Wall and IM Recording server requirements

This page helps you to configure the server for your Verba Ethical Wall/IM Recording System. Please note, that Verba Technologies *does not sell server hardware, OS and database licenses.*

This table outlines typical server sizing and recommended hardware and software configurations:

Ethical Wall

For Cisco deployments, both the Media Repository and the Compliance (Recording) Servers are needed. For Skype for Business (Lync) deployments only the Media Repository is needed.

IM Recording

Both the Media Repository and the Compliance Servers are needed.

Server Role	Media Repository (MR)	Compliance Server (CS) (Recording Server)	Both functions on one server (combined MR and CS)
Server Platform	Any industry standard PC server		
CPU	Quad-core Intel Xeon 2.4 GHz or higher with Hyperthreading rule of thumb: <ul style="list-style-type: none"> • 100 messages per second per core, but minimum of 2 cores for Compliance Servers • 1 Media Repository needed per 500 simultaneous web user sessions, with a minimum of 2 cores • Performance is highly dependent on the actual traffic 		
Memory	8 GB	4GB	8GB
Hard disk	System disk - 80 GB or more		
Network	1x Gigabit Ethernet	1x Gigabit Ethernet (if you use a virtual server you need to dedicate a physical port to the virtual server instance - available on VMware)	
Operating system	Microsoft Windows Server 2012 R2 Microsoft Windows Server 2016 Microsoft Windows Server 2019 <i>Standard Edition, latest service packs installed</i> Important! We support the English versions of Microsoft server software!		
Database	Microsoft SQL Server 2012 Microsoft SQL Server 2014 Microsoft SQL Server 2016 Microsoft SQL Server 2017 <i>Express, Standard or Enterprise Edition, latest service packs installed</i> Express Edition is bundled for free, recommended up to 1.000.000 events See SQL Server requirements <i>If you have an existing SQL Server cluster, we recommend using that as a Verba database (in that case, 4 GB RAM is enough on the MR and MR+CS servers).</i>		
Virtualization	VMware recommended, see Virtualization . IMPORTANT! Hyper-V is currently NOT supported for passive (SPAN port-based) recorders.		

Antivirus	Make sure your Antivirus software does not scan database, media and log folders.
Power	Redundant Power Supply UPS recommended

Desktop requirements for standard search and replay workstations

Hardware and 3rd party software requirements for client computers accessing the web-based user interface:

Computer platform	Multimedia PC
CPU	Intel Pentium 4 or later
Memory	1 GB
Network	10/100 LAN interface card or WiFi adapter
Operating system	Microsoft Windows XP Microsoft Windows Vista Microsoft Windows 7 Microsoft Windows 8 Microsoft Windows 10
Browser	Microsoft Internet Explorer 8.x or later Mozilla Firefox 2.x or later Google Chrome 2.x or later
Display	1024x768 resolution or higher with 16-bit color palette
Other	Monitor, keyboard, mouse

Size your disks

- [Understanding RAID](#)
- [Storage requirements](#)

Understanding RAID

Using RAID in Verba servers is a strongly recommended option. This topic provides a brief description of each RAID levels with comments on applying them in Verba servers. Verba Media Repository and Recording Server components are different from hard disk point of view. Verba Media Repository runs the database server and the web server, which are transfer-rate-sensitive applications and the Recording Server component runs the recorder engine, which is a write intensive program. Both component require fault tolerance to provide high availability in such mission critical applications like recording. To understand the RAID requirements for Verba servers we provide a comparison for RAID levels too.

The term RAID applies to an architecture that safeguards data - if a disk fails, data is reconstructed. Data is "striped" across several disks. An extra disk is used to store parity information, which is used to reconstruct data.

This architecture ensures that users can always access the data they need at any time.

One side-effect of using RAID, of course, is that the MTBF (Mean Time Between Failure) figures for a RAID subsystem are statistically worse than if only a single drive is involved. If you have a RAID system consisting of, say, four drives and one controller, each with an MTBF of five years, one component of the subsystem will fail, on average, every twelve months. However, against this is the fact that the data held on the RAID subsystem will be safe and it only takes a couple of minutes to replace the faulty drive and for the subsystem to start rebuilding the set.

There are six different levels of RAID and each one is designed to provide greater resilience than the previous level.

RAID comparison

RAID	Advantage	Disadvantage
RAID 0	High performance. No cost penalty - all storage is available for use.	Significantly reduced data availability. No fault-tolerance
RAID 1	Excellent data availability. Higher read performance than a single disk.	Expensive - 50% waste of space. Moderately slower write performance.
RAID 2	Excellent data availability. High performance.	Expensive - requires twice the desired disk space.
RAID 3	Good data availability. High performance for transfer rate intensive applications. Cost effective - only one extra disk is required for parity.	Can satisfy only one I/O request at a time. Poor small, random I/O performance.
RAID 4	Good data availability. High performance for read operations. Cost effective - only one extra disk is required for parity.	Poor write performance. Poor small, random I/O performance.
RAID 5	Good data availability. High performance in request rate intensive applications. Cost effective - only one extra disk is required.	Poor write performance. No performance gain in data transfer rate intensive applications.

RAID configuration recommendations for Verba Recording System

We strongly recommend to use RAID 0 + 1 configurations for all Verba Recording System deployments. This RAID configuration allows to span multiple hard disks and provide mirroring capabilities. This RAID configuration has the best write performance, which is critical for the recording process.


Storage requirements

This article helps disk size dimensioning. Required storage size depends upon the **number and length of calls** and the **applied codec**.

- [Estimate your storage requirements](#)
- [Voice](#)
 - [Supported voice codecs for recording](#)
 - [Voice codecs for storage and playback](#)
 - [Stereo voice recording](#)
 - [Silence Suppression for voice recording \(Voice Activity Detection, VAD\)](#)
 - [Enabling the silence suppression \(VAD\) on the recorder service side](#)
 - [Selecting a storage codec which supports silence suppression](#)
- [Video](#)
 - [Supported video codecs for recording](#)
 - [Video codecs for storage and playback](#)
- [Screen](#)
 - [Screen codecs for storage and playback](#)

Estimate your storage requirements

You can **download the Excel [Verba Storage Calculator Sheet](#)** to estimate your storage requirements for **IM, voice, video, telepresence and screen recording** applications. It also provides you information on **database** storage sizing.

 The calculator sheet includes **Excel macros**, which might be disabled when the file is downloaded from the site. Please **Enable Editing** and **Enable Content** (to turn on macros) when Excel is asking for it, otherwise the calculator will not work.

Voice

Supported voice codecs for recording

The system supports recording of the following voice codecs:

Codec name	Sample rates
G.711 A-law, G.711 μ -law	8Khz
G.723	8Khz
G.726-16, G.726-24, G.726-32, G.726-40	8Khz
G.728	8Khz
G.729, G.729A, G.729B, G.729AB	8Khz
GSM	8Khz
iLBC	8Khz
RED	8Khz

G.722	16Khz
SILK	8Khz, 16Khz
Microsoft RTAudio (X-MSRTA)	8Khz, 16Khz
G.722.1	16Khz, 32Khz
Siren7, Siren14	16Khz, 32Khz
Speex	8Khz, 16Khz, 32Khz
Opus	8Khz, 16Khz, 48Khz
CELT	8Khz, 16Khz, 32Khz, 48Khz
L8 (PCM8)	8Khz, 16Khz, 32Khz, 48Khz
L16 (PCM16, Cisco Wideband)	8Khz, 16Khz, 32Khz, 48Khz
MP4A-LATM	48Khz
MPEG4-generic	48Khz
AAC-LD	48Khz

Voice codecs for storage and playback

The Verba system is able to store audio files in many file formats with different codecs. The sample rate of the output file depends on the sample rate of the input codec (see above).

Supported formats:

Codec for storing media	File format	Sample rate	Bandwidth	1-minute file size	1-hour file size
PCM16	wav	8Khz	128 Kbps	960 KB	56.3 MB
		16Khz	256 Kbps	1.9 MB	112.5 MB
		32Khz	512 Kbps	3.8 MB	225 MB
		48Khz	768 Kbps	5.6 MB	337.5 MB
PCM8	wav	8Khz	64 Kbps	480 KB	28.1 MB
		16Khz	128 Kbps	960 KB	56.3 MB
		32Khz	256 Kbps	1.9 MB	112.5 MB
		48Khz	384 Kbps	2.8 MB	168.8 MB
G.711 (both A and μ)	wav	8Khz	64 Kbps	480 KB	28.1 MB
		16Khz	128 Kbps	960 KB	56.3 MB
		32Khz	256 Kbps	1.9 MB	112.5 MB
		48Khz	384 Kbps	2.8 MB	168.8 MB
MSADPCM	wav	8Khz	32 Kbps	240 KB	14.1 MB
		16Khz	64 Kbps	480 KB	28.1 MB
		32Khz	128 Kbps	960 KB	56.3 MB
		48Khz	192 Kbps	1.4 MB	84.4 MB

GSM FR Most used	wav	8Khz	13,2 Kbps	99 KB	5.8 MB
Speex	ogg	8Khz	6 Kbps	45 KB	2.6 MB
		16Khz	16 Kbps	120 KB	7 MB
		32Khz	24 Kbps	180 KB	10.5 MB
High Quality Speex	ogg	8Khz	10 Kbps	75 KB	4.4 MB
		16Khz	24 Kbps	180 KB	10.5 MB
		32Khz	32 Kbps	240 KB	14.1 MB
Opus	ogg	8Khz	9 Kbps	67.5 KB	4 MB
		16Khz	18 Kbps	135 KB	7.9 MB
		24Khz	24 Kbps	180 KB	10.5 MB
		48Khz	32 Kbps	240 KB	14.1 MB
High Quality Opus	ogg	8Khz	14 Kbps	105 KB	6.2 MB
		16Khz	24 Kbps	180 KB	10.5 MB
		24Khz	32 Kbps	240 KB	14.1 MB
		48Khz	48 Kbps	360 KB	21.1 MB

In addition to the audio codecs above, the system also supports other codecs for storing voice recordings in the system. These additional audio codecs and file formats are not supported by the recorders in the system, these files are usually imported into the platform from 3rd party / legacy systems.

- WAVE container
 - G.723.1 (Mono / Stereo)
 - G.729 (Mono / Stereo)
 - G.722 (Mono / Stereo)
 - G.726 (Mono / Stereo)
- MP3
- M4A
- VOX
- AU

Stereo voice recording

With stereo recording, the caller and the callee are recorded into two separate channels; caller in the left channel and the callee in the right channel. This enables listening to the participants separately during the playback.

In the case of stereo recording mode, the recorded media file sizes have to be multiplied by two. There are two exceptions:

- GSM FR does not support stereo recording
- In the case of Speex codec, the multiplier is only 1.2X

Silence Suppression for voice recording (Voice Activity Detection, VAD)

The size of the recorded media files can be reduced by enabling the silence suppression. This is achieved by not writing data to disk when there is only silence in the voice calls. In this case, the size of the recorded media will depend on how much silence there is in the call, but the **average reduction in the file size is 25%**.

Silence suppression can be enabled in two ways:

Enabling the silence suppression (VAD) on the recorder service side

Verba supports silence suppression in the recording service. This is not available in the case of Skype for Business or passive recording. The VAD settings can be found under the **Unified Call Recorder \ Media Recorder \ Media Splitting** node in the server configuration.

Selecting a storage codec which supports silence suppression

There are several codecs which natively support silence suppression. This enables the size reduction of the recorded media files regardless of the recorded platform. The list of these codecs is the following:

- Speex with silence suppression
- High Quality Speex with silence suppression
- Opus with silence suppression
- High Quality Opus with silence suppression

Video

Supported video codecs for recording

The system supports the recording of the following video codecs:

- H.261
- H.263
- H.263+
- H.263++
- H.264
- H.264 SVC
- VP8

Video codecs for storage and playback

The system records the video stream into a proprietary file format (Verba Media Format -VMF) which includes the raw audio and video network streams. When video recording is enabled for a user, the system only creates a single recording which includes both audio and video. The size of the VMF file depends on the original network streams captured during recording.

The system offers transcoding for the VMF files which can be configured as a data management policy or manually invoked from the Player /Viewer. In both cases, a target file format has to be selected from the available options. The system currently supports the following file formats, audio and video codecs, resolutions and bandwidth (which defines the quality of the video for the target resolution, it also defines the size of the output file):

- MPEG-4 (AAC + H.264), High Definition 1280x720 48KHz Stereo, 1564 kbit/sec
- Windows Media, Mobile Device 320x240 16KHz Stereo, 256 kbit/sec
- Windows Media, Mobile Device 320x240 16KHz Stereo, 384 kbit/sec
- Windows Media, Mobile Device 320x240 16KHz Stereo, 512 kbit/sec
- Windows Media, Internet 640x480 16KHz Stereo, 384 kbit/sec
- Windows Media, Internet 640x480 16KHz Stereo, 512 kbit/sec
- Windows Media, Internet 640x480 16KHz Stereo, 768 kbit/sec
- Windows Media, High Definition 1280x720 48KHz Stereo, 1024 kbit/sec
- Windows Media, High Definition 1280x720 48KHz Stereo, 1512 kbit/sec
- Windows Media, High Definition 1280x720 48KHz Stereo, 2096 kbit/sec
- Windows Media, Full High Definition 1920x1080 48KHz Stereo, 1512 kbit/sec
- Windows Media, Full High Definition 1920x1080 48KHz Stereo, 2096 kbit/sec
- Windows Media, Full High Definition 1920x1080 48KHz Stereo, 3192 kbit/sec
- MPEG-4 (AAC + H.264), Low Definition 176x144 16KHz Mono, 60 kbit/sec
- MPEG-4 (AAC + H.264), Low Definition 176x144 16KHz Mono, 80 kbit/sec
- MPEG-4 (AAC + H.264), Low Definition 176x144 16KHz Mono, 100 kbit/sec

- MPEG-4 (AAC + H.264), Standard Definition 480x360 48KHz Stereo, 448 kbit/sec
- MPEG-4 (AAC + H.264), Standard Definition 480x360 48KHz Stereo, 628 kbit/sec
- MPEG-4 (AAC + H.264), Standard Definition 480x360 48KHz Stereo, 896 kbit/sec
- MPEG-4 (AAC + H.264), High Definition 1280x720 48KHz Stereo, 2128 kbit/sec
- MPEG-4 (AAC + H.264), High Definition 1280x720 48KHz Stereo, 2692 kbit/sec

Screen

Screen codecs for storage and playback

The system stores screen recordings in a proprietary file format (Verba Media Format -VMF) which includes the desktop screen content in the selected format. The screen captures are automatically multiplexed with the corresponding voice recordings which result in new, updated VMF files which include the recorded audio streams and the screen capture.

All numbers below are given per minute, using 4 frames/ second recording. These shall be used as guidelines, they can not represent exact storage requirements. Storage requirements are strongly effected by screen capture rate (saved frames per second), screen resolution, color depth and amount of changes on the screen during recording.

Compressing algorithm		Average business app Data entry forms (few changes on screen)	Multiple applications (window switching) Application with window scrolling (browser) (many changes on screen)
Verba Screen Codec	1024x768 32bit color	0.1-0.3 Mbyte/min	0.5-1.5 Mbyte/min
Verba Screen Codec	1280x1024 32bit color	0.2-0.6 Mbyte/min	0.8-5 Mbyte/min
Windows Media Screen Codec	Constant bitrates are selectable between 768 kbps - 2 mbps (5-15 Mbyte/min)		

The system can record all resolutions, color depths, multiscreen setups, but the following recommendations help to dramatically lower disk space requirements of the recordings:

- Use the minimum possible screen resolution that still fulfills the usability requirements
- Use lower bit color depths
- Turn off background picture on the desktop

The system offers transcoding for the VMF files which can be configured as a data management policy or manually invoked from the Player /Viewer. In both cases, a target file format has to be selected from the available options. The system currently supports the following file formats, video codecs, resolutions and bandwidth/quality:

- MPEG-4 (H.264), Medium Quality, 512 kbit/sec
- Windows Media, Low Quality, 512 kbit/sec
- Windows Media, Medium Quality, 1024 kbit/sec
- Windows Media, High Quality, 1512 kbit/sec
- Windows Media, Ultra Hight Quality, 2048 kbit/sec
- MPEG-4 (H.264), Low Quality, 384 kbit/sec
- MPEG-4 (H.264), High Quality, 768 kbit/sec
- MPEG-4 (H.264), Ultra High Quality, 1024 kbit/sec
- Verba Screen Format, Low Quality
- Verba Screen Format, Medium Quality
- Verba Screen Format, High Quality
- Verba Screen Format, Ultra High Quality

SQL Server requirements

- [SQL Server editions](#)
- [Scalability](#)
- [Resiliency](#)
- [Database memory and storage requirements](#)
- [SQL Server authentication and permissions](#)
 - [Additional permissions for SQL Server Standard or Enterprise Edition](#)
- [SQL Server services](#)
- [Language, collation, and case sensitivity](#)
- [Azure SQL Requirements and Limitations](#)

SQL Server editions

The system uses a standard Microsoft SQL Server database to store the system configuration parameters for each server and the conversation metadata (CDR) for each conversation.

We recommend reviewing this topic and selecting your SQL Server edition based on your requirements.

For more information on the differences between the SQL Server editions, see <https://docs.microsoft.com/en-us/sql/sql-server/editions-and-components-of-sql-server-2017>

Supported SQL Server versions:

- SQL Server 2014
- SQL Server 2016
- SQL Server 2017
- SQL Server 2019
- Azure SQL Database
- Azure SQL Managed Instance

Scalability

Conversations stored in the system at any moment	Recommended SQL Server edition
less than 1,000,000 conversations and instant messages	Express Edition
more than 1,000,000 conversations and instant messages	Standard or Enterprise Edition In very large deployments, partitioning has to be enabled, which is only available in Enterprise Editions or Standard Edition of SQL Server 2016 SP1 or later For more information, see Database table partitioning

If you have configured [Data management policies](#) in your system that automatically remove calls, you can plan for the maximum amount of calls that you store in the system at any moment, and not the total amount of conversations you have recorded.

Resiliency

Different SQL Server editions, support different resiliency features. Choose the editions, which is most suitable for the resiliency requirements of the deployment. For highly available deployments, we recommend using Always On availability groups which are available in Enterprise and Standard (basic version) editions only.

Feature	Enterprise	Standard	Express
Database mirroring	Yes	Yes Full safety only	Witness only
Always On failover cluster instances	Yes The number of nodes is the operating system's maximum	Yes Support for 2 nodes	No
Always On availability groups	Yes Up to 8 secondary replicas, including 2 synchronous secondary replicas	Yes, basic only Requires SQL Server 2016 or later	No

Database memory and storage requirements

You can download the Excel [Verba Storage Calculator Sheet](#) to estimate your storage and database sizing requirements.

If the database is running on a Verba server, then please make sure that it is not allocating too much memory for itself, decreasing the performance of other components on the machine.

It is strongly recommended that you leave at least half of the RAM free for use by other Verba components.

For instructions on how to do this, please refer to <https://msdn.microsoft.com/en-us/library/ms178067.aspx>

SQL Server authentication and permissions

The system supports both SQL Server Authentication and Windows Authentication for SQL Server connections. Using Windows Authentication, the system relies on the Windows service logon credentials for authentication with the SQL Server. The Verba system requires the following SQL Server roles configured for the Windows service user account:

SQL Server role	Description
dbcreator	It is a database server level role and is required only during the installation to create the <i>verba</i> database. If you would like to avoid granting this database server level role to the user, you can create the <i>verba</i> database first and then proceed with the installation.
db_owner	It is a <i>verba</i> database level role and required for the system for normal operation.
sysadmin	Either sysadmin or the permissions described in the Additional permissions for SQL Server Standard or Enterprise Edition section is required to install the SQL Server Agent Job

For more information on SQL Server server and database level roles, see <https://msdn.microsoft.com/en-us/library/ms188659.aspx> and <https://msdn.microsoft.com/en-us/library/ms189121.aspx>.

For general information on SQL Server principals, see <https://msdn.microsoft.com/en-us/library/ms181127.aspx>

Additional permissions for SQL Server Standard or Enterprise Edition

When SQL Server Standard or Enterprise Edition is being used (usually in the case of larger systems), the Verba installer also tries to install a SQL Server Agent job. For this, several additional user permissions are required.

First of all, in order to check if the SQL Server Agent service is running on the SQL server and for storing historical index usage for optimal maintenance, the user needs the **View Server State** permission for the SQL server.

To query the maintenance jobs, the **SELECT** permission on the **msdb.dbo.sysjobs** and **msdb.dbo.sysjobs_view** has to be granted to the user.

For the job installation itself, the **EXECUTE** permission for the **msdb.dbo.sp_add_job**, **msdb.dbo.sp_add_jobstep**, **msdb.dbo.sp_update_job**, **msdb.dbo.sp_add_jobschedule**, and the **msdb.dbo.sp_add_jobserver** stored procedures have to be granted for the user.

The permissions for the SQL user can be granted with the following script. Please run the script as-is, only modify the two parameters (@login and @db_name) at the top:

[SQL-Server-requirements-Additional-Permissions.sql](#)

SQL Server services

For the Verba system, the following SQL Server services must be enabled and running (other services are not required):

- SQL Server
- SQL Server Browser if named instances are used
- SQL Server Agent to run the maintenance jobs (not available on Express Edition and Azure SQL Database)

Language, collation, and case sensitivity

The user account, configured in Verba to access the database (SQL Server user or domain user) must have the **Default Language** configured to **English**. For more information on creating a login and configuring the default language, see <https://docs.microsoft.com/en-us/sql/relational-databases/security/authentication-access/create-a-login>

The system supports any collation with the following requirements:

- The system does not support Case Sensitive (CS) databases, nor servers, the collation has to be Case Insensitive (CI) and the Server has to be Case Insensitive (CI) too.
- Other collation configuration options can be specified according to the specific requirements

For more information on collation, see <https://docs.microsoft.com/en-us/sql/relational-databases/collations/collation-and-unicode-support>

Azure SQL Requirements and Limitations

	Azure SQL Database	Azure SQL Managed Instance
Authentication	Only SQL Server authentication is supported	Only SQL Server authentication is supported
SQL Agent Job	Not supported, jobs will be executed by the web application	Supported
Linked Server	Not supported	Supported
Max database size	https://learn.microsoft.com/en-us/azure/azure-sql/database/resource-limits-vcore-single-databases?view=azuresql	Up to currently available instance storage size (depending on the number of vCores).

		https://learn.microsoft.com/en-us/azure/azure-sql/managed-instance/resource-limits?view=azuresql
Max tempdb size	https://learn.microsoft.com/en-us/azure/azure-sql/database/resource-limits-vcore-single-databases?view=azuresql	General Purpose: Limited to 24 GB/vCore Business Critical: Up to currently available instance storage size https://learn.microsoft.com/en-us/azure/azure-sql/managed-instance/resource-limits?view=azuresql

Network requirements

This article summarizes the general network requirements for the system. Several integrations have specific requirements set by the corresponding vendor. These requirements can be found in the documentation of the respective vendors.

Parameter	Recommended maximum value	Description
General Network Latency	250ms	Round trip latency for common TCP based protocols such as signaling, CTI, communication protocols between internal components
Recorded Media Latency	500ms	One way latency for RTP based media delivery. For trader voice integration where the media records are triggered by voice activity, it is recommended to minimize the delay to keep the CTI/CDR events in sync.
Recorded Media Jitter	250ms	Jitter represents the variation in latency which is compensated by the buffers in the recorder. High jitter can cause packet and data loss due to de-jitter buffer overflow.
Media Packet Loss	<0.1%	Some packet loss can be tolerated in case of audio but can cause significant data loss for video streams if keyframes are lost.
Relayed Media Latency	150ms	One way latency for proxied RTP media streams
Relayed Media Jitter	30ms	Jitter represents the variation in latency which has to be low for media streams relayed by the proxy server.

IPv6 support

The Verba system supports IPv4, IPv6 and mixed IPv4 + IPv6 environments. This page summarizes the supported features and limitations for IPv6.

Features support matrix

	IPv4	IPv6	IPv4+IPv6
Accessing web UI	Yes	Yes	Yes
Central configuration	Yes	Yes	Yes
Search, call retrieval and playback	Yes	Yes	Yes
Reporting	Yes	Yes	Yes
PC-based silent monitoring	Yes	Yes	Yes
Phone-based silent monitoring	Yes	Yes	No
Desktop agent - screen recording	Yes	Yes	Yes
Desktop agent - call muting	Yes	Yes	Yes
Cisco Announcement	Yes	Yes	Yes
Cisco ViQ/VoH	Yes	Yes	Yes
Skype For Business Announcement	Yes	No	No

Recording integration support matrix

	IPv4	IPv6	IPv4+IPv6
Skype for Business	Yes	No	No
SPAN based Passive Recording	Yes	No	No
SIP Proxy-based Recording	Yes	No	No
Dial-in Recording and Playback (Verba IVR Portal)	Yes	Yes	No
Dial-in Recording	Yes	Yes	Yes
Cisco Network Based	Yes	Yes	Yes
Cisco CUBE DP forking	Yes	No	No
Cisco Gateway Recording (XCC)	Yes	No	No
Avaya DMCC/MR	Yes	No	No
ACME SIPREC	Yes	Yes	Yes

BroadSoft SIPREC	Yes	Yes	Yes
Metaswitch Perimeta SIPREC	Yes	Yes	Yes
Generic SIPREC	Yes	Yes	Yes
Tango Networks	Yes	Yes	Yes
Truphone	Yes	Yes	Yes
Symphony	Yes	Yes	Yes
Huawei UC	Yes	Yes	Yes
Zenitel AlphaCom	Yes	Yes	Yes
BT ITS	Yes	No	No
BT IP Trade	Yes	No	No
Speakerbus	Yes	No	No
IPC Unigy	Yes	No	No
Bosch Telex	Yes	Yes	No
Generic RTP (Radio)	Yes	Yes	No
SMS (SMPP)	Yes	Yes	Yes

Storage integration support matrix

	IPv4	IPv6	IPv4+IPv6
Amazon S3	Yes	No	No
Microsoft Azure Storage	Yes	No	No
Bloomberg Vault	Yes	No	No
EMC Centera	Yes	No	No
CyberTwice eRecorder HD	Yes	Yes	Yes
Exchange Web Services (EWS)	Yes	Yes	Yes
External Verba Media Repository	Yes	Yes	Yes
Hitachi Content Platform	Yes	Yes	Yes
Network Storage	Yes	Yes	Yes
Amazon S3 Compatible Storage	Yes	No	No
SFTP	Yes	No	No
Smash	Yes	Yes	Yes

EMC Isilon SmartLock	Yes	Yes	Yes
SMTP	Yes	Yes	Yes
NetApp SnapLock	Yes	No	No
IBM Tivoli Storage Manager	Yes	No	No
Actiance Vantage	Yes	No	No
Verint	Yes	No	No

Import source integration support matrix

	IPv4	IPv6	IPv4+IPv6
Centile	Yes	Yes	Yes
Cisco MediaSense	Yes	No	No
Cloud9	Yes	Yes	Yes
RingCentral	Yes	Yes	Yes
CyberTwice eRecorder HD	Yes	Yes	Yes
Verba REST API	Yes	Yes	Yes
Cisco Spark	Yes	No	No
Bloomberg IM	Yes	No	No
Verint	Yes	No	No

Virtualization

All Verba server roles can be virtualized. Most of the customer deployments are using virtualization today. The guidelines in the [Server sizing and requirements](#) article are based on virtualized environments.

Certain Verba server roles run real-time media applications, and as such requires low-latency access to resources to perform according to specification and to sizing guidelines. This document provides an overview of the recommendations for provisioning the servers in a virtualized environment. Failure to follow the configuration recommendations provided can result in the loss of recording, application functionality, and data loss.

Tested and verified hypervisors

Verba server roles are tested and verified on the following virtualization platforms:

- [VMware ESXi](#)
- [Microsoft Hyper-V](#)

The system can be deployed on Cisco UC servers and Cisco ISR gateways as well. Both platforms use VMware vSphere for virtualization:

- [Co-residency with virtualized Cisco UC applications](#)
- [Co-residency on Cisco SRE modules](#)

Other hypervisors

The system can be virtualized on other platforms as well, but Verba does not certify or test other platforms besides the ones mentioned above. It is the responsibility of the partner or the customer to verify interoperability on other platforms. It is highly recommended to read all the recommendations for the supported virtualization platforms and apply the same recommendations when applicable. Customers have already deployed Verba on:

- Nutanix AVH (KVM based hypervisor)
- Amazon EC2 (Xen based hypervisor)
- Azure Hypervisor.

VMware

Certain Verba server roles run real-time media applications, and as such requires low-latency access to resources to perform according to specification and to sizing guidelines. This document provides an overview of the recommendations for provisioning the servers in a VMware environment. Failure to follow the configuration recommendations provided can result in the loss of recording, application functionality, and data loss.

Version support

Supported virtualization environments for the server-side are listed.

- VMware ESXi 6.x/7.x

Recommendations

The following table lists the recommendations for VMware deployments for the specific server roles:

	Recommendation	Applicable Server Roles
Memory	Set 100% memory reservation. Reserving physical RAM on the VM guest prevents memory ballooning from occurring. If memory ballooning does occur, due to insufficient physical RAM, delays and recording loss can occur due to memory swapping.	Recording Server Media Collector and Proxy Server Announcement Server
	Set with the appropriate size in GBs (according to server role)	All
CPU	Reserve 100% of the CPU, which guarantees exclusive pCPU access, which in turn helps to reduce vCPU halt/wake-up cost	Recording Server Media Collector and Proxy Server Announcement Server
	Do not over-provision pCPUs, because it can lead to performance impacts because of additional sharing of last-level cache (LLC) and reduces the performance of latency-sensitive VMs that use virtual NICs (vNICs) for network I/O	Recording Server Media Collector and Proxy Server Announcement Server
	Configure the appropriate number of vCPUs (defined in the sizing guide according to server role)	All
	The physical host must have extra processing available for scheduling, network handling, device interrupt handling, and other related tasks. To prevent any loss of recording, do not over-commit the CPUs on a host. The equivalent of one physical CPU core must be available to handle these tasks.	All

Disk	Disk subsystem should be correctly sized based on the required capacity and performance	Recording Server
Network	Enable promiscuous mode on the virtual interface when network port mirroring (passive) recording is used	Recording Server Media Collector and Proxy Server
	<p>The VMXNET3 driver should be used for any NICs that are being used for recording unless the NIC is configured as a pass-through mechanism (such as SR-IOV) to bypass the network virtualization layer, in which case the native driver is required.</p> <p>Enable Receive Side Scaling (RSS) for high-performance network settings. Network driver configuration settings:</p> <ul style="list-style-type: none"> • Large Rx buffers: 8192 Byte (max) • Max Tx queues: 8 (max) • Maximum number of RSS processors: 8 (max) • Receive Side Scaling: enabled • RSS base processor number: not preset (default) • Rx ring #1 size: 4096 Byte • Rx ring #2 size: 4096 Byte • Small Rx buffers: 8096 Byte • Tx ring size: 4096 Byte • Wake on magic packet: disabled • Wake on pattern match: disabled 	Recording Server Media Collector and Proxy Server Announcement Server
	<p>Recorder servers perform real-time processing, making them latency-sensitive. VMware recommends the use of its latency-sensitivity features in such an environment to virtualize the Recorder and associated applications:</p> <ul style="list-style-type: none"> • To bypass the network virtualization layer, if the hardware supports it, use a passthrough mechanism such as SR-IOV • To avoid contention for network bandwidth in high capacity environments, consider using a separate physical NIC (pNIC) for latency-sensitive VMs • If you do not use a passthrough mechanism and there is contention for network bandwidth, use Network I/O Control (NetIOC) 	Recording Server Media Collector and Proxy Server Announcement Server
Other	Install the VMWare Tools application on the VM guest machines	All
	Make all power management unavailable in both the Basic Input/Output System (BIOS) and vSphere.	All
	Do not use snapshotting in business hours, because snapshotting causes the VM host to pause execution on virtual machines. Sometimes, all virtual machines on the host are paused. Use of snapshotting during business hours can result in recording loss.	Recording Server Media Collector and Proxy Server Announcement Server

<p>Do not use High Availability (HA), vMotion, and Distributed Resource Scheduler (DRS) in business hours, because these features cause the VM host to pause execution on virtual machines. Sometimes, all virtual machines on the host are paused. Use of these features can result in recording loss.</p>	<p>Recording Server</p> <p>Media Collector and Proxy Server</p> <p>Announcement Server</p>
---	--

If the required CPU and memory resources are not available for the VMs, problems will manifest during high-stress periods. During high-stress periods, use of system resources in real-time rapidly increases. Reserving the required resources ensures the integrity of the system and its performance at the stated level in all conditions. When reservations are not set correctly, the following problems can occur:

- Excessive packet drops can lead to data loss
- Shared memory and memory ballooning can cause recording loss because memory is used by other virtual machines and is not instantly available
- Shared CPUs can cause recording and packet loss when sudden surges of network activity require more processing power
- Incorrectly sized disk subsystems cause recording loss when shared by multiple applications.

Additional information

The following documents from VMware discuss how to virtualize latency-sensitive applications:

- <http://www.vmware.com/files/pdf/techpaper/VMW-Tuning-Latency-Sensitive-Workloads.pdf>
- <http://www.vmware.com/files/pdf/techpaper/latency-sensitive-perf-vsphere55.pdf>
- <https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/vsphere-esxi-vcenter-server-67-performance-best-practices.pdf>

Microsoft Hyper-V

Certain Verba server roles run real-time media applications, and as such requires low-latency access to resources to perform according to specification and to sizing guidelines. This document provides an overview of the recommendations for provisioning the servers in a Hyper-V environment. Failure to follow the configuration recommendations provided can result in the loss of recording, application functionality, and data loss.

Version support

Supported virtualization environments for the server-side are listed.

- Windows Server 2012 R2 Hyper-V
- Windows Server 2016 Hyper-V
- Windows Server 2019 Hyper-V

Recommendations

The following table lists the recommendations for Hyper-V deployments for the specific server roles:

	Recommendation	Applicable Server Roles
Memory	Set 100% memory reservation. Reserving physical RAM on the VM guest prevents memory ballooning from occurring. If memory ballooning does occur, due to insufficient physical RAM, delays and recording loss can occur due to memory swapping.	Recording Server Media Collector and Proxy Server Announcement Server
	Set with the appropriate size in GBs (defined in the sizing guide according to server role)	All
CPU	Reserve 100% of the CPU, which guarantees exclusive pCPU access, which in turn helps to reduce vCPU halt/wake-up cost	Recording Server Media Collector and Proxy Server Announcement Server
	Configure the appropriate number of vCPUs (defined in the sizing guide according to server role)	All
	The physical host must have extra processing available for scheduling, network handling, device interrupt handling, and other related tasks. To prevent any loss of recording, do not over-commit the CPUs on a host. The equivalent of two physical CPU core must be available to handle these tasks.	All
Disk	Disk subsystem should be correctly sized based on the required capacity and performance	Recording Server

Network	Enable promiscuous mode on the virtual interface when network port mirroring (passive) recording is used	Recording Server Media Collector and Proxy Server
	<p>Enable Receiver Side Scaling (RSS) for high-performance network settings. Network driver configuration settings:</p> <ul style="list-style-type: none"> • Maximum number of RSS processors: number of cores • Maximum number of RSS queues: number of cores • Receive Side Scaling: enabled • Receive buffer size: 32 Mbyte • Send buffer size: 32 Mbyte 	Recording Server Media Collector and Proxy Server Announcement Server
Other	Do not use snapshotting in business hours, because snapshotting causes the VM host to pause execution on virtual machines. Sometimes, all virtual machines on the host are paused. Use of snapshotting during business hours can result in recording loss.	Recording Server Media Collector and Proxy Server Announcement Server

If the required CPU and memory resources are not available for the VMs, problems will manifest during high-stress periods. During high-stress periods, use of system resources in real-time rapidly increases. Reserving the required resources ensures the integrity of the system and its performance at the stated level in all conditions. When reservations are not set correctly, the following problems can occur:

- Excessive packet drops can lead to data loss
- Shared memory and memory ballooning can cause recording loss because memory is used by other virtual machines and is not instantly available
- Shared CPUs can cause recording and packet loss when sudden surges of network activity require more processing power
- Incorrectly sized disk subsystems cause recording loss when shared by multiple applications.

Additional information

The following documents from Microsoft discuss how to plan and optimize Hyper-V:

- <https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/plan/plan-hyper-v-scalability-in-windows-server>
- <https://docs.microsoft.com/en-us/windows-server/administration/performance-tuning/role/hyper-v-server/>

Co-residency with virtualized Cisco UC applications

Cisco provides support for co-residency of UC virtual machines with Cisco non-UC virtual machines and/or 3rd-party application virtual machines, including Verba Recording System, for select applications and versions. There are various limitations, which may apply, so please see official support policy at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/collaboration-virtualization-sizing.html. This page has also added diagrams and explanatory text to clarify common FAQ from partners, customers, and Cisco field.

In addition to Cisco Unified Communications (UC) applications sold with Cisco Business Edition 6000 / 7000, Cisco now allows the installation of a broader range of Cisco and third-party virtualized applications on the servers.

This means virtualized third-party UC applications, including Verba, that are included in the Cisco Developer Network, Marketplace Solutions Catalog for Collaboration.

Key rules to consider:

- The degree of co-residency support varies by UC app/version - check the matrices and use the most restrictive policy for a given app mix: https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/collaboration-virtualization-sizing.html
- Verba virtual machines are allowed on Cisco Business Edition 6000 / 7000. For more information refer to the following article: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/BE6000/Coresidency/10-x/BE6K_coRes.html
- For Cisco TAC to effectively provide support, customers may be asked to do tasks described in this Cisco TAC Technote. Do not deploy Verba in a co-resident way if this is an issue. http://www.cisco.com/en/US/products/ps6884/products_tech_note09186a0080bbd913.shtml
- If Verba virtual machines will be co-resident, there are new rules imposed on both the UC VMs and on the Verba VMs.

Co-residency on Cisco SRE modules

SRE-V overview

Cisco Services Ready Engine (SRE) Service Module offer a branch-office infrastructure platform that adds computing resources to the **Generation 2 of the Cisco Integrated Services Router (ISR G2)** product line.

Cisco SRE-V enables the **VMware vSphere Hypervisor** to be provisioned on a Cisco SRE modules and host one or multiple virtual machines running **Microsoft Windows Server or Linux**.

Verba deployed on SRE-V

Using SRE-V you can install and **run Verba directly on your routers** (Cisco ISR-G2).

This enables the following architecture options:

- **local, standalone recording system deployed on a router** - in small firms you can run Verba Media Repository (MR) and Verba Recording Server (RS) at the same time (even in one virtual machine) on the router as the SRE modules include a RAID-based disk layer where calls can be archived
- **satellite recorder of a centralized recording system deployed on a router** - in branch office deployments you can run a Verba RS server, in order to move the network sensitive real-time recording function close to your phones and/or local gateway(s) in the branch, while deploying the Verba MR in a centralized location

The Verba RS can record using all Verba supported Cisco recording methods, including BiB forking and gateway recording methods.

Silent Monitoring

Overview


Verba Recording System provides silent monitoring capabilities seamlessly for contact center supervisors or for other administrators. Depending on the privilege settings, users can list the ongoing calls and activate the silent monitoring function, directly from the web-based user interface.

The silent monitoring feature is available as a standard built-in function, it does not require any special licenses. The advanced monitoring architectures provide a robust solution with extremely low latency during the monitoring.

Silent Monitoring Modes

Web-Based Silent Monitoring

The Verba Web Interface allows the monitoring of the voice and IM conversations once the recording is configured. For the voice monitoring, the **Verba Media Codec** has to be installed on the monitoring client PC, and it's only available in **Internet Explorer**.

 The audio driver of some terminal server solutions (ex: Citrix) may interfere with the Verba Media Codec. In cases like that the recommended solution for voice monitoring is either the Cisco Central Silent Monitoring or the Verba Phone-Based Silent Monitoring.

Cisco Central Silent Monitoring

The Cisco Central Silent Monitoring relies on the RTP forking capability of the Cisco endpoints and uses the Cisco Java Telephony API (JTAPI) interface. It also provides whisper coaching functionality. Besides the Verba Web Interface, it's also available through the [Verba phone service](#). For the list of the compatible phone devices, see: [Central Cisco silent monitoring with RTP forking](#)

For the configuration, see: [Configuring Central Silent Monitoring and Whisper Coaching](#)

Verba Phone-Based Silent Monitoring

The Verba Phone-Based Silent monitoring can be used similar way as the Cisco Central Silent Monitoring, except that it relies on the recording solution. Because of that, it's available for most of the phone systems. The only requirement is setting up a SIP connection with the Verba Recording Server.

For the configuration see: [Configuring Phone-based Silent Monitoring](#)

Desktop Screen Monitoring

With the Verba Desktop Agent, it's possible to monitor the screens of the endpoints nearly real-time (1 FPS). The Agent View allows monitoring up to 25 desktop screens simultaneously with 1 frame per 5 seconds.

	Web-Based Silent Monitoring	Cisco Central Silent Monitoring	Verba Phone-Based Silent Monitoring	Desktop Screen Monitoring
--	-----------------------------	---------------------------------	-------------------------------------	---------------------------

Silent monitoring through the web interface	YES			YES
Silent monitoring through phone		YES	YES	
PBX side configuration required		YES	YES	
Verba Media Codec required	YES			
Verba Desktop Agent required				YES
Available platforms	ALL *	CISCO ONLY	ALL *	ALL
Recording required	YES		YES	
Available in Agent View	YES			YES

* Except for Dial-in or analog recording.

Data models

- [Overview](#)
- [Standard data model](#)
- [Advanced data model for voice / trader voice data model](#)
- [Advanced data model for instant messaging](#)

Overview

The system stores data in different models depending on the type of data. This approach ensures that the data is stored in an optimized fashion to lower infrastructure costs and offer a good user experience. The system offers the following data models:

Data Model	Description	Integrations	Modalities	Availability
Standard	A single conversation entry (CDR) in the database is linked to a single media file (1-to-1 relationship), suitable for normal phone calls, instant messages, files, etc.	All except the ones listed under advanced data models	All	Any
Advanced for Voice or Trader Voice	Conversation entries (CDRs) in the database can be linked to multiple media files (Many-to-Many relationships), suitable for trader voice recordings	BT IPTrade BT ITS IPC Unigy Speakerbus Cloud9 Call Data API Genesys Active Recording	Voice	9.4 or later
Advanced for Instant Messages	Conversation entries (CDRs) in the database can be linked to multiple media records and chat messages (Many-to-Many relationships), suitable for modern instant message platforms	Microsoft Teams	Instant Message and Attachments	9.6 or later

Standard data model

In the standard data model, the system stores a single record in the database which represents the recorded conversation, and there is a single media file recorded for the session.

The standard data model is suitable for most integrations where the communication record can reference the recorded conversation in its entirety and a single media file is created to store the media.

Advanced data model for voice / trader voice data model

The advanced data model was created to support an optimized storage model for trader voice recordings. This model allows Many-to-Many relations between CDR entries and media files by differentiating 2 types of records in the database:

- CDR-only: CDR-only records contain CDR information and reference to one or more Media-only records
- Media-only: One media-only record is shared across multiple CDR-only records (e.g. channel mixing, BT IPTrade TPO recording)



This data model allows storing a single copy of the media in the case of mixed recording channels for turret based recording or BT IPTrade TPO based recording where multiple calls/sessions are referencing a single media entry. The Media-Only records are generated based on voice activity (VOX) for most trader voice integrations. It means that the recorder service creates a Media-Only record in the database (and related media file on the disk) whenever voice activity is detected in the recorded streams. Separately, CDR-Only records are created based on the available CTI/metadata information. The 2 record types are linked in the database, creating a many-to-many relationship. Since normally only CDR-Only records have the complete metadata, the system hides the Media-Only records by default during search and playback (display of Media-Only records can be enabled). Media-Only records are basically technical records representing an optimized storage model. When a user plays back or downloads a CDR-Only record, the system automatically looks for related Media-Only records in the database, downloads the media files from storage and creates a single audio file matching the time interval of the CDR-Only record. This process is called stitching.

This data model only supports voice recordings, video and screen modalities are not supported due to the complex media processing during playback.

The trader voice data model is enabled by the default for the supported integrations. If the trader voice-specific data model is disabled (not recommended), the system will use the standard data model for trader voice recordings. In the case of open lines in a mixed recording channel, it means that each CDR will have a separate media file entry containing the same data.

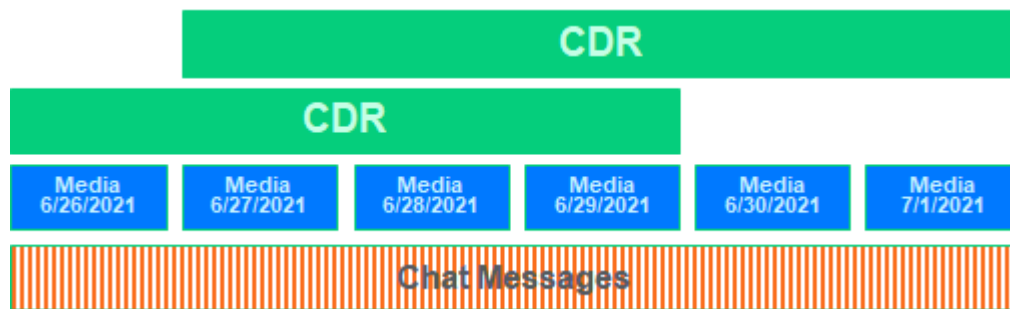
Generally, there is no difference between the data models when it comes to features, although certain features work slightly differently when the system uses the advanced data model. The following table describes the effect of the advanced data model on key features:

Feature	Operation for advanced data model for voice
Search	CDR-only (and standard) records are shown by default, the user can switch to show Media-only records as well. Related Media-Only records can be filtered and displayed for a selected CDR-Only record.
Playback	Requires post processing to stitch and cut Media-only records to CDR-only records. Seamlessly integrated into web based playback, media files are generated temporarily and cached. Playback of Media-Only records is also possible, in that case, not stitching is done.
Silent Monitoring	Not supported
Data retention	Set for both CDR-only and Media-only records, for more information see Data retention On WORM storages: only Media-only records have retention period setting
Deletion	Media-only records have their own retention, for more information see Data retention
Voice quality check and transcoding	Applies to media-only records
Transcription	Supported for CDR-only records using media stitching
Export	Calls can be exported either with stitched media (standard model) or as per advanced/turret model
Import	Both standard and advanced/turret model is supported
Desktop/agent screen recording	Not supported

Advanced data model for instant messaging

This model is designed for modern instant message platforms like Microsoft Teams which provides advanced features like message threads with replies, rich content with images, file attachments, stickers, animated GIFs, emoticons, reactions, etc. This model allows Many-to-Many relations between CDR entries and media records and chat messages by differentiating 3 types of records in the database:

- CDR-only: CDR-only records contain CDR information representing a chat conversation/room (usually from a recorded user point of view) and reference to one or more Media-only records
- Media-only: a Media-Only record represents the chat messages for a day (in UTC timezone) for a chat conversation/room, one media-only record is shared across multiple CDR-only records
- Chat messages: chat message records represent single chat messages, these records are linked to Media-Only records, and through that CDR-Only records



This data model allows storing a single copy of the chat messages in the case of chat conversations/rooms where multiple conversation records are referencing a single media entry (e.g. from multiple recorded users' points of view). The Media-Only records are generated on a daily basis (in UTC timezone) for each chat conversation/room. Chat messages are then stored individually and referenced by the daily Media-Only records. Separately, CDR-Only records are created to represent the chat conversation or room from the recorded users' points of view. The 2 record types are linked in the database, creating a many-to-many relationship. Since normally only CDR-Only records have the complete metadata, the system hides the Media-Only records by default during search and display (display of Media-Only records can be enabled). Media-Only records are basically technical records representing an optimized storage model. When a user views a CDR-Only record, the system automatically looks for related Media-Only records and related chat messages in the database.

The following table describes the effect of the advanced data model on key features:

Feature	Operation for advanced data model for instant messages
Search	<p>CDR-only records are shown by default, the user can switch to show Media-only records as well. Related Media-Only records can be filtered and displayed for a selected CDR-Only record.</p> <p>Records are displayed in a special way:</p> <ul style="list-style-type: none"> • The system displays a CDR-Only record with start times only (no end time or duration) representing a whole hour if there was at least one message captured during that hour. A single chat conversation can be represented by multiple CDR-Only records displayed in the search results with hourly splitting. This way the system is able to show the chat conversations mixed with other record types which are more session-centric with actual start and end times. • The start of the Media-Only records set to the first message received for the day and the end time is always the end of the day in UTC timezone
Display	Seamlessly integrated into the web based viewer, shows the chat conversation in rich content format with lazy loading
Data retention	Set for Media-only records only, for more information see Data retention
Deletion	Media-only records have retention setting only, for more information see Data retention
Export	<p>A separate policy based export is available to export data in SMTP format only, see Advanced IM Export policy</p> <p>Advanced export, standard policy based export (including direct export) are not supported</p>

Import	Not supported
Labeling / Case rules	Not supported

Install

Installing your Verba Recording System

Correct installation of your Verba Recording System ensures stable operation of your system.

Installation steps:

- [Step 1 - Download your Verba Install Kit](#)
- [Step 2 - Install your Verba Server\(s\)](#)
- [Step 3 - \(Optional\) Install your Verba Desktop Recorders](#)

Step 1 - Download your Verba Install Kit

Download your **Verba Install Kit** from support site (requires login) and place it on your servers.

If you have no login for the Support Site register here: <http://support.verba.com>

Step 2 - Install your Verba Server(s)

 Make sure your servers fulfill the requirements of our [Select your server](#) page. The Verba Recording System supports [Virtualization](#).

Based on the chosen [deployment architecture and recording method](#), you can start installing the Verba servers and components.

- **Single server** - your Media Repository and Recording Server components will be installed **on a single server**.
- **Multiple servers** - you will install a Media Repository and standalone Recording Servers **on multiple servers**.

[After all servers are prepared](#), start [Installing your Verba servers](#).

Step 3 - (Optional) Install your Verba Desktop Recorders

The Verba Desktop Recorder component provides desktop recording services. It **requires a Verba server** deployed in your network for operation. This component is required if you plan to use **desktop screen capturing**.

Start [Installing the Verba Desktop Agent](#).

Table of contents

- [Installing the Verba Desktop Agent](#)
- [Installing Verba Unified Media Codec](#)
- [Installing your Verba servers](#)
- [Upgrade procedure from Carin recorders](#)
- [Verba Remote Installation Service Description](#)
- [Installing the Verba Lync extension for Lync 2010](#)
- [Installing the Verba Lync extension for Lync 2013](#)
- [Requesting and assigning certificates](#)
- [Verba PowerShell Deployment Toolkit](#)
- [How to Install your Verba license](#)

- [Adding the Logon As A Service Right](#)
- [How to switch from Oracle to OpenJDK Java Runtime Environment](#)

Do you need installation help?

You can [book a remote installation session](#) with our support team.

Installing the Verba Desktop Agent

❗ A **Verba Media Repository must be installed** before starting Desktop Agent installation. **The desktop agent installer kit checks only a limited set of hardware and 3rd party software prerequisites**, it is very important to fully understand the [requirements](#) before the installation procedure.

❗ Make sure that the following **TCP ports are open** on the desktops where the Verba Desktop Agent is deployed: **10012 (TCP), 4433 (TCP)**. See [Firewall configuration](#).

Manual installation

Installation

Please follow the steps below to install the Verba Desktop Agent:

Step 1 - Launch the **VerbaDesktop.msi** installer **as Administrator**

Step 2 - The install kit starts installing Verba components. Simply press the **Next** button to start the installation.

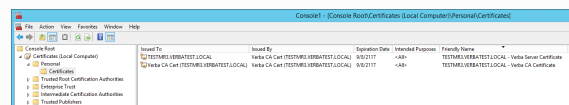
Step 3 - Read the Verba license agreement carefully before you click **Next** button.

Step 4 - Select the destination folder for the Verba Desktop Agent. You can change the default setting by clicking on the Change button and selecting another folder. If you have finished the destination folder configuration, press the **Next** button.

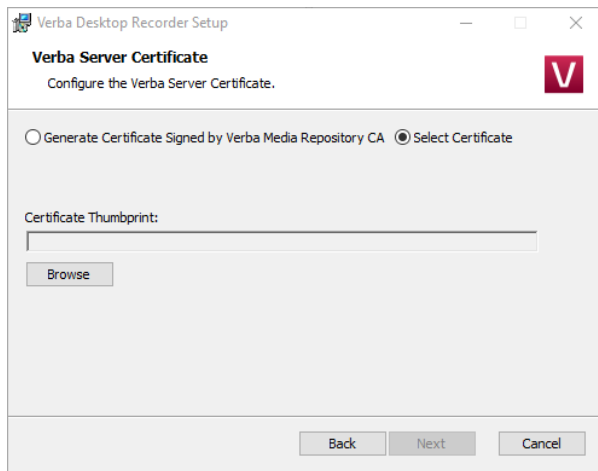
Step 5a - If a Verba CA is being used, then select the **"Generate Certificate Signed by Verba Media Repository CA"** option, then click on the **Generate** button. In the Generate the Verba Server Certificate window provide the address of the first Media Repository server, the Verba administrator username and password, then click **Generate**. Finally, click on the **Next** button. (If this option is being used, Step 5b can be skipped.)

Step 5b - If there is an existing certificate from a previous Verba Desktop Agent installation (in case of reinstall or upgrade), or a pre-generated certificate for the desktop exists (requested from a local or a 3rd party CA), then select the **"Select Certificate"** option, then click on the **Browse** button.

❗ **Certificates generated by the Verba CA**
Based on the Friendly Name of the certificates the server and the CA certificate can be identified easily. On the screenshot, the first one is the server certificate and the second one is the CA certificate.



Issued To	Issued By	Expiration Date	Intended Purpose	Friendly Name
TESTMRL08BATEST.LOCAL	Verba CA Cert (TESTMRL08BATEST.LOCAL)	30/11/17	A&B	TESTMRL08BATEST.LOCAL - Verba Server Certificate
Verba CA Cert (TESTMRL08BATEST.LOCAL)	Verba CA Cert (TESTMRL08BATEST.LOCAL)	30/11/17	A&B	TESTMRL08BATEST.LOCAL - Verba CA Certificate

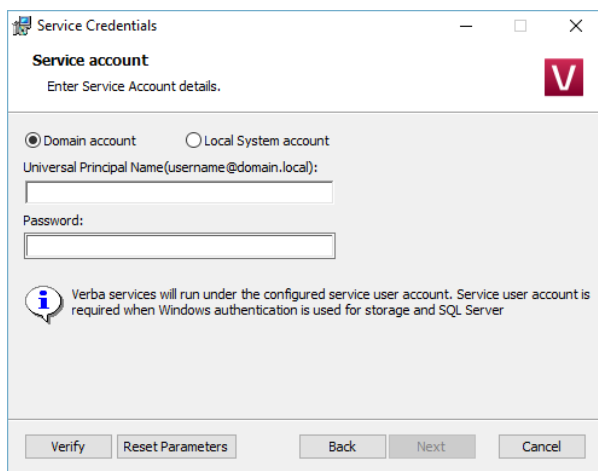


Step 6 - Select the service account type. If the Domain Account is selected then please note the followings:

- The account name has to be entered with the domain
- The Domain Account have to be part of the Local Administrators group and requires the Log on as a service right

When do I need domain account?

- If the media files will be stored on a network location. In this case, the same account has to be used for the services.
- If windows authentication will be used for the SQL connection (Step 7). In this case, the same account has to be used for the services.



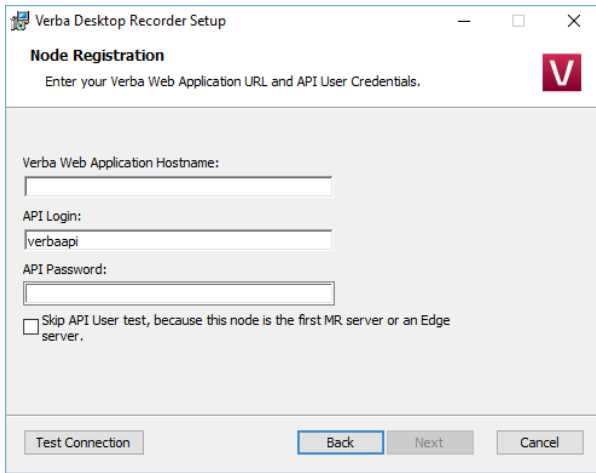
Step 7a - The Verba installer is asking for the MS SQL Server credentials. The server name can be entered either as an IP address or an FQDN. Both SQL server based and windows authentication is supported. All Verba servers and components have to use the same database! If SQL Mirroring is being used or AlwaysOn with Multi-Subnet failover, then a different SQL Driver has to be selected. In this case, the driver has to be installed on the server. Click 'Test Connection' to verify your input. If the tests were successful, click **Next**.

Step 7b - If the incoming connection from the desktop is not possible (because of firewall), then uncheck the "Enable Automatic Node Registration" setting. In this case, the desktop has to be added manually to the server list in the System \ Servers menu after the installation. Click **Next**.

Database connection troubleshooting tips

- Try to ping the database server. Try to connect to the 1433 port on the database server. (telnet or Test-NetConnection)
- Check if the user has the DB Creator role.
- If Windows Authentication used then check if the user has the Local Administrator group membership and the 'Logon as a service right'.
- Check if the correct instance name is provided at the SQL Server name. If there are multiple instances, then the SQL Server Browser service must run on the SQL server side.
- If you installed SQL Server Express Edition, then check if the TCP/IP protocol is enabled under the SQL Server Network Configuration in the SQL Server Configuration Manager.

Step 8 - Provide the address of the Verba Media Repository server, and the API user password. The API user created at **Step 14** during the installation of the Media Repository server.



The screenshot shows a window titled "Verba Desktop Recorder Setup" with a "Node Registration" section. Below the title bar, it says "Enter your Verba Web Application URL and API User Credentials." There are three input fields: "Verba Web Application Hostname:", "API Login:" (with "verbaapi" entered), and "API Password:". Below these fields is a checkbox labeled "Skip API User test, because this node is the first MR server or an Edge server." At the bottom, there are four buttons: "Test Connection", "Back", "Next", and "Cancel".

Verba API instead of direct database connection

If the direct database connection is not possible from the desktop PCs, the Verba Desktop Agent can use the Verba API connection for reaching the database. In this case, the Verba Web Application will work as a proxy between the Verba Desktop Agent and the database.

Step 9 - Click **Next** again to start installing the services. When it's done, click **Finish** to exit the installer.


ⓘ The Verba Desktop Agent **must be configured** from the central web interface before it can work. For more information see [Configuring the Verba Desktop Agent](#)

Unattended installation

The Verba Desktop Agent installation package provides an **unattended installation feature** to support automated, enterprise-wide installation of the software. The installer is MSI based. For more information see [Installer Parameters](#)

Installing Verba Unified Media Codec

The Verba system is able to store recorded video and telepresence calls in a unique format called VF (Verba Media Format). Standard Windows Media Player cannot support this file type, so the Verba Unified Media Codec has to be installed on every computer, which would like to playback VF files.

 You will need this codec for **silent monitoring** (listening to ongoing calls) over the web application. For silent monitoring, please make sure to **open UDP port range 16384-16500 on your client PCs**, where you install the Verba Unified Media Codec.

Manual installation

Installation

Please follow the steps below to install the Verba Unified Media Codec:

Step 1 - Launch the **VerbaCodec.msi** installer

Step 2 - Press the **Next** button to start the installation

Step 3 - Read the Verba license agreement and **accept** it, before you click **Next** button

Step 4 - Installer asks for the destination folder(default: C:\Program Files\Verba Media Codec\), click the **Change** button to change it.

Step 5 - Press the **Install** button. Verba setup will copy and install the codec files.

Update

Please follow the steps below to update the Verba software:

Step 1 - Launch the **VerbaCodec.msi** installer file

Step 2 - Press the **Next** button to start the update (If the installer finds a newer or the same version of the product on the computer, the update is not possible. Press the **Finish** button.)

Step 3 - Please press the **Install** button. Verba setup will copy and update the components onto the server.

Step 4 - After the successful update, please **Restart** the computer to start the updated services.

Unattended installation

The Verba Unified Media Codec installation package provides an **unattended installation feature** to support the automated, enterprise-wide installation of the software. The installer is MSI based.

Installation

The MSI installer file can be located in the Verba Recording System installation package.

Put the Verba Unified Media Codec MSI installer into a local folder on your desktop PC. Customize the following command for your environment:

```
msiexec /i VerbaCodec.msi /quiet /LE verbacodec_install.txt
```

Parameters:

Command Line Parameter	Description
/i	Installation action.
VerbaCodec.msi	Name of the Verba Unified Media Codec MSI package.
/quiet	Invokes quiet/unattended installation.
/LE verbacodec_install.txt	Write the error log into the verbacodec_install.txt file.

Update

The MSI installer file can be located in the Verba Recording System installation package.

Put the Verba Unified Media Codec installer into a local folder on your desktop PC. Customize the following command for your environment:

```
msiexec /i VerbaCodec.msi /quiet /LE verbacodec_update.txt
```

Parameters:

Command Line Parameter	Description
/i	Installation action.
VerbaCodec.msi	Name of the Verba Unified Media Codec MSI package.
/quiet	Invokes quiet/unattended installation.
/LE verbacodec_update.txt	Write the error log into the verbacodec_install.txt file.

Troubleshooting

For more verbose logging in case of an installation error use /L*v instead of /LE.

Uninstallation

Command example:

```
msiexec /X VerbaCodec.msi /quiet /LE verbacodec_uninstall.txt
```

Parameters:

Command Line Parameter	Description
/X	Uninstallation action.
VerbaCodec.msi	Name of the Verba Desktop Recorder MSI package.
/quiet	Invokes quiet/unattended installation.
/LE verbacodec_uninstall.txt	Write the error log into the verbacodec_install.txt file.

Troubleshooting

After you've installed the Verba Media Codec and you are still not able to playback Verba video files or start Silent Monitoring, please follow the instructions below:

Step 1 Close all browser window and media player

Step 2 Open a command prompt as administrator

Step 3 Navigate to Verba Media Codec's folder with the following command: **cd C:\Program Files\Verba Media Codec**

Step 4 Run the following command in the codec's folder: **regsvr32 verbacodec.dll** (If registration was successful a dialog panel is prompted)

Step 5 Test the playback

If the playback works with a downloaded file, but not in Internet Explorer, please follow the instructions below:

Step 1 Close all browser window and media player

Step 2 Open the Start menu, type "regedit" and press Enter.

Step 3 Locate and then select the following registry entry **HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\TabProcGrowth**

Step 4 Delete the selected key

Step 5 Test the playback

Installing your Verba servers

Overview of installation types

In your Verba Recording System you have components for media repository, network-based recorders and desktop recorders. Correct installation is crucial.

Step 1 - Prepare your server

Prepare your server based on the following steps:

- [Operating system configuration](#)
- [Firewall configuration](#)
- [Antivirus scanning exclusions for Verba servers](#)

For all installation types you will **start with the following steps**:

1. Unzip the **Verba Install Kit**
2. Run the **autorun** program, it will open the installer framework window
3. Click **Open Prerequisites Installer Tool** under point **2 Install Prerequisites**
4. **Install all missing prerequisites** from top to bottom

We recommend you turn off

Step 2 - Install SQL Server

Please refer to the [SQL Server installation](#) article.

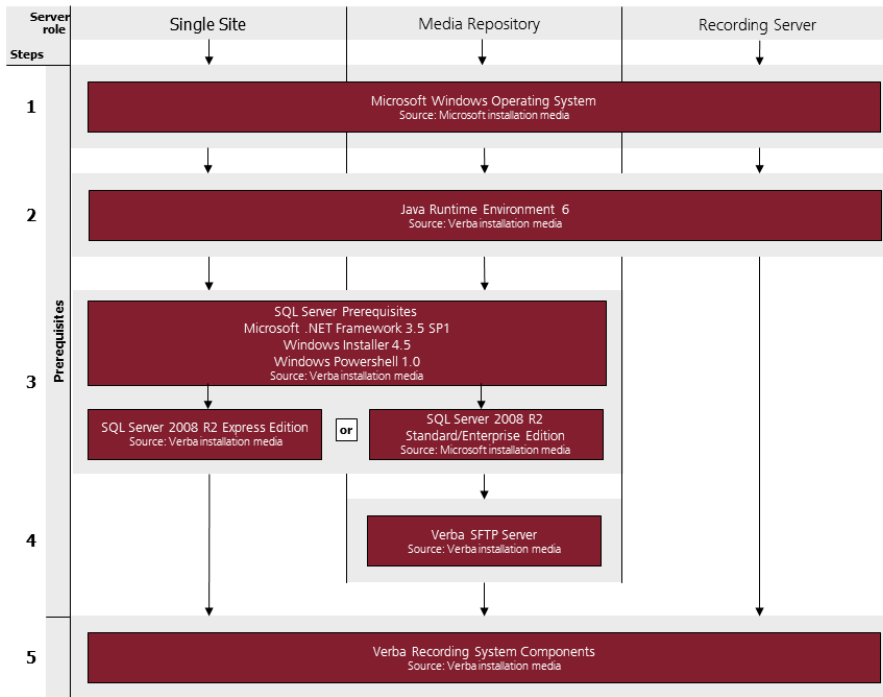
Step 3 - Install the Verba software

Your Verba Recording System can have one central component, the **Media Repository** and multiple **Recording Servers**.

The following diagram shows the major installation steps for the three major Verba installation types:

- [Installing the Verba Media Repository](#) - Database and the web application without the recording engine
- [Installing a Verba Recording Server](#) - Recording engine without database and web application
- [Installing a single server Verba solution](#) - When the Media Repository and Recording Server are installed on a single server

Server installation overview



The following topics guide you through the installation:

- [Prepare your server](#)
- [SQL Server installation](#)
- [Install the Verba software](#)
- [Upgrading your Verba system](#)

Prepare your server

Overview

The Verba Recording System has specific server requirements that must be met before the installation of the Verba components can be started. The **Verba server installation pack** includes the **Verba Recording System Prerequisites** tool that opens when you start your installation.

i We also provide standalone **Verba Recording System Prerequisites** tool to evaluate if all software requirements are met by your system without download the entire installation pack. The exact same functionality can be found in the installation pack, this is provided for installations where server OS and Verba installation are done by different teams.

You can download the installation files from the [support site](#).

Verba Recording System Prerequisites tool

i We recommend you **use our installation pack** to install your system, it guides you through the requirements below. This chapter is only for documentation purposes.

This tool asks a couple of **questions** about your installation before it creates a customized prerequisite list. ('-' means that the question does not have any effect whether the requirement is shown or not, or it is not applicable.)

Question 1: Verba components	Question 2: SQL Server	Question 3: SQL Server Management Studio	Prerequisite title	Hint provided by the tool	Mode	Installer in the installation pack
-	-	-	Verify Windows version	The Verba Recording System server components require one of the following operating systems: <ul style="list-style-type: none">• Windows Server 2012 R2• Windows Server 2016• Windows Server 2019 The Verba Desktop Recorder supports Windows 8, Windows 8.1, Windows 10	Mandatory	-
-	-	-	No existing Verba installation	If you are installing a new system, you should uninstall your existing Verba Recording System before installation. If you are upgrading this system, you do not have to use this Deployment Planner, just exit and run the Verba MSI Installer directly.	Mandatory	-

-	-	-	Verify Administrator Privileges	The Windows User that installs the Verba Recording System must have Administrator privileges. Please add your user to the Administrators group.	Mandatory	-
-	-	-	No Pending Windows Restart	There should be no Windows restart operation pending on your server, since it might interfere with your new installation.	Mandatory	-
-	-	-	Install Windows Installer 4.5	The Verba MSI installer package requires Windows Installer 4.5.	Mandatory	Included
Single Server or Media Repository	-	-	Uninstall Internet Information Server	The Verba Recording System comes with a built-in Tomcat-based web application that collides with the Microsoft IIS web server. Follow these steps to uninstall it: Step 1 - Open Windows Server Manager Step 2 - Click Roles in the tree on the left Step 3 - Click Remove Roles on the right Step 4 - Click Next Step 5 - Uncheck Web Server (IIS) Step 6 - Click Next Step 7 - Click Remove	Mandatory	-
All	-	-	Install Java SE 11 RE	Java Runtime is required by multiple Verba Recording System services. Both Oracle and OpenJDK Java 11 runtimes are supported.	Mandatory	Included
Single Server or Media Repository	-	When selected	Install Microsoft .Net Framework 4.6.2	Microsoft .NET Framework 4.6.2 is required by the Microsoft SQL Server Management Studio. Follow these steps to install it: Step 1 - Open Windows Server Manager Step 2 - Click Features in the tree on the left Step 3 - Click Add Features on the right Step 4 - Click Next Step 5 - Select .Net Framework 4.6.2 Features Step 6 - Open the tree below the .Net feature and uncheck WCF activation (important) Step 7 - Click Next Step 8 - Click Install	Mandatory	Included
Single Server or Media Repository	When SQL Server Express is selected	-	Install SQL Server 2012 Express or newer	Microsoft SQL Server Express Edition provides free of charge SQL database server backend for the Verba Recording System. We recommend to use Standard or Enterprise edition if you are planning to store and search more than 500.000 calls in your recording system.	Mandatory	Included
Single Server or Media Repository	When SQL Server is selected	-	Install SQL Server 2012 or newer	Microsoft SQL Server provides SQL database server functionality for the Verba Recording System	Mandatory	Not included

Single Server or Media Repository	-	When selected	Install SQL Server Management Studio	The Microsoft SQL Server Management Studio provides management capabilities for Microsoft SQL Server.	Optional	Not included
Single Server or Media Repository	When installed on other server	When not selected	Install SQL Server Native Client x64	The Verba Recording System uses Microsoft SQL Server to store data and is capable of using the advanced failover functionality of the SQL Server Native Client 10.0 database driver.	Mandatory	Included
Single Server or Media Repository	When installed on other server	When not selected	Install SQL Server Native Client	The Verba Recording System uses Microsoft SQL Server to store data and is capable of using the advanced failover functionality of the SQL Server Native Client 10.0 database driver.	Mandatory	Included
Single Server or Media Repository	-	-	Install Windows Desktop Experience (Windows Server 2012 R2)	In case you plan to use PC desktop screen and video call recording features or want to playback mp3/mp4/m4a files, then your Verba Media Repository requires the Windows Desktop Experience feature. Follow these steps to install it: Step 1 - Open Windows Server Manager Step 2 - Click Features in the tree on the left Step 3 - Click Add Features on the right Step 4 - Click Next Step 5 - Select Desktop Experience Step 6 - Click Next Step 7 - Click Install Step 8 - Restart the server (Important)	Recommended	-
Single Server or Media Repository	-	-	Configure Virus Scanning	If not configured properly, any virus scanner on this server can severely impact the performance and reliability of your recording system. Please make sure you turn off background virus scanning of all your Verba media and log folders.	Recommended	-
Single Server or Media Repository	-	-	Verify Time Settings	The Verba Recording System stores all dates in timezone independent UTC time and presents correct local time to each user. Please verify: <ul style="list-style-type: none"> • Server time zone matches your local time zone • Server time is correct 	Recommended	-
Single Server or Media Repository	-	-	Use Separate System and Media Disk	For reliability, performance and backup reasons, we recommend you use separate disk volumes for system and recorded media. C: (System Disk) D: (Media Disk)	Recommended	-

Further information

Find more information in these articles:

- [Operating system configuration](#)

- [Firewall configuration](#)
- [Antivirus scanning exclusions for Verba servers](#)

Operating system configuration

Please read the following topic carefully before you begin Verba installation! In order to maximize your satisfaction with the Verba recording system please read the following carefully and follow the guidelines of this topic before you begin software installation.

⚠ It is important that you follow this topic when you build your Verba servers. Failure to comply with the guidelines in this topic may lead to degraded performance and eventual data loss in your Verba environment. Verba Technologies is not responsible for the security of the HW, operating system and database layers of the Verba recording system. The customer shall install and configure these in accordance with industry best practices for security.

Please follow the following guidelines during the installation of your Windows operating system.

In case you install your server from a customized Windows installer or image please try to configure the installed server according to the guidelines below.

Disk partitioning

The Verba Recording System does not require special disk partitioning, but in order to achieve the best performance and better serviceability we have some recommendations.

- **System (e.g. C:\)** - Operating System and application binaries: minimum 80 GB
- **Media (e.g. D:\)** - Media and database files: the rest of the capacity, please use the storage calculator tool to properly size the hard disks

Regional and Language Options

Set these options to your normal local settings.

Date and Time Settings

For correct time handling please set timezone properly on all servers.

NTP-based time synchronization is strongly recommended.

It is important to note that most date/time information is stored in UTC standard time format in Verba. On the web interface these times are converted to the actual users local time zone. The following table summarizes the time zones used by Verba's different system elements to present date information:

System elements		Time zone
User interfaces	Web interfaces	Time zone setting of the Verba user that logs into the web interface.
	Configuration interfaces	Time zone setting of the computer that runs the configuration tools.
	Log files	Local time on the computer that writes the log.
Internal storage	SQL database (e.g. call data)	UTC time
	Configuration data	UTC time

Network settings (during installation)

During installation just pick the "typical" settings or configure the network according to your policies. Network settings shall be reconfigured for Verba after the Windows installation is complete.

Install Critical Security Updates and disable automatic updates

After installation please use Windows Update to install the latest patch level for your Windows Server. Be sure that the automatic updates are disabled.

Update firmware and driver versions

Please consult the hardware vendors support site and verify that the following most important items are upgraded to the latest recommended version:

- chipset driver
- network card driver
- the RAID controller drivers, RAID controller firmware
- disk firmware

⚠ Since Verba is a high disk I/O application you should be extra careful with your disk I/O subsystems, such as RAID controllers and disks.

Network configuration

The following configuration in this topic should only be applied to Recording Server servers or servers where the Media Repository and Recording Server are installed together.

Step 1 Rename network interfaces

In the Network Connections window change the name of the recording interface to **Recording Port**, the other interface can get the name Network access. These new interface names are not used by the Verba system. Verba recording ports must be configured later on. Naming the interface will however avoid confusion in your IT team.

Step 2 Configure the "Recording" interface

If passive recording technology is used, open the properties sheet of this interface and disable Client for Microsoft Networks and File and Printer Sharing. For other recording methods, use the default settings.

Click Show icon in notification area when connected to show the icon to administrators.

Disable Windows Firewall

Disable Windows Firewall on the server in order to provide communication among the networked system components. If your company policy does not allow you to do this, carefully open all ports, which are required for Verba (more information: [Firewall configuration](#)).

⚠ Make sure you are reactivating your Windows Firewall after the installation with the proper port and executable exception rules.

Firewall configuration

The components of the system use several network ports for communication. These ports must be open and accessible and not blocked by network or server firewalls. The firewall requirements are available for the following integrations:

- [Firewall configuration for Skype for Business - Lync deployments](#)
- [Firewall configuration for Ethical Wall deployments](#)
- [Firewall configuration for Avaya recording deployments](#)
- [Firewall configuration for Cisco recording deployments](#)
- [Firewall Configuration for IPC Unigy recording deployments](#)
- [Firewall configuration for BT IP Trade recording deployments](#)
- [Firewall configuration for BT ITS recording deployments](#)
- [Firewall configuration for Speakerbus recording deployments](#)
- [Firewall configuration for Microsoft Teams recording deployments](#)
- [Firewall configuration for SIPREC recording deployments](#)
- [Firewall configuration for Genesys active recording deployments](#)

Firewall configuration for Skype for Business - Lync deployments

This chapter summarizes the required inbound firewall configuration for Lync recording deployments. For more general information see [Firewall configuration](#).

Server	Verba Server Role	Service name	Source	Port	Protocol	Notes
SQL Server	-	-	All Verba Servers	1433	TCP	SQL connection
Lync Front-End Server / SBA	Lync Filter	Verba Node Manager Agent	Verba Media Repository	4433	TCP	Central configuration from Verba Web Application
		Verba Lync Filter Service	All Verba Servers	10017	TCP	Service API port
		Verba Lync IM Filter Service	All Verba Servers	10019	TCP	Service API port
Lync Front-End Server / SBA with Mediation Server role	Media Collector and Lync Filter	Verba Node Manager Agent	Verba Media Repository	4433	TCP	Central configuration from Verba Web Application
		Verba Lync Filter Service	All Verba Servers	10017	TCP	Service API port
		Verba Lync IM Filter Service	All Verba Servers	10019	TCP	Service API port
		Verba Media Collector and Proxy Service	All Verba Servers	10024	TCP	Service API port
		Verba Media Collector and Proxy Service	Lync Front-End Server / SBA	10201	TCP	Communication with the Verba Lync Filter services
		Verba Media Collector and Proxy Service	Verba Recording Server	11112	TCP	Communication with Verba Passive Recording services
Lync Mediation Server	Media Collector and Proxy Server	Verba Node Manager Agent	Verba Media Repository	4433	TCP	Central configuration from Verba Web Application
		Verba Media Collector and Proxy Service	All Verba Servers	10024	TCP	Service API port
		Verba Media Collector and Proxy Service	Lync Front-End Server / SBA	10201	TCP	Communication with the Verba Lync Filter services
		Verba Media Collector and Proxy Service	Verba Recording Server	11112	TCP	Communication with Verba Passive Recording services
Lync Edge Server	Media Collector and Proxy Server	Verba Node Manager Agent	Verba Media Repository	4433	TCP	Central configuration from Verba Web Application

		Verba Media Collector and Proxy Service	All Verba Servers	10024	TCP	Service API port
		Verba Media Collector and Proxy Service	Lync Front-End Server / SBA	10201	TCP	Communication with the Verba Lync Filter services
		Verba Media Collector and Proxy Service	Verba Recording Server	11112	TCP	Communication with Verba Passive Recording services
Verba Proxy Server	Media Collector and Proxy Server	Verba Node Manager Agent	Verba Media Repository	4433	TCP	Central configuration from Verba Web Application
		Verba Media Collector and Proxy Service	All Verba Servers	10024	TCP	Service API port
		Verba Media Collector and Proxy Service	Lync Front-End Server / SBA	10201	TCP	Communication with the Verba Lync Filter services
		Verba Media Collector and Proxy Service	Verba Recording Server	11112	TCP	Communication with Verba Passive Recording services
		Verba Media Collector and Proxy Service	Any	16384 - 65535	UDP	Media port range used for relaying
Verba Announcement Server	Announcement Server	Verba Node Manager Agent	Verba Media Repository	4433	TCP	Central configuration from Verba Web Application
		Verba Recording Announcement Service	Lync Front-End Server / SBA	6000	TCP	SIP communication with Lync
		Verba Recording Announcement Service	Lync Front-End Server / SBA	10210	TCP	Communication with Verba Lync Filter services
		Verba Recording Announcement Service	Verba Recording Server	12222	TCP	Communication with Verba Passive Recording services
		Verba Recording Announcement Service	Any	1024 - 65535	UDP	Media port range, depends on Lync configuration
Verba Recording Server	Recording Server	Verba Node Manager Agent	Verba Media Repository	4433	TCP	Central configuration from Verba Web Application
		Verba Passive Recording Service	All Verba Servers All Verba Desktop Agents (if used) (plus all playback stations if silent monitoring is used)	10000	TCP/UDP	Service API port
		Verba Media Collector and Proxy Service	All Verba Servers	10024	TCP	Service API port

Verba Media Collector and Proxy Service	Lync Front-End Server / SBA	10201	TCP	Communication with the Verba Lync Filter services
Verba Media Collector and Proxy Service	Any	16384 - 65535	UDP	Media port range used for relaying
Verba Recording Announcement Service	Lync Front-End Server / SBA	6000	TCP	SIP communication with Lync
Verba Recording Announcement Service	Lync Front-End Server / SBA	10210	TCP	Communication with Verba Lync Filter services
Verba Recording Announcement Service	Any	1024 - 65535	UDP	Media port range, depends on Lync configuration
Verba Lync IM Recorder Service	Lync Front-End Server / SBA	10220	TCP	Communication with Verba Lync IM Filter services
Verba Dial-in Recorder Service	All Verba Servers All Verba Desktop Agents (if used) (plus all playback stations if silent monitoring is used)	10006	TCP	Service API port
Verba Dial-in Recorder Service	Lync Front-End Server / SBA	5065	TCP	SIP communication with Lync
Verba Dial-in Recorder Service	Any	16384 - 65535	UDP	Media port range, depends on Lync configuration

Verba Media Repository Server

Media Repository

Verba Web Application	Any	80	TCP	Used for HTTP-based web access
Verba Web Application	Any	443	TCP	Used for HTTPS-based web access
Verba Media Streamer and Content Server Service	Any	10105	TCP	Media port for playback via HTTP
Verba Media Streamer and Content Server Service	Any	10106	TCP	Media port for playback via HTTPS
Verba Storage Management Service	Verba Recording Server	20111	TCP	Communication with Verba Storage Management services, used for secure file upload
Verba Recording Announcement Service	Lync Front-End Server / SBA	6000	TCP	SIP communication with Lync
Verba Recording Announcement Service	Lync Front-End Server / SBA	10210	TCP	Communication with Verba Lync Filter services
Verba Recording Announcement Service	Verba Recording Server	12222	TCP	Communication with Verba Passive Recording services

	Verba Recording Announcement Service	Any	1024 - 65535	UDP	Media port range, depends on Lync configuration
	SQL Server (if co-located on Verba Media Repository)	All Verba Servers	1433	TCP	SQL connection

Firewall configuration for Ethical Wall deployments

Cisco

Server	Server Role	Service name	Source	Port	Protocol	Notes
SQL Server	-	-	All Verba Servers	1433	TCP	SQL connection
Verba Compliance Server	Compliance Server	Verba Node Manager Agent	Verba Media Repository	4433	TCP	Central configuration from Verba Web Application
		Verba Cisco Compliance Service	Cisco Unified Presence Server	10042 - 1004x	TCP	Compliance server connection, one port is needed for every Cisco Presence Server in the topology
		Verba Cisco Compliance Service	Cisco Unified Communication Manager	10041	TCP	Compliance server connection for Cisco Unified Communication Manager
Verba Media Repository Server	Media Repository	Verba Web Application	Any	80	TCP	Used for HTTP based web access
		Verba Web Application	Any	443	TCP	Used for HTTPS based web access

Skype for Business (Lync)

Server	Server Role	Service name	Source	Port	Protocol	Notes
SQL Server	-	-	All Verba Servers	1433	TCP	SQL connection
Verba Media Repository Server	Media Repository	Verba Web Application	Any	80	TCP	Used for HTTP based web access
		Verba Web Application	Any	443	TCP	Used for HTTPS based web access
Lync Front-End Server / SBA	Lync Filter	Verba Node Manager Agent	Verba Media Repository	4433	TCP	Central configuration from Verba Web Application
Verba Announcement Server	Announcement Server	Verba Node Manager Agent	Verba Media Repository	4433	TCP	Central configuration from Verba Web Application
		Verba Recording Announcement Service	Lync Front-End Server / SBA	6000	TCP	SIP communication with Lync
		Verba Recording Announcement Service	Lync Front-End Server / SBA	10211	TCP	Communication with Verba Lync Filter services

Firewall configuration for Avaya recording deployments

This chapter summarizes the required firewall configuration for Avaya recording deployments. For more general information see [Firewall configuration](#).

Common ports

Server	Server Role	Service name	Source	Port	Protocol	Notes
SQL Server	-	-	All Verba Servers	1433	TCP	SQL connection
Verba Media Repository Server	Media Repository	Verba Web Application	Any	80	TCP	Used for HTTP-based web access
		Verba Web Application	Any	443	TCP	Used for HTTPS-based web access
		Verba Storage Management Service	Verba Recording Server	20111	TCP	Communication with Verba Storage Management services, used for secure file upload
		Verba Media Streamer and Content Server Service	Any	10105	TCP	Media port for playback via HTTP
		Verba Media Streamer and Content Server Service	Any	10106	TCP	Media port for playback via HTTPS

Avaya Central Recording

Server	Server Role	Service name	Source	Port	Protocol	Notes
Verba Recording Server	Recording Server	Verba Node Manager Agent	Verba Media Repository	4433	TCP	Central configuration from Verba Web Application
		Verba Unified Call Recorder Service	Avaya Media Resource	16384 - 65535	UDP	Media port range
		Verba Avaya Recorder Service	All Verba Servers All Verba Desktop Agents (if used) (plus all playback stations if silent monitoring is used)	10003	TCP	Service API port
		Verba Avaya Recorder Service	Any	10014	TCP	Recording control port
		Verba Avaya Recorder Service	Any	10013	TCP	Service API port
		Verba Avaya Recorder Service	Any	10099	TCP	Service API port
Avaya Application Enablement Services	CTI Server	Avaya Application Enablement Services	Verba Avaya Recorder Service	4721	TCP	AES communication port (unsecured)
		Avaya Application Enablement Services	Verba Avaya Recorder Service	4722	TCP	AES communication port (secure)

Firewall configuration for Cisco recording deployments

This chapter summarizes the required firewall configuration for Cisco recording deployments. For more general information see [Firewall configuration](#).

Server	Server Role	Service name	Source	Port	Protocol	Notes
SQL Server	-	-	All Verba Servers	1433	TCP	SQL connection
Verba Media Repository Server	Media Repository	Verba Web Application	Any	80	TCP	Used for HTTP based web access
		Verba Web Application	Any	443	TCP	Used for HTTPS based web access
		Verba Media Streamer and Content Server Service	Any	10105	TCP	Media port for playback via HTTP
		Verba Media Streamer and Content Server Service	Any	10106	TCP	Media port for playback via HTTPS
		Verba Storage Management Service	Verba Recording Server	20111	TCP	Communication with Verba Storage Management services, used for secure file upload
		SQL Server (if co-located on Verba Media Repository)	All Verba Servers	1433	TCP	SQL connection
Cisco network-based recording						
Verba Recording Server	Recording Server	Verba Node Manager Agent	Verba Media Repository	4433	TCP	Central configuration from Verba Web Application
		Verba Unified Call Recorder Service	Any	16384 - 65535	UDP	Media port range
		Verba Unified Call Recorder Service	Cisco Unified Call Manager	5060	TCP	SIP signaling communication port
		Verba Unified Call Recorder Service	All Verba Servers All Verba Desktop Agents (if used)	10031	TCP	Service API port
		Cisco JTAPI Service	Verba Media Repository	10014	TCP	Service API port
		Verba Unified Call Recorder Service	Verba Recording Server	10500	TCP	Recording Director - Media Recorder connector
		Verba Cisco Central Silent Monitoring Service	Any	10013	TCP	Service API port (when phone-based silent monitoring is used)
		Cisco JTAPI Service	Verba Recording Server	11200	TCP	JTAPI service registration port
Cisco Unified Communication Manager	Communication Manager	JTAPI	Cisco JTAPI Service	2748	TCP	Used for JTAPI connection
		JTAPI	Cisco JTAPI Service	2749	TCP	Used for secure JTAPI connection

		JTAPI	Cisco JTAPI Service	2789	TCP	Used for JTAPI connection
Cisco gateway recording						
Verba Recording Server	Recording Server	Verba Node Manager Agent	Verba Media Repository	4433	TCP	Central configuration from Verba Web Application
		Verba Cisco UC Gateway Recorder Service	Gateway	16384 - 65535	UDP	Media port range
Cisco Instant Message capture						
Verba Recording Server	Recording Server	Verba Node Manager Agent	Verba Media Repository	4433	TCP	Central configuration from Verba Web Application
		Verba Cisco Compliance Service	Cisco Unified Presence Server	10042 - 1004x	TCP	Compliance server connection, one port is needed for every Cisco Presence Server in the topology
Cisco ethical wall						
Verba Recording Server	Compliance Server	Verba Node Manager Agent	Verba Media Repository	4433	TCP	Central configuration from Verba Web Application
		Verba Cisco Compliance Service	Cisco Unified Presence Server	10042 - 1004x	TCP	Compliance server connection, one port is needed for every Cisco Presence Server in the topology
		Verba Cisco Compliance Service	Cisco Unified Communication Manager	10041	TCP	Compliance server connection for Cisco Unified Communication Manager

Firewall Configuration for IPC Unigy recording deployments

This chapter summarizes the required firewall configuration for IPC Unigy recording deployments.

Server	Server Role	Service name	Source	Port	Protocol	Notes
SQL Server	-	-	All Verba Servers	1433	TCP	SQL connection
All Verba Servers	-	Verba Node Manager Agent	Verba Media Repository	4433	TCP	Central configuration from Verba Web Application
Verba Media Repository Server	Media Repository	Verba Web Application	Any	80	TCP	Used for HTTP-based web access
		Verba Web Application	Any	443	TCP	Used for HTTPS-based web access
		Verba Media Streamer and Content Server Service	Any	10105	TCP	Media port for playback via HTTP
		Verba Media Streamer and Content Server Service	Any	10106	TCP	Media port for playback via HTTPS
		Verba Storage Management Service	Verba Recording Server	20111	TCP	Communication with Verba Storage Management services, used for secure file upload
		SQL Server (if co-located on Verba Media Repository)	All Verba Servers	1433	TCP	SQL connection
Verba Recording Server	Recording Director	Verba Unified Call Recorder Service	IPC CCM	1024 - 65535	TCP	CTI communication port range
		Verba Unified Call Recorder Service	IPC CCM	5060 / 5061	TCP	SIP signaling communication port (non-secure / secure)
	Media Recorder	Verba Unified Call Recorder Service	Any	16384 - 65535	UDP	Media port range
		Verba Unified Call Recorder Service	Verba Recording Server	10500	TCP	Recording Director - Media Recorder connector
	Recording Director Media Recorder	Verba Unified Call Recorder Service	All Verba Servers All Verba Desktop Agents (if used)	10031	TCP	Service API port

Firewall configuration for BT IP Trade recording deployments

This chapter summarizes the required firewall configuration for BT IP Trade recording deployments.

Server	Server Role	Service name	Source	Port	Protocol	Notes
SQL Server	-	-	All Verba Servers	1433	TCP	SQL connection
All Verba Servers	-	Verba Node Manager Agent	Verba Media Repository	4433	TCP	Central configuration from Verba Web Application
Verba Media Repository Server	Media Repository	Verba Web Application	Any	80	TCP	Used for HTTP-based web access
		Verba Web Application	Any	443	TCP	Used for HTTPS-based web access
		Verba Media Streamer and Content Server Service	Any	10105	TCP	Media port for playback via HTTP
		Verba Media Streamer and Content Server Service	Any	10106	TCP	Media port for playback via HTTPS
		Verba Storage Management Service	Verba Recording Server	20111	TCP	Communication with Verba Storage Management services, used for secure file upload
		SQL Server (if co-located on Verba Media Repository)	All Verba Servers	1433	TCP	SQL connection
Verba Recording Server	Recording Director	Verba Unified Call Recorder Service	Any	8000 / 8001	TCP	CTI/Call Control communication port range (Primary / Secondary Server)
	Media Recorder	Verba Unified Call Recorder Service	Any	16384 - 65535	UDP	Media port range (for turret replay, outbound traffic must be allowed)
		Verba Unified Call Recorder Service	Verba Recording Server	10500	TCP	Recording Director - Media Recorder connector
	Recording Director Media Recorder	Verba Unified Call Recorder Service	All Verba Servers All Verba Desktop Agents (if used)	10031	TCP	Service API port

Firewall configuration for BT ITS recording deployments

This chapter summarizes the required firewall configuration for BT ITS recording deployments.

Server	Server Role	Service name	Source	Port	Protocol	Notes
SQL Server	-	-	All Verba Servers	1433	TCP	SQL connection
All Verba Servers	-	Verba Node Manager Agent	Verba Media Repository	4433	TCP	Central configuration from Verba Web Application
Verba Media Repository Server	Media Repository	Verba Web Application	Any	80	TCP	Used for HTTP-based web access
		Verba Web Application	Any	443	TCP	Used for HTTPS-based web access
		Verba Media Streamer and Content Server Service	Any	10105	TCP	Media port for playback via HTTP
		Verba Media Streamer and Content Server Service	Any	10106	TCP	Media port for playback via HTTPS
		Verba Storage Management Service	Verba Recording Server	20111	TCP	Communication with Verba Storage Management services, used for secure file upload
		SQL Server (if co-located on Verba Media Repository)	All Verba Servers	1433	TCP	SQL connection
Verba Recording Server	Media Recorder	Verba Unified Call Recorder Service	IPSI Card	53250-53251	UDP	Default media port range; can be configured in global_config
		BT Heartbeat and Directory Service				For additional information, please consult BT
		Verba Unified Call Recorder Service	Verba Recording Server	10500	TCP	Recording Director - Media Recorder connector
	Recording Director	Verba Unified Call Recorder Service	All Verba Servers All Verba Desktop Agents (if used)	10031		Service API port

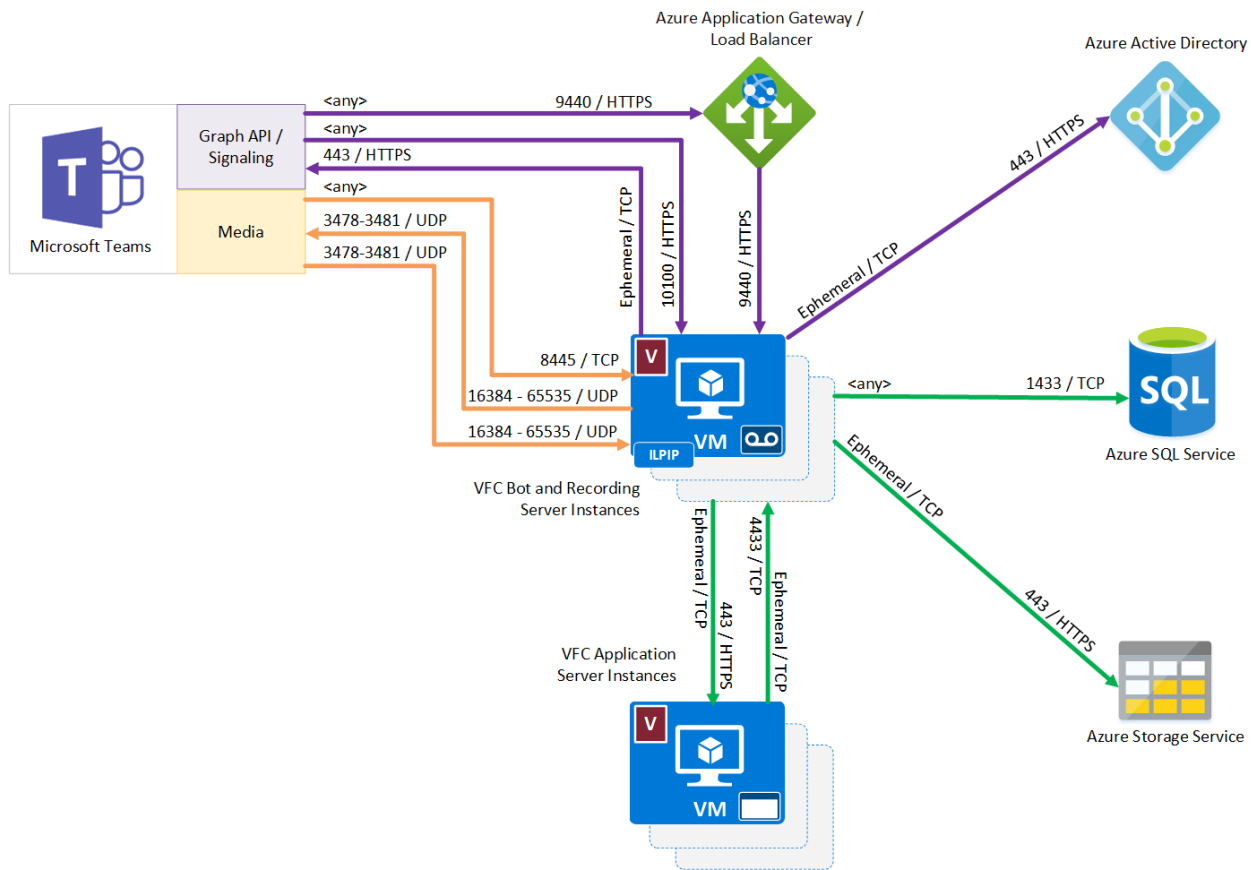
Firewall configuration for Speakerbus recording deployments

This chapter summarizes the required firewall configuration for Speakerbus recording deployments.

Server	Server Role	Service name	Source	Port	Protocol	Notes
SQL Server	-	-	All Verba Servers	1433	TCP	SQL connection
All Verba Servers	-	Verba Node Manager Agent	Verba Media Repository	4433	TCP	Central configuration from Verba Web Application
Verba Media Repository Server	Media Repository	Verba Web Application	Any	80	TCP	Used for HTTP-based web access
		Verba Web Application	Any	443	TCP	Used for HTTPS-based web access
		Verba Media Streamer and Content Server Service	Any	10105	TCP	Media port for playback via HTTP
		Verba Media Streamer and Content Server Service	Any	10106	TCP	Media port for playback via HTTPS
		Verba Storage Management Service	Verba Recording Server	20111	TCP	Communication with Verba Storage Management services, used for secure file upload
		SQL Server (if co-located on Verba Media Repository)	All Verba Servers	1433	TCP	SQL connection
Verba Recording Server	Recording Director	Verba Unified Call Recorder Service	Speakerbus iCDS Service	7788	TCP	CTI communication port
	Media Recorder	Verba Unified Call Recorder Service	Any	3000-3007	UDP	Media port range
		Verba Unified Call Recorder Service	Verba Recording Server	10500	TCP	Recording Director - Media Recorder connector
	Recording Director Media Recorder	Verba Unified Call Recorder Service	All Verba Servers All Verba Desktop Agents (if used)	10031	TCP	Service API port

Firewall configuration for Microsoft Teams recording deployments


This chapter summarizes the required firewall configuration for Microsoft Teams recording deployments.



Inbound rules

Server	Server Role	Service name	Source	Port	Protocol	Notes
SQL Server	-	-	All Verba Servers	1433	TCP	SQL connection
All Verba Servers	-	Verba Node Manager Agent	Verba Media Repository	4433	TCP	Central configuration from Verba Web Application
Verba Media Repository Server	Media Repository	Verba Web Application	Any	80	TCP	Used for HTTP-based web access
		Verba Web Application	Any	443	TCP	Used for HTTPS-based web access
		Verba Media Streamer and Content Server Service	Any	10105	TCP	Media port for playback via HTTP

		Verba Media Streamer and Content Server Service	Any	10106	TCP	Media port for playback via HTTPS
		Verba Storage Management Service	Verba Recording Server	20111	TCP	Communication with Verba Storage Management services, used for secure file upload
		SQL Server (if co-located on Verba Media Repository)	All Verba Servers	1433	TCP	SQL connection
Verba Recording Server	Recording Server	Verba Microsoft Teams Bot Service	Any It can be only restricted to Azure networks, Microsoft cannot restrict the Teams side to specific IP ranges at the moment. To download Azure IP ranges, see https://www.microsoft.com/en-us/download/details.aspx?id=56519 Make sure that the IP addresses of the VMs running the bot service are allowed.	8445	TCP	Media control port for Teams
	Recording Server	Verba Microsoft Teams Bot Service	Any It can be only restricted to Azure networks, Microsoft cannot restrict the Teams side to specific IP ranges at the moment. To download Azure IP ranges, see https://www.microsoft.com/en-us/download/details.aspx?id=56519 Make sure that the IP addresses of the VMs running the bot service are allowed.	9440	TCP	<ul style="list-style-type: none"> ■ Call invite from Teams ■ HTTPS health probe for Azure Traffic Manager and Application Gateway
	Recording Server	Verba Microsoft Teams Bot Service	Any It can be only restricted to Azure networks, Microsoft cannot restrict the Teams side to specific IP ranges at the moment. To download Azure IP ranges, see https://www.microsoft.com/en-us/download/details.aspx?id=56519 Make sure that the IP addresses of the VMs running the bot service are allowed.	10100	TCP	Call control port for Teams
	Recording Server	Verba Microsoft Teams Bot Service	Verba Recording Server / Verba Unified Call Recorder Service	10501	TCP	Recording Director connection (it is recommended to deploy the bot and the recording service on the same VM)
	Recording Server	Verba Microsoft Teams Bot Service	Verba Recording Server / Verba Unified Call Recorder Service	10502	TCP	Media Recorder connection (it is recommended to deploy the bot and the recording service on the same VM)

Recording Server	Verba Microsoft Teams Bot Service	13.107.64.0/18, 52.112.0.0/14, 52.122.0.0/15, 2603:1063::/39	16384 - 65535	UDP	Media port range
<div style="border: 1px solid #ccc; padding: 10px; background-color: #fff9e6;"> <p> The above IP ranges can be changed by Microsoft and it is possible that this Knowledge Base is not in sync with Microsoft's documentation. Please double-check the currently needed IP ranges on the Microsoft Documentation: https://docs.microsoft.com/en-us/office365/enterprise/urls-and-ip-address-ranges#skype-for-business-online-and-microsoft-teams</p> </div>					
Recording Server	Verba Microsoft Teams Bot Service	Any	10038	TCP	Bot service API port
Recording Server	Verba Unified Call Recorder Service	All Verba Servers All Verba Desktop Agents (if used) (plus all playback stations if silent monitoring is used)	10031	TCP	Service API port

Outbound rules

The Microsoft Teams Bot Service is considered as a standard Microsoft Teams endpoint and the standard firewall rules can be applied.

The following Microsoft documentation contains all the required endpoints and ports which has to be accessible for a Teams endpoint:
[Office 365 URLs and IP address ranges](#) (section Skype for Business Online and Microsoft Teams)

In addition, the Microsoft Teams Bot Service uses Microsoft Graph API via the <https://graph.microsoft.com/v1.0> endpoint for sending requests to Microsoft Teams (e.g.: Call answer, Azure AD queries)

Make sure that the Microsoft Teams Bot Service is able to use the OCSP (Online Certificate Status Protocol) to validate the certificates issued by a public CA. The used SDKs check the certificate validity from time to time. It is necessary to allow the bot to connect the public certificate services over OCSP.

Firewall configuration for SIPREC recording deployments

This chapter summarizes the required firewall configuration for Microsoft Teams recording deployments.

Server	Server Role	Service name	Source	Port	Protocol	Notes
SQL Server	-	-	All Verba Servers	1433	TCP	SQL connection
All Verba Servers	-	Verba Node Manager Agent	Verba Media Repository	4433	TCP	Central configuration from Verba Web Application
Verba Media Repository Server	Media Repository	Verba Web Application	Any	80	TCP	Used for HTTP-based web access
		Verba Web Application	Any	443	TCP	Used for HTTPS-based web access
		Verba Media Streamer and Content Server Service	Any	10105	TCP	Media port for playback via HTTP
		Verba Media Streamer and Content Server Service	Any	10106	TCP	Media port for playback via HTTPS
		Verba Storage Management Service	Verba Recording Server	20111	TCP	Communication with Verba Storage Management services, used for secure file upload
		SQL Server (if co-located on Verba Media Repository)	All Verba Servers	1433	TCP	SQL connection
Verba Recording Server	Recording Director	Verba Unified Call Recorder Service	Verba Recording Server	10500	TCP	Recording Director - Media Recorder connection
	Media Recorder	Verba Unified Call Recorder Service	Any	16384 - 65535	UDP	Media port range
	Recording Director	Verba Unified Call Recorder Service	Any	5060	TCP	SIP signaling communication port
	Recording Director	Verba Unified Call Recorder Service	Any	5061	TCP	Secure SIP signaling communication port
	Recording Director Media Recorder	Verba Unified Call Recorder Service	All Verba Servers All Verba Desktop Agents (if used) (plus all playback stations if silent monitoring is used)	10031	TCP	Service API port

Firewall configuration for Genesys active recording deployments


This chapter summarizes the required firewall configuration for Genesys active recording deployments.

Server	Server Role	Service name	Source	Port	Protocol	Notes
SQL Server	-	-	All Verba Servers	1433	TCP	SQL connection
All Verba Servers	-	Verba Node Manager Agent	Verba Media Repository	4433	TCP	Central configuration from Verba Web Application
Verba Media Repository Server	Media Repository	Verba Web Application	Any	80	TCP	Used for HTTP-based web access
		Verba Web Application	Any	443	TCP	Used for HTTPS-based web access
		Verba Media Streamer and Content Server Service	Any	10105	TCP	Media port for playback via HTTP
		Verba Media Streamer and Content Server Service	Any	10106	TCP	Media port for playback via HTTPS
		Verba Storage Management Service	Verba Recording Server	20111	TCP	Communication with Verba Storage Management services, used for secure file upload
		SQL Server (if co-located on Verba Media Repository)	All Verba Servers	1433	TCP	SQL connection
Verba Recording Server	Recording Server	Verba Unified Call Recorder Service	Genesys Media Server	5060	TCP	SIP signaling communication port
		Verba Unified Call Recorder Service	Any	16384 - 65535	UDP	Media port range
		Verba Unified Call Recorder Service	All Verba Servers All Verba Desktop Agents (if used) (plus all playback stations if silent monitoring is used)	10031	TCP	Service API port

		Verba Genesys CTI Service	Verba Recording Server	11300	TCP	CTI service registration port
		Verba Genesys CTI Service	Verba Media Repository	10040	TCP	Service API port

Antivirus scanning exclusions for Verba servers

To ensure that the antivirus scanner does not interfere with the operation of the Verba system, you must exclude specific processes and directories for each Verba server or server role on which you run an antivirus scanner. The following processes and directories should be excluded:

 Directory and file locations listed below are the default locations for the Verba system. For any locations for which you did not use the default, exclude the locations you specified instead of the default locations specified in this article.

Media Repository and Recording Server Role:


Verba Processes:

Verba Service Name	Executable Name
Requirement for Java Services: <ul style="list-style-type: none">• Verba Avaya DMCC/JTAPI Service• Verba Cisco JTAPI Service• Verba Cisco Central Silent Monitoring Service• Verba Cisco Compliance Service• Verba Web Application	wrapper.exe
Verba Passive Recorder Service	verbaengine.exe
Verba Media Collector and Proxy Service	recorderproxy.exe
Verba Legacy Cisco Central Recorder Service	nativerecorder.exe
Verba Analogue and Radio Recorder Service (Verba General Media Recorder Service)	mediareceiver.exe
Verba Legacy Cisco Gateway Recorder Service	ciscogatewayrec.exe
Verba Labeling Service	label-processor.exe
Verba Media Utility Service (Verba Waveformatter Service)	waveform.exe
Verba Media Streamer and Content Server Service	mediastreamer.exe
Verba Legacy IP Trade Recorder Service	verbaiptrade.exe
Verba Screen Capture Multiplexer Service	multiplexer.exe
Verba Unified Call Recorder Service	unifiedrec.exe
Verba Active Recorder and Streamer Service	activerecorder.exe
Verba Storage Management Service = verbastorage.exe	verbastorage.exe
Verba Media Transcoder Service	transcoder.exe
Verba System Monitor Service	verbasysmon.exe
Verba Centile Connector	centile-connector.exe
Verba Node Manager Agent Service	verbaagent.exe

Verba SfB/Lync Announcement Service	rec-announcement.exe
Verba CDR and Archived Content Importer Service	cdrimport.exe
Verba SfB/Lync IM Recorder Service	lyncchatrecorder.exe
Verba Cisco MediaSense Connector	mediasense-connector.exe
Verba Speech Analytics Service	speech-analytics.exe
(Verba TroubleshootingTool)	verbacapture.exe
(Verba TroubleshootingTool)	verbareport.exe
Verba Web Application Service	tomcat9.exe

Built-in Microsoft SQL Server Express processes:

- %ProgramFiles%\Microsoft SQL Server\MSSQL{nn}.MSSQLSERVER\MSSQL\Binn\SQLServr.exe
- %ProgramFiles%\Microsoft SQL Server\MSRS{nn}.MSSQLSERVER\Reporting Services\ReportServer\Bin\ReportingServicesService.exe
- %ProgramFiles%\Microsoft SQL Server\MSAS{nn}.MSSQLSERVER\OLAP\Bin\MSMDSrv.exe

 Anti-virus exceptions for SQL Server processes are only necessary if the SQL Server is co-located with the Verba server. The list above shows the default paths and processes for a built-in MS SQL Express Server, but the installed SQL Server version and location can be different in each deployment.

The following table identifies versions for the paths. {nn} is the version value used in the instance ID.

Version	{NN}
SQL Server 2019 (15.x)	15
SQL Server 2017 (14.x)	14
SQL Server 2016 (13.x)	13
SQL Server 2014 (12.x)	12
SQL Server 2012 (11.x)	11

Directories and Files:

- The installation folder (%programfiles%\Verba)
- The configured media folder (%programfiles%\Verba\media)
- The configured log folder (%programfiles%\Verba\log)

Media Collector and Lync Filter Server Role:

Verba Processes:

Verba Service Name	Executable Name
Verba Legacy Remote Capture Service	remote-capture.exe
Verba Media Collector and Proxy Service	recorderproxy.exe

Verba SfB/Lync Call Filter Service	LyncFilterConsole.exe
Verba SfB/Lync Communication Policy Service	lyncethicalwall.exe
Verba SfB/Lync IM Filter Service	lyncimfilter.exe
Verba System Monitor Service	verbasysmon.exe
Verba Node Manager Agent Service	verbaagent.exe

Folders:

- The installation folder (%programfiles%\Verba)
- The configured log folder (%programfiles%\Verba\log)

Media Collector and Proxy Server Role:

Verba Processes:

Verba Service Name	Executable Name
Verba Legacy Remote Capture Service	remote-capture.exe
Verba Media Collector and Proxy Service	recorderproxy.exe
Verba System Monitor Service	verbasysmon.exe
Verba Node Manager Agent Service	verbaagent.exe

Folders:

- The installation folder (%programfiles%\Verba)
- The configured log folder (%programfiles%\Verba\log)

Announcement Server Role:

Verba Processes:

Verba Service Name	Executable Name
Verba SfB/Lync Announcement Service	rec-announcement.exe
Verba System Monitor Service	verbasysmon.exe
Verba Node Manager Agent Service	verbaagent.exe

Directories and Files:

- The installation folder (%programfiles%\Verba)
- The configured log folder (%programfiles%\Verba\log)

Speech Analytics Server Role:

Verba Processes:

Verba Service Name	Executable Name
--------------------	-----------------

Verba Labeling Service	label-processor.exe
Verba Speech Analytics Service	speech-analytics.exe
Verba System Monitor Service	verbasysmon.exe
Verba Node Manager Agent Service	verbaagent.exe

Directories and Files:

- The installation folder (%programfiles%\Verba)
- The configured media folder (%programfiles%\Verba\media)
- The configured log folder (%programfiles%\Verba\log)

Desktop Agent Role:

Verba Processes:

Verba Service Name	Executable Name
Verba Screen Capturing Service	agentcontroller.exe
Verba Screen Capturing Service	captureagent.exe
Verba Storage Management Service	verbastorage.exe
Verba System Monitor Service	verbasysmon.exe
Verba Node Manager Agent Service	verbaagent.exe

Directories and Files:

- The installation folder (%programfiles%\Verba)
- The configured media folder (%programfiles%\Verba\media)
- The configured log folder (%programfiles%\Verba\log)

Offline Player Role:

Verba Processes:

- verbaplayer.exe

Directories and Files:

- The installation folder (%programfiles%\Verba)

SQL Server installation

To learn more about selecting the SQL Server version, editions and requirements, see [SQL Server requirements](#).


Installing a Microsoft SQL Server instance

In the Verba install kit, we provide a simple, unattended installation procedure for Microsoft SQL Server Express (see the Prerequisites Installer Tool).

For information on how to install other Microsoft SQL server editions, please refer to the following articles.

[https://technet.microsoft.com/en-us/library/bb500395\(v=sql.110\).aspx](https://technet.microsoft.com/en-us/library/bb500395(v=sql.110).aspx)

[https://msdn.microsoft.com/library/bb500469\(v=sql.120\).aspx](https://msdn.microsoft.com/library/bb500469(v=sql.120).aspx)

 When installing .NET framework as a prerequisite of MS SQL server, make sure that **HTTP Activation is NOT** installed (can be found under WCF Services)


Feature selection

The following features need to be selected during the install:

- Database Engine Services
- Full -Text and Semantic Extractions for Search
- (Management Tools - Complete) Not necessary but recommended.

On the **collation** tab please make sure that the **case-sensitive** checkbox is left UNCHECKED. Verba requires a case-insensitive server.

 Some of the options may be part of the MS SQL Management Studio install pack if you are using a separate installer.

 After the Full-Text Search feature added or removed from an existing SQL Server installation, the Verba Web Application Service has to be restarted.

Instance configuration

It is recommended to install the Verba database as the default instance, however, the system supports named instances as well.

Database configuration

The **Containment type** setting of the Verba database has to be left on **None**.

Services

For the Verba system, the following SQL Server services must be enabled and running (other services are not required):

- SQL Server
- SQL Server Browser if named instances are used
- SQL Server Agent to run the maintenance jobs (not available on Express Edition)

Services accounts

Use the built-in System account and set it to Network service and check the SQL Server Agent to start at the end of the setup.

Collation

Choose the collation based on the requirement. The system does not support Case Sensitive (CS) collations, only Case Insensitive (CI) collations are supported.

Account provisioning

If you would like to use SQL authentication, then select **Mixed Mode authentication**. Set the sa password and **make a note of it**. The Verba installer will need this information.

If you would like to use Windows Authentication, then select **Windows Authentication**.

Make sure you have the necessary database roles assigned to the user account which is configured for the system. For more information see [SQL Server requirements](#).

Using the Verba Prerequisites tool to install SQL Server Express edition

MS SQL Server Express Edition unattended installer is included in the Verba install media.

Please, follow the steps below to install MS SQL Server Express Edition:

Step 1 - Copy the Verba Installation kit to the appropriate drive.


Step 2 - Click on the **setup.exe** file

Step 4 - Select the type of Verba server that you will be installing on this machine. (Single server solution or Media Repository)

Step 5 - Click on **Install SQL Server Express** and then on the button with the same name

Step 6 - The unattended installation starts automatically.

Set the **sa** password in the corresponding batch file. This information will need to be entered during the installation process of the Verba servers.

 Verba utilizes the SQL Server's full-text index feature when searching for specific phrases in Instant Message recordings. The full-text index feature is not part of SQL Server Express edition by default, it is only included in SQL Server Express with Advanced Services.

Install the Verba software

- [Prerequisites](#)
- [Installing the required prerequisites](#)
- [Installing a Verba Media Repository](#)
- [Installing a Verba Recording Server](#)
- [Installing a Verba Single Server solution](#)
- [Installing a Verba Announcement Server](#)
- [Installing a Verba Speech Analytics Server](#)
- [Installing the Verba Media Collector and Proxy component](#)
- [Installing the Verba Skype for Business - Lync Filter](#)
- [Changing the role of a Verba server](#)
- [Installer Parameters and Unattended Installation](#)

Prerequisites

The following table lists all required prerequisites for the available Verba server roles:

Verba Server Role	Prerequisite	Mandatory / Optional	Download / Notes	Included in the installer package
Application Server / Media Repository and Recording Server	Java SE 11 Runtime Environment (Windows x64)	Mandatory	Both Oracle and OpenJDK Java 11 runtimes are supported. OpenJDK JRE 11 download: https://adoptium.net/temurin/releases/?version=11 (Operating System: Windows, Architecture: x64, Package Type: JRE, Version: 11)	Yes (OpenJDK)
	Visual Studio C++ Runtime 2015, 2017 and 2019 (x64)	Mandatory	https://aka.ms/vs/16/release/VC_redist.x64.exe If the installer fails you need to download and install the following Windows Update packages: <ul style="list-style-type: none"> • KB2919355 • KB2999226 	Yes
	Microsoft .Net Framework 4.8	Mandatory	https://dotnet.microsoft.com/download/dotnet-framework/net48	Yes
	Media Foundation	Optional	Required for screen capture multiplexing and media transcoding for the following services: <ul style="list-style-type: none"> • Verba Storage Management Service • Verba Screen Capture Multiplexer Service • Verba Import Service • Verba Speech Analytics Service • Verba Media Streamer and Content Server Service • Verba Media Utility Service 	No
	WinPcap Service	Optional	Required for Skype for Business / Lync recording and network port mirroring based recording http://www.winpcap.org/install/bin/WinPcap_4_1_3.exe	Yes
	Microsoft ODBC Driver 17 (x64)	Mandatory	https://www.microsoft.com/en-us/download/details.aspx?id=56567	Yes
	Skype for Business/Lync Management Shell	Optional	Required for Skype for Business / Lync Archive import https://technet.microsoft.com/en-us/library/dn933921.aspx	No
Application Server / Media Repository	Java SE 11 Runtime Environment (Windows x64)	Mandatory	Both Oracle and OpenJDK Java 11 runtimes are supported. OpenJDK JRE 11 download: https://adoptium.net/temurin/releases/?version=11 (Operating System: Windows, Architecture: x64, Package Type: JRE, Version: 11)	Yes (OpenJDK)
	Visual Studio C++ Runtime 2015, 2017 and 2019 (x64)	Mandatory	https://aka.ms/vs/16/release/VC_redist.x64.exe If the installer fails you need to download and install the following Windows Update packages: <ul style="list-style-type: none"> • KB2919355 • KB2999226 	Yes

	Microsoft .Net Framework 4.8	Mandatory	https://dotnet.microsoft.com/download/dotnet-framework/net48	Yes
	Media Foundation	Optional	Required for screen capture multiplexing and media transcoding for the following services: <ul style="list-style-type: none"> • Verba Storage Management Service • Verba Screen Capture Multiplexer Service • Verba Import Service • Verba Speech Analytics Service • Verba Media Streamer and Content Server Service • Verba Media Utility Service 	No
	Microsoft ODBC Driver 17 (x64)	Mandatory	https://www.microsoft.com/en-us/download/details.aspx?id=56567	Yes
	Skype for Business/Lync Management Shell	Optional	Required for Skype for Business / Lync Archive import https://technet.microsoft.com/en-us/library/dn933921.aspx	No
Recording Server	Java SE 11 Runtime Environment (Windows x64)	Mandatory	Both Oracle and OpenJDK Java 11 runtimes are supported. OpenJDK JRE 11 download: https://adoptium.net/temurin/releases/?version=11 (Operating System: Windows, Architecture: x64, Package Type: JRE, Version: 11)	Yes (OpenJDK)
	Visual Studio C++ Runtime 2015, 2017 and 2019 (x64)	Mandatory	https://aka.ms/vs/16/release/VC_redist.x64.exe If the installer fails you need to download and install the following Windows Update packages: <ul style="list-style-type: none"> • KB2919355 • KB2999226 	Yes
	Microsoft .Net Framework 4.8	Mandatory	https://dotnet.microsoft.com/download/dotnet-framework/net48	Yes
	WinPcap Service	Optional	Required for Skype for Business / Lync recording and network port mirroring based recording http://www.winpcap.org/install/bin/WinPcap_4_1_3.exe	Yes
	Microsoft ODBC Driver 17 (x64)	Mandatory	https://www.microsoft.com/en-us/download/details.aspx?id=56567	Yes
	Media Foundation	Optional	Required for screen capture multiplexing and media transcoding for the following services: <ul style="list-style-type: none"> • Verba Import Service 	No
		Microsoft .Net Framework 4.8	Mandatory	https://dotnet.microsoft.com/download/dotnet-framework/net48
Verba Media Collector and Lync Filter	Microsoft .Net Framework 4.8	Mandatory	https://dotnet.microsoft.com/download/dotnet-framework/net48	Yes (in the main package)
	WinPcap Service	Mandatory	Required for Lync recording and network port mirroring based recording http://www.winpcap.org/install/bin/WinPcap_4_1_3.exe	Yes (in the main package)
Verba Media Collector and Proxy Server	Microsoft .Net Framework 4.8	Mandatory	https://dotnet.microsoft.com/download/dotnet-framework/net48	Yes (in the main package)

	WinPcap Service	Mandatory	Required for Skype for Business / Lync recording and network port mirroring based recording http://www.winpcap.org/install/bin/WinPcap_4_1_3.exe	Yes (in the main package)
Verba Announcement Server	Microsoft .Net Framework 4.8	Mandatory	https://dotnet.microsoft.com/download/dotnet-framework/net48	Yes (in the main package)
	Unified Communications Managed API 4.0 Runtime	Mandatory	https://www.microsoft.com/en-us/download/details.aspx?id=34992	No
Verba Speech Analytics Server	Microsoft .Net Framework 4.8	Mandatory	https://dotnet.microsoft.com/download/dotnet-framework/net48	Yes (in the main package)
	Microsoft ODBC Driver 17 (x64)	Mandatory	https://www.microsoft.com/en-us/download/details.aspx?id=56567	Yes (in the main package)
	Media Foundation	Optional	Required for media transcoding for the following services: <ul style="list-style-type: none"> Verba Speech Analytics Service 	No
	Visual Studio C++ Runtime 2015, 2017 and 2019 (x64)	Mandatory	https://aka.ms/vs/16/release/VC_redist.x64.exe If the installer fails you need to download and install the following Windows Update packages: <ul style="list-style-type: none"> KB2919355 KB2999226 	Yes (in the main package)
Verba Desktop Recorder	Visual Studio C++ Runtime 2015, 2017 and 2019 (x64)	Mandatory	https://aka.ms/vs/16/release/VC_redist.x64.exe If the installer fails you need to download and install the following Windows Update packages: <ul style="list-style-type: none"> KB2919355 KB2999226 	Yes (in the main package)
	Microsoft ODBC Driver 17 (x64)	Mandatory	Required for advanced SQL Server features: always-on, failover partner https://www.microsoft.com/en-us/download/details.aspx?id=56567	Yes (in the main package)

Installing the required prerequisites

For a detailed overview on the prerequisites, visit the [Prerequisites](#) page.

The Verba installer kit contains a prerequisite checking tool. You can use it to install all the third party software prerequisites before starting the Verba installer.

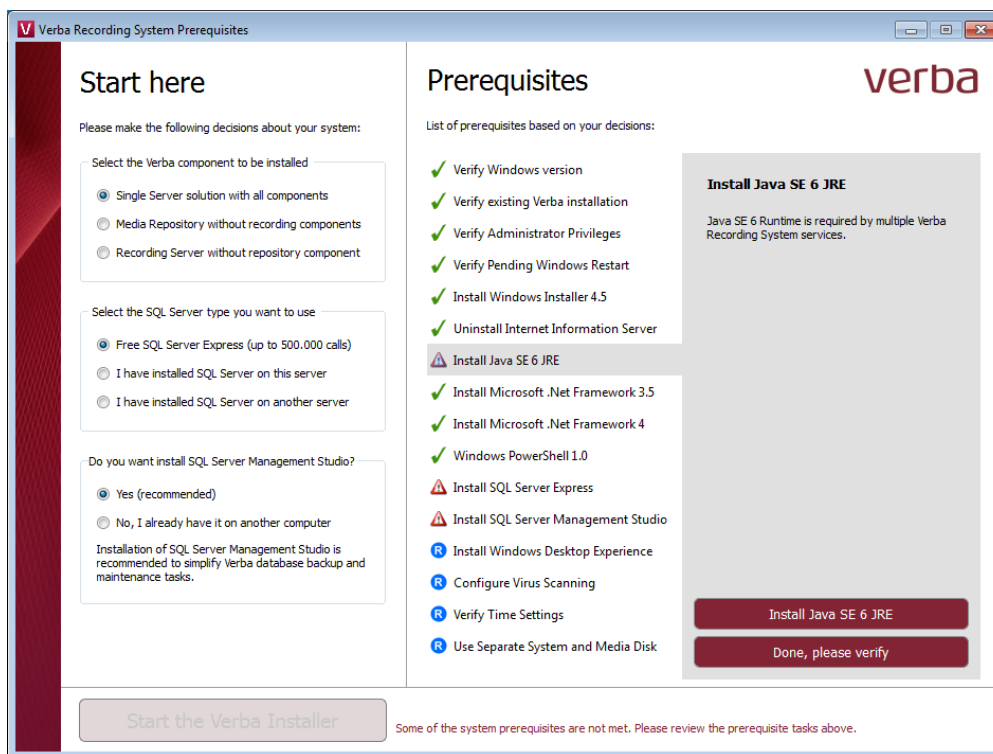
The tool is only suitable for the following server roles:

- Verba Media Repository and Recording Server
- Verba Media Repository
- Verba Recording Server
- Verba Lync Filter
- Verba Media Collector and Lync Filter
- Verba Media Collector and Proxy Server
- Verba Announcement Server
- Verba Speech Analytics Server

Please follow the steps below to install the prerequisites for your Verba system:

Step 1 - Unzip the Verba Install Kit to a local drive of the server.

Step 2 - Launch the prerequisite tool by starting setup.exe in the VerbaInstallKit folder. The following image illustrates this step.



Step 3 - Select the Verba server role to be installed in the top right corner. Depending on your choice, the list of prerequisites on the right will dynamically change to show only the required software for that Verba component.

Step 4 - Select the SQL server you want to use. The Verba installation package contains the free Microsoft SQL Server Express edition. It's recommended that you install it if you don't have a separate SQL database server in your system.

Step 5 - Decide if you want to install SQL Server Management Studio on this server for easier database management (recommended).

Step 6 - Use the list on the right to check, install and verify the required third party software. They are included in the Verba installation package, so you can install them by selecting them from the list then clicking on the install button located at the bottom of the list.

Step 7 - After a prerequisite is installed, click the **Done, please verify** button, to verify it.


Step 8 - Repeat steps 6 and 7 until all the prerequisites are installed.

Step 9 - Click **Start the Verba Installer** to start installing the Verba Recording System.

After this point please refer to the corresponding article depending on the server role you chose to install.

- Media Repository: <http://kb.verba.com/display/docs/Installing+a+Verba+Media+Repository>
- Recording Server: <http://kb.verba.com/display/docs/Installing+a+Verba+Recording+Server>
- Single Server: <http://kb.verba.com/display/docs/Installing+a+Verba+Single+Server+solution>

Installing a Verba Media Repository

 If you haven't already done so, please make sure all the prerequisites are installed for your Media Repository. Refer to <http://kb.verba.com/display/docs/Installing+the+required+prerequisites>

The Verba Media Repository is the central controlling component of the Recording System. It contains the management web application and various other services necessary for the system to function. This component should always be installed first when deploying a new system. If you don't have a separate SQL server to install the database on, this server will run the Verba database services as well.


Please follow the steps below to install a Verba Media Repository. Note that, all Installer components must be run as Administrator.

Step 1 - The install kit starts installing Verba components. Simply press the **Next** button to start the installation.

Step 2 - Read the Verba license agreement carefully before you check the "I accept the terms in the License Agreement" checkbox, then click **Next** button.

Step 3 - Select the **Media Repository** role from the list. Click **Next**.

Step 4 - Select the destination folder for Verba system and the desired location of the media files. You can change the default setting by clicking on the Change button and selecting another folder. Network share also can be provided for the media folder. If you have finished the destination folder configuration, press the **Next** button.

 Drive root cannot be provided for the media folder (ex: D:\). A folder has to be created.

Step 5a - If the server is going to be the first Media Repository server in the deployment, and pre-generated certificates won't be used, then select the "**Generate Certificate Signed by Verba Media Repository CA**" option, and check the "**First Media Repository in the deployment**" checkbox. Click on the **Generate** button, and in the Generate the Verba Server Certificate window click **Generate**. Finally, click on the **Next** button. (If this option is being used, then Step 5b and Step 5c can be skipped.)

Step 5b - If the server won't be the first Media Repository server in the deployment, and pre-generated certificates won't be used, then select the "**Generate Certificate Signed by Verba Media Repository CA**" option, then click on the **Generate** button. In the Generate the Verba Server Certificate window provide the address of the first Media Repository server, the administrator username and password, then click **Generate**. Finally, click on the **Next** button. (If this option is being used, Step 5c can be skipped.)

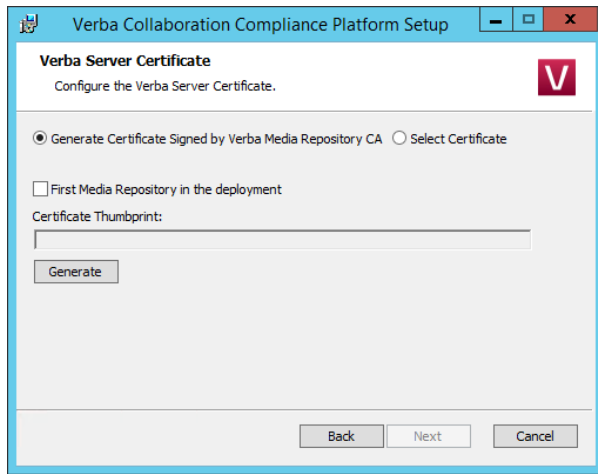
Step 5c - If there is an existing certificate from a previous Verba installation (in case of reinstall or upgrade), or a pre-generated certificate for the server exists (requested from a

Certificates generated by Verba CA vs pre-generated certificates

In case of using the Verba-generated certificates, the first Media Repository server becomes a CA also. During the installation of the other Verba components, the server certificates will be requested from this CA. This is done through the TCP port 443 with SSL. The server certificates and the CA certificate will be placed in the certificate stores of the servers automatically, to the Personal folder. The certificates generated by the Verba CA uses SHA512 for the signature algorithm, and RSA2048 for the public key.

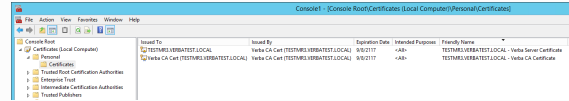
If certificates are generated for the Verba servers in advance using an other CA, then make sure that the certificates are placed into the certificate stores of the servers under the Personal folder, and the CA certificates are placed into the Personal or into the Trusted Root Certification Authorities folder. The only requirement for the server certificates is making the private key exportable.

local or a 3rd party CA), then select the "**Select Certificate**" option, then click on the **Browse** button. If the server was a CA previously, then select the CA certificate also by clicking on the **Browse** button under the CA Certificate Thumbprint.



Certificates generated by the Verba CA

Based on the Friendly Name of the certificates the server and the CA certificate can be identified easily. On the screenshot, the first one is the server certificate and the second one is the CA certificate.



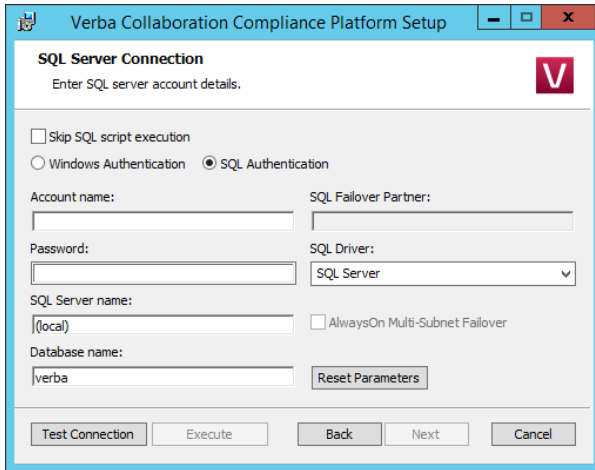
Step 6.1 - The Verba installer is asking for the MS SQL Server connection details. These settings will be used for all Verba services on the server, and the same settings has to be used during the installation of the other Verba components also.

- Both SQL server based and windows authentication is supported. If a domain account will be used for the SQL connection, then select **Windows Authentication**. In case of windows authentication, the Account name has to be provided in UPN or domain\username format. Please provide a **DB Creator** role user account for the connection.
- The server name can be entered either as an IP address or an FQDN.
- The Verba database doesn't have to be created in advance. The installer will create a database with the name given in the "Database Name" setting, and build the schema.
- If SQL Mirroring is being used or AlwaysOn with Multi-Subnet failover, then a different SQL Driver has to be selected. In this case, the driver has to be installed on the server.

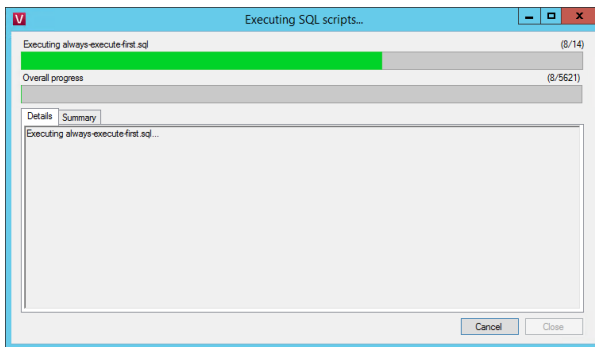
Step 6.2 - Click '**Test Connection**' to verify your input.

Database connection troubleshooting tips

- Try to ping the database server. Try to connect to the 1433 port on the database server. (telnet or Test-NetConnection)
- Check if the user has the necessary roles assigned, refer to [SQL Server requirements](#) for more information
- If Windows Authentication used then check if the user has the Local Administrator group membership and the 'Logon as a service right'.
- Check if the correct instance name is provided at the SQL Server name. If there are multiple instances, then the SQL Server Browser service must run on the SQL server side.
- If you installed SQL Server Express Edition, then check if the TCP/IP protocol is enabled under the SQL Server Network Configuration in the SQL Server Configuration Manager.



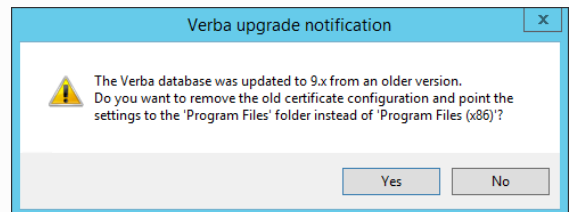
Step 6.3 - If the test was successful, click on the **Execute** button. The installer will start executing the scripts on the database, so it created the database schema. In the case of upgrade, the installer upgrades the existing schema. The script log will be saved to C:\Users\[user]\AppData\Local\Temp\ folder. If an error occurs during the script execution, it can be restarted by closing the window, then clicking on the Execute button again in the installer window.



Step 6.3 - Click on the **Close** button. In the installer window, click **Next**.

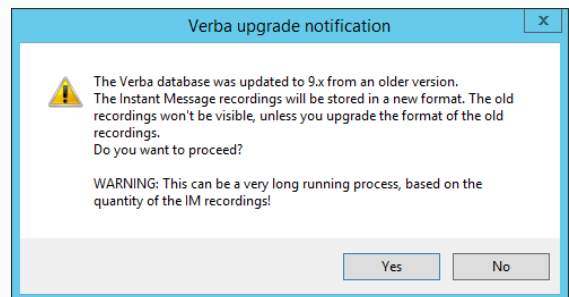
Upgrading from Verba 8.x to Verba 9.x

From version 9.0, the Verba software changed to x64 platform from x86, and also introduced a new Windows certificate-based secure API for the internal connection between the Verba services. When upgrading from Verba 7.x or 8.x, the installer offers changing the configuration stored in the database according to the new settings. In this case, all settings pointing to the "Program Files (x86)" folder will be changed to "Program Files", and all settings related to the old security configuration will be removed.

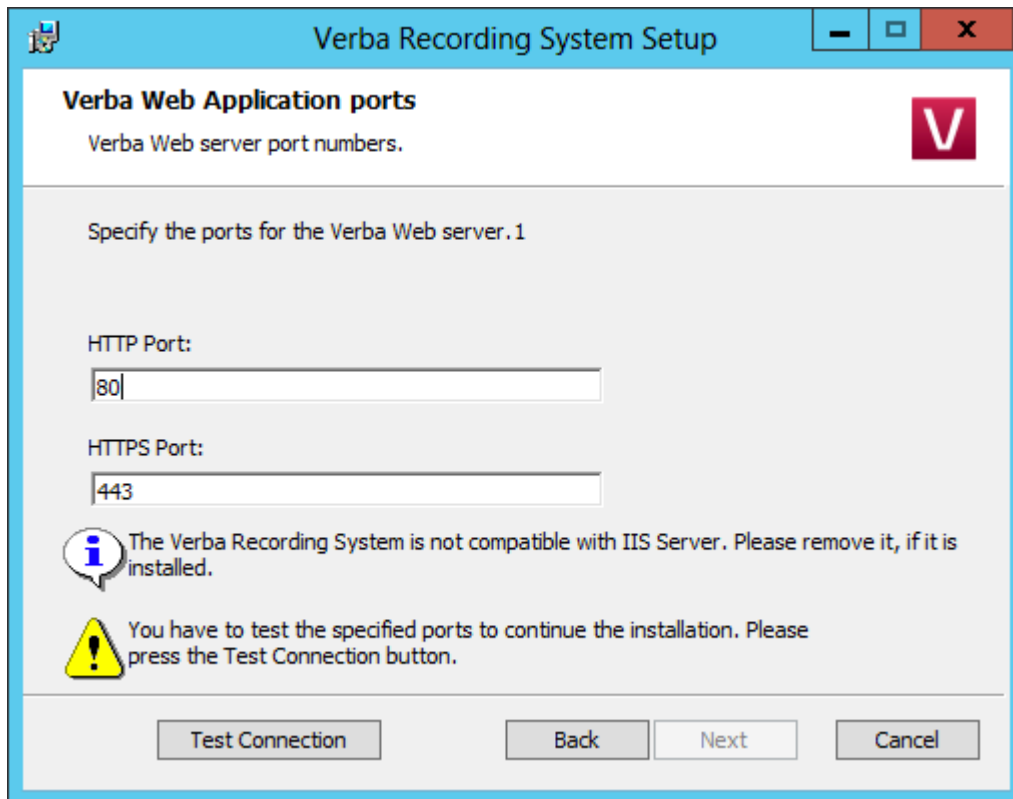


The installer also offers upgrading the schema of the IM recordings. If this step is skipped, then the old recordings won't be visible in the Verba web interface.

Note that this step can take hours to execute!



Step 7 - Please specify the ports for running the Verba web server. Click the **Test Connection** button to check if they are free. If one of them is taken you will be asked for another port number (you are not allowed to run more than one HTTP server on the same port). It is recommended to use the default 80 and 443 port numbers. If successful, click Next.



Step 8a - If this is a new Verba installation, and there is no pre-created SSL certificate for the HTTPS connection, then select the **"Generate Self-signed Certificate"** option, then click on the **Generate** button. In the "Generate the Verba Web server SSL Certificate" window, enter a **password** for the certificate, provide the Subject Alternative names, then click **Generate**. In this case a verba-tomcat.crt and a verba-tomcat.key file will be generated in the C:\ root. Click on the **Next** button. (If this option is being used, then Step 9b can be skipped)

Step 8b - If this is not a new Verba installation (in case of reinstall or upgrade), or there is a pre-created SSL certificate for the HTTPS connection, then select the **"Select Certificate"** option. Under the Certificate Path, click on the **Browse** button, and provide the **.crt file**. Under the Certificate Key Path click on the **Browse** button, and provide the **.key file**. Provide the password of the SSL certificate. Click on the **Next** button.

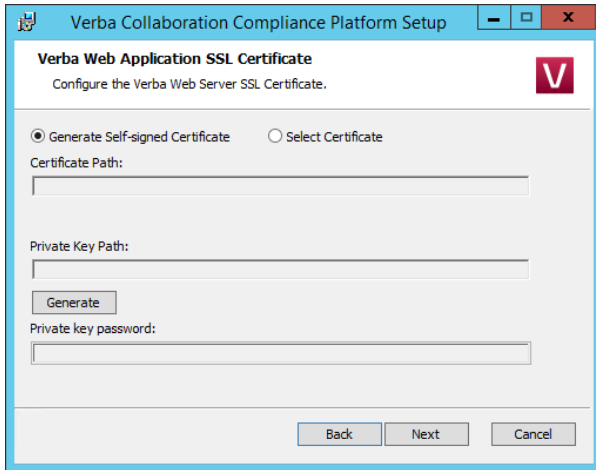
Subject Alternatives Names for the SSL Certificate

To make sure that the browser always going to trust the certificate, provide every possible address at the Subject Alternative Names. The recommended addresses are:

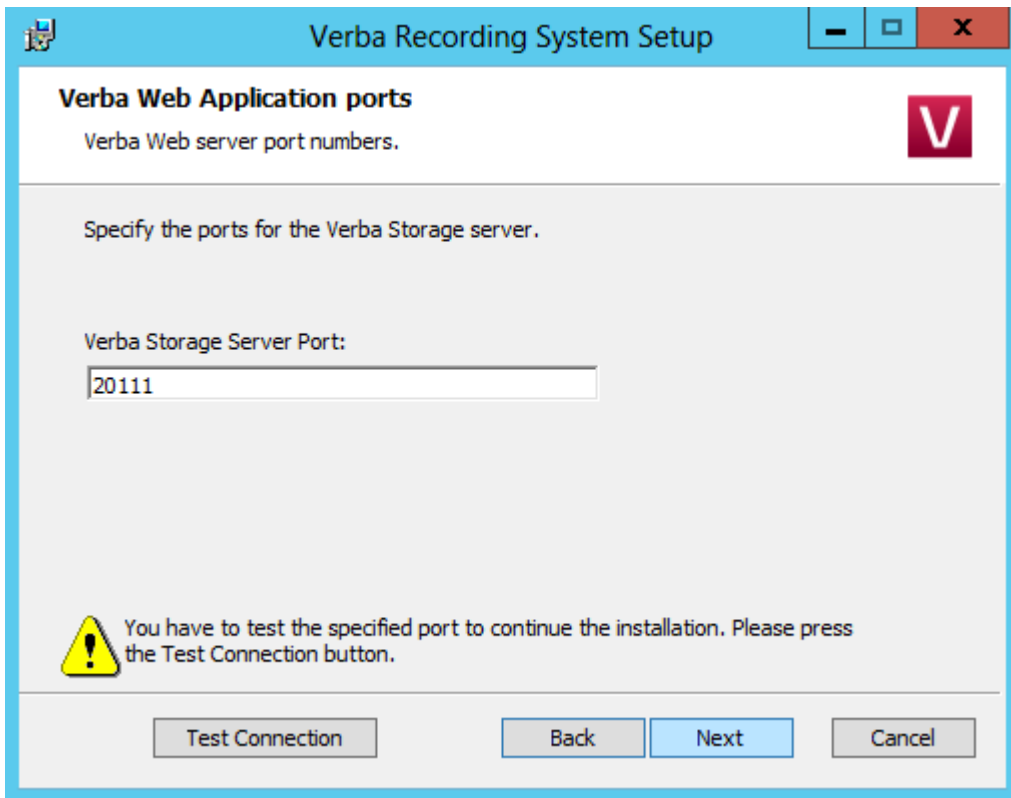
- The hostname of the server.
- The FQDN of the server.
- The IP address of the server.
- "localhost"
- Aliases
- If load-balancer is being used, then it's hostname, FQDN and IP address.

Certificates in .pfx or .p12 format

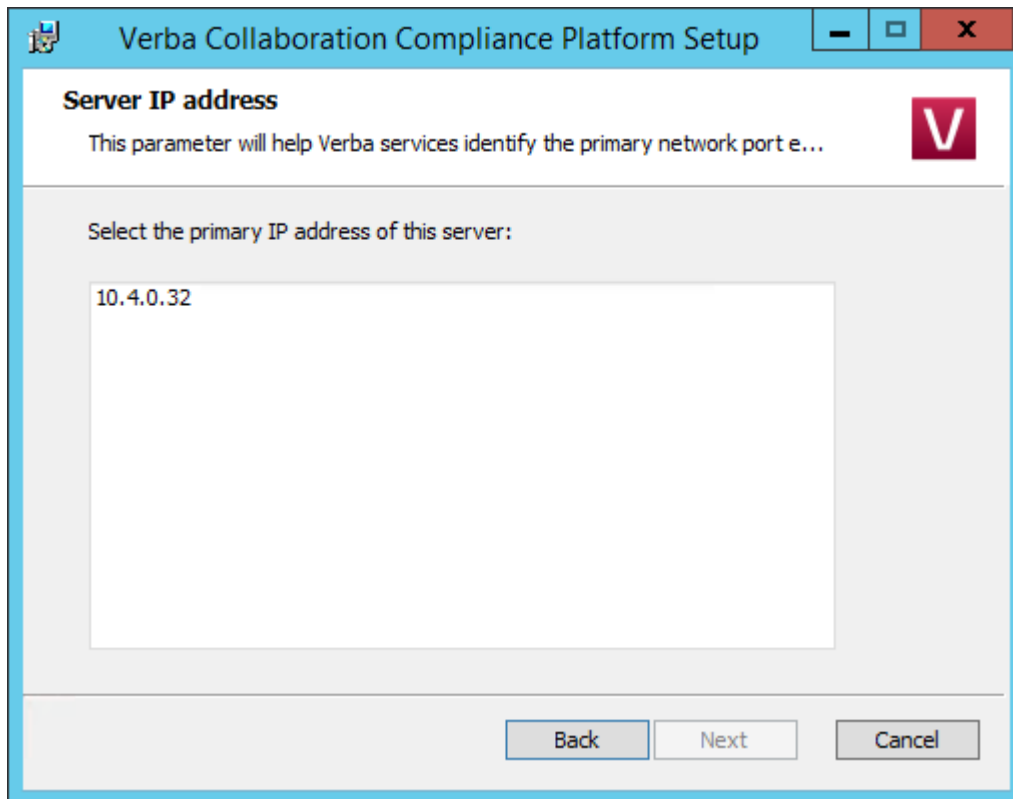
If the SSL certificate is in .pfx or .p12 format, then it has to be converted to a pair of .crt and .key files. For the conversion process, please refer to the "Creating .key and .crt files from .p12 or .pfx file" section in the [Installing an SSL certificate for HTTPS access](#) article.



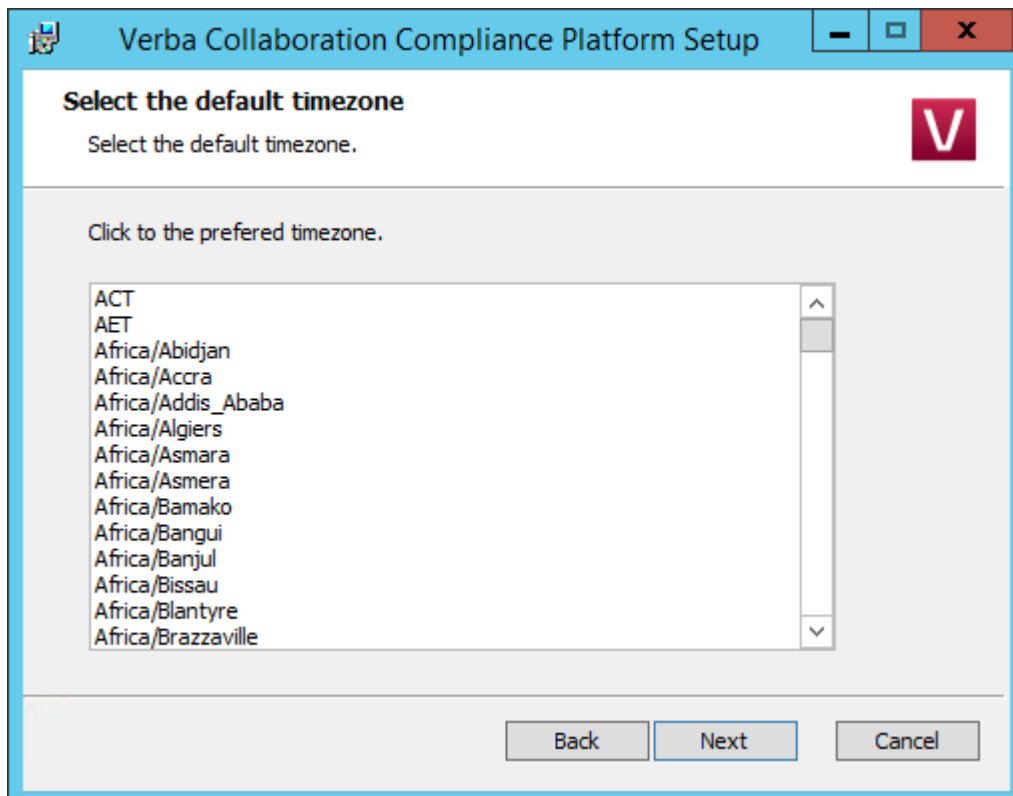
Step 9 - Please specify a free port for the Verba storage server. Use the **Test Connection** button to check the port's availability. If successful, click **Next**.



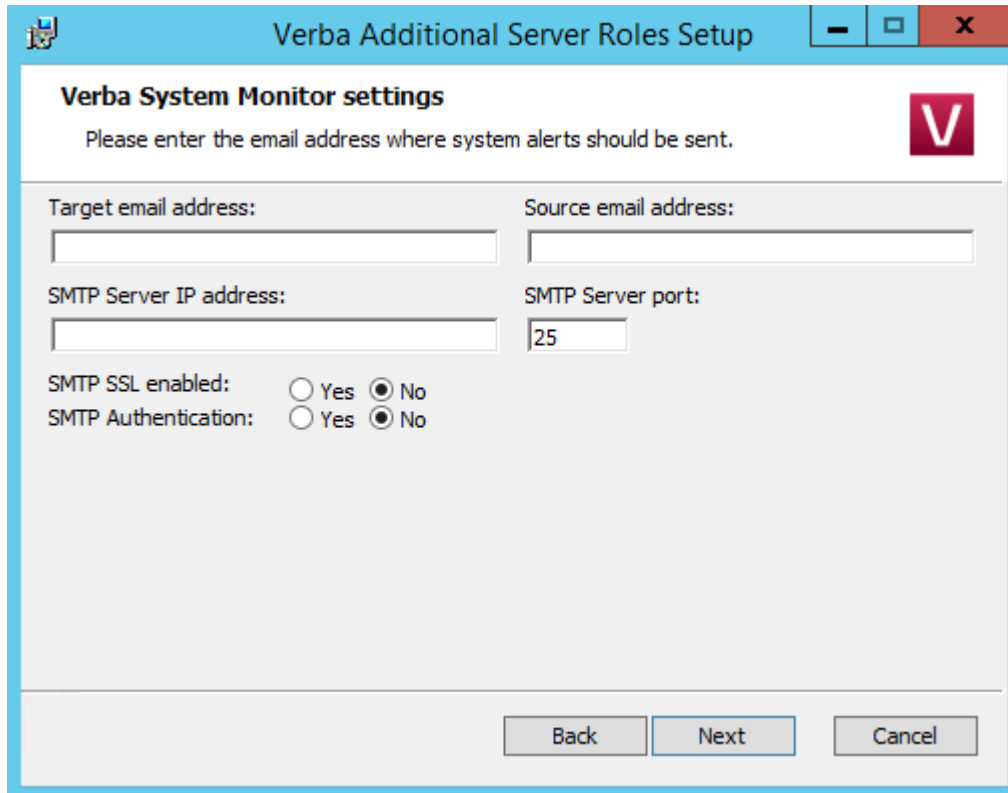
Step 10 - Select the primary IP address of the server from the list, then click **Next**.



Step 11 - Select the desired time zone from the list, then click **Next**.

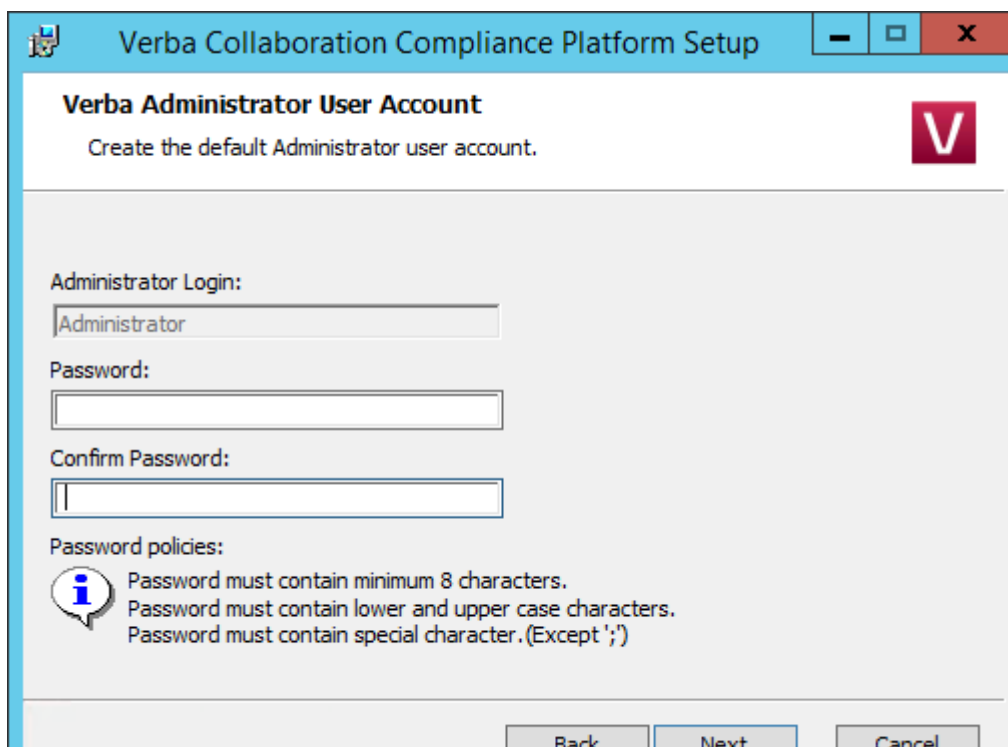


Step 12 - Please provide a target email address, a source email address and an SMTP server address for system alerts. If authentication required then please enter the credentials. The target email address will receive alerts concerning the various services of the recording system. This step can be skipped and the details can be provided or modified after the installation. When you are done, click **Next**.



The screenshot shows a Windows-style dialog box titled "Verba Additional Server Roles Setup". The main heading is "Verba System Monitor settings" with a red 'V' logo. Below the heading is the instruction: "Please enter the email address where system alerts should be sent." The form contains four input fields: "Target email address:", "Source email address:", "SMTP Server IP address:", and "SMTP Server port:". The "SMTP Server port" field has the value "25" entered. Below these fields are two rows of radio buttons: "SMTP SSL enabled:" with "Yes" and "No" options (where "No" is selected), and "SMTP Authentication:" with "Yes" and "No" options (where "No" is selected). At the bottom of the dialog are three buttons: "Back", "Next", and "Cancel".

Step 13 - Enter a password for the Administrator login then click **Next**.



The screenshot shows a Windows-style dialog box titled "Verba Collaboration Compliance Platform Setup". The main heading is "Verba Administrator User Account" with a red 'V' logo. Below the heading is the instruction: "Create the default Administrator user account." The form contains three input fields: "Administrator Login:" with the value "Administrator" entered, "Password:", and "Confirm Password:". Below these fields is a section for "Password policies:" which includes an information icon and three bullet points: "Password must contain minimum 8 characters.", "Password must contain lower and upper case characters.", and "Password must contain special character. (Except ';')". At the bottom of the dialog are three buttons: "Back", "Next", and "Cancel".



Step 14 - Enter a password for the Verba API user then click **Next**. Note that this user going to be required at the installation of the other Verba components.

The screenshot shows a Windows-style window titled "Verba Collaboration Compliance Platform Setup". The main content area is titled "Verba API User Account" with the instruction "Create the API user account." and a red "V" logo. Below the title, there are three input fields: "API User Login:" containing the text "verbaapi", "Password:", and "Confirm Password:". Underneath these fields, a section titled "Password policies:" includes an information icon and three bullet points: "Password must contain minimum 8 characters.", "Password must contain lower and upper case characters.", and "Password must contain special character. (Except ';')". At the bottom of the window, there are three buttons: "Back", "Next", and "Cancel".

Step 15 - Click **Next** again to start installing the services. When it's done, click **Finish** to exit the installer.

Installing a Verba Recording Server

i If you haven't already done so, please make sure all the prerequisites are installed for your Recording Server. Refer to <http://kb.verba.com/display/docs/Installing+the+required+prerequisites>

The Verba Recording Server role is responsible for the various recording tasks. The media files will only be stored temporarily on these servers, they will upload the media files to the configured media repository and apply updates to the Verba database (usually located on the Media Repository server or a separate SQL server).

Before starting to install a Recording Server, please make sure that you already have a Media Repository installed and that the PC you are installing the Recording Server on can reach the server containing the database.

Step 1 - The install kit starts installing Verba components. Simply press the **Next** button to start the installation.

Step 2 - Read the Verba license agreement carefully before you click **Next** button.

Step 3 - Select the **Recording Server** role from the list. Click **Next**.

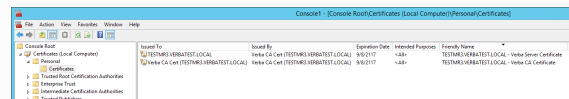
Step 4 - Select the destination folder for Verba system and the desired location of the media files. You can change the default setting by clicking on the Change button and selecting another folder. Please note that this is just a temporary folder for the media files. After the recording completed the files will be uploaded to the right location. If you have finished the destination folder configuration, press the **Next** button.

i Drive root cannot be provided for the media folder (ex: D:\). A folder has to be created. In case of the Recording Server, the media folder is just a temporary folder. The recording services are working in this folder during the recording, but when the recording completes, the files usually uploaded to a Media Repository server or to another location. Therefore, this always should be on the local disk.

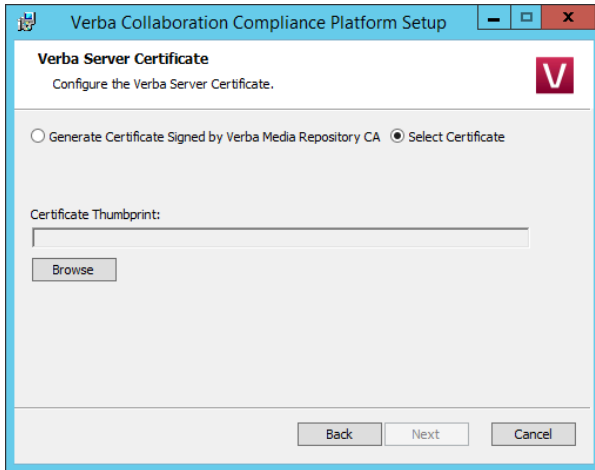
Step 5a - If a Verba CA is being used, then select the **"Generate Certificate Signed by Verba Media Repository CA"** option, then click on the **Generate** button. In the Generate the Verba Server Certificate window provide the address of the first Media Repository server, the Verba administrator username and password, then click **Generate**. Finally, click on the **Next** button. (If this option is being used, Step 5b can be skipped.)

Step 5b - If there is an existing certificate from a previous Verba installation (in case of reinstall or upgrade), or a pre-generated certificate for the server exists (requested from a local or a 3rd party CA), then select the **"Select Certificate"** option, then click on the **Browse** button.

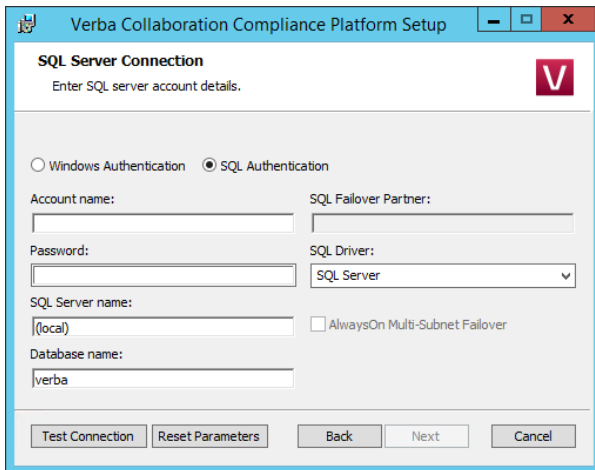
i **Certificates generated by the Verba CA**
Based on the Friendly Name of the certificates the server and the CA certificate can be identified easily. On the screenshot, the first one is the server certificate and the second one is the CA certificate.



Issued To	Issued By	Expiration Date	Intended Purpose	Friendly Name
TESTMRS-HERBATTEST.LOCAL	Verba CA Cert (TESTMRS-HERBATTEST.LOCAL)	8/8/2117	code	TESTMRS-HERBATTEST.LOCAL - Verba Server Certificate
Verba CA Cert (TESTMRS-HERBATTEST.LOCAL)	Verba CA Cert (TESTMRS-HERBATTEST.LOCAL)	8/8/2117	code	TESTMRS-HERBATTEST.LOCAL - Verba CA Certificate



Step 6 - The Verba installer is asking for the MS SQL Server credentials. The server name can be entered either as an IP address or an FQDN. Both SQL server based and windows authentication is supported. In case of windows authentication, the Account name has to be provided in UPN or domain\username format. All Verba servers and components have to use the same database! If SQL Mirroring is being used or AlwaysOn with Multi-Subnet failover, then a different SQL Driver has to be selected. In this case, the driver has to be installed on the server. Click ' **Test Connection**' to verify your input. If the tests were successful, click **Next**.



Step 7 - Provide the address of the Verba Media Repository server, and the API user password. The API user created at **Step 14** during the installation of the Media Repository server.



Database connection troubleshooting tips

- Try to ping the database server. Try to connect to the 1433 port on the database server. (telnet or Test-NetConnection)
- Check if the user has the necessary roles assigned, refer to [SQL Server requirements](#) for more information
- If Windows Authentication used then check if the user has the Local Administrator group membership and the 'Logon as a service right'.
- Check if the correct instance name is provided at the SQL Server name. If there are multiple instances, then the SQL Server Browser service must run on the SQL server side.
- If you installed SQL Server Express Edition, then check if the TCP/IP protocol is enabled under the SQL Server Network Configuration in the SQL Server Configuration Manager.

Verba Collaboration Compliance Platform Setup

Node Registration

Enter your Verba Web Application URL and API User Credentials.

Verba Web Application Hostname:

API Login:

API Password:

Test Connection Back Next Cancel

Step 8 - Select the primary IP address of the server from the list, then click **Next**.

Verba Collaboration Compliance Platform Setup

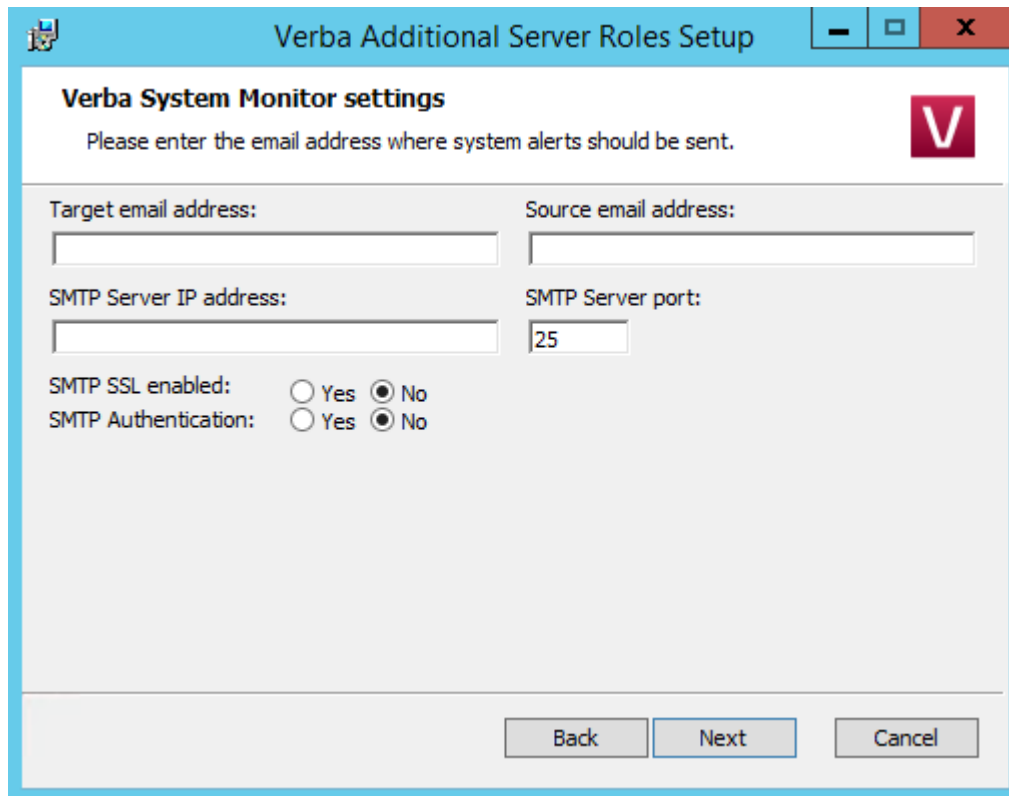
Server IP address

This parameter will help Verba services identify the primary network port e...

Select the primary IP address of this server:

Back Next Cancel

Step 9 - Please provide a target email address, a source email address and an SMTP server address for system alerts. If authentication required then please enter the credentials. The target email address will receive alerts concerning the various services of the recording system. This step can be skipped and the details can be provided or modified after the installation. When you are done, click **Next**.



The screenshot shows a Windows-style dialog box titled "Verba Additional Server Roles Setup". The main content area is titled "Verba System Monitor settings" and includes a sub-instruction: "Please enter the email address where system alerts should be sent." The settings are organized into four input fields: "Target email address:", "Source email address:", "SMTP Server IP address:", and "SMTP Server port:". The "SMTP Server port" field contains the value "25". Below these fields are two radio button options: "SMTP SSL enabled:" with "Yes" and "No" options, and "SMTP Authentication:" with "Yes" and "No" options. Both "No" options are selected. At the bottom of the dialog are three buttons: "Back", "Next", and "Cancel".

Step 10 - Click **Next** again to start installing the services. When it's done, click **Finish** to exit the installer.

Installing a Verba Single Server solution

i If you haven't already done so, please make sure all the prerequisites are installed for your Single Server. Refer to <http://kb.verba.com/display/docs/Installing+the+required+prerequisites>

The Single Server role combines the features and functions of a Verba Recording Server and Media Repository in one server. The management interface, system services, and recording functions will all run on the same server. If you don't use a separate SQL server, the database will be located on this server as well.

Please follow the steps below to install a Verba Single Server solution. Note that, all Installer components must be run as Administrator.

Step 1 - The install kit starts installing Verba components. Simply press the **Next** button to start the installation.

Step 2 - Read the Verba license agreement carefully before you click **Next** button.

Step 3 - Select the **Single Server** role from the list. Click **Next**.

Step 4 - Select the destination folder for Verba system and the desired location of the media files. You can change the default setting by clicking on the Change button and selecting another folder. If you have finished the destination folder configuration, press the **Next** button.

i Drive root cannot be provided for the media folder (ex: D:\). A folder has to be created.

Step 5a - If the server is going to be the first Single Server (Media Repository) server in the deployment, and pre-generated certificates won't be used, then select the **"Generate Certificate Signed by Verba Media Repository CA"** option, and check the **"First Media Repository in the deployment"** checkbox. Click on the **Generate** button, and in the Generate the Verba Server Certificate window click **Generate**. Finally, click on the **Next** button. (If this option is being used, then Step 5b and Step 5c can be skipped.)

Step 5b - If the server won't be the first Single Server (Media Repository) server in the deployment, and pre-generated certificates won't be used, then select the **"Generate Certificate Signed by Verba Media Repository CA"** option, then click on the **Generate** button. In the Generate the Verba Server Certificate window provide the address of the first Media Repository server, the administrator username and password, then click **Generate**. Finally, click on the **Next** button. (If this option is being used, Step 5c can be skipped.)

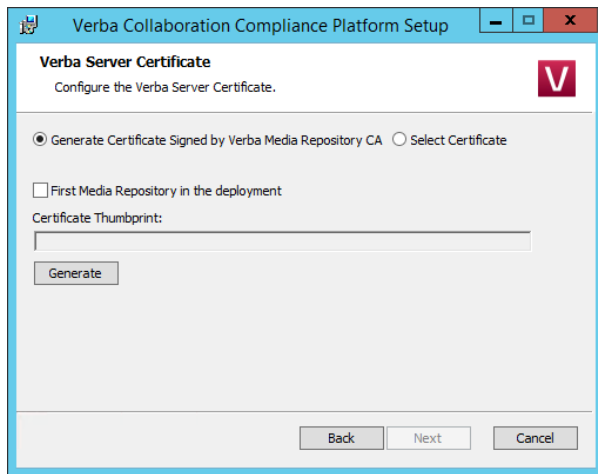
Step 5c - If there is an existing certificate from a previous Verba installation (in case of reinstall or upgrade), or a pre-generated certificate for the server exists (requested from a local or a 3rd party CA), then select the **"Select Certificate"** option, then click on the **Browse** button. If the

i Certificates generated by Verba CA vs pre-generated certificates

In case of using the Verba-generated certificates, the first Single Server (Media Repository) server becomes a CA also. During the installation of the other Verba components, the server certificates will be requested from this CA. This is done through the TCP port 443 with SSL. The server certificates and the CA certificate will be placed in the certificate stores of the servers automatically, to the Personal folder. The certificates generated by the Verba CA uses SHA512forthesignaturealgorithm, andRSA2048 for the public key.

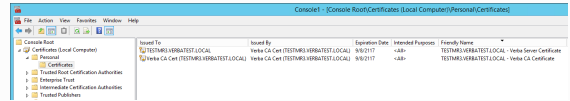
If certificates are generated for the Verba servers in advance using another CA, then make sure that the certificates are placed into the certificate stores of the servers under the Personal folder, and the CA certificates are placed into the Personal or into the Trusted Root Certification Authorities folder. The only requirement for the server certificates is making the private key exportable.

server was a CA previously, then select the CA certificate also by clicking on the **Browse** button under the CA Certificate Thumbprint.



Certificates generated by the Verba CA

Based on the Friendly Name of the certificates the server and the CA certificate can be identified easily. On the screenshot, the first one is the server certificate and the second one is the CA certificate.



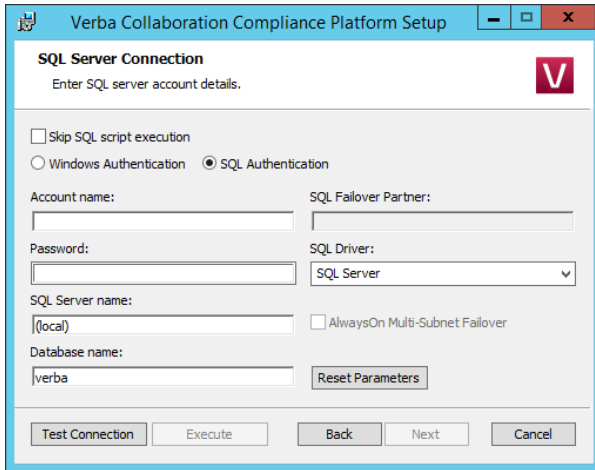
Step 6.1 - The Verba installer is asking for the MS SQL Server connection details. These settings will be used for all Verba services on the server, and the same settings has to be used during the installation of the other Verba components also.

- Both SQL server based and windows authentication is supported. If a domain account will be used for the SQL connection, then select **Windows Authentication**. In case of windows authentication, the Account name has to be provided in UPN or domain\username format. Please provide a **DB Creator** role user account for the connection.
- The server name can be entered either as an IP address or an FQDN.
- The Verba database doesn't have to be created in advance. The installer will create a database with the name given in the "Database Name" setting, and build the schema.
- If SQL Mirroring is being used or AlwaysOn with Multi-Subnet failover, then a different SQL Driver has to be selected. In this case, the driver has to be installed on the server.

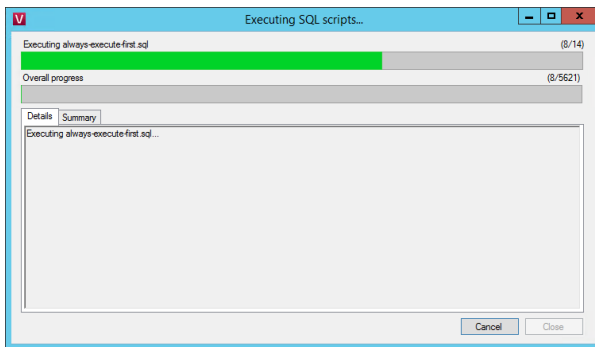
Step 6.2 - Click '**Test Connection**' to verify your input.

Database connection troubleshooting tips

- Try to ping the database server. Try to connect to the 1433 port on the database server. (telnet or Test-NetConnection)
- Check if the user has the necessary roles assigned, refer to [SQL Server requirements](#) for more information.
- If Windows Authentication used then check if the user has the Local Administrator group membership and the 'Logon as a service right'.
- Check if the correct instance name is provided at the SQL Server name. If there are multiple instances, then the SQL Server Browser service must run on the SQL server side.
- If you installed SQL Server Express Edition, then check if the TCP/IP protocol is enabled under the SQL Server Network Configuration in the SQL Server Configuration Manager.



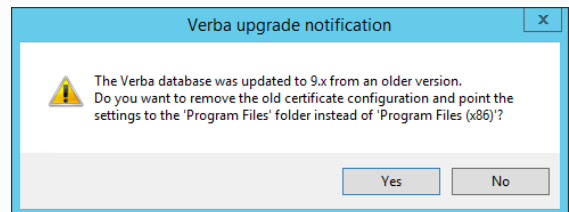
Step 6.3 - If the test was successful, click on the **Execute** button. The installer will start executing the scripts on the database, so it created the database schema. In the case of upgrade, the installer upgrades the existing schema. The script log will be saved to C:\Users\[user]\AppData\Local\Temp\ folder. If an error occurs during the script execution, it can be restarted by closing the window, then clicking on the Execute button again in the installer window.



Step 6.3 - Click on the **Close** button. In the installer window, click **Next**.

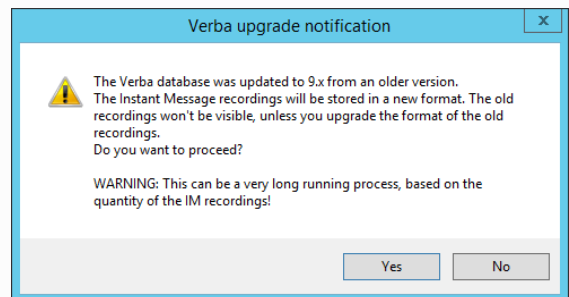
Upgrading from Verba 8.x to Verba 9.x

From version 9.0, the Verba software changed to x64 platform from x86, and also introduced a new Windows certificate-based secure API for the internal connection between the Verba services. When upgrading from Verba 7.x or 8.x, the installer offers changing the configuration stored in the database according to the new settings. In this case, all settings pointing to the "Program Files (x86)" folder will be changed to "Program Files", and all settings related to the old security configuration will be removed.

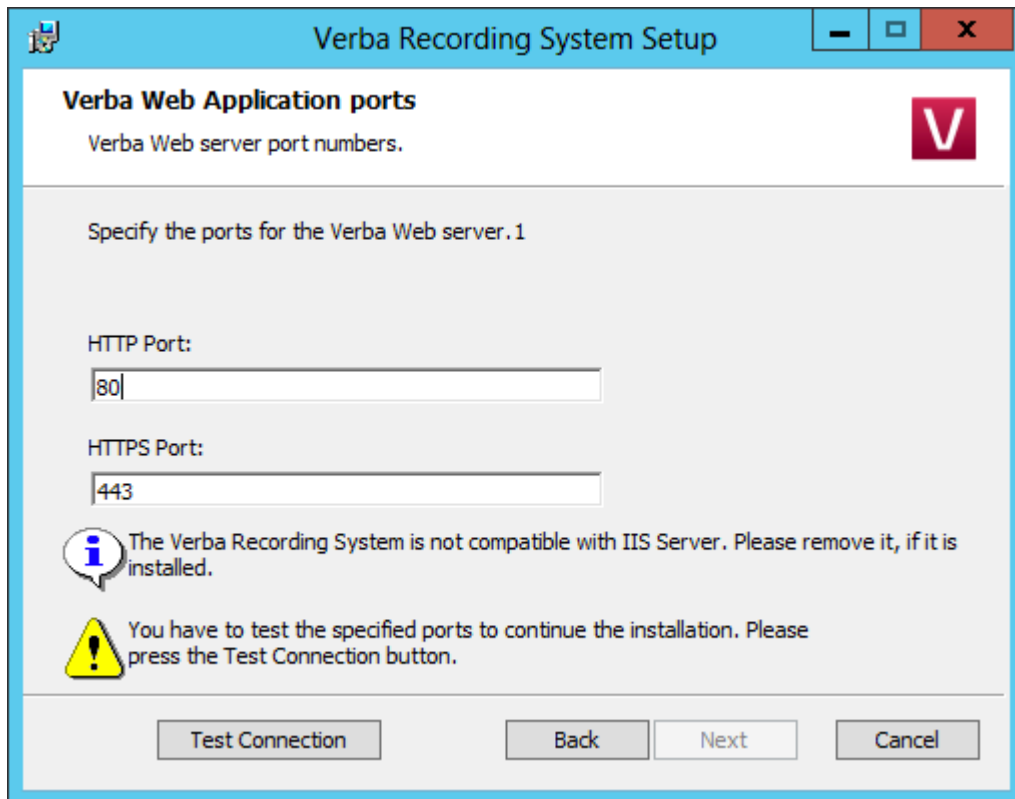


The installer also offers upgrading the schema of the IM recordings. If this step is skipped, then the old recordings won't be visible in the Verba web interface.

Note that this step can take hours to execute!



Step 7 - Please specify the ports for running the Verba web server. Click the **Test Connection** button to check if they are free. If one of them is taken you will be asked for another port number (you are not allowed to run more than one HTTP server on the same port). It is recommended to use the default 80 and 443 port numbers. If successful, click Next.



Step 8a - If this is a new Verba installation, and there is no pre-created SSL certificate for the HTTPS connection, then select the **"Generate Self-signed Certificate"** option, then click on the **Generate** button. In the "Generate the Verba Web server SSL Certificate" window, enter a **password** for the certificate, provide the Subject Alternative names, then click **Generate**. In this case a verba-tomcat.crt and a verba-tomcat.key file will be generated in the C:\ root. Click on the **Next** button. (If this option is being used, then Step 9b can be skipped)

Step 8b - If this is not a new Verba installation (in case of reinstall or upgrade), or there is a pre-created SSL certificate for the HTTPS connection, then select the **"Select Certificate"** option. Under the Certificate Path, click on the **Browse** button, and provide the **.crt file**. Under the Certificate Key Path click on the **Browse** button, and provide the **.key file**. Provide the password of the SSL certificate. Click on the **Next** button.

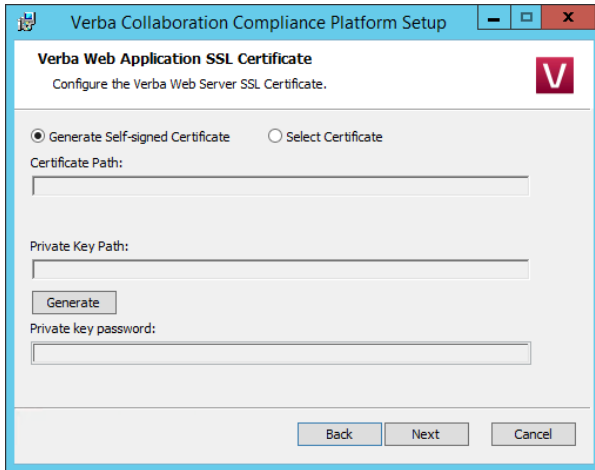
Subject Alternatives Names for the SSL Certificate

To make sure that the browser always going to trust the certificate, provide every possible address at the Subject Alternative Names. The recommended addresses are:

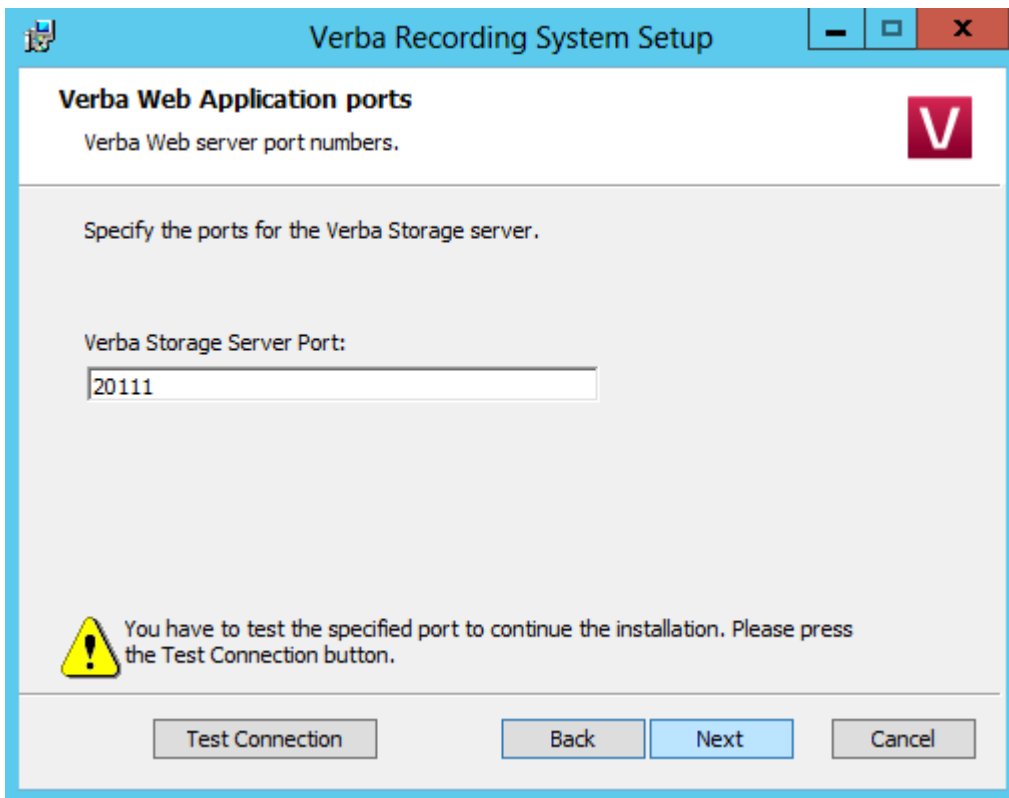
- The hostname of the server.
- The FQDN of the server.
- The IP address of the server.
- "localhost"
- Aliases
- If load-balancer is being used, then it's hostname, FQDN and IP address.

Certificates in .pfx or .p12 format

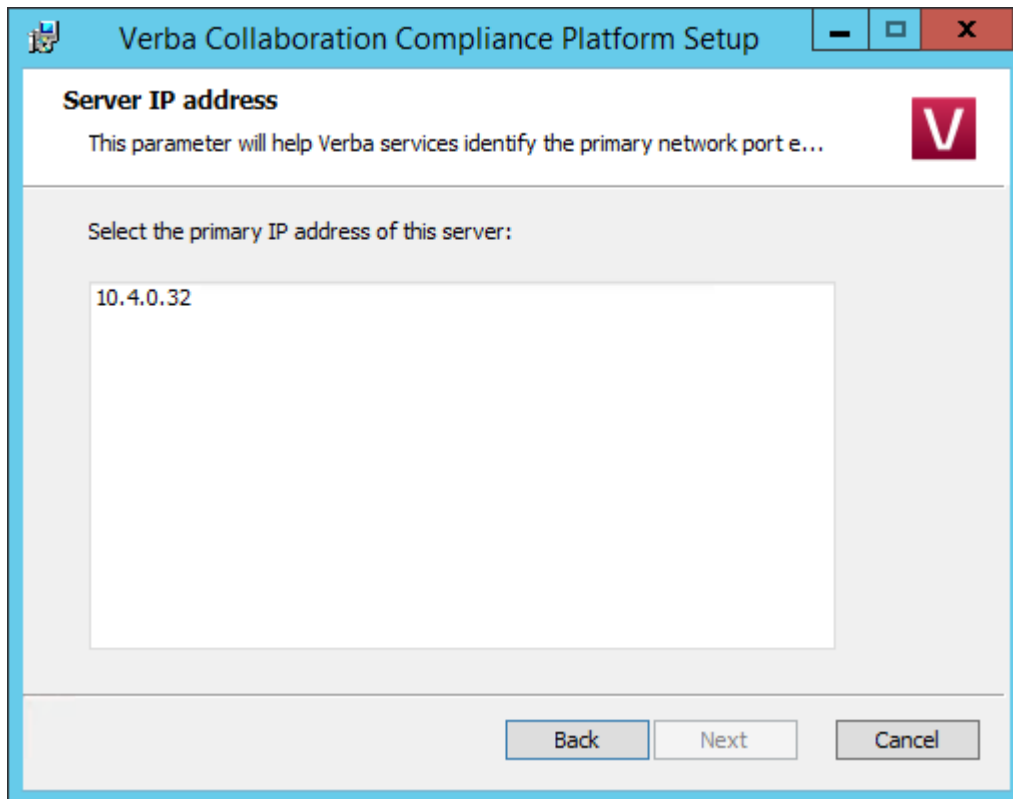
If the SSL certificate is in .pfx or .p12 format, then it has to be converted to a pair of .crt and .key files. For the conversion process, please refer to the "Creating .key and .crt files from .p12 or .pfx file" section in the [Installing an SSL certificate for HTTPS access](#) article.



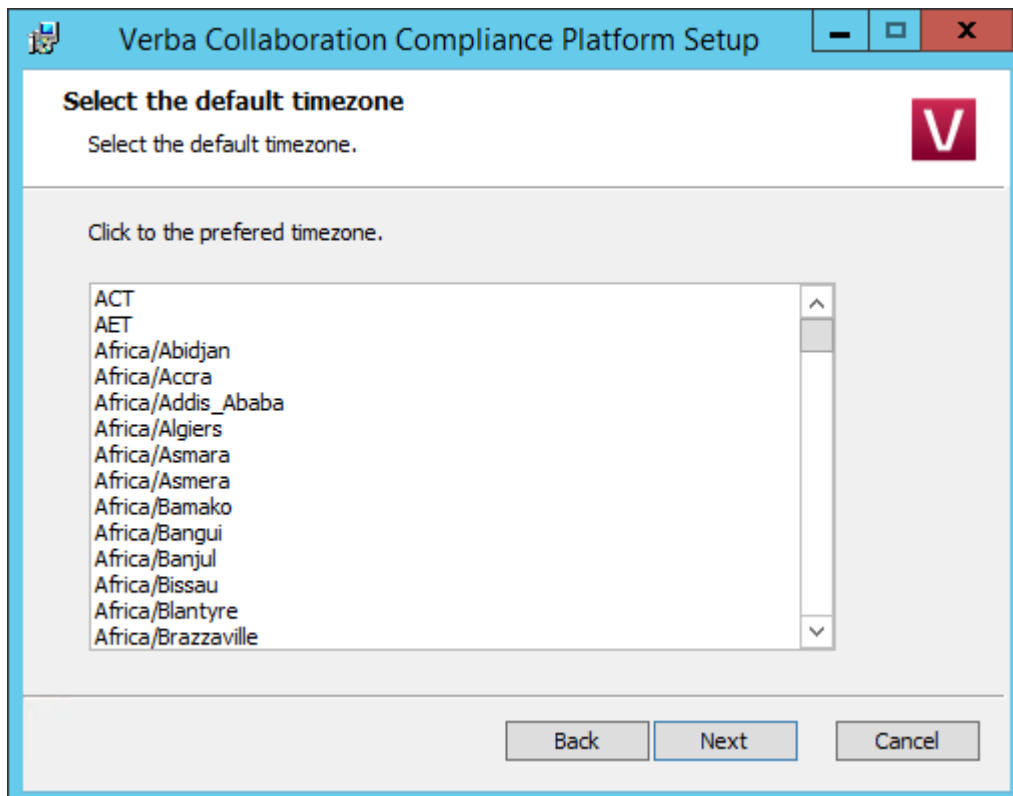
Step 9 - Please specify a free port for the Verba storage server. Use the **Test Connection** button to check the port's availability. If successful, click **Next**.



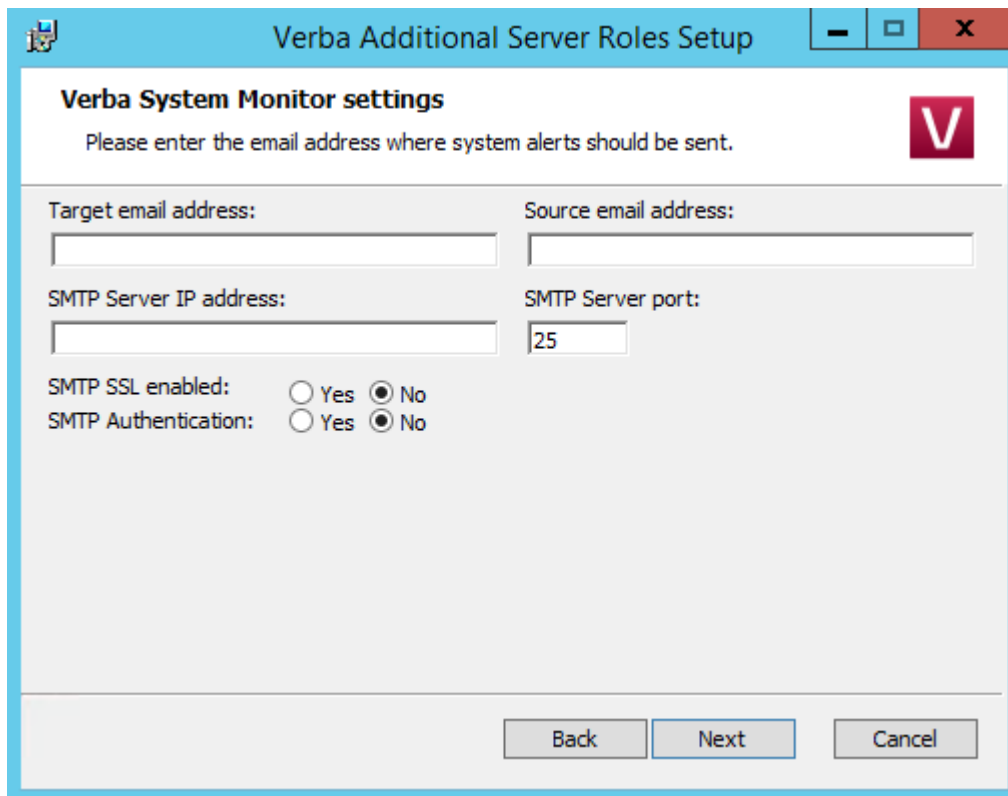
Step 10 - Select the primary IP address of the server from the list, then click **Next**.



Step 11 - Select the desired time zone from the list, then click **Next**.

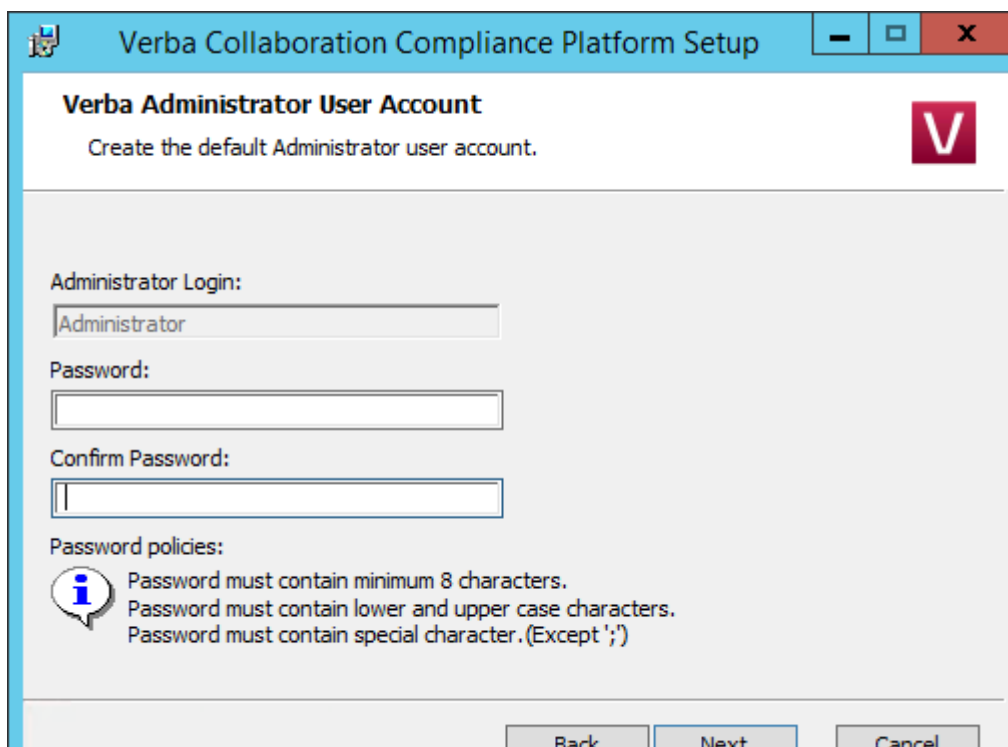


Step 12 - Please provide a target email address, a source email address and an SMTP server address for system alerts. If authentication required then please enter the credentials. The target email address will receive alerts concerning the various services of the recording system. This step can be skipped and the details can be provided or modified after the installation. When you are done, click **Next**.



The screenshot shows a Windows-style dialog box titled "Verba Additional Server Roles Setup". The main heading is "Verba System Monitor settings" with a red 'V' logo. Below the heading is the instruction: "Please enter the email address where system alerts should be sent." The form contains four input fields: "Target email address:", "Source email address:", "SMTP Server IP address:", and "SMTP Server port:". The "SMTP Server port" field has the value "25" entered. Below the input fields are two rows of radio buttons: "SMTP SSL enabled:" with "Yes" and "No" options (where "No" is selected), and "SMTP Authentication:" with "Yes" and "No" options (where "No" is selected). At the bottom of the dialog are three buttons: "Back", "Next", and "Cancel".

Step 13 - Enter a password for the Administrator login then click **Next**.



The screenshot shows a Windows-style dialog box titled "Verba Collaboration Compliance Platform Setup". The main heading is "Verba Administrator User Account" with a red 'V' logo. Below the heading is the instruction: "Create the default Administrator user account." The form contains three input fields: "Administrator Login:" with the value "Administrator" entered, "Password:", and "Confirm Password:". Below the input fields is a section for "Password policies:" which includes an information icon and three bullet points: "Password must contain minimum 8 characters.", "Password must contain lower and upper case characters.", and "Password must contain special character. (Except ';')". At the bottom of the dialog are three buttons: "Back", "Next", and "Cancel".



Step 14 - Enter a password for the Verba API user then click **Next**. Note that this user going to be required at the installation of the other Verba components.

The screenshot shows a Windows-style window titled "Verba Collaboration Compliance Platform Setup". The main content area is titled "Verba API User Account" with the instruction "Create the API user account." and a Verba logo (a red square with a white 'V'). Below the title, there are three input fields: "API User Login:" containing the text "verbaapi", "Password:", and "Confirm Password:". Underneath these fields, a section titled "Password policies:" includes an information icon and three bullet points: "Password must contain minimum 8 characters.", "Password must contain lower and upper case characters.", and "Password must contain special character. (Except ';')". At the bottom of the window, there are three buttons: "Back", "Next", and "Cancel".

Step 15 - Click **Next** again to start installing the services. When it's done, click **Finish** to exit the installer.

Installing a Verba Announcement Server

You can install the server using the provided MSI installation package (VerbaAdditionalServices.msi):

! Do not install the VerbaAdditionalRoles.msi on a Combo, Media Repository or Recording server because the Verba Announcement Service is already installed there and you will end up with corrupt registry settings.

Step 1 - The install kit starts installing Verba components. Simply press the **Next** button to start the installation.

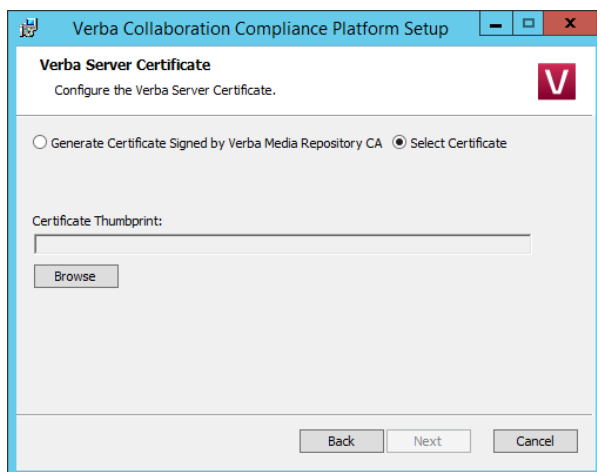
Step 2 - Read the Verba license agreement carefully before you click **Next** button.

Step 3 - Select the **Announcement Server** role from the list. Click **Next**.

Step 4 - Select the destination folder for Verba software. You can change the default setting by clicking on the Change button and selecting another folder. If you have finished the destination folder configuration, press the **Next** button.

Step 5a - If a Verba CA is being used, then select the **"Generate Certificate Signed by Verba Media Repository CA"** option, then click on the **Generate** button. In the Generate the Verba Server Certificate window provide the address of the first Media Repository server, the administrator username and password, then click **Generate**. Finally, click on the **Next** button. (If this option is being used, Step 5b can be skipped.)

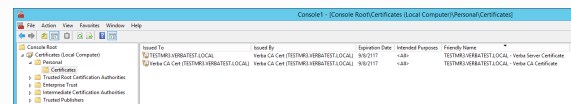
Step 5b - If there is an existing certificate from a previous Verba installation (in case of reinstall or upgrade), or a pre-generated certificate for the server exists (requested from a local or a 3rd party CA), then select the **"Select Certificate"** option, then click on the **Browse** button.



Step 6a - The Verba installer is asking for the MS SQL Server credentials. The server name can be entered either as an IP address or an FQDN. Both SQL server based and windows authentication is supported. In case of windows authentication, the Account name has to be provided in UPN or domain\username format. All Verba servers and components have to use the same database! If SQL Mirroring is being used or AlwaysOn with Multi-Subnet

i Certificates generated by the Verba CA

Based on the Friendly Name of the certificates the server and the CA certificate can be identified easily. On the screenshot, the first one is the server certificate and the second one is the CA certificate.



Issued To	Issued By	Expiration Date	Intended Purpose	Friendly Name
TESTMARIABRATTEST.LOCAL	Verba CA Cert (TESTMARIABRATTEST.LOCAL)	30/12/17	code	TESTMARIABRATTEST.LOCAL - Verba Server Certificate
Verba CA Cert (TESTMARIABRATTEST.LOCAL)	Verba CA Cert (TESTMARIABRATTEST.LOCAL)	30/12/17	code	TESTMARIABRATTEST.LOCAL - Verba CA Certificate

i Database connection troubleshooting tips

- Try to ping the database server. Try to connect to the 1433 port on the database server. (telnet or Test-NetConnection)
- Check if the user has the necessary roles assigned, refer to [SQL Server requirements](#) for more information

failover, then a different SQL Driver has to be selected. In this case, the driver has to be installed on the server. Click ' **Test Connection** ' to verify your input. If the tests were successful, click **Next**.

Step 6b - If the incoming connection from the server is not possible (because the server is in DMZ for example), then uncheck the "**Enable Automatic Node Registration**" setting. In this case, the server has to be added manually to the server list in the System \ Servers menu after the installation. Click **Next**.

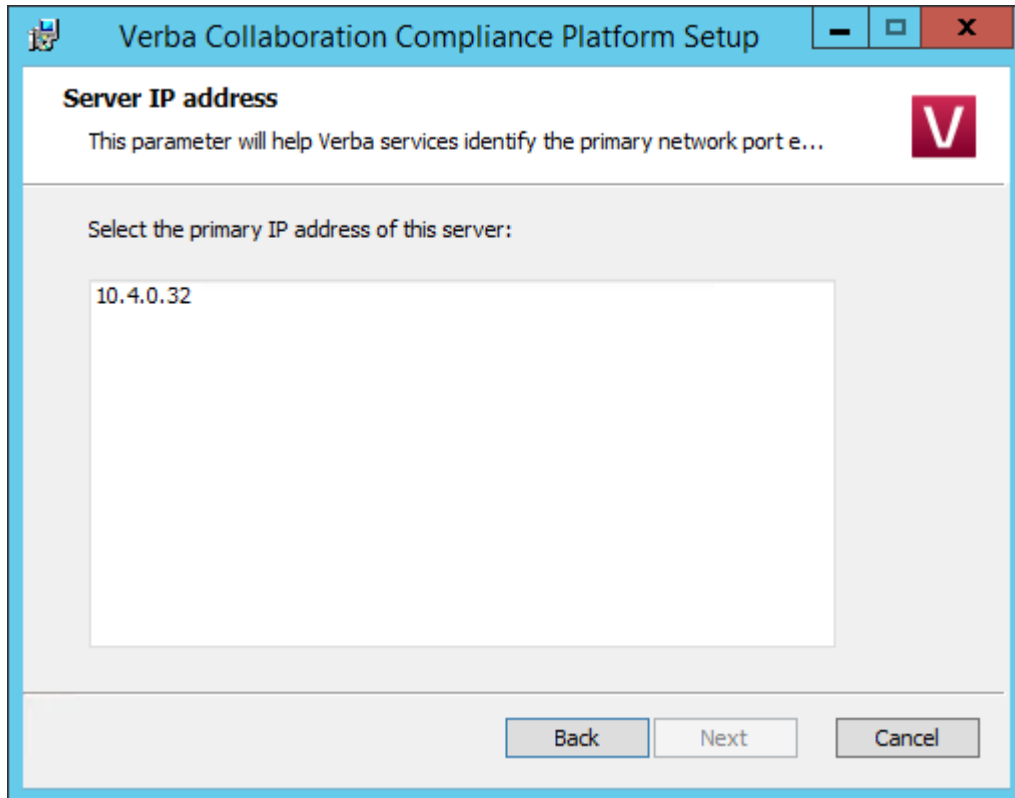
The screenshot shows the 'Verba Additional Server Roles Setup' dialog box with the 'SQL Server Connection' tab selected. The title bar reads 'Verba Additional Server Roles Setup'. Below the title bar, the text 'SQL Server Connection' is displayed, followed by the instruction 'Enter SQL server account details.' and a red 'V' logo. The dialog contains several fields and options: a checked checkbox for 'Enable Automatic Node Registration (SQL Connection Required)', radio buttons for 'Windows Authentication' and 'SQL Authentication' (the latter is selected), text boxes for 'Account name:', 'Password:', and 'Database name:' (containing 'verba'), a dropdown for 'SQL Driver:' (set to 'SQL Server'), and a text box for 'SQL Server name:' (containing '(local)'). There is also an unchecked checkbox for 'AlwaysOn Multi-Subnet Failover'. At the bottom, there are buttons for 'Test Connection', 'Reset Parameters', 'Back', 'Next', and 'Cancel'.

- If Windows Authentication used then check if the user has the Local Administrator group membership and the 'Logon as a service right'.
- Check if the correct instance name is provided at the SQL Server name. If there are multiple instances, then the SQL Server Browser service must run on the SQL server side.
- If you installed SQL Server Express Edition, then check if the TCP/IP protocol is enabled under the SQL Server Network Configuration in the SQL Server Configuration Manager.

Step 7 - Provide the address of the Verba Media Repository server, and the API user password. The API user created at **Step 14** during the installation of the Media Repository server.

The screenshot shows the 'Verba Collaboration Compliance Platform Setup' dialog box with the 'Node Registration' tab selected. The title bar reads 'Verba Collaboration Compliance Platform Setup'. Below the title bar, the text 'Node Registration' is displayed, followed by the instruction 'Enter your Verba Web Application URL and API User Credentials.' and a red 'V' logo. The dialog contains three text boxes: 'Verba Web Application Hostname:', 'API Login:' (containing 'verbaapi'), and 'API Password:'. At the bottom, there are buttons for 'Test Connection', 'Back', 'Next', and 'Cancel'.

Step 8 - Select the primary IP address of the server from the list, then click **Next**.



Step 9 - Please provide a target email address, a source email address and an SMTP server address for system alerts. If authentication required then please enter the credentials. The target email address will receive alerts concerning the various services of the recording system. This step can be skipped and the details can be provided or modified after the installation. When you are done, click **Next**.

Verba Additional Server Roles Setup

Verba System Monitor settings

Please enter the email address where system alerts should be sent.

Target email address:

Source email address:

SMTP Server IP address:

SMTP Server port:

SMTP SSL enabled: Yes No

SMTP Authentication: Yes No

Back Next Cancel

Step 10 - Click **Next** again to start installing the services. When it's done, click **Finish** to exit the installer.

- ✔ For the configuration of the Verba Announcement service, refer to [Installing and configuring the Verba SfB - Lync Announcement service](#)

Installing a Verba Speech Analytics Server

You can install the server using the provided MSI installation package (VerbaAdditionalServices.msi):

! Do not install the VerbaAdditionalRoles.msi on a Combo or Media Repository server because the Verba Speech Analytics Service is already installed there and you will end up with corrupt registry settings.

Step 1 - The install kit starts installing Verba components. Simply press the **Next** button to start the installation.

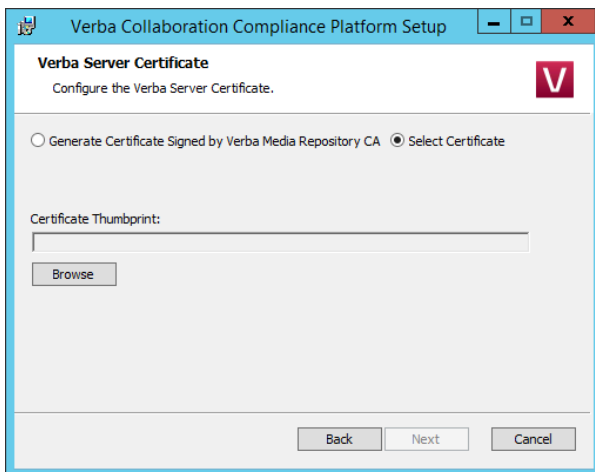
Step 2 - Read the Verba license agreement carefully before you click **Next** button.

Step 3 - Select the **Speech Analytics Server** role from the list. Click **Next**.

Step 4 - Select the destination folder for Verba software. You can change the default setting by clicking on the Change button and selecting another folder. If you have finished the destination folder configuration, press the **Next** button.

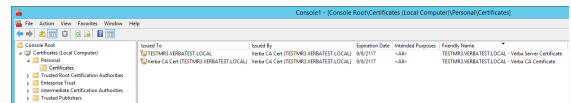
Step 5a - If a Verba CA is being used, then select the **"Generate Certificate Signed by Verba Media Repository CA"** option, then click on the **Generate** button. In the Generate the Verba Server Certificate window provide the address of the first Media Repository server, the administrator username and password, then click **Generate**. Finally, click on the **Next** button. (If this option is being used, Step 5b can be skipped.)

Step 5b - If there is an existing certificate from a previous Verba installation (in case of reinstall or upgrade), or a pre-generated certificate for the server exists (requested from a local or a 3rd party CA), then select the **"Select Certificate"** option, then click on the **Browse** button.



Step 6a - The Verba installer is asking for the MS SQL Server credentials. The server name can be entered either as an IP address or an FQDN. Both SQL server based and windows authentication is supported. In case of windows authentication, the Account name has to be provided in UPN or domain\username format. All Verba servers and

i **Certificates generated by the Verba CA**
Based on the Friendly Name of the certificates the server and the CA certificate can be identified easily. On the screenshot, the first one is the server certificate and the second one is the CA certificate.



i **Database connection troubleshooting tips**

- Try to ping the database server. Try to connect to the 1433 port on the database server. (telnet or Test-NetConnection)

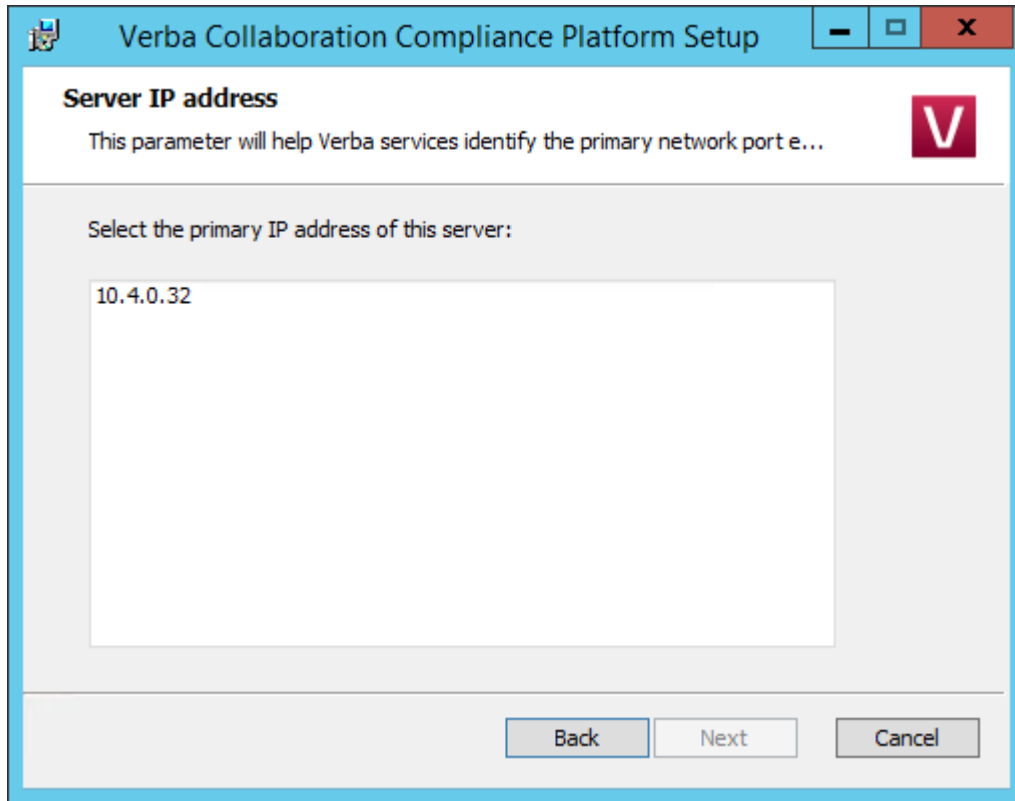
components have to use the same database! If SQL Mirroring is being used or AlwaysOn with Multi-Subnet failover, then a different SQL Driver has to be selected. In this case, the driver has to be installed on the server. Click ' **Test Connection** ' to verify your input. If the tests were successful, click **Next**.

Step 6b - If the incoming connection from the server is not possible (because the server is in DMZ for example), then uncheck the "**Enable Automatic Node Registration**" setting. In this case, the server has to be added manually to the server list in the System \ Servers menu after the installation. Click **Next**.

- Check if the user has the necessary roles assigned, refer to [SQL Server requirements](#) for more information.
- If Windows Authentication used then check if the user has the Local Administrator group membership and the 'Logon as a service right'.
- Check if the correct instance name is provided at the SQL Server name. If there are multiple instances, then the SQL Server Browser service must run on the SQL server side.
- If you installed SQL Server Express Edition, then check if the TCP/IP protocol is enabled under the SQL Server Network Configuration in the SQL Server Configuration Manager.

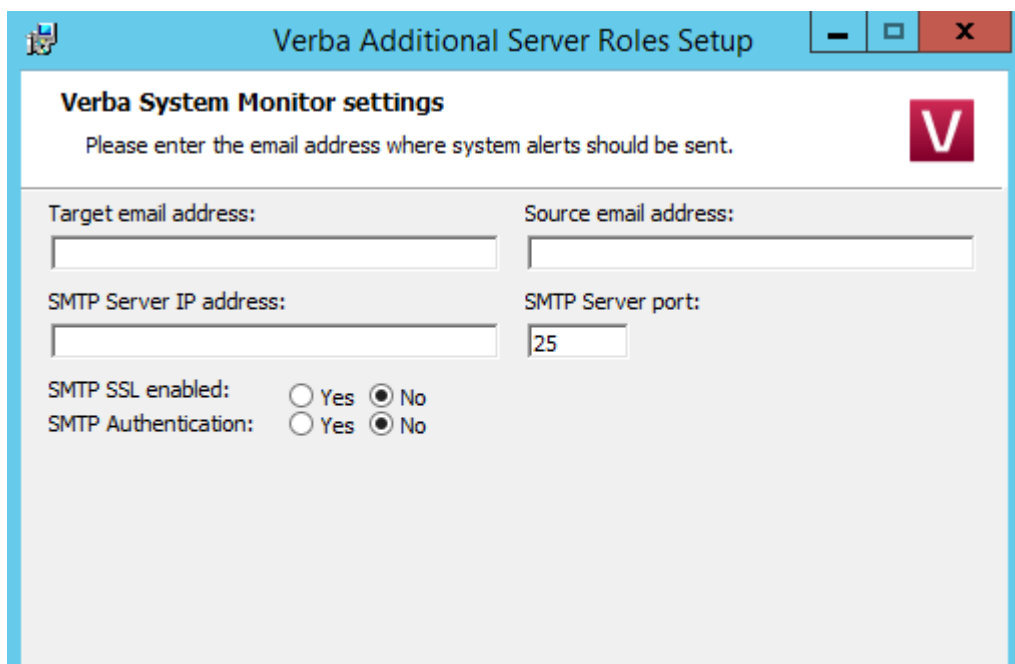
Step 7 - Provide the address of the Verba Media Repository server, and the API user password. The API user created at **Step 14** during the installation of the Media Repository server.

Step 8 - Select the primary IP address of the server from the list, then click **Next**.

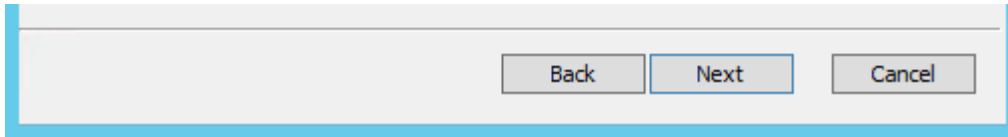


The screenshot shows a window titled "Verba Collaboration Compliance Platform Setup". The main heading is "Server IP address". Below the heading, there is a sub-heading "This parameter will help Verba services identify the primary network port e...". A text box contains the IP address "10.4.0.32". At the bottom of the window, there are three buttons: "Back", "Next", and "Cancel".

Step 9 - Please provide a target email address, a source email address and an SMTP server address for system alerts. If authentication required then please enter the credentials. The target email address will receive alerts concerning the various services of the recording system. This step can be skipped and the details can be provided or modified after the installation. When you are done, click **Next**.



The screenshot shows a window titled "Verba Additional Server Roles Setup". The main heading is "Verba System Monitor settings". Below the heading, there is a sub-heading "Please enter the email address where system alerts should be sent.". There are four text input fields: "Target email address:", "Source email address:", "SMTP Server IP address:", and "SMTP Server port:". The "SMTP Server port:" field contains the value "25". There are two radio button options: "SMTP SSL enabled:" with "Yes" and "No" options, and "SMTP Authentication:" with "Yes" and "No" options. The "No" option is selected for both.



Step 10 - Click **Next** again to start installing the services. When it's done, click **Finish** to exit the installer.

Installing the Verba Media Collector and Proxy component

The Verba Media Collector and Proxy component is responsible for capturing the media streams on the node it's installed on and forwarding it to a Verba Recording Server. In a Lync environment, it's typically installed on the Edge server or the Mediation server depending on your recording needs.

! Do not install the VerbaAdditionalRoles.msi on a SingeServer or Recording Server because the Verba Media Collector and Proxy Service is already installed there and you will end up with corrupt registry settings.

Please follow the steps below to install the component:

Step 1 - The install kit starts installing Verba components. Simply press the **Next** button to start the installation.

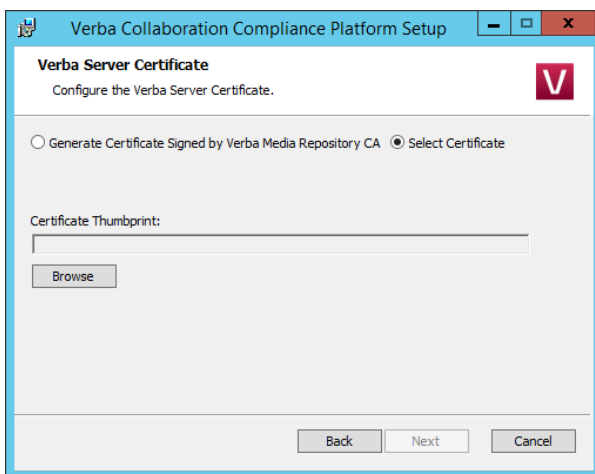
Step 2 - Read the Verba license agreement carefully before you click **Next** button.

Step 3 - Select the **Media Collector & Proxy Server** role from the list. Click **Next**.

Step 4 - Select the destination folder for Verba software. You can change the default setting by clicking on the Change button and selecting another folder. If you have finished the destination folder configuration, press the **Next** button.

Step 5a - If a Verba CA is being used, then select the **"Generate Certificate Signed by Verba Media Repository CA"** option, then click on the **Generate** button. In the Generate the Verba Server Certificate window provide the address of the first Media Repository server, the administrator username and password, then click **Generate**. Finally, click on the **Next** button. (If this option is being used, Step 5b can be skipped.)

Step 5b - If there is an existing certificate from a previous Verba installation (in case of reinstall or upgrade), or a pre-generated certificate for the server exists (requested from a local or a 3rd party CA), then select the **"Select Certificate"** option, then click on the **Browse** button.



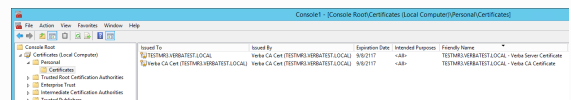
! Servers in DMZ and Verba CA

If the server is in DMZ (for example in case of Edge servers), then the server certificate cannot be requested directly from the Verba CA, and **Step 5b** has to be selected. In this case, there are two prerequisites:

- The server certificate has to be downloaded from the Verba Web Interface, and imported into the server's certificate store manually. For the certificate downloading guide see: [Server Certificates](#)
- The CA certificate of the Verba CA has to be manually exported from the certificate store of the first Media Repository (or Singel) server, then imported manually into the server's certificate store.

i Certificates generated by the Verba CA

Based on the Friendly Name of the certificates the server and the CA certificate can be identified easily. On the screenshot, the first one is the server certificate and the second one is the CA certificate.



Step 6a - The Verba installer is asking for the MS SQL Server credentials. The server name can be entered either as an IP address or an FQDN. Both SQL server based and windows authentication is supported. In case of windows authentication, the Account name has to be provided in UPN or domain\username format. All Verba servers and components have to use the same database! If SQL Mirroring is being used or AlwaysOn with Multi-Subnet failover, then a different SQL Driver has to be selected. In this case, the driver has to be installed on the server. Click ' **Test Connection** ' to verify your input. If the tests were successful, click **Next**.

Step 6b - If the incoming connection from the server is not possible (because the server is in DMZ for example), then uncheck the "**Enable Automatic Node Registration**" setting. In this case, the server has to be added manually to the server list in the System \ Servers menu after the installation. Click **Next**.



Database connection troubleshooting tips

- Try to ping the database server. Try to connect to the 1433 port on the database server. (telnet or Test-NetConnection)
- Check if the user has the necessary roles assigned, refer to [SQL Server requirements](#) for more information.
- If Windows Authentication used then check if the user has the Local Administrator group membership and the 'Logon as a service right'.
- Check if the correct instance name is provided at the SQL Server name. If there are multiple instances, then the SQL Server Browser service must run on the SQL server side.
- If you installed SQL Server Express Edition, then check if the TCP/IP protocol is enabled under the SQL Server Network Configuration in the SQL Server Configuration Manager.

The screenshot shows the 'Verba Additional Server Roles Setup' window with the 'SQL Server Connection' tab selected. The window title is 'Verba Additional Server Roles Setup'. Below the title bar, it says 'SQL Server Connection' and 'Enter SQL server account details.' There is a Verba logo (a red 'V' in a square) in the top right corner. The main area contains several settings:

- Enable Automatic Node Registration (SQL Connection Required)
- Windows Authentication SQL Authentication
- Account name: [text box]
- SQL Follower Partner: [text box]
- Password: [text box]
- SQL Driver: [dropdown menu showing 'SQL Server']
- SQL Server name: [(local)]
- AlwaysOn Multi-Subnet Failover
- Database name: [verba]

 At the bottom, there are five buttons: 'Test Connection', 'Reset Parameters', 'Back', 'Next', and 'Cancel'.

Step 7 - Provide the address of the Verba Media Repository server, and the API user password. The API user created at **Step 14** during the installation of the Media Repository server.

Verba Collaboration Compliance Platform Setup

Node Registration

Enter your Verba Web Application URL and API User Credentials.

Verba Web Application Hostname:

API Login:

API Password:

Test Connection Back Next Cancel

Step 8 - Select the primary IP address of the server from the list, then click **Next**.

Verba Collaboration Compliance Platform Setup

Server IP address

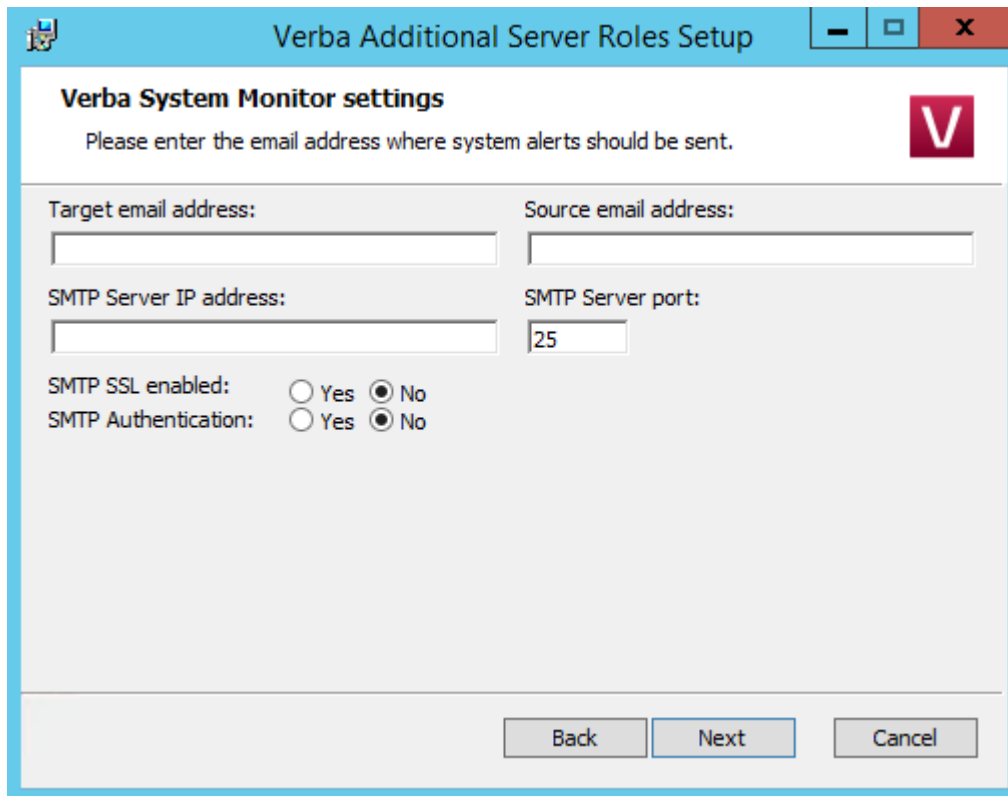
This parameter will help Verba services identify the primary network port e...

Select the primary IP address of this server:

10.4.0.32

Back Next Cancel

Step 9 - Please provide a target email address, a source email address and an SMTP server address for system alerts. If authentication required then please enter the credentials. The target email address will receive alerts concerning the various services of the recording system. This step can be skipped and the details can be provided or modified after the installation. When you are done, click **Next**.



The screenshot shows a Windows-style dialog box titled "Verba Additional Server Roles Setup". Inside, there is a section titled "Verba System Monitor settings" with a red 'V' logo. Below the title, it says "Please enter the email address where system alerts should be sent." The form contains several input fields: "Target email address:" (empty), "Source email address:" (empty), "SMTP Server IP address:" (empty), and "SMTP Server port:" (containing "25"). There are also two radio button options: "SMTP SSL enabled:" with "Yes" and "No" (selected), and "SMTP Authentication:" with "Yes" and "No" (selected). At the bottom, there are three buttons: "Back", "Next", and "Cancel".

Step 10 - Click **Next** again to start installing the services. When it's done, click **Finish** to exit the installer.

Installing the Verba Skype for Business - Lync Filter

Overview

For the complete overview of the installation process, visit [Microsoft Skype for Business](#)

The Verba system uses the Microsoft Skype for Business / Lync Server SDK and specific components have to be installed on **all Microsoft SfB/Lync Front-End servers (including SBSs and SBAs)** where recorded/controlled users are located. For mediation and AVMCU based recording, the Media Collector component needs to be installed as well. There are two different Verba server roles available:

The **Lync Filter** server role contains the following services:

- Verba SfB/Lync Call Filter Service: required for voice/video call recording
- Verba SfB/Lync IM Filter Service: required for IM and persistent chat recording
- Verba SfB/Lync Communication Policy Service: required for ethical wall deployments

The **Media Collector and Lync Filter** server role contains the following services:


- Verba Media Collector & Proxy Service: required for mediation and AVMCU based recording
- Verba SfB/Lync Call Filter Service: required for voice/video call recording
- Verba SfB/Lync IM Filter Service: required for IM and persistent chat recording
- Verba SfB/Lync Communication Policy Service: required for ethical wall deployments

Follow the guidelines of this chapter to install the Verba SfB/Lync Filter component on the Microsoft SfB/Lync servers:

- [Prerequisites](#)
- [Installing the Verba components](#)
- [Registering the Verba components into the SfB/Lync environment](#)
 - [Verba SfB/Lync Call Filter Service](#)
 - [Verba SfB/Lync IM Filter Service](#)
 - [Verba SfB/Lync Communication Policy Service](#)
- [Verifying and removing the Verba components](#)

Prerequisites

- There is at least one Verba Media Repository or Verba Media Repository & Recording Server installed
- Use a Windows user account for the installation with the following privileges:
 - **Local Administrator**
 - **RTCUniversalServerAdmins**
- Create a new service user account in the domain for the Verba services (e.g.svcverbalync):
 - The service user account can be the same as the one used on other Verba servers.
 - Add the service user account to the following **local** groups on **all Front-End server(s), SBSs and SBAs**:
 - **Administrators**
 - **RTC Server Applications**
 - [Add the Logon As A Service Right](#) for the service user account

 Configure the service user account and group memberships in a way, that it **does not violate your Group Policies**. If the group membership or privileges of the service user account is modified during regular Group Policy processing, the Verba system will **stop recording conversations or enforcing communication policies**.

- Install the software prerequisites: [Installing the required prerequisites](#)
- Configure the firewall on the SfB/Lync servers: [Firewall configuration for Skype for Business - Lync deployments](#)

Installing the Verba components

! Make sure you are running the MSI package from an **administrator command prompt**.

Step 1 - Locate and run the **VerbaAdditionalRoles.msi** package from administrator command prompt. The install kit starts installing Verba components. Simply press the **Next** button to start the installation.

Step 2 - Read the Verba license agreement carefully before you click the **Next** button.

Step 3 - Select the server role and click **Next**.

- **Lync Filter** for proxy based recording and ethical wall deployments.
- **Media Collector & Lync Filter** role for mediation and AVMCU based recording deployments.

Step 4 - Select the destination folder for the Verba SfB/Lync Filter. You can change the default setting by clicking on the **Change** button and selecting another folder. If you have finished the destination folder configuration, press the **Next** button.

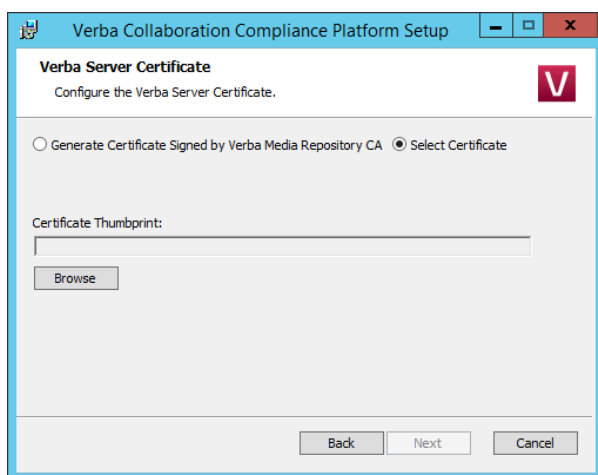
Step 5a - If a Verba CA is being used, then select the **"Generate Certificate Signed by Verba Media Repository CA"** option, then click on the **Generate** button. In the Generate the Verba Server Certificate window provide the address of the first Media Repository server, the administrator username and password, then click **Generate**. Finally, click on the **Next** button. (If this option is being used, Step 5b can be skipped.)

Step 5b - If there is an existing certificate from a previous Verba installation (in case of reinstall or upgrade), or a pre-generated certificate for the server exists (requested from a local or a 3rd party CA), then select the **"Select Certificate"** option, then click on the **Browse** button.

! Certificates generated by the Verba CA

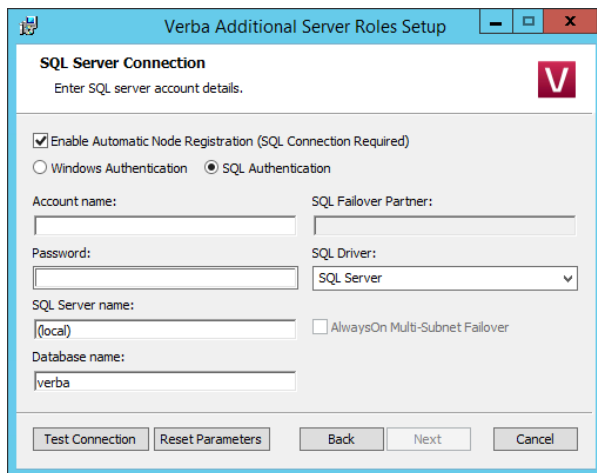
Based on the Friendly Name of the certificates the server and the CA certificate can be identified easily. On the screenshot, the first one is the server certificate and the second one is the CA certificate.

Issued To	Issued By	Expiration Date	Intended Purpose	Friendly Name
TESTLAB\VERBATEST.LOCAL	Verba CA Cert (TESTLAB\VERBATEST.LOCAL)	30/11/17	code	TESTLAB\VERBATEST.LOCAL - Verba Server Certificate
Verba CA Cert (TESTLAB\VERBATEST.LOCAL)	Verba CA Cert (TESTLAB\VERBATEST.LOCAL)	30/11/17	code	TESTLAB\VERBATEST.LOCAL - Verba CA Certificate



Step 6a - The Verba installer is asking for the MS SQL Server credentials. The server name can be entered either as an IP address or an FQDN. Both SQL server based and windows authentication is supported. In case of windows authentication, the Account name has to be provided in UPN or domain\username format. All Verba servers and components have to use the same database! If SQL Mirroring is being used or AlwaysOn with Multi-Subnet failover, then a different SQL Driver has to be selected. In this case, the driver has to be installed on the server. Click ' **Test Connection**' to verify your input. If the tests were successful, click **Next**.

Step 6b - If the incoming connection from the server is not possible (because the server is in DMZ for example), then uncheck the "**Enable Automatic Node Registration**" setting. In this case, the server has to be added manually to the server list in the System \ Servers menu after the installation. Click **Next**.



The screenshot shows the 'Verba Additional Server Roles Setup' dialog box, specifically the 'SQL Server Connection' tab. The dialog has a title bar with the text 'Verba Additional Server Roles Setup' and standard window controls. Below the title bar, the text 'SQL Server Connection' is displayed, followed by the instruction 'Enter SQL server account details.' and a red 'V' logo. The main area contains several settings: a checked checkbox for 'Enable Automatic Node Registration (SQL Connection Required)', radio buttons for 'Windows Authentication' and 'SQL Authentication' (the latter is selected), input fields for 'Account name:' and 'Password:', a dropdown menu for 'SQL Driver:' set to 'SQL Server', an input field for 'SQL Server name:' containing '(local)', an unchecked checkbox for 'AlwaysOn Multi-Subnet Failover', and an input field for 'Database name:' containing 'verba'. At the bottom, there are five buttons: 'Test Connection', 'Reset Parameters', 'Back', 'Next', and 'Cancel'.

Database connection troubleshooting tips

- Try to ping the database server. Try to connect to the 1433 port on the database server. (telnet or Test-NetConnection)
- Check if the user has the necessary roles assigned, refer to [SQL Server requirements](#) for more information.
- If Windows Authentication used then check if the user has the Local Administrator group membership and the 'Logon as a service right'.
- Check if the correct instance name is provided at the SQL Server name. If there are multiple instances, then the SQL Server Browser service must run on the SQL server side.
- If you installed SQL Server Express Edition, then check if the TCP/IP protocol is enabled under the SQL Server Network Configuration in the SQL Server Configuration Manager.

Step 7 - Provide the address of the Verba Media Repository server, and the API user password. The API user created at **Step 14** during the installation of the Media Repository server.

The screenshot shows a window titled "Verba Collaboration Compliance Platform Setup" with a blue header bar. Below the header, the title "Node Registration" is displayed in bold, followed by the instruction "Enter your Verba Web Application URL and API User Credentials." A red square logo with a white 'V' is in the top right corner. The main area contains three input fields: "Verba Web Application Hostname:" (empty), "API Login:" (containing "verbaapi"), and "API Password:" (empty). At the bottom, there are four buttons: "Test Connection", "Back", "Next", and "Cancel".

Step 8 - Select the primary IP address of the server from the list, then click **Next**.

The screenshot shows a window titled "Verba Collaboration Compliance Platform Setup" with a blue header bar. Below the header, the title "Server IP address" is displayed in bold, followed by the instruction "This parameter will help Verba services identify the primary network port e...". A red square logo with a white 'V' is in the top right corner. The main area contains the text "Select the primary IP address of this server:" above a large white text area containing the IP address "10.4.0.32". At the bottom, there are three buttons: "Back", "Next", and "Cancel".

Step 9 - Provide the username and the password for the service user. Use the **Verify logon** and the **Verify memberships** buttons to check if the service user account has sufficient rights. If either of the tests fails, please make sure it has all the necessary


privileges mentioned at **Step 2** of the **Prerequisites** section. If the service user account has the proper privileges and the test keeps failing, then you can also click the **Skip Role Check** checkbox. Click **Next** to continue.

Filter Service account
Enter service account details.

Specify the logon account for the Sfb/Lync Filter services.

Universal Principal Name (username@domain.local):

Password:

 Domain user needed by the Verba Sfb/Lync Filter, which can log on as service, and it's member of the required groups:
[Installing the Verba Sfb/Lync Filter](#)


Skip Role Check. Not assigning these roles to the service user will result in the failure of the software components.

Step 10 - Please provide a target email address, a source email address and an SMTP server address for system alerts. If authentication required then please enter the credentials. The target email address will receive alerts concerning the various services of the recording system. This step can be skipped and the details can be provided or modified after the installation. When you are done, click **Next**.

Step 11 - Click **Next** again to start installing the services. When it's done, click **Finish** to exit the installer.

Registering the Verba components into the SfB/Lync environment

The Verba applications have to be added as new server applications to the SfB/Lync system. Open the **Skype for Business / Lync Server Management Shell** from the Start Menu and use the following command(s):

 The Verba applications needs to be registered only once per frontend pool.

Verba SfB/Lync Call Filter Service

Required for voice/video call recording.

```
New-CsServerApplication -Identity "Service:Registrar:lync-pool-address.yourdomain.com/VerbaLyncF
```

Verba SfB/Lync IM Filter Service

Required for IM and persistent chat recording.

```
New-CsServerApplication -Identity "Service:Registrar:lync-pool-address.yourdomain.com/LyncChatRe
```

Verba SfB/Lync Communication Policy Service

Required for ethical wall deployments.

```
New-CsServerApplication -Identity "Service:Registrar:lync-pool-address.yourdomain.com/EthicalWallinit"
New-CsServerApplication -Identity "Service:Registrar:lync-pool-address.yourdomain.com/EthicalWallinit" -Priority <UserServicesPriority>
```

<UserServicesPriority> is the current priority of the User Services Lync server application. The reason for this is that the EthicalWallinit application needs to run before this. After this, the User Services application will have the priority of *its initial priority+1*. You can use the `Get-CsServerApplication` command to see what priority that service currently has.

Verifying and removing the Verba components

You can verify the list of the registered server applications using this command from the **Lync Server Management Shell**:

```
Get-CsServerApplication
```

You can always remove these filters if you make a configuration mistake:

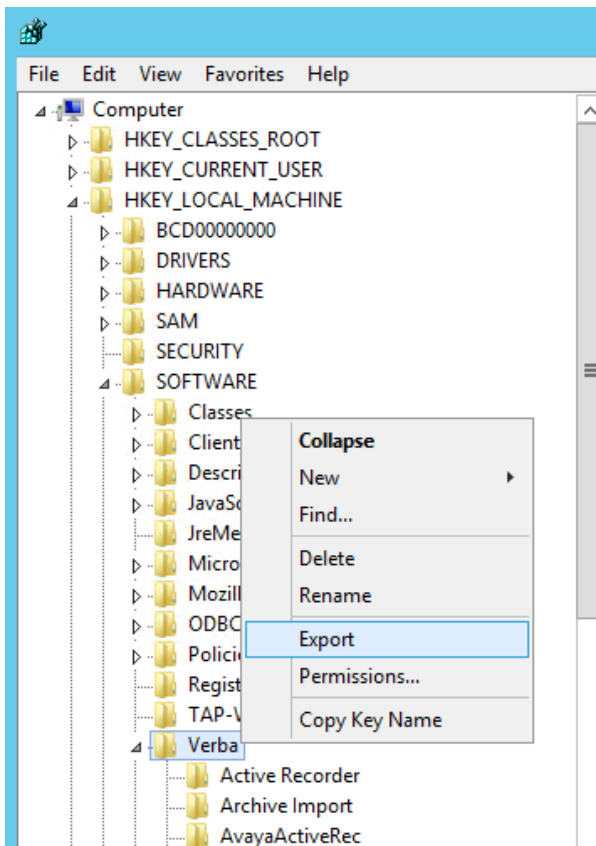
```
Remove-CsServerApplication -Identity "Service:Registrar:lync-pool-address.yourdomain.com/VerbaLync"
Remove-CsServerApplication -Identity "Service:Registrar:lync-pool-address.yourdomain.com/LyncChannel"
Remove-CsServerApplication -Identity "Service:Registrar:lync-pool-address.yourdomain.com/EthicalWallinit"
Remove-CsServerApplication -Identity "Service:Registrar:lync-pool-address.yourdomain.com/EthicalWallinit"
```

Changing the role of a Verba server

If the requirements are changing, or if the wrong role was installed because of a mistake, the role of an already installed Verba server or component can be changed.

The optional steps are required only when the existing configuration needs to be preserved.

Step 1 (Optional) - If the existing settings of the installed services are required after the role change, the Verba registry has to be exported. Open the Start menu, type "regedit" and press Enter. The Registry Editor opens. Go to the **HKEY_LOCAL_MACHINE\SOFTWARE\Verba** node. Right-click on the Verba key, then select **Export**.



Step 2 - Uninstall the Verba application from the server.

Examples

The configuration usually needed to be preserved when:

- Changing between Single Server and Recording Server roles, and the configuration of the recording services are required.
- Changing from SfB/Lync Filter to Media Collector and Filter role, and the configuration of the filter service(s) is required.

⚠ During the uninstallation, the Verba registry set also becomes removed. If the configuration needs to be preserved, then export the registry set as described at **Step 1**.

Step 3 - Install the Verba application as usual, but now by using the desired role. For the installation guides, see: [Install the Verba software](#)


Step 4 (Optional) - Open the Start menu, type "regedit" and press Enter. The Registry Editor opens. Click on the **File \ Import** menu, and import the registry set previously exported at **Step 1**.

Step 5 (Optional) - Edit the **HKEY_LOCAL_MACHINE\SOFTWARE\Verba\Storage\Role** value. The new value should represent the new role of the server.

Verba role	Registry code
Single Server	Combo
Media Repository	MR
Recording Server	RS
Lync Filter	LF
Media Collector and Proxy	RC
Media Collector and Lync Filter	LFRC
Announcement Server	AS

Step 6 - Open the Verba Web Interface and go to the **System \ Servers** menu.

Step 7 - Select the changed Verba server node from the list, then click on the **Delete** button.


 When deleting a server from the list, the configuration stored in the central database will be removed. If the configuration needs to be preserved, then export the registry set as described at **Step 1**.

Step 8 - On the Verba server list page, click on the **Add New Verba Server** link at the upper right corner.

Step 9 - Provide the FQDN of the server at the **Hostname**, select the new role at the **Role** setting, select a **Configuration Profile**, then click **Save**.

Step 10 - Go to the **Change Configuration Settings** tab.


Step 11 - Select the "**Use configuration only from the server's local registry**" option, then click on the **Start** button.

 When selecting the local registry, the configuration is copied into the central database.

Verba Server Configuration

TESTMR1.VERBATEST.LOCAL | Differences found between configurations

Verba Server Data	Change Configuration Settings	Service Control	Service Activation	Configuration Tasks
-------------------	--------------------------------------	-----------------	--------------------	---------------------

 Configuration differences were found between the central database and the server's local configuration. Please decide how to resolve these differences.

- Use central database configuration in case of profile values, otherwise use the server's local configuration (recommended)
- Use configuration only from central database
- Use configuration only from server's local registry

Step 12 (Optional) - Go to the **Service Activation** tab and activate the previously used services. Start the services at the **Service Control** tab.

Installer Parameters and Unattended Installation

The Verba msi installers files can be started from the command line with additional parameters. The installers can be started the following way:

```
msiexec /i VerbaRecording.msi [logging setting] [/quiet] [verba parameters]
```

Logging setting

Loggin can be added by the /L parameter, plus the letters which specify the required information. For example /LE means logging the errors only, or /LEI means logging the errors and the status messages. For Verba, the recommended setting is /L*V. After the logging setting, a file name also has to be specified for the output, for example "/L*V installer.log". The following table describes the available options:

Letter	Log entries
V	Verbose output
O	Out-of-disk-space messages
I	Status messages
C	Initial UI parameters
E	All error messages
W	Non-fatal warnings
A	Startup of actions
R	Action-specific records
M	Out-of-memory or fatal exit information
U	User requests
P	Terminal properties
X	Extra debugging information.
*	Wildcard for adding all parameters, except the V and X.
+	Append to existing file
!	Flush each line to the log

Quiet Mode

Quiet mode enables the installation of the Verba software with a single command, without using the GUI. In this case, all settings going to be set based on the provided parameters.

 If quiet mode is used, the SKIPSQLSEQUENCE=1 parameter is mandatory!

Verba parameters

Parameter	Description	Mandatory	Default value	Sample
SELECTEDROLE	<p>The role to be installed on the server. Available values:</p> <ul style="list-style-type: none"> • MR - Media Repository • RS - Recording Server • Combo - Single Server • AS - Announcement Server • LF - SfB/Lync Filter • LFRC SfB/Lync Filter and Media Collector • RS - Media Collector and proxy • SA - Speech Analytics Server 	Yes		SELECTEDROLE=RS
FILTERINSTALLFOLDER	Application installation folder.		C:\Program Files\Verba\	FILTERINSTALLFOLDER=D:\Apps\Verba\
MEDIA	Media folder.		C:\Program Files\Verba\media\	MEDIA="D:\Verba media\"
USEADVANCEDAPI	<p>Sets if the advanced certificate based secure communication going to be used.</p> <ul style="list-style-type: none"> • 0 - Legacy mode • 1 - Advanced certificate based connections 		1	USEADVANCEDAPI=0
VCERTTHUMLABEL	The thumbprint or path of the server certificate.			VCERTTHUMLABEL=6B5A1D380F5D73BB3A9C0E
VCERTPASS	The password of the server certificate, if file path was provided at the VCERTTHUMLABEL parameter.			VCERTPASS=your_password_here
VCACERTTHUMLABEL	The thumbprint of the CA certificate. (Verba CA)			VCACERTTHUMLABEL=7E2349566838AB58306B/
VSERVICEUSERNAME	Username for the service user. If not set, then Local System is going to be used as a service account.	Yes, if the VNATIVELOGON is set to 1.		VSERVICEUSERNAME=contoso\srv-verba
VSERVICEUSERPASSWORD	Password for the service user.	Yes, if the VSERVICEUSERNAME is set.		VSERVICEUSERPASSWORD=your_password_here
SKIPSQLSEQUENCE	<p>Sets if the SQL database going to be created.</p> <ul style="list-style-type: none"> • 0 - The installer creates the database, and builds the schema • 1 - No database creation 	Yes, if the installer runs in quiet mode.	0	SKIPSQLSEQUENCE=1
SKIPREGISTRATIONCHECK	If set to 1, the node won't register itself in the Verba database.		0	SKIPREGISTRATIONCHECK=1

SERVERNAMEFORMAT	Sets format for the registration. <ul style="list-style-type: none">• 0 - NETBIOS name• 1 - FQDN		1	SERVERNAMEFORMAT=0
VNATIVELOGON	Sets authentication type for the SQL access. <ul style="list-style-type: none">• 0 - SQL account• 1 - Windows account		0	VNATIVELOGON=1
SQLADDRESS	The address of the SQL server.		(local)	SQLADDRESS=sql1
SQLCATALOG	The name of the SQL database.		verba	SQLCATALOG=verba
SQLUSER	SQL username.		sa	SQLUSER=contoso\srv-verba
SQLPASSWORD	SQL password.			SQLPASSWORD=your_password_here
VSSLCERTIFICATEPATH	Path to the SSL certificate . crt file.			VSSLCERTIFICATEPATH=C:\certs\verbassl.crt
VSSLKEYPATH	Path to the SSL certificate . key file.			VSSLKEYPATH=C:\certs\verbassl.key
VSSLPASSWORD	SSL certificate key password.			VSSLPASSWORD=your_password_here
LOGON_USERNAME	Username for the service user at the filter services.	Yes, if the SELECTEDROLE is set to LF or LFRC.		LOGON_USERNAME=contoso\srv-verba
LOGON_PASSWORD	Password for the service user at the filter services.	Yes, if the SELECTEDROLE is set to LF or LFRC.		LOGON_PASSWORD=your_password_here
RESOLVEDIPV4	The IP address of the server.			RESOLVEDIPV4=192.168.1.13
ADMIN_PASSWORD	Administrator password.	Yes, if the SELECTEDROLE is set to MR or Combo.		ADMIN_PASSWORD=your_password_here
MRHOST	First Media Repository server address.			MRHOST=testmr1
API_PASSWORD	API user password.			API_PASSWORD=your_password_here
ENCRYPTEDPASSWORDS	Sets the format of the passwords provided in the parameters. If set to 1, all the passwords (VCERTPASS, VSERVICEUSERPASSWORD, SQLPASSWORD, VSSLPASSWORD, LOGON_PASSWORD, ADMIN_PASSWORD, API_PASSWORD) have to be provided in an encrypted format.		0	ENCRYPTEDPASSWORDS=1

Upgrading your Verba system

Upgrading a Verba system consist of various steps executed by the installer and includes some manual step also. Before starting the upgrade make sure you have the followings available:

- New Verba system installers
- Valid license file
- Existing Verba system installer in case you need to roll back during the upgrade process
- [Servers, OS, database](#), and [prerequisites \(Java, .Net, etc.\)](#) meeting the requirements of the new system
- A clear and definite plan for the upgrade including backup plan, upgrade plan and rollback plan
- Since the upgrade might require to stop recording for a while, make sure it does not interfere with your business and regulations
- When you have a complex deployment, make sure you have the right engineering resources available knowledgeable of Verba deployments

Verba does not support partial upgrades, all system components and servers need to be upgraded at once. There might be exceptions, but it needs to be authorized and confirmed by a Verba representative.

Verba supports upgrade from version 5 up to the latest version following the procedures described in this document.

If you are aware of any customization (custom database procedures, triggers or customized web interface including branding) in your system, please contact your Verba representative before the upgrade.

The following list briefly outlines the upgrade process:

- Backup Verba database and prepare it for the upgrade process
- Backup existing servers and verify server and OS compatibility
- Uninstall the existing Verba software
- Install the new Verba software
- Configure servers
- Test the new system

Backup Verba database and prepare it for the upgrade process

During the upgrade process, the database has to be altered to support the new version of the software. In order to ensure a fallback option is available, it is mandatory to create a full backup of your Verba database.

For more information, see <https://docs.microsoft.com/en-us/sql/relational-databases/backup-restore/create-a-full-database-backup-sql-server>

Upgrading from 9.3 or earlier

With version 9.4, several database performance improvements were implemented, and this caused major changes in the database. The upgrade process may take significantly longer, (up to 30 minutes for every million records, depending on the resources of the SQL server) when you upgrade from version 9.3 or earlier to version 9.4 or later.

The number of the records currently in the database can be checked by running the following SQL query:

Query for the number of entries in the database

```
SELECT COUNT(*) FROM v_section
```

Based on the number of the database records, SQL version and available free space the following configurations are required.

Step 1 - Optionally set the recovery mode to simple. When the upgrade is complete, you can change it back to its original setting. This step is recommended if the disk space available for the transaction log is limited.

For more information, see <https://docs.microsoft.com/en-us/sql/relational-databases/backup-restore/view-or-change-the-recovery-model-of-a-database-sql-server>

Step 2 - Set the SQL Server Agent service to automatic start and start it (except when using SQL Express Edition, which does not include the SQL Server Agent service). For more information, see <https://docs.microsoft.com/en-us/sql/ssms/agent/autostart-sql-server-agent-sql-server-management-studio>

Step 3 - Optionally rebuild the indexes on the database tables. If the database contains more than one million entries, it is recommended to run the [manual-index-rebuild.sql](#) on the Verba database before the upgrade. This script should be run outside of business hours.

Database partitioning (9.5 or earlier)

With version 9.6 partitioning was added as a recommended step during the installation, when more than 100 million conversations are expected to be stored in the database. The installer configures database partitioning only for future conversations. In order to improve performance for the already recorded conversations, it is possible to add partitioning for historical records.

For more information, see: [Database table partitioning](#)

Backup Verba servers and verify server and OS compatibility

In order to ensure that you can restore the system at any point during the upgrade procedure, you need to make a backup of the entire system.

The easiest and most efficient way to backup your current system is to create snapshots of your (virtual) servers. If your upgrade fails, you can simply restore the system by loading the snapshots.

The uninstall process does not affect or delete the database and the media folders. However, other data needs to be removed from the server. If you would like to keep the application log files for some reason, you need to back the log folder to an external location first.

Follow the steps below to backup the servers to be able to restore the system if you need to roll back changes.

Step 1 - Make a note of all active Verba services on the servers by navigating to **Service Activation** tab under **System / Servers** for 9.x or later versions and under **Administration / Verba Services** in earlier versions. You will need this information when you re-apply the configuration on the servers running the new version.

Step 2 - Stop all Verba services on all servers. If you need to continue recording or you want to minimize downtime, you can continue recording on the Verba Recording Servers by disabling the database access. Before doing so, please consult your Verba representatives to confirm the available options and compatibility issues between the existing and the new system.

Step 3 - Check if your media folders or storage targets are not under C:\Program Files (x86)\Verba. If your media folders or storage targets are under C:\Program Files (x86)\Verba, move the folder to another, more appropriate location.

Step 4 - Optionally make a copy of your log folders to an external location on all servers.

Step 5 - Optionally make a copy of the C:\Program Files (x86)\Verba\resources\webapp\ folder on the Media Repository server to backup branding and other web application customization.

Step 6 - Make a copy of the server registry under HKLM\SOFTWARE\Wow6432Node\Verba key.

Step 7 - Check server configuration (CPU, memory, disk, network), operating system and database version compatibility for the new Verba version.

Uninstall Verba servers

Step 1 - Check that you have valid and up to date backups of your servers, and you verified server and OS compatibility with the new version.

Step 2 - Uninstall the Verba Media Repository Server first, unless you have a single server in your deployment.

Step 3 - Check that you do not have remaining files under C:\Program Files (x86)\Verba folder. If you have, check that no media folder is used under this folder and you made a backup of all relevant content (for instance log files). After checking all of these, delete the content of the folder.

Step 4 - Check that you do not have remaining entries under HKLM\SOFTWARE\Wow6432Node\Verba key. If you have, delete them completely.

Step 5 - Repeat Step 2 through Step 4 for all other Verba servers, including the ones installed on external servers such as Lync/SfB servers.

Install Verba servers

Once you completed the uninstall of your servers, you can go ahead and install the new version.

Step 1 - Run the prerequisites tool from the new installer package to check if there is any missing prerequisite. Install the missing ones and make sure you have Java Runtime version 11 installed on Verba Media Repository and Verba Recording Servers.

Step 2 - Install the new version on the Verba Media Repository server first. The installer will automatically update your database, it can take hours depending on the size of your database.


Step 3 - Install the new version on all Verba Recording Servers and other server roles.

Configure Verba servers and test

Once you installed the new version on your servers, you need to apply the previous configuration and test the new system.

Step 1 - Login to the web interface and navigate to the Verba server and select the **Service Activation** tab. Activate all Verba service according to the previous configuration.

Step 2 - Navigate to **Change Configuration Settings** tab. The system will offer you an option to apply the previous configuration (the configuration in the database) on the server. Select the **Use configuration only from central database** option, or you can manually select the appropriate option below.

 If you select the **Use configuration only from server's registry** option, you will overwrite the working configuration and the system needs to be set up again. Use this with care.

Step 3 - Press **Start** and follow the instructions on the screen to apply the new configuration on the server.

Step 4 - Repeat these steps for all Verba servers in your deployment.

Step 5 - If you have added new servers during the upgrade, simply configure them using an existing configuration template or direct server configuration.

Step 6 - Now you have finished the upgrade. Check all configuration settings (especially the new ones) and execute your test plan to ensure that your system is functioning properly.

Roll back to the previous version

If you encounter any issues during the upgrade and you are unable to resolve them, you need to roll back to the previous, working copy. If you have managed to create server snapshots, you can simply restore them. If you need to manually restore the system, follow the steps below:

- Step 1** - Uninstall the new Verba servers by following the uninstall steps above. Make sure you execute the manual checks also.
- Step 2** - Run the prerequisites tool from the previous installer package. Make sure you have the right Java Runtime on the server.
- Step 3** - Restore the Verba database from the backup.
- Step 4** - Install the Verba Media Repository server first.
- Step 5** - Install the previous version on all other servers.
- Step 6** - Apply the configuration on the servers and test the configuration by following the steps described above.

Upgrade procedure from Carin recorders

The Carin - Verba upgrade procedure consists of three essential steps.

- [Making a backup of the existing Carin installation](#)
- [Removing the existing Carin installation](#)
- [Installing and configuring Verba Recording System and restoring from backup](#)

Making a backup of the existing Carin installation

Step 1 Registry backup - Launch **regedit** from Start - Run..., Navigate to **HKEY_LOCAL_MACHINE/SOFTWARE**, right click on **Carin** and choose Export

Step 2 Media backup - After the registry backup is done, close regedit, open a file manager, navigate to the Carin media folder (by default it is **C:\Program Files\Carin\media**) and backup all files and directories

Step 3 Database backup - After the media file copying procedure is finished, open **Microsoft SQL Management Studio**, connect to the database engine, right click on the database named **carin**, select **Tasks** and choose **Detach...**


Navigate the file manager to the Microsoft SQL Server Data directory (default: **C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Data**) and backup the **carin.mdf** database file.

Removing the existing Carin installation

Before starting the uninstallation procedure, please make sure that you have completed the steps in the previous part, and you have a valid backup of the registry values, the media files and the database.

Step 1 Launch **Add or Remove Programs** from **Control Panel**, select **Carin** and choose **Uninstall**

Step 2 Make sure you backed up the media files from this directory before! Start a file manager, navigate to **C:\Program Files** (assuming default installation path) and delete the **Carin** directory.

 Make sure you have read and done everything in the **Making backups of existing installation** part, and also have valid backups of **registry data, database and media files**.

Verba Technologies **does not** take responsibility for any data loss occurring during self-made upgrade.

Installing and configuring Verba Recording System and restoring from backup

In order to install the new Verba Recording System, please see [Installation Overview](#).

After the regular installation procedure is finished, please follow these steps to restore the backups. The SQL script files mentioned in this topic can be located and downloaded from the Verba Technologies Portal's **Support site**

Step 1 Open **Control Panel, Administrative Tools** and launch **Services**

Step 2 Select all running **Verba** services and stop them one by one


Step 3 Start **Microsoft SQL Management Studio** and connect to the database server

Step 4 Right click on the database named **verba**, select **Tasks** and choose **Detach...**

Step 5 Attach the **carin** database from the backup, by right clicking on **Databases**, and selecting **Attach...**

Step 6 After the attachment is finished, rename the **carin** database to **verba**, or run **rename-database.sql**

Step 7 Execute the SQL script **update-from-carin.sql**.


 This procedure can take several hours, depending on the database size and record count.

Step 8 Execute **update.sql**

Step 9 After the update script has stopped, start the previously stopped Verba services in **Services**

Step 10 Configure the Verba Recording System and the Verba services via the **Web Interface**.

Step 11 Copy the media files from the backup to **C:\Program Files\Verba\media** (assuming default installation path)

 After these steps are completed, **every** password stored in the system, including the database connection's password has to be re-entered, and saved!

Verba Remote Installation Service Description

This document describes how Verba Technologies will help you with your software installations when you are ordering installation services.

The purpose of this document is to outline the information needed and tasks to be completed during the Installation services for the Verba Recording System product line. Since this installation will be conducted by Verba Technologies personnel from an off-site location (in order to reduce installation fees and expenses) Remote Desktop software will be utilized to complete these tasks. Verba Technologies uses the services of LogMeIn, a web based remote desktop support service. Verba Technologies can support additional forms of remote desktop or temporary VPN access at the client's request.

Verba Technologies respects your confidentiality and acknowledges the trust bestowed when 3rd party vendors access your network, and will only use this connection to fulfill the installation requirements of the Client. For further information on Verba Technologies' remote support services please see: <http://www.verba.com/group/support/service-description>

About the information below:

- [Information to be collected before installation](#)
- [Client's Responsibilities](#)
 - [Pre-installation tasks](#)
 - [Installation Tasks](#)
 - [Post Installation Tasks](#)
- [Verba Technologies' Responsibilities](#)
 - [Pre-Installation](#)
 - [Installation Tasks](#)
 - [Post Installation Tasks](#)

Information to be collected before installation

To complete the installation the Verba Technologies support engineer will need the following information from the client, prior to scheduling the installation.

Verba Server Hardware/Software information

- CPU type:
- RAM size:
- HDD size/drives:
- Operating System:
- IP Address:
- Hostname:

Cisco UCM Admin information:

- Version:
- IP/Hostname:
- Administrator user:
- Administrator password: (can be kept confidential and entered by Client)

Gateway information:

- Gateway Model(s):
- IP address(es):
- Cisco Switch Model(s):
- Cisco IP Phone Models:

Verba Installation/Configuration settings

- Log File location:
- Database File location:
- Media File location:
- Outgoing SMTP Server:

- Email account for system alerts:
- SNMP server:
- Type of Recording Method: (Passive or Central)

Client's Responsibilities

Pre-installation tasks

- Verba Server is ready (hardware is configured and Operating System installed) and can be accessed via the internet or via a remote desktop from a computer with internet access
- Provide installation information to Verba (see above)
- Configure Monitor Session/SPAN port to capture traffic from the applicable VLAN/switches
- Provide list of users and extensions/directory numbers
- Provide User/Group mapping and which users are Group Supervisors and/or Group Administrators (All users are members of the default group when created)
- Download the installation files and put them onto the server computer (provide location information to Verba if different from C:\Downloads\)

Installation Tasks

- Have a knowledgeable IT person responsible for this implementation who is available during the agreed upon days/times
- Access the Verba Support website to initiate a Remote Desktop Session (<http://support.verba.com> - login required)
- The computer to be controlled needs to have access to: (Verba server or Desktop)
 - Remotely control the server
 - The internet
 - The Cisco UCM Administration webpage

Post Installation Tasks

- Complete and sign user acceptance testing script from a PC (other than the Verba Server) and return to Verba
- Configure Additional Users, Groups, Extensions as needed
- Configure Additional IP Phones for XML Service access as needed
- Configure SQL Server and Media file backup schedule and archiving schedule as desired

Verba Technologies' Responsibilities

Pre-Installation

- Set time/date for Remote Desktop Support Session
- Send client server requirement information and other information needed
- Make installation files available to client (secured web access) to download

Installation Tasks

- Install Prerequisite items: Java, .NET etc.
- Install and configure SQL Server database
- Install and configure Verba Server Components
- Install and configure the Verba Node Manager
- Validate initial settings and database connectivity
- Validate SPAN port data capture
- Configure Users and user privileges
- Configure User to Extension mapping with recording mode
- Configure User to Group mapping with privileges

Post Installation Tasks

- Configure Cisco UCM phone service for Verba phone service users (Optional)
- Configure Email/SNMP Alerts for basic system monitoring
- Knowledge transfer: Walk through basic user navigation
- Knowledge transfer: Walk through basic system administration and node manager
- Provide Client with Product Support Online access account information

Installing the Verba Lync extension for Lync 2010

The Verba Lync Extension allows to control Lync conference recording directly in the Lync desktop client running Windows OS.

Client registry settings

The extension can be enabled by entering the following registry entries:

Windows Registry Editor Version 5.00

```
[HKEY_CURRENT_USER\Software\Microsoft\Communicator\ContextPackages\{8551F06A-BCA1-40ED-A57F-04EE5  
"Name"="Meeting Recorder"  
"InternalURL"="http://verbaMR.contoso.com/verba/silverlight/LyncMeetingRecorderExtension2010.jsp"  
"ExternalURL"="http://verbaMR.contoso.com/verba/silverlight/LyncMeetingRecorderExtension2010.jsp"  
"ExtensibilityWindowSize"=dword:00000001
```

Description of the fields:

Name	Description
Name	The name of the application. It is displayed in the Lync menu and at the bottom of the Extension window.
InternalURL ExternalURL	Specifies the application URL in the Microsoft Lync Server 2010 domain. The application automatically detects which URL to use, InternalURL or ExternalURL, based on the client location.
ExtensibilityWindowSize	Sets the minimum size of the extension window. 0 = small (300 x 200 pixels), 1 = medium (400 x 600 pixels), 2 = large (800 x 600 pixels).

For more detailed information, please refer to the documentation at [http://msdn.microsoft.com/en-us/library/office/hh378557\(v=office.14\).aspx](http://msdn.microsoft.com/en-us/library/office/hh378557(v=office.14).aspx)

Adding the server to Trusted Sites

In addition to applying the configuration to the local registry on the client computers, the <http://verbaMR.contoso.com> address needs to be added to the Trusted Sites in the Internet Explorer.

Installing the Verba Lync extension for Lync 2013

The Verba Lync Extension allows to control Lync conference recording directly in the Lync desktop client running Windows OS.

Client registry settings

The extension can be enabled by entering the following registry entries:

```
Windows Registry Editor Version 5.00
```

```
[HKEY_CURRENT_USER\Software\Microsoft\Communicator\ContextPackages]
```

```
[HKEY_CURRENT_USER\Software\Microsoft\Communicator\ContextPackages\{8551F06A-BCA1-40ED-A57F-04EE5
```

```
"Name"="Meeting Recorder"
```

```
"InternalURL"="http://verbaMR.contoso.com/verba/silverlight/LyncMeetingRecorderExtension2010.jsp"
```

```
"ExternalURL"="http://verbaMR.contoso.com/verba/silverlight/LyncMeetingRecorderExtension2010.jsp"
```

```
"ExtensibilityWindowSize"=dword:00000001
```

Description of the fields:

Name	Description
Name	The name of the application. It is displayed in the Lync menu and at the bottom of the Extension window.
InternalURL ExternalURL	Specifies the application URL in the Microsoft Lync Server 2013 domain. The application automatically detects which URL to use, InternalURL or ExternalURL, based on the client location.
ExtensibilityWindowSize	Sets the minimum size of the extension window. 0 = small (300 x 200 pixels), 1 = medium (400 x 600 pixels), 2 = large (800 x 600 pixels).

For more detailed information, please refer to the documentation at [http://msdn.microsoft.com/en-us/library/office/jj933101\(v=office.15\).aspx](http://msdn.microsoft.com/en-us/library/office/jj933101(v=office.15).aspx)

Adding the server to Trusted Sites

In addition to applying the configuration to the local registry on the client computers, the <http://verbaMR.contoso.com> address needs to be added to the Trusted Sites. Lync 2013 has its own location for trusted sites in the registry. This means that you cannot add the server to Trusted Site using Internet Explorer / Internet Options (like in Lync 2010); you need to use a separate registry key. The format for the registry key looks like this:

```
Windows Registry Editor Version 5.00
```

```
[HKEY_CURRENT_USER\Software\Microsoft\Office\Lync\Security\Trusted Sites]
```

```
[HKEY_CURRENT_USER\Software\Microsoft\Office\Lync\Security\Trusted Sites\verbaMR.contoso.com]
```

```
"https"=dword:00000001
```

```
"http"=dword:00000000
```

This sample indicates that <https://verbaMR.contoso.com> will be trusted. If the same URL with HTTP should be trusted, then flip the “http” part to a 1.

Requesting and assigning certificates

Certificates are required in several cases when configuring Verba. An SSL certificate is required when a trusted HTTPS access have to be configured to the web application. Certificates are used as well when file encryption and integrity protection or the recording announcement is a requirement. Anyway, all certificates can be replaced used between the Verba services to establish a secure connection.

Certificates can be requested from a 3rd party provider, or from the local CA.

Request a new certificate from the local CA using Microsoft Management Console

Step 1 - Right click (or open it in Windows Server 2008 R2) on the **Start** menu and click on **Run**. Type **mmc.exe** and press enter.

Step 2 - Go to the **File / Add/Remove Snap-in...** menu.

Step 3 - From the list on the left side select **Certificates** and click on the **Add** button.

Step 4 - Select **Computer Account** then click **Next**. On the next page, select **Local Computer** then click **Finish**. In the MMC windows press **OK**.

Step 5 - Expand the **Certificates** and right click on the **Personal** node. Select the **All Tasks / Request New Certificate** menu.

Step 6 - On the first page click **Next**. Select a **Certificate Enrollment Policy** then click **Next**.

Step 7 - Select a certificate type. On the right side expand the **Details** then click on the **Properties**.

Step 8 - Set the properties of the certificate based on the purpose:

Type of Certificate	Properties
Certificate for SSL connection for trusted HTTPS access	Subject tab: <ul style="list-style-type: none">Under the Subject name section set the Type to Full DN and Add the server FQDN as Value in the following format: CN=servername.yourdomain.com Under the Alternative name section set the Type to DNS and add the following Values:<ul style="list-style-type: none">The IP address of the server where the web application hosted.The hostname of the server where the web application hosted.The FQDN of the server where the web application hosted.(Optional) The loadbalancer hostname and/or FQDN.(Optional) External URL.
Certificate for Encryption	Private Key tab: <ul style="list-style-type: none">Under the Key options section turn on the 'Make private key exportable' setting.
Certificate for Signing	Private Key tab: <ul style="list-style-type: none">Under the Key options section turn on the 'Make private key exportable' setting
Certificate for the Announcement service	<ul style="list-style-type: none">Subject tab:<ul style="list-style-type: none">Under the Subject name section set the Type to Full DN and Add the trusted application server pool FQDN as Value in the following format: CN=poolfqdn.yourdomain.comUnder the Alternative name section set the Type to DNS and add the following Values:<ul style="list-style-type: none">The FQDNs of the Announcement servers.The FQDN of the trusted application pool.General tab:<ul style="list-style-type: none">Provide a friendly name. This name have to be configured in the Announcement Service configuration.

Step 9 - In the Certificate Properties window click **OK**, then click **Enroll**.

Request a new certificate from the local CA for Announcement service using PowerShell

Certificate can be requested by the following command in PowerShell:

```
Request-CsCertificate -New -Type default -FriendlyName "Announcement service" -CA ca.contoso.com\
```

If there is more than one nodes in the Trusted Application pool then an additional parameter required for the other nodes:

```
Request-CsCertificate -New -Type default -FriendlyName "Announcement service" -CA ca.contoso.com\
```

Description of the parameters:

Parameter	Description	Sample value
-FriendlyName	The friendly name of the certificate	"Announcement Service"
-CA	The address of the local Certificate Authority	ca.contoso.com\ContosoCA
-ComputerFQDN	The FQDN of the Trusted Application pool	servername.yourdomain.com
-DomainName	The FQDNs of the other Announcement Server nodes	"server2.yourdomain.com,server3.yourdomain.com"

Generating a key pair and Certificate Signing Request with Java Keytool, then signing it with the CA and exporting the certificate

When requesting a certificate from the CA directly is not possible, then a custom request have to be created and sign it with the CA. Then it will be possible to create certificate signed with the CA.

Step 1 - Generating a key pair.

Run the following command for generating a new key pair (public and private):

```
"%JAVA_HOME%\bin\keytool" -genkey -keysize 1024 -keyalg RSA -validity 36500 -keystore verba.jks -
```

Parameter name	Description	Sample values
-keysize	The size of the key. The bigger the size, the strongest the encryption.	1024 2048
-keyalg	The algorithm used for the key.	RSA
-keypass	The password used for protecting the private key.	P@ssw0rd123
-validity	The validity of the keys in days.	365 3650
-keystore	The store where the keys will be stored. It can be a new keystore (it will be created) or an existing one.	verba.jks C:\verba.keystore
-storepass	The password used to protect the keystore. This must be specified if we using an existing keytoe which is proteted.	P@ssw0rd123
-alias	An alias for the generated key pair.	tomcat

-dname	The subject of the certificate.	"CN=verbaserver-fqdn" "CN=verbaserver-fqdn, OU=IT, O=IT, L=Little Rock, ST=Arkansas, C=US"
--------	---------------------------------	---

Step 2 - Generating a Certificate Signing Request (CSR).

Run the following command:

```
"%JAVA_HOME%\bin\keytool" -certreq -alias tomcat -keyalg RSA -file request.csr -keystore verba.jk
```

Parameter name	Description	Sample values
-alias	The alias for the generated key pair. It has to match to the one provided at the previous step.	tomcat
-keyalg	The algorithm used for the key. It has to match to the one provided at the previous step.	RSA
-file	The name of the generated CSR file.	request.csr C:\temp\request.csr
-keystore	The store where the keys are stored. It has to match to the one provided at the previous step.	verba.jsk C:\verba.keystore

Step 3 - Sign the CSR file with the CA.

Step 4 - Add the signed certificate to the keystore.

Run the following command for adding the root CA certificate to the keystore:

```
"%JAVA_HOME%\bin\keytool" -import -alias root -keystore verba.jks -trustcacerts -file root.cer
```

(Optional) Run the following command for adding the intermediate CA certificate to the keystore:

```
"%JAVA_HOME%\bin\keytool" -import -alias inter -keystore verba.jks -trustcacerts -file intermedia
```

Parameter name	Description	Sample values
-alias	The alias for the generated key pair. It has to match to the one provided at the previous step.	tomcat
-keystore	The store where the keys will be stored. It has to match to the one provided at the previous step.	verba.jsk C:\verba.keystore
-file	The CA certificate file.	ca-certificate.cer C:\temp\ca-certificate.cer

Run the following command for adding the signed certificate to the keystore:

```
"%JAVA_HOME%\bin\keytool" -import -alias tomcat -keystore verba.jks -file signed-certificate.cer
```

Parameter name	Description	Sample values
----------------	-------------	---------------

-alias	The alias for the generated key pair. It has to match to the one provided at the previous step.	tomcat
-keystore	The store where the keys will be stored. It has to match to the one provided at the previous step.	verba.jks C:\verba.keystore
-file	The signed certificate file.	signed-certificate.cer C:\temp\signed-certificate.cer

Step 5 - Export the signed certificate with the private key.

Run the following command:

```
"%JAVA_HOME%\bin\keytool" -importkeystore -srckeystore verba.jks -alias tomcat -destkeystore verb
```

Parameter name	Description	Sample values
-srckeystore	The store where the keys are stored. It has to match to the one provided at the previous step.	verba.jks C:\verba.keystore
-alias	The alias for the generated key pair. It has to match to the one provided at the previous step.	tomcat
-destkeystore	The name of the certificate file.	verba.p12
-deststoretype	The type of the exported certificate file.	PKCS12

Step 6 (Optional) - Import the certificate to the Windows Certificate Store.

Double click on the exported .p12 file, then click on the **Install Certificate...** button. Select **Local Computer** then click **Next**. On the next page click **Next**, then **Finish**.

Private Key tab:

- Under the Key options section turn on the 'Make private key exportable' setting.
- Subject tab:
 - Under the Subject name section set the Type to Full DN and Add the trusted application server pool FQDN as Value in the following format: CN=[poolfqdn.yourdomain.com](#)
 - Under the Alternative name section set the Type to DNS and add the following Values:
 - The FQDNs of the Announcement servers.
 - The FQDN of the trusted application pool.
- General tab:
 - Provide a friendly name. This name has to be configured in the Announcement Service configuration.

Verba PowerShell Deployment Toolkit

The Verba PowerShell Deployment Toolkit simplifies the process of the Verba deployments and upgrades in large environments. The toolkit consists of two PowerShell files:

- **autoinstall.ps1** : Configurable PowerShell script for uninstalling, installing and upgrading Verba servers and components.
- **verba-*.psm1** : A PowerShell library which contains a collection of functions usable for Verba deployments. For the documentation of the functions see: [Verba PowerShell Deployment Library](#)

Preparations

Verba Prerequisites

The Verba PowerShell Deployment Toolkit does not install the prerequisites of the Verba services (Java, Visual C++, etc.) nor does the registration of the SfB/Lync Filter application in the SfB/Lync pool. These have to be done manually.

Deployment Toolkit Prerequisites

⚠ Make sure the x64 version of PowerShell (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe) is being used!

On the machine where the Verba Powershell Deployment Toolkit will be started, the **SqlServer Powershell module** has to be installed. Do the following steps in order to install the module:

Step 1 - Download and install [PowerShell 5.1](#). After the installation, restart the machine.

Step 2 - Open PowerShell as administrator.

ⓘ Script execution policy

Script execution may be restricted in the domain. In order to remove the restriction, execute the following command:

```
Set-ExecutionPolicy -ExecutionPolicy Unrestricted -Scope LocalMachine -Force
```

Step 3 - Execute the following command. This will set the security protocol being used at the subsequent commands when communicating through the internet.

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
```

Step 4 - Execute the following command. When asked, type in **Yes** and press enter to allow the operation. This will download the NuGet package provide provider, and registers it as the default repository for PowerShell modules.

```
Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force
```

Step 5 - Execute the following command. When asked, type in **Yes** and press enter to allow the operation. This will download the SqlServer module.

ⓘ Installing the SqlServer module without internet connection

The SqlServer module can be installed also without an internet connection. Do the same commands on another computer with an internet connection, then copy the C:\Program Files\WindowsPowerShell\Mod

```
Install-Package -Name SqlServer -RequiredVersion 21.1.18235 -AllowClobber
```

Group Memberships

The **Windows User who runs the script (logged in to the server)** must be added to the following local groups at **all Verba servers**.

- **Administrators**
- **Remote Management Users**

Database

If database mirroring is used, make sure that the primary database (based on the Verba configuration) is the principal!

Configuration

The Verba PowerShell Deployment Toolkit can be configured by editing the `autoinstall.ps1` file. The configuration part can be found at the beginning of the file, between the "Configuration" and "End of configuration" lines (except the `$Servers` variable). Edit the values of the following variables:

Variable	Description	Example value
<code>[string]\$InstallerPath</code>	A network folder that contains the Verba executables (VerbaRecording.msi, VerbaAdditionalRoles.msi). The network folder has to be accessible for the windows user which is used for running the script.	"\\storage\Verba\8.8\"
<code>[string]\$TempPath</code>	The folder path for temporary files. This folder will be created on each server.	"C:\verba_install\"
<code>[string]\$AppPath</code>	Verba installation directory.	"C:\Program Files\Verba\"
<code>[bool]\$Test</code>	Tests the servers The script test the following: <ul style="list-style-type: none">• If the script can log into the server• If the Verba prerequisites are installed• If the server can reach the database server on port 1433• Is there enough disk space	<code>\$true</code>
<code>[bool]\$Uninstall</code>	Sets whether the script will uninstall the specified servers. The script removes the Verba software, the registry set and the files from the server. This setting is ignored when <code>\$Upgrade=\$true</code> is used.	<code>\$false</code>
<code>[bool]\$Install</code>	Installs the Verba application on the servers. This setting is ignored when <code>\$Upgrade=\$true</code> is used.	<code>\$false</code>
<code>[bool]\$BackupConfiguration</code>	Backups the list of the activated services and the registry from the servers. The filenames going to be the hostnames of the servers. If the files already exist, the filename going to end with <code>.bak</code> . This setting is ignored when <code>\$Upgrade=\$true</code> is used.	<code>\$false</code>
<code>[bool]\$RestoreConfiguration</code>	Restores the list of the activated services and the registry from the files named with the corresponding server hostnames. This setting is ignored when <code>\$Upgrade=\$true</code> is used.	<code>\$false</code>

[bool]\$Upgrade	<p>Sets whether the script will upgrade the specified servers. The upgrade involves the following process:</p> <ul style="list-style-type: none"> • Backups the existing configuration in the registry and the list of activated Verba services. • Uninstalls the current Verba software. • Installs the new version using the executables specified at the \$path value. • Restores the previously saved configuration (registry). • Activates and starts the Verba services based on the previous configuration. <p>If turned on, then the \$Uninstall, \$Install, \$Backupconfiguration and \$Restoreconfiguration values will be ignored.</p>	\$false
[bool]\$KeepLogs	Sets whether the script should remove the log folder in case of uninstalling or upgrading.	\$false
[bool]\$ResetAPIPassword	Set to \$true if you want to reset the API user's password. It is recommended when you are upgrading from 8.x.	\$false
[bool]\$RemoveLegacyCertificateSettings	Set to \$true if you want to delete old legacy certificate settings from the profiles. It is recommended when you are upgrading from 8.x.	\$false
[bool]\$SkipNodeRegistrationCheck	Set \$true if you want to skip the node registration check, so the script will register the Servers with NETBIOS name by default. It is recommended if you are upgrading from 8.x.	\$false
[bool]\$UpdateIMFormat	Set to \$true if you want to update the old IM schema in the database. It is recommended when you are upgrading from 8.x. Depending on the amount of recordings, this process can take a while.	\$false
[string]\$APIUsername	Verba API username.	"verbaapi"
[string]\$APIPassword	Verba API password.	"P@ssw0rd"
[string]\$AdministratorUsername	Verba Administrator username.	"administrator"
[string]\$AdministratorPassword	Verba Administrator password.	"P@ssw0rd"
[string]\$SSLCertificateSubject	The subject of the SSL certificate generated for the Web Application. The script will generate a self-signed certificate with this subject.	"testmr1.verbatest.local"
[int]\$StartupType	<p>The startup type of the Verba services:</p> <ul style="list-style-type: none"> • 0: Disabled • 1: Manual • 2: Automatic • 3: AutomaticDelayed 	2
[string]\$ServiceUsername	The Windows domain account used as a service account in the case of the Verba SfB/Lync Filter installation.	"contoso\verba-service"
[string]\$ServicePassword	The password of the Windows domain account.	"P@ssw0rd"
[string]\$DatabaseHost	The hostname of the server where the Verba database hosted.	"SQLSERVER"
[string]\$DatabaseName	The name of the Verba database.	"Verba"

[bool]\$SQLAuth	Sets whether SQL Authentication will be used for the SQL connection. If set to 0, then Windows authentication will be used for the SQL connection.	\$true
[string]\$DatabaseUsername	Username for the SQL connection. If the \$sqlAuth setting is set to 1, then a SQL user has to be provided. If the \$sqlAuth setting is set to 0, then a Windows domain user has to be provided in "domain\user" format.	"verba-user"
[string]\$DatabasePassword	The password of the SQL connection.	"P@ssw0rd"
[bool]\$MultiSubnetFailover	Set to \$true, if Always-On database is being used with Multi-Subnet Failover.	\$false
[bool]\$DBPartitioning	Set to \$true, if you want to turn on database partitioning. This improves the performance in the case of large databases.	\$true
[bool]\$EncryptedPasswords	#Set to \$true, if you are providing the passwords (\$APIPassword, \$AdministratorPassword, \$ServicePassword, \$DatabasePassword, and -SSLCertificatePassword at the \$Servers) in encrypted format	\$false
[bool]\$EnableCloudMode	Experimental feature. Sets whether cloud mode will be used for the Node Manager	\$false
[string]\$MRPoolName	Experimental feature. The Media Repository pool name.	"testmr1"
[int]\$MRPortNumber	Experimental feature. The port used at the Media Repository for the incoming registration requests.	4432
[string]\$TokenPassword	Experimental feature. The password of the registration token.	"P@ssw0rd"

Server configuration

The servers can be configured not at the beginning of the script, but below, at line 133. The \$Servers variable is an array of VerbaServer objects. New items can be added with the New-VerbaServer command. The command parameters are the following:

Parameter	Description	Mandatory	Example value
-FQDN	The FQDN, hostname, or IP address of the server to install.	Yes	"verbars.contoso.local"
-Role	The Verba server role to install. Accepted values: Combo, MR, RS, LF, LFRC, RC, SA, SS	Yes	Combo
-UseLegacyAPI	Switch parameter. If present, the legacy, less secure connection will be used between the Verba services (Verba 8.x and older).	Yes, if the -UseAdvancedAPI parameter is not present	
-UseAdvancedAPI	Switch parameter. If present, the new, certificate-based connection will be used between the Verba services (Verba 9.0 and later). If present, either the -ServerCertThumbprint or the -GenerateCertificates parameter is mandatory.	Yes, if the -UseLegacyAPI parameter is not present	

-ServerCertThumbprint	The thumbprint of the server certificate that will be used for the connection between the Verba services. The certificate must be in the Windows Certificate Store.	Yes, if the -GenerateCertificates parameter is not present	" a909502dd82ae41433e6f83886b00d4277a32a7b "
-GenerateCertificates	Switch parameter. If present, the script will generate certificates. If present, either the -CA or the -CAFQDN parameter is mandatory.	Yes, if the -ServerCertThumbprint parameter is not present	
-CA	Switch parameter. If present, the script will generate a self-signed certificate for CA certificate, and a server certificate using this CA certificate.	Yes, if the -GenerateCertificates is present, and the -CAFQDN parameter is not present	
-CAFQDN	The FQDN of the Verba MR or Combo server that acts as a CA. The script will request a server certificate from this server.	Yes, if the -GenerateCertificates is present, and the -CA parameter is not present	"verbamr.contoso.local"
-SSLCertificatePath	Path to the .crt file that will be used as an SSL certificate by the Verba Web Application. The file must exist at the given location. In order to generate this file from .pfx or .p12 file, see: Installing an SSL certificate for HTTPS access	Yes, if the -Role parameter is set to MR or Combo, and the -GenerateSSLCertificate parameter is not present	"C:\certs\verba.crt"
-SSLCertificateKeyPath	Path to the .key file that will be used as an SSL certificate by the Verba Web Application. The file must exist at the given location. In order to generate this file from .pfx or .p12 file, see: Installing an SSL certificate for HTTPS access	Yes, if the -Role parameter is set to MR or Combo, and the -GenerateSSLCertificate parameter is not present	"C:\certs\verba.key"
-SSLCertificatePassword	The password of the .key file.	Yes, if the -Role parameter is set to MR or Combo, and the -GenerateSSLCertificate parameter is not present	"P@ssw0rd"
-GenerateSSLCertificate	Switch parameter. If present, the script will generate a self-signed SSL certificate for the Web Application. If present, the -SSLCertificateRequest parameter is mandatory.	Yes, if the -Role parameter is set to MR or Combo, and none of the following parameters are present: -SSLCertificatePath, -SSLCertificateKeyPath, -SSLCertificatePassword	
-SSLCertificateRequest	Certificate request object for the SSL certificate that will be used for the Web Application.	Yes, if the -GenerateSSLCertificate parameter is present	\$sslCertificate

-LocalIP	<p>Local IP configuration for the server. If not provided, the IP address of the first NIC will be used. If provided, then the given IP address will be used.</p> <p>It is also possible to provide a partial IP address as a wildcard with the asterisk symbol. In this case, the script will check the IP addresses of the NICs, and the first one will be used that is matching the provided wildcard. If none of the IP addresses are matching to the wildcard, then the first NIC IP will be used.</p>	No	<p>"192.168.1.1"</p> <p>"192.*"</p>
----------	---	----	-------------------------------------

Examples:

Install server with legacy configuration (Verba 8.x) without Advanced API, and self-signed SSL certificate

```
$servers = @(
(New-VerbaServer -FQDN "verbamr.contoso.local" -Role MR -UseLegacyAPI -GenerateSSLCertificate -SSLCertificateRequest
$sslCertificate),
(New-VerbaServer -FQDN "verbars.contoso.local" -Role RS -UseLegacyAPI)
)
```

Install server with legacy configuration (Verba 8.x) without Advanced API, and 3rd party SSL certificate


```
$servers = @(
(New-VerbaServer -FQDN "verbamr.contoso.local" -Role MR -UseLegacyAPI -SSLCertificatePath "C:\certs\verba.crt" -
SSLCertificateKeyPath "C:\certs\verba.key" -SSLCertificatePassword "P@ssw0rd"),
(New-VerbaServer -FQDN "verbars.contoso.local" -Role RS -UseLegacyAPI)
)
```

Install Verba 9.x with Verba self-signed CA generated server certificates, and self-signed SSL certificate

```
$servers = @(
(New-VerbaServer -FQDN "verbamr.contoso.local" -Role MR -UseAdvancedAPI -GenerateCertificates -CA -GenerateSSLCertificate -
SSLCertificateRequest $sslCertificate),
(New-VerbaServer -FQDN "verbars.contoso.local" -Role RS -UseAdvancedAPI -GenerateCertificates -CAFQDN "verbamr.contoso.local"),
)
```

Install Verba 9.x with existing server certificates and existing SSL certificates

```
$servers = @(
(New-VerbaServer -FQDN "verbamr.contoso.local" -Role MR -UseAdvancedAPI -ServerCertThumbprint
"7E3C477D6A308ADAAE1AA9E2C5AE8BE0744A6BD1" -SSLCertificatePath "C:\certs\verba.crt" -SSLCertificateKeyPath "C:\certs\verba.
key" -SSLCertificatePassword "P@ssw0rd"),
(New-VerbaServer -FQDN "verbars.contoso.local" -Role RS -UseAdvancedAPI -ServerCertThumbprint
"7E3C477D6A308ADAAE1AA9E2C5AE8BE0744A6BD1"),
)
```

 When the configuration is done, the script can be started.

Running the Deployment Toolkit

In order to run the Deployment Toolkit, start the autoinstall.ps1 script with an administrator PowerShell.


```
CredSSP Authentication Configuration for WS-Management
CredSSP authentication allows the server to accept user credentials from a remote computer. If you enable CredSSP
authentication on the server, the server will have access to the user name and password of the client computer if the
client computer sends them. For more information, see the Enable-WSManCredSSP Help topic.
Do you want to enable CredSSP authentication?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): y

cFg          : http://schemas.microsoft.com/wbem/wsman/1/config/service/auth
lang         : en-US
Basic        : false
Kerberos     : true
Negotiate    : true
Certificate  : false
CredSSP      : true
CbtHardeningLevel : Relaxed

CredSSP Authentication Configuration for WS-Management
CredSSP authentication allows the user credentials on this computer to be sent to a remote computer. If you use CredSSP
authentication for a connection to a malicious or compromised computer, that computer will have access to your user
name and password. For more information, see the Enable-WSManCredSSP Help topic.
Do you want to enable CredSSP authentication?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): y
cFg          : http://schemas.microsoft.com/wbem/wsman/1/config/client/auth
lang         : en-US
Basic        : true
Digest       : true
Kerberos     : true
Negotiate    : true
Certificate  : true
CredSSP      : true
```

Running the Deployment Toolkit using Command Line Parameters

Instead of providing the settings by modifying the `autoinstall.ps1` file, the setting values can be also provided directly using command line parameters. If a parameter is not provided, the script will use the default values within the file.

The following example shows how to start the script using command line parameters:

```
$p = Get-Location
Import-Module -Name "$($p.Path)\Verba-Deployment-Toolkit.psml"

$sslCertificate = New-VerbaCertificateRequest -Subject "verbamr.contoso.local"

$servers = @(
(New-VerbaServer -FQDN "verbamr.contoso.local" -Role MR -UseAdvancedAPI -GenerateCertificates -C
(New-VerbaServer -FQDN "verbars.contoso.local" -Role RS -UseAdvancedAPI -GenerateCertificates -C
)

.\autoinstall.ps1 -InstallerPath "\\255.255.255.255\Releases" -TempPath "C:\verba_temp" -AppPath
```

Verba PowerShell Deployment Library

The Verba PowerShell library makes it possible to automate functions, that would normally need to be done manually.

The available commands are detailed in the table below.

Syntax	Parameters	Description
<code>Install-RemoteVerbaServer -Host \$host -Role \$role [-WindowsAuth] [-sqlAuth] -SqlServerAddress \$sqlserveraddress-DatabaseName \$databasename -SqlUser \$sqluser -SqlPassword \$sqlpassword -WindowsUser \$windowsuser -WindowsPassword \$windowspassword -Installerpath \$installerpath -ManagementAddress \$managementaddress -MrPoolName \$mrpoolname -MrPort \$mrport -Cloudmode \$cloudmode -TokenPassword \$tokenpassword -Path \$path</code>	<ul style="list-style-type: none">• Host Type: String The hostname of the server where the Verba software will be installed• Role Type: String The Verba server role to be installed.• WindowsAuth Type: Switch Sets whether windows authentication will be used for the SQL access.• sqlAuth Type: Switch Sets whether SQL authentication will be used for the SQL access.• SqlServerAddress Type: String The hostname of the server where the Verba database hosted.• DatabaseName Type: String The name of the Verba database.• SqlUser Type: String The SQL user name to be used if the -sqlAuth switch is used• SqlPassword Type: String The SQL password to be used if the -sqlAuth switch is used• WindowsUser Type: String The windows user name to be used if the -WindowsAuth switch is used• WindowsPassword Type: String The windows password to be used if the -WindowsAuth switch is used• InstallerPath Type: String The path to the Verba executables.• ManagementAddress Type: String The IP address of the server• MrPoolName Type: String The name of the Media Repository pool if the -Cloudmode is set to 1	Installs the Verba software on the provided host based on the provided parameters.

	<ul style="list-style-type: none"> • MrPort Type: Int Default: 4432 The registration port of the Media Repository if the -Cloudmode is set to 1 • Cloudmode Type: Int Default: 0 Sets whether the cloud mode is turned on. • TokenPassword Type: String The token password if the -Cloudmode is set to 1. • Path Type: String Default: "C:\Program Files (x86)\Verba" The installation folder 	
<pre>Install-VerbaApplication -Role \$role [-WindowsAuth] [-sqlAuth] -SqlServerAddress \$SqlServerAddress -DatabaseName \$DatabaseName -SqlUser \$SqlUser -SqlPassword \$SqlPassword -WindowsUser \$WindowsUser -WindowsPassword \$WindowsPassword -InstallerPath \$InstallerPath -ManagementAddress \$ManagementAddress - MrPoolName \$MrPoolName -MrPort \$MrPort -Cloudmode \$Cloudmode -TokenPassword \$TokenPassword -Path \$path</pre>	<ul style="list-style-type: none"> • Role Type: String The Verba server role to be installed. • WindowsAuth Type: Switch Sets whether windows authentication will be used for the SQL access. • sqlAuth Type: Switch Sets whether SQL authentication will be used for the SQL access. • SqlServerAddress Type: String The hostname of the server where the Verba database hosted. • DatabaseName Type: String Default: "verba" The name of the Verba database. • SqlUser Type: String Default: "sa" The SQL user name to be used if the -sqlAuth switch is used • SqlPassword Type: String The SQL password to be used if the -sqlAuth switch is used • WindowsUser Type: String Default: "VERBALABS\Administrator" The windows user name to be used if the -WindowsAuth switch is used • WindowsPassword Type: String The windows password to be used if the -WindowsAuth switch is used • InstallerPath Type: String The path to the Verba executables. 	<p>Installs the Verba software on the local host based on the provided parameters.</p>

	<ul style="list-style-type: none"> • ManagementAddress Type: String Default: The IP address of the host provided at the -SqlServerAddress The IP address of the server • MrPoolName Type: String The name of the Media Repository pool if the -Cloudmode is set to 1 • MrPort Type: Int Default: 4432 The registration port of the Media Repository if the -Cloudmode is set to 1 • Cloudmode Type: Int Default: 0 Sets whether the cloud mode is turned on. • TokenPassword Type: String The token password if the -Cloudmode is set to 1. • Path Type: String Default: "C:\Program Files (x86)\Verba" The installation folder 	
<p>Get-VerbaManagemntIP - Hostname \$hostname</p>	<ul style="list-style-type: none"> • Hostname Type: String The hostname of the server 	<p>Returns the IP address of the provided host.</p>
<p>Set-MultstringRegValue -Hostname \$hostname -Subkey \$subkey -Value \$value -Arr \$arr</p>	<ul style="list-style-type: none"> • Hostname Type: String The hostname of the server • Subkey Type: String The path to the registry key • Value Type: String The name of the value to change • Arr Type: String[] The multi-string data to set 	<p>Sets a multi-string registry value on the provided host.</p>
<p>Copy-VerbaInstaller -Hostname \$hostname -Role \$role -WorkingFolder \$workingfolder \$Source \$source</p>	<ul style="list-style-type: none"> • Hostname Type: String The hostname of the server • Role Type: String The role to be installed • WorkingFolder Type: String The temporary folder to be created on the server • Source Type: String The path to the folder where the executables can be found 	<p>Copies the executables from the source folder to the work folder on the provided host.</p>

<p>Install-VerbaDatabase -DbHost \$dbhost -DbName \$dbname -SqlUser \$sqluser -SqlPassword \$sqlpassword -sqlScriptFolder [-WinAuth]</p>	<ul style="list-style-type: none"> • DbHost Type: String The hostname of the SQL server • DbName Type: String The name of the Verba database • SqlUser Type: String The username to be used for the SQL connection • sqlPassword Type: String The password to be used for the SQL connection • sqlScriptFolder Type: String Default: "C:\Program Files (x86)\Verba\resources\db" The path to the folder where the SQL scripts can be found 	<p>Installs a Verba database using the scripts found in the provided folder.</p>
<p>Get-VerbaSQLExecutionInfo -DbHost \$dbhost -DbName \$dbname -SqlUser \$sqluser -SqlPassword \$sqlpassword -sqlScriptName \$sqlscriptname</p>	<ul style="list-style-type: none"> • DbHost Type: String The hostname of the SQL server • DbName Type: String The name of the Verba database • SqlUser Type: String The username to be used for the SQL connection • sqlPassword Type: String The password to be used for the SQL connection • sqlScriptName Type: String The name of the SQL script 	<p>Provides execution info about the provided SQL script.</p>
<p>Uninstall-VerbaApplication -Hostname \$hostname [-keepLogs]</p>	<ul style="list-style-type: none"> • Hostname Type: String The hostname of the server • keepLogs Type: Switch Sets whether the log files should be kept or not 	<p>Uninstalls the Verba software from the provided host.</p>
<p>Copy-VerbaDatabaseScripts -Hostname \$hostname -TargetFolder \$targetfolder</p>	<ul style="list-style-type: none"> • Hostname Type: String The hostname of the server • TargetFolder Type: String The target folder on the provided host 	<p>Copies the Verba database scripts from the local Verba installation folder to the provided host.</p>

<p>Export-VerbaRegistry -Hostname \$hostname -BackupPath \$backuppath -KeyName \$keyname</p>	<ul style="list-style-type: none"> • Hostname Type: String The hostname of the server • BackupPath Type: String The path where the registry will be saved to. • KeyName Type: String Default: "SOFTWARE\Wow6432Node\Verba" The key which will be exported. 	<p>Exports the specified registry set to the provided path from the provided host.</p>
<p>Import-VerbaRegistryBackup -Hostname \$hostname -BackupPath \$backuppath</p>	<ul style="list-style-type: none"> • Hostname Type: String The hostname of the server • BackupPath Type: String The path where the registry is saved. 	<p>Imports the provided registry set on the provided host.</p>
<p>Set-VerbaServices -Hostname \$hostname -BackupPath \$backuppath -StartupType \$startuptype [-Restart]</p>	<ul style="list-style-type: none"> • Hostname Type: String The hostname of the server • BackupPath Type: String The path where the backup of the activated services can be found. • StartupType Type: Int The startup type of the restored services: 0 - disabled, 1 - manual, 2 - Automatic, 3 - AutomaticDelayed • Restart Type: Switch Set whether the services will be started 	<p>Sets the startup type of the Verba services based on the provided backup on the provided host.</p>
<p>Export-VerbaActiveServices -Hostname \$hostname -BackupPath \$backuppath</p>	<ul style="list-style-type: none"> • Hostname Type: String The hostname of the server • BackupPath Type: String The path where the list of the activated services will be saved to. 	<p>Creates a backup about the activated Verba services on the provided host.</p>
<p>Get-VerbaRegistryEntry -key \$key</p>	<ul style="list-style-type: none"> • key Type: Microsoft.Win32.RegistryKey The registry key which will be read 	<p>Writes out the registry set under the provided key.</p>

How to Install your Verba license

✔ If you logging into the Verba Web Interface for the first time after the initial installation, the Upload License File page will appear by default. Skip to **Step 3**.

If you have received a **long coded license string**, you can just **copy/paste** that into Verba.

If you have a **license file**, you can **upload it**.

See the detailed steps below.

❗ If you have multiple servers running the Verba Web Application, the license has to be applied to all servers.

Please follow the guidelines below to install your Verba license:

Step 1 - Navigate to the **System/License** menu item.

Step 2 - On the top right corner of the screen click on the **Upload License File** link.

Step 3 - On the **Upload License File** screen there are two possibilities:

- **Paste License** - You can simply copy/paste the received license string.
- **Upload License File** - Upload the received .lic license file that includes the license string.

Upload License File [Back to License Information](#)

⚠ Your email alert settings are missing or incomplete. [Learn how to configure.](#)

Paste License:

Upload

License File: [Browse...](#)

Upload

Step 4 - If the license string or file is proper and the upload was successful, the Web application will show the updated License Information.

Step 5a - Once the license is uploaded, if the License Activation section shows that the license is activated, there are no further steps.

License Activation

The License on this system is **activated**.

Step 5b - If the License Activation shows not activated, the license **needs activation**. There are 60 days to do this. Open a support ticket at connect.verint.com, and send the activation code. The Verba support team will provide an activated license shortly.

License Activation

The License on this system is **not activated**, since it is active on another server.

Submit a Request at support.verba.com and ask for the activation of your license.

Make sure you include the following activation code: **d52c7fbe-99f2-4e9d-a3dc-4523f47cd020**

Step 6 - If the Verba support team provided the activated license, open the Verba Web Interface, and navigate to the **System/License** menu again.

Step 7 - On the top right corner of the screen click on the **Upload License File** link

Step 8 - Upload the activated license.

Adding the Logon As A Service Right

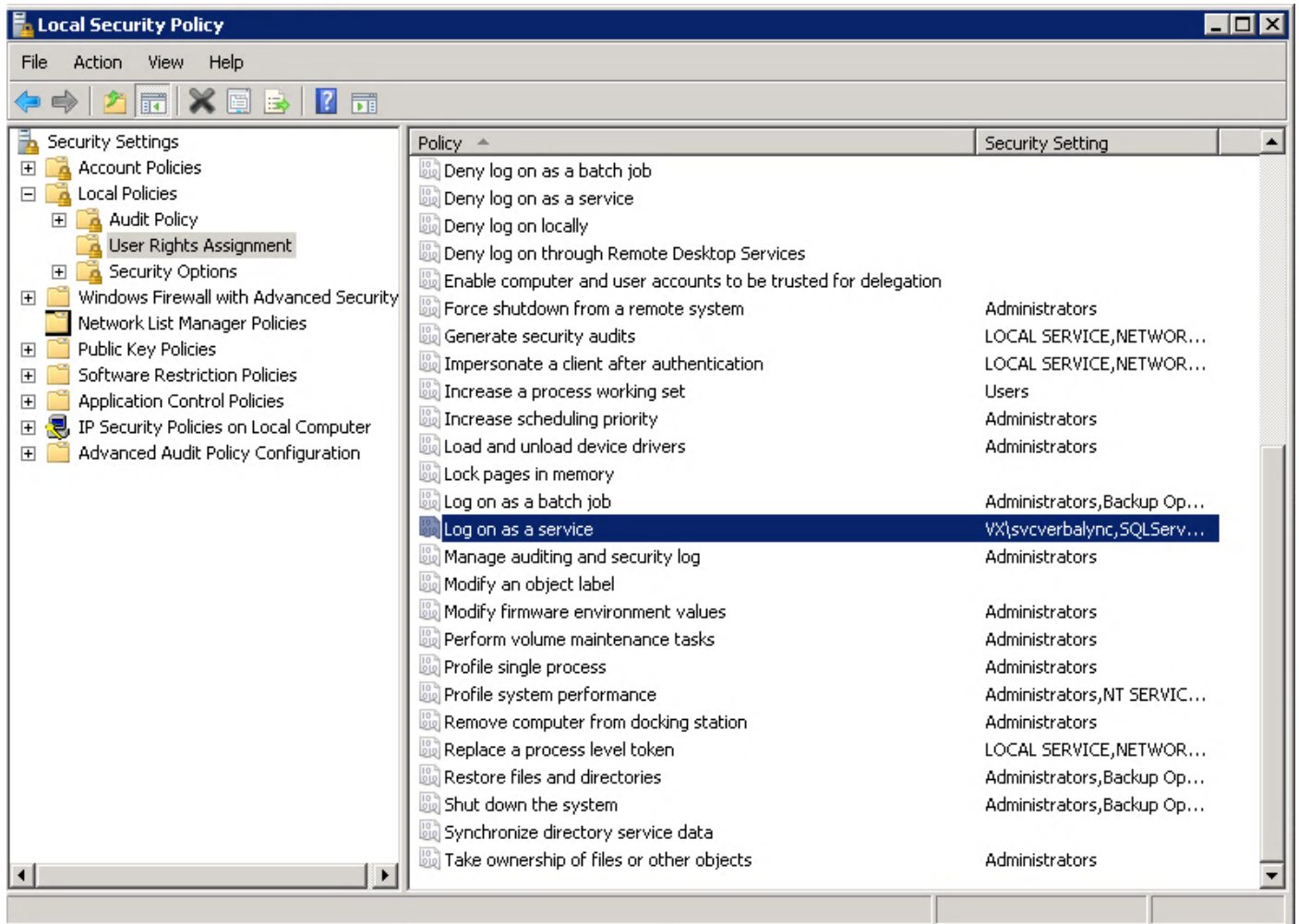
You can add the "Logon as a service" right to an account on the server by following these steps:

Step 1 - Open **Local Security Policy**.

Step 2 - In the console tree, double-click **Local Policies**, and then click **User Rights Assignments**.

Step 3 - In the details pane, double-click **Log on as a service**.

Step 4 - Click **Add User or Group**, and then add the appropriate account to the list of accounts that possess the Log on as a service right.



How to switch from Oracle to OpenJDK Java Runtime Environment

This article describes the steps required to replace Oracle Java Runtime Environment (JRE) to the OpenJDK equivalent. The download links point to the [Adoptium OpenJDK](#) (formerly Adopt OpenJDK) binaries.

Step 1 - Verify your Verba version and check the supported Java version and download the OpenJDK runtime as follows:

Verba version	Java version	Download link
8.x	Java SE 8 Runtime Environment 32 bit	https://adoptium.net/releases.html?variant=openjdk8&jvmVariant=hotspot Choose the <ul style="list-style-type: none">• Operation System: Windows• Architecture: x86• JRE option
9.0, 9.1 and 9.2	Java SE 8 Runtime Environment 64 bit	https://adoptium.net/releases.html?variant=openjdk8&jvmVariant=hotspot Choose the <ul style="list-style-type: none">• Operation System: Windows• Architecture: x64• JRE option
9.3 or later	Java SE 11 Runtime Environment 64 bit	https://adoptium.net/releases.html?variant=openjdk11&jvmVariant=hotspot Choose the <ul style="list-style-type: none">• Operation System: Windows• Architecture: x64• JRE option

Step 2 - Copy the downloaded OpenJDK package (msi) to the Verba server and install it using the following command-line command:

```
msiexec /i [OpenJDK_installer.msi] INSTALLLEVEL=2
```

Step 3 - Check the JAVA_HOME variable in a new command line window using the command::

```
echo %JAVA_HOME%
```

You should see the path to your OpenJDK installation.

Step 4 - Change the following Windows Registry setting:

HKLM\SOFTWARE\WOW6432Node\Apache Software Foundation\Procrun 2.0\VerbaWebApp\Parameters\Java\Jvm

to

Verba 8.x	C:\Program Files\Eclipse Adoptium\jre-[version]-hotspot\bin\server\jvm.dll
Verba 9.x	C:\Program Files\Eclipse Adoptium\jre-[version]-hotspot\bin\server\jvm.dll

Change the [version] part to the actual folder name!

Step 5 - Restart all Verba services using Java:

- Verba Cisco JTAPI Service
- Verba Avaya DMCC/JTAPI Service
- Verba Web Application Service
- Verba Cisco Central Silent Monitoring Service
- Verba Cisco Compliance Service
- Verba Cloud Compliance Service

Step 6 - Verify functionality by making tests covering your basic use cases.

Rolling back changes

In case the system does not work properly after switching to OpenJDK or you want to continue using Oracle JRE, follow the steps below to roll back the changes:

Step 1 - Verify that you have Oracle JRE still installed on the Verba server. If not, install the required Oracle JRE depending on the Verba version.

Step 2 - Change the JAVA_HOME and PATH variables back to the original values pointing to the Oracle JRE installation.

Step 3 - Change the HKLM\SOFTWARE\WOW6432Node\Apache Software Foundation\Procrun 2.0\VerbaWebApp\Parameters\Java\Jvm registry setting back to 'auto'.

Step 4 - Restart all Java services using Java.

Configure

Configuring your Verba Recording System

The Verba Recording System needs configuration both in your network and in the system itself.

Your Verba Recording System comes with an advanced web-based [Central Configuration](#) solution that lets you:

- configure all your server and desktop recorders from a single web interface
- automatically push the configuration to all local and remote components
- keep track all configuration changes for auditing purposes

You can access the Central configuration solution with your administrator account under **Administration / Verba Servers**.

Configuration steps:

- [Step 1 - Apply the license](#)
- [Step 2 - Pull the server specific settings from the server registries](#)
- [Step 3 - Configure Verba and the UC platform for recording](#)
- [Step 4 - Configuring media file upload](#)
- [Step 5 - Configuring extensions](#)
- [Step 6 - Check the functionality of your Verba system](#)
- [Step 7 - Configure backup](#)

Step 1 - Apply the license

The first step has to be done after the installation is applying the license.

[How to Install your Verba license](#)

Step 2 - Pull the server specific settings from the server registries

Before being able to configure your Verba system, there are some initial configuration steps.

[How to pull the server specific settings after the initial installation](#)

Step 3 - Configure Verba and the UC platform for recording

Different phone system and recording modes require different settings in the Verba Recording System.

Unified Communication:

[Cisco recording](#)

[Skype for Business / Lync recording](#)

[Avaya recording](#)

[RingCentral recording](#)

Team Collaboration:

[Microsoft Teams recording \(voice, video, screen share\)](#)

[Microsoft Teams Chat Recording](#)

[Cisco Webex Teams recording](#)

[Symphony recording](#)

Trading:

[BT Trading \(IP Trade\) recording](#)

[BT ITS recording](#)

[Speakerbus recording](#)

[Cloud9 recording](#)

[IPC Unigy recording](#)

Mobile:

[Mobile recording \(Singtel, Truphone, Tango, Movius\)](#)

[SMS recording](#)

Messaging:

[Bloomberg IM recording](#)

Other:

[Other SIP-based recordings:](#)

- Broadsoft Broadworks
- ACME Packet / Oracle SBC
- Avaya ESBC
- Cisco UBE (CUBE) SBC
- Polycom RMX MCU
- Metaswitch Perimeta SBC
- Cisco VCS
- Intracom VCOM
- Huawei

[Passive recording:](#)

- Standard SIP based platforms
- Asterisk (SIP only)
- Mitel MiCloud Telepo
- Telstra TIPT
- Aastra (SIP only)
- Alcatel (SIP only)

[IP-based Radio recording](#)

[Analog recording](#)

Configuring the Verba Dial-in Recorder

The Verba Dial-in Recorder provides rich features including leaving and playback audio/video recordings. For the configuration steps see: [Configuring the Verba Dial-in Recorder Service](#)

Configuring Phone-based Silent Monitoring for Skype for Business / Lync or Cisco

Using the Verba Dial-in Recorder, it's also possible to set up phone-based silent monitoring for Skype for Business, or for Cisco without using the Built-in Bridge. For the configurations steps see: [Configuring Phone-based Silent Monitoring](#)

Configuring the Verba Desktop Agent

The Verba Desktop Agent is required for several features like Agent View, call recording pop-up/control, screen recording, and PCI DSS. For the configuration steps see: [Configuring the Desktop Agent](#)

Step 4 - Configuring media file upload

If the Recorder Server is not co-located with the Media Repository or there are multiple Recorder Servers, then the media files have to be uploaded to a single location. For the upload options see [Configuring media file upload](#)


Step 5 - Configuring extensions

After finalizing the configuration of the recording services, make sure you have added the extensions you want to record to the Verba extension list. This can be done manually ([Extension list](#)) or using [Active Directory Synchronization](#).

Step 6 - Check the functionality of your Verba system

There are several steps should be taken in order to verify the system readiness before going into production. For the most important verification steps, see: [Verifying System Readiness](#)

Step 7 - Configure backup

 It is highly important that you [properly configure Backup of your Media Repository](#). All other components can be reinstalled and reconfigured if your Media Repository is restored.

Configuring Verba for Cisco recording

Verba supports voice, video and Jabber IM recording in the Cisco environments. In addition to this, other Cisco features also can be utilized.

Prerequisites

Before deploying the solution, select the right deployment option and recording method based on the requirements. The Verba system can be deployed in [multiple ways](#), supporting various recording methods.

Before starting the configuration, every Verba server, and component have to be installed. For more information: [Cisco](#)

Configuring Verba for Cisco Voice and Video recording

- The **Network-based Cisco recording** option utilizes the standard recording API of the Cisco UCM for recording **voice calls**. For configuration instructions for both Verba and Cisco UCM side see: [Configuring Verba for Cisco network-based recording](#).
- The **Proxy-based Cisco recording** option allows the recording of **any call types** in a Cisco environment. For configuration instructions for both Verba and Cisco UCM side see: [Configuring Verba for Cisco proxy-based recording](#).

Configuring Verba for Cisco IM recording

The configuration steps are different based on the IM&P server version.

- [Configuring Cisco Unified IM and Presence 10.x, 11.x, 12.x and Verba for Jabber IM recording](#)
- [Configuring Cisco Unified IM and Presence 8.x, 9.x, and Verba for Jabber IM recording](#)

Configuring Verba for Cisco Jabber File Transfer recording

Verba capable of recording the files shared during P2P chat sessions, persistent chat rooms, and ad-hoc chat conferences. For the configuration, see: [Configuring Verba for Cisco Jabber File Transfer recording](#)

Configuring Other Verba features for Cisco

[Configuring Central Silent Monitoring and Whisper Coaching](#)

[Advanced Call Recording Rules](#)

[Configuring the Cisco IP Phone Service](#)

[Configuring the Verba Cisco MediaSense connector](#)

[Cisco UCCX Integration](#)

[Cisco UCCE Integration](#)

[Genesys Integration for Cisco Network-Based Recording](#)

[Configuring Cisco UC Gateway for recording](#)

[Configuring Verba Cisco Recording Announcement for Inbound PSTN Calls](#)

[Configuring Verba Cisco Recording Announcement for Outbound PSTN Calls](#)

[Configuring Cisco Expressway for recording through Mobile and Remote Access \(MRA\)](#)

Configuring Verba for Cisco network-based recording

The Cisco network-based recording option in Verba allows recording voice/audio calls forked either at the gateways or at the phones. This recording option relies on the standard Cisco recording and monitoring APIs to provide a seamless integration with the Cisco collaboration solution.

Preparation

In order to use the Cisco network-based recording options, the configuration of the Cisco Unified Communication Manager and the recorded devices is required.

For the configurations steps see [Configuring Cisco UCM for network based recording](#).

Firewall configuration

Refer to [Firewall configuration for Cisco recording deployments](#) for more information.

Configuring the Verba Unified Call recorder service for Cisco network-based recording

Step 1 - In the Verba Web Interface go to **System > Servers > Select your Recording (or Single) Server > Click on the Service Activation** tab.

Step 2 - Activate the **Verba Unified Call Recorder Service** by clicking on the



icon.

Step 3 - Activate the **Verba Cisco JTAPI Service** by clicking on the



icon.

Step 4 - Click on the **Change Configuration Settings** tab.

Step 5 - Expand the **Cisco JTAPI Configuration \ Basics** node.

Step 6 - Add a new JTAPI connection by clicking on the



icon.

Step 7 - In the right panel, provide the JTAPI **User**, **Password**, and the **IP address** of the CUCM. If there are more nodes, then provide them separated by comma.

Cisco UCM Clusters	
User	<input type="text" value="VerbaJTAPI"/>
Password	<input type="password" value="*****"/>
IP Address(es)	<input type="text" value="10.4.1.20"/>

Step 8 - Click **Save**.

Connecting to multiple CUCM clusters with JTAPI

It's also possible to connect to multiple CUCM clusters with a single Verba Recording Server. Additional connections can be configured by clicking on the



icon.

Legacy configuration

If the Verba server is connecting to only one CUCM cluster, then the legacy settings can be used also. In this case, the configuration can be provided at the **Cisco UCM IP Address(es)**, **JTAPI User Name** and **JTAPI User Password** settings.

Cisco JTAPI Configuration

Basics

Cisco UCM Cluster(s): VerbaJTAPI:1vcYm2yq7F5WuQ3y8oQQ==@10.4.1.20

Cisco UCM IP Address(es):

JTAPI User Name:

JTAPI User Password:

Step 9 - Expand the **Unified Call Recorder \ Media Recorder \ Cisco JTAPI Integration** node. Set the **Cisco JTAPI Integration Enabled** setting to **Yes**.

Step 10 - Provide the Verba Cisco JTAPI service connection(s) at the **Cisco JTAPI Services** setting with the "servername:port" format, one per line. If it is on the same server and using the default port, then enter **localhost:11200**.

Step 11 - Under the **Unified Call Recorder \ Recording Providers \ General** node set the **Internal Domain, Numbers Pattern** setting. This has to be a regex which matches to all internal numbers.

Unified Call Recorder

Media Recorder

Incoming Connection

Basic

Advanced

Cisco JTAPI Integration

Cisco JTAPI Integration Enabled: Yes

Cisco JTAPI Services: localhost:11200

Cisco Partition Based Multitenant Processing: No

Overload Thresholds

Recording Providers

General

Internal Domain, Numbers Pattern: \d{4}

SIP URI Modification: Remove domain part for numbers only

Use Recording Rules: Yes

Enable Performance Based Loadbalancing for Recorders: No

Use Overloaded Recorder as Last Effort: Yes

Step 12 (Optional) - If secure SIP Trunk connection is used, then under the **SIP / SIPREC** node click on the



icon at the **Secure SIP Ports** setting. In the right panel, provide an incoming **port** and the certificate settings, then click **Save**. Note that the port 5060 cannot be used by default because it's configured at the SIP Port setting already, so that has to be changed first in that case.

Secure SIP Ports

Port: 5061

SSL/TLS Certificate: b2 63 71 4e 26 4c b6 2a 6f 26 57 71 2a 5b 68 c4 5f f1 cf 2b

SSL/TLS Key:

SSL/TLS Key Password:

SSL/TLS Trust List: 9d 1d a6 43 f4 f4 53 4e 05 a2 08 7b 39 f1 b5 b3 2f 94 a0 11

Secure SIP Trunk Connection

If secure SIP Trunk connection is required, the following settings have to be set:

SSL/TLS Certificate: The thumbprint of the Verba server certificate being used for the connection. This has to be the same certificate which was upload to the CUCM.

SSL/TLS Trust List: The thumbprint of the CUCM server certificate, or the thumbprint of the CA certificate which issued the CUCM server certificate. Alternatively, "*" can be used. In this case, every certificate going to be trusted, whose CA certificate can be found in under the Trusted Root Certificate Authorities folder. If left empty, every certificate going to be trusted.

Alternatively, .crt/.cer and .key files can be used. In this case, UNC paths can be provided in the SSL/TLS Certificate and the SSL/TLS Key settings, and the SSL/TLS Key Password has to be provided.

Step 13 - Under the **SIP / SIPREC** node click on the



icon at the **SIP Trunk Status Monitoring** setting.

Step 14 - In the right panel provide the CUCM IP address at the **Destination IP Address** setting and set the **Timeout (seconds)** setting. If the default values were used in the SIP Profile at the CUCM side, then set it to **120**.

SIP Trunk Status Monitoring

Destination IP Address	<input type="text" value="10.4.1.20"/>
Timeout (seconds)	<input type="text" value="120"/>


Step 15 - Click on the **Save** button on the bottom. If multiple SIP trunks are connecting from separate CUCMs or there are multiple CUCM nodes for the same SIP trunk, then repeat the steps 13-14.

Step 16 - Save the changes by clicking on the



icon.

Step 17 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

 **There are tasks to be executed regarding the configuration of this Verba Server.**
If you would like to execute these tasks now, please [click here](#) .

Step 18 - Click on the **Service Control** tab.

Step 19 - Start the **Verba Cisco JTAPI Service** and the **Verba Unified Call Recorder Service** by clicking on the



icon.

Step 20 - Repeat the steps on all Recording servers if there are multiple.

Configure extensions

In order to make a directory number recorded, several CUCM side configuration steps also required. For the configuration steps, see [Adding a new extension for recording in Cisco UCM](#).

After finalizing the configuration of the recording services, make sure you have added the extensions you want to record to the Verba extension list. This can be done manually ([Extension details](#)) or using [Active Directory Synchronization](#).

Configure Cisco Cube 2N recording

For Cisco Cube 2N recording follow the steps of the network-based recording configuration. It is important to the both of the recorder server need to have own JTAPI service, what connect for the same CUCM with the same JTAPI user. On the secondary recorder server set the **Unified Call Recorder \ Secondary Recording Service** setting to **Yes** and repeat the steps from the **step 16**.

Unified Call Recorder

- Media Recorder
- Recording Providers

Secondary Recording Service: Yes

Configuring advanced network-based recording

With the advanced network-based recording configuration load-balancing and mid-call failover can be achieved. For the configuration steps see [Configuring recording high availability](#).


Service configuration reference

For the service configuration references see:

- [Cisco JTAPI Configuration settings](#)
- [Unified Call Recorder service configuration reference for Cisco network based recording](#)

Configuring Cisco UCM for network based recording

In order to use the Cisco network-based recording options, configuration of the Cisco Unified Communication Manager and the recorded devices is required. The guide below contains all the necessary configuration steps, for the official Cisco configuration guide, refer to [Features and Services Guide for Cisco Unified Communications Manager, Release 10.0\(1\) - Monitoring and Recording](#).

 The recording system's reliability depends on both Cisco and Verba software components. We highly recommend to [have a look at these known recording affecting Cisco bugs](#), and install necessary updates.

Cisco UCM configuration


The initial Cisco UCM configuration for central recording includes the following steps:

- Step 1** - [Create and configure the SIP trunk\(s\)](#) pointing to the Verba Recording Director(s), for encrypted call recording, [create secure SIP trunk\(s\)](#)
- Step 2** - [Configure call routing](#) that let the Cisco UCM to direct calls to the recorder (includes configurations for multiple recorders)
- Step 3** - [Create a recording profile](#) used by the recorded lines/extensions
- Step 4** - [Create an application user for the JTAPI integration](#) that provides recording control and detailed CDR information (Recommended)
- Step 5** - [Disable the unsupported iSAC and G.722 codec](#)
- Step 6** - [Review the codec guidelines for network based recording](#) (Recommended)
- Step 7** - [Configure transcoder resources](#) (required if configuring the inter-region codec guidelines is not possible)
- Step 8** - [Configure a recording notification tone](#) (optional)
- Step 9** - [Configure gateway preferred media forking](#) (optional, available since CUCM 10.0)

Configuring the Verba system

For more information, see [Configuring Verba for Cisco network-based recording](#).

Adding and removing extensions

 When Cisco network-based recording is used, the system can record only those extensions that are properly configured in the Cisco UCM. It is not enough to add extensions in the Verba system.

Follow the steps below to add and remove extensions to/from central recording in Cisco UCM:

- [Add new extensions](#) to network-based recording (follow these steps to [add extensions with Extension Mobility](#))
- [Remove extensions](#) from network-based recording

Creating an application user for the JTAPI connection

Create an application user for the JTAPI application

For secure JTAPI connection refer to [Configuring Secure JTAPI](#).

Execute the following steps in your Cisco UCM web administration interface:

Step 1 - Navigate to **User Management / Application User / Add New** menu item.


Step 2 - Fill out all necessary fields and make a note of the **User ID** and **Password** fields, because you will have to set them in the Verba Recording System. E.g. you can call it **VerbaJTAPI**.

Step 3 - Click **Save**.

Step 4 - Scroll down to **Permissions Information** section and click on the **Add to Access Control Group** button.

Step 5 - Add the following groups to the application user by selecting them from the list, then clicking on the **Add Selected** button:

- **Standard CTI Enabled**
- **Standard CTI Allow Control of Phones supporting Connected Xfer and conf** (necessary for Cisco 89xx or 99x SIP phones)
- **Standard CTI Allow Control of Phones supporting Rollover Mode**

 If controlled recording mode is being used, then the **Standard CTI Allow Call Recording** group membership is also required.
If the [Central Silent Monitoring and Whisper Coaching](#) is being used, then the **Standard CTI Allow Call Monitoring** group membership is also required.

Step 6 - Click **Save**.

Configuring Secure JTAPI

Follow the guide below to configure secure JTAPI connection between the Verba and the Cisco systems.

- [Cisco UCM configuration](#)
 - [Service activation](#)
 - [Create/Configure the application user](#)
- [Verba server configuration](#)
 - [Configure the secure connection on the Verba server](#)

Cisco UCM configuration

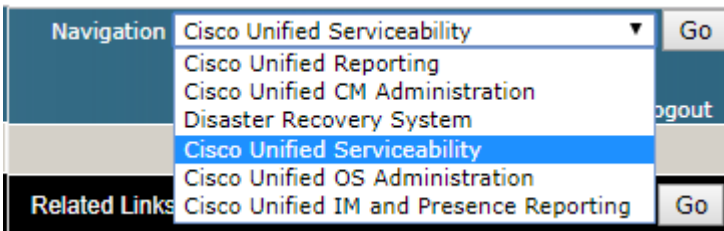
i CUCM security

The secure JTAPI configuration requires the CUCM to be in mixed mode. For the necessary configuration steps, refer to the official Cisco configuration guide: [CUCM Mixed Mode with Tokenless CTL](#)

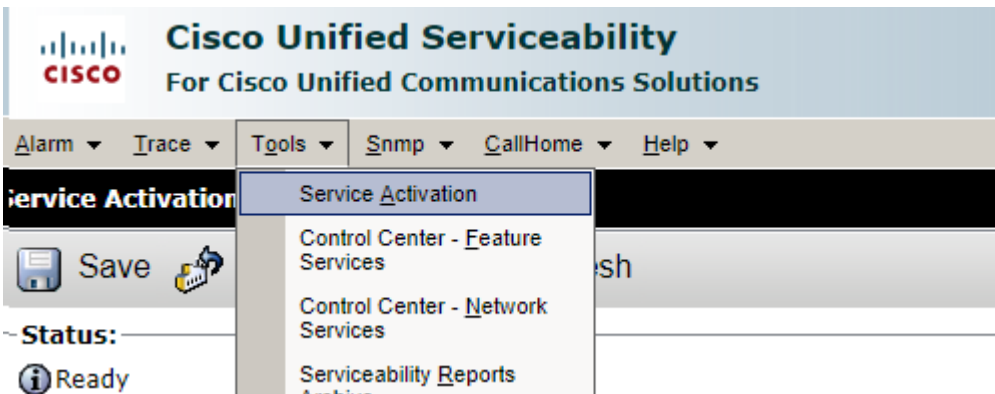
Service activation

Check if the Certificate Authority Proxy Function (CAPF), Certificate Trust List Provider (CTL), and CTIManager services are activated.

Step 1 - Open the Cisco Unified Serviceability **Navigation > Cisco Unified Serviceability > Go.**



Step 2 - Open the **Tools > Service activation**



Step 3 - Select the server(s) and press Go

Service Activation

Select Server

Server*

Step 4 - Make sure that both **Cisco CTL Provider** and **Cisco Certificate Authority Proxy Function** are activated.

Security Services		
	Service Name	Activation Status
<input checked="" type="checkbox"/>	Cisco CTL Provider	Activated
<input checked="" type="checkbox"/>	Cisco Certificate Authority Proxy Function	Activated

Step 5 - If the functions were not active, restart the CUCM server. You will now have CCM listening on TCP port 2443 for secure SCCP connections and CTIManager listening on 2749 for secure JTAPI/QBE connections.

Create/Configure the application user

Step 1 - Open the Cisco Unified CM Administration **Navigation > Cisco Unified CM Administration > Go**.

Navigation

Step 2 - Create an application user based on [Creating an application user for the JTAPI connection](#)

Step 3 - On the **User Management / Application User / Application User Configuration** add the user to the groups' CTI Enabled, CTI Secure Connection, and CTI Allow Reception of SRTP Key Material under **Permissions Information** for the user.

Permissions Information

Groups

- Standard CTI Allow Control of Phones supporting Co
- Standard CTI Allow Control of Phones supporting Ro
- Standard CTI Allow Reception of SRTP Key Material
- Standard CTI Enabled
- Standard CTI Secure Connection

Roles

- Standard CTI Allow Control of Phones supporting Conne
- Standard CTI Allow Control of Phones supporting Rollov
- Standard CTI Allow Reception of SRTP Key Material
- Standard CTI Enabled
- Standard CTI Secure Connection

[View Details](#)

ⓘ Adding the user to the Secure CTI and SRTP Key Material groups mean that this JTAPI user will ONLY be allowed to connect on the secure port of 2749 using certs.

Step 4 - Under **Users > User Settings > Application User CAPF Profile** select Add new.

ⓘ Each instance of the Verba Cisco JTAPI Service must have its own CAPF profile. If more than one server is configured, the process of configuring the CAPF profile has to be repeated for each of them.

Select the correct application user, define an Instance ID, and select the certificate operation of Install / Upgrade, and save. The Certificate Operation Status will be **Operation Pending**

- Application User CAPF Profile

Application User*

Instance Id*

- Certification Authority Proxy Function (CAPF) Information

Certificate Operation*

Authentication Mode*

Authentication String

Key Order*

RSA Key Size (bits)*

EC Key Size(Bits)

Operation Completes By : : : (YYYY:MM:DD:HH)

Certificate Operation Status: None

Verba server configuration

Configure the secure connection on the Verba server

Step 1 - Go to **Applications > Plugins**, and download the JTAPI client for your operating system



Step 2 - Install the downloaded client on the server and start the JTAPI preferences tool

Step 3 - Configure the Cisco Unified tab with the IP of the CUCM and the log folder on the Log Destination tab

Step 4 - On the Security tab, enable security tracing and configure the fields according to the environment, check the **Enable Secure Connection** and press **OK**.

The screenshot shows the 'Security' tab in the Cisco Unified Communications Manager configuration interface. The 'JTAPI Tracing' section is active, and the following settings are visible:

- Enable Security Tracing
- Select Trace Level: Error
- User Name: VerbaSJTAPl
- Instance ID: Verba
- Authentication String: 4729554434
- TFTP Server IP-Address: 10.110.78.200
- TFTP Server Port(Default:69): 69
- CAPF Server IP-Address: 10.110.78.200
- CAPF Server Port(Default:3804): 3804
- Certificate Path: C:\Program Files\Cis
- Certificate Passphrase: (empty)
- Enable Secure Connection
- FIPS Compliant
- Certificate Update Status: Not Updated
- Buttons: Delete Certificate, Update Certificate
- Bottom Buttons: Add, Remove, OK, Cancel

Step 5 - Check the \lib\ folder for a **JtapiClientKeyStore** file. If the file is created, the **Certificate Operation Status** in CUCM will change.

Step 6 - Copy the **JTAPI.ini** file to **Verba\bin** folder overwriting the original. The file contains the **SecurityProperty** description for the location of the certificate.

Step 7 - In the Verba Web Interface go to **System > Servers > Select your Recording (or Single) Server > Service Control** tab, and start /restart the **Verba Cisco JTAPI Service**.

Step 8 - Verify the connection

Adding a new extension for recording in Cisco UCM

Overview

There are three major steps you do when you are adding a new extension:

- Enable **built-in-bridge**
- Configure **recording on the line**
- Add the **phone device to the JTAPI user**
- Add the directory number as **recorded extension** in Verba

You can see the detailed steps below.

Configure phones for recording

Step 1 - Select **Device / Phone** menu item and select the desired phone.

Step 2 - On the configuration page enable the **Built-In Bridge**.

Step 3 - Select the **line** you would like to enable recording on.

Step 4a - Set **Recording Option** to **Automatic Call Recording Enabled**.

Step 4b - If advanced call recording rules or controlled recording mode is used, then set **Recording Option** to **Selective (Application Invoked) Call Recording Enabled**.

Step 5 - Set **Recording Profile** to the previously created profile.

Step 6 - Set **Recording Media Source** according to your preference (gateway versus phone). If you go ahead with gateway preferred you should [configure gateway and callmanager accordingly](#). Please note this feature has certain requirements on gateway, call routing and callmanager version (available since CUCM 10.0 and IOS 15.3(3)M - ISRG2 with SIP trunking).

Step 7 - Click on the **Save** button.

Line 1 on Device SEP001F9EAC1601

Display (Internal Caller ID)	John Harrison	D
person receiving a call may not see the proper identity of t		
ASCII Display (Internal Caller ID)	John Harrison	
Line Text Label		
ASCII Line Text Label		
External Phone Number Mask		
<hr/>		
(i)		
Ring Setting (Phone Active)	Use System Default	▼ Ap
Call Pickup Group Audio Alert Setting (Phone Idle)	Use System Default	▼
Call Pickup Group Audio Alert Setting (Phone Active)	Use System Default	▼
Recording Option*	Automatic Call Recording Enabled	▼
Recording Profile	Recorder profile	▼
Monitoring Calling Search Space	< None >	▼

You need to **reset every phone you configure** for recording.

Step 8 - Assign the device to the JTAPI application user. Go to **User Management / Application User**, select the Verba JTAPI user and add the device to the **Controlled**

Devices list.

Step 9 - Click on the **Save** button.

Device Information

Available Devices	SEP000DED47D9BC SEP0017596E9DAF SEP0019D2030E7A SEP001D09DB9981 SEP0026B9994E43	<input type="button" value="Find more Phones"/> <input type="button" value="Find more Route Points"/>
▼ ▲		
Controlled Devices	SEP001EF7C21C32 SEP001EF7C21CA6 SEP001F9EAC1601 SEP00215554A792	
Available Profiles		
▼ ▲		
CTI Controlled Device Profiles		▼ ▲

Final Stage: Configure extensions

After finalizing the configuration of the recording services, make sure you have added the extensions you want to record to the Verba extension list. This can be done [manually](#) or using [Active Directory Synchronization](#).

Adding an extension with Extension Mobility in Cisco UCM

Configure phones for recording

Step 1 - Select **Device / Phone** menu item and select the phone where the user will log in with **Extension Mobility**.

Step 2 - On the configuration page enable the **Built In Bridge**.

Step 3 - Go to **Device / Device Settings / Device Profile** and select the profile that is configured to use with **Extension Mobility**.

Step 4 - Select the line you would like to enable recording on.

Step 5 - Set **Recording Option** to **Automatic Call Recording Enabled**.

Step 6 - Set **Recording Profile** to the previously created profile.

Step 7 - Click on the **Save** button.

Line 1 on Device SEP001F9EAC1601	
Display (Internal Caller ID)	John Harrison D
person receiving a call may not see the proper identity of t	
ASCII Display (Internal Caller ID)	John Harrison
Line Text Label	
ASCII Line Text Label	
External Phone Number Mask	
Visual Message Waiting Indicator Policy*	Use System Policy ▼
Audible Message Waiting Indicator Policy*	Default ▼
Ring Setting (Phone Idle)*	Ring ▼
Ring Setting (Phone Active)	Use System Default ▼ Ap
Call Pickup Group Audio Alert Setting (Phone Idle)	Use System Default ▼
Call Pickup Group Audio Alert Setting (Phone Active)	Use System Default ▼
Recording Option*	Automatic Call Recording Enabled ▼
Recording Profile	Recorder profile ▼
Monitoring Calling Search Space	< None > ▼

Step 8 - Assign the device to the JTAPI application user. Go to **User Management / Application User**, select the Verba JTAPI user and add the device to the **Controlled Devices** list.

Step 9 - Click on the **Save** button.

Device Information

Available Devices

SEP000DED47D9BC
SEP0017596E9DAF
SEP0019D2030E7A
SEP001D09DB9981
SEP0026B9994E43

Controlled Devices

SEP001EF7C21C32
SEP001EF7C21CA6
SEP001F9EAC1601
SEP00215554A792

Available Profiles

CTI Controlled Device Profiles

Step 9 - Go to **User Management / End User** and select the user that is using the **Extension Mobility** feature with the extension.

Step 10 - Tick **Allow Control of Device from CTI** and click **Save**.

Extension Mobility

Available Profiles

Controlled Profiles

7975EM

Default Profile

7975EM

Presence Group*

Standard Presence group

SUBSCRIBE Calling Search Space

< None >

Allow Control of Device from CTI

Enable Extension Mobility Cross Cluster

Removing extensions from recording in Cisco UCM

Remove extensions from recordings

Step 1 - Select **Device / Phone** menu item and select the desired phone.

Step 2 - Optionally disable the **Built In Bridge**. If you are using features like barge-in, which require the built-in-bridge, do not disable it.

Step 3 - Select the line you would like to disable recording on.

Step 4 - Set **Recording Option** to **Call Recording disabled**.

Step 5 - Set **Recording Profile** to **None**.

Step 6 - Click on the **Save** button.

Recording Option*	Call Recording Disabled
Recording Profile	< None >
Monitoring Calling Search Space	< None >
<input checked="" type="checkbox"/> Log Missed Calls	

 You need to **reset every phone you configure** for recording.

Step 7 - Remove the device from the JTAPI application user. Go to **User Management / Application User** and remove the device from the **Controlled Devices** list.

Step 8 - Click on the **Save** button.

Device Information		
Available Devices	<div style="border: 1px solid gray; padding: 2px;">SEP000DED47D9BC SEP0017596E9DAF SEP0019D2030E7A SEP001D09DB9981 SEP0026B9994E43</div> <div style="text-align: right; margin-top: 5px;">▼ ▲</div>	<div style="border: 1px solid gray; padding: 2px; width: fit-content; margin-top: 5px;">Find more Phones</div> <div style="border: 1px solid gray; padding: 2px; width: fit-content; margin-top: 5px;">Find more Route Points</div>
Controlled Devices	<div style="border: 1px solid gray; padding: 2px;">SEP001EF7C21C32 SEP001EF7C21CA6 SEP001F9EAC1601 SEP00215554A792</div> <div style="text-align: right; margin-top: 5px;">▼ ▲</div>	
Available Profiles	<div style="border: 1px solid gray; height: 40px;"></div> <div style="text-align: right; margin-top: 5px;">▼ ▲</div>	
CTI Controlled Device Profiles	<div style="border: 1px solid gray; height: 40px;"></div> <div style="text-align: right; margin-top: 5px;">▼ ▲</div>	


Uploading Certificate for SIP Trunk Security Profile

Configure SIP trunk for recording encrypted calls

From Cisco Unified Communications Manager 8.0 the RTP forking-based recording interface enables the recording of encrypted calls. In order to enable this option, various configuration tasks have to be accomplished. Please follow the instructions below to properly configure the Cisco Unified Communications Manager and the Verba Recording System.

Prerequisite



A certificate is required for the secure SIP connection between the Verba servers and the Call Managers. The certificate must have an exportable private key, and the signature / hash algorithm of the certificate can't be higher than **SHA256** (SHA512 isn't supported by the Call Manager). It doesn't have to be a publicly signed certificate, it can be generated by the local domain CA. No specific requirements for the certificate subject or SAN.

 The certificate used for the secure SIP connection has to be added in the certificate store of the Verba Recording Server also, where the secure SIP connection will terminate. When importing, the private key has to be left **exportable**.


Upload the Recording Server certificate to the CUCM

- Step 1** - Login to the Cisco Unified OS Administration interface.
- Step 2** - Select **Security / Certificate Management** menu.
- Step 3** - Click on the **Upload Certificate** button.
- Step 4** - Select the **CallManager-trust** certificate.
- Step 5** - Enter an optional description.
- Step 6** - Click **Upload File** button, and select the previously exported certificate.

Upload Certificate

 Upload File  Close

Status

 Status: Ready


Upload Certificate

Certificate Name*


Root Certificate

Description

Upload File

 *- indicates required item.

Step 7 - After successful upload, the new certificate should appear on the list and it has a name containing the hostname of the Verba Recording Server.

 If you have multiple nodes (publisher+subscribers) in your cluster you must install the recorder's certificate on each node.

Configuring recording notifications in Cisco UCM

Configure optional recording notification tones

Step 1 - Select **System / Service** parameters from the menu.

Step 2 - Select the current Cisco UCM server.

Step 3 - Then select the **Cisco CallManager** service.

Step 4 - Enable or disable recording notification tone parameters in **Clusterwide Parameters (Feature - Call Recoding)** group.

Step 5 - Click on the **Save** button.

Clusterwide Parameters (Feature - Call Recording)		
Play Recording Notification Tone To Observed Target *	False	False
Play Recording Notification Tone To Observed Connected Parties *	False	False

Creating a recording profile in Cisco UCM

Create a new recording profile

To provision line appearances of users for call recording, one or more call recording profiles should be created. A recording profile can then be selected for a line appearance. To create a recording profile, a Unified CM administrator has to open Device Setting page and select Recording Profile.

Step 1 - Select **Device / Device Settings / Recording Profile**, and click on the **Add New** button.

Step 2 - Set a **Name** for the profile.

Step 3 - Set **Recording Destination Address** to the directory number previously set at the **Route Pattern**.

Step 4 - Click on the **Save** button.

Put your section name here

Name*	<input type="text" value="Recorder profile"/>
Recording Calling Search Space	<input type="text" value="< None >"/>
Recording Destination Address*	<input type="text" value="9999"/>

 Ensure that the selected Calling Search Space is able to call the Partition of the SIP trunk.

Disable the unsupported iSAC codec

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 or you configured the network regions in such ways, that transcoders are inserted. Cisco IP phones can use codecs that transcoders do not support, so it is recommended to disable codecs, which are not supported by the Verba Recording System and/or you do not have transcoder support. Verba Recording System supports G.711, G.729, G.722 and iLBC, but **does not support iSAC**.

This feature was introduced in CUCM 8.5(1)SU1.

It is possible that when trying to transfer incoming external calls, the gateway trying to change the codec. But since the Built-in Bridge doesn't support this codec change the call drops. Because of this the G.722 codec also should be disabled for the recorded phones.

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

- G722 Codec **Enabled for All Devices Except Recording-Enabled Devices**
- iLBC Codec Enabled for All Devices
- iSAC Codec **Enabled for All Devices Except Recording-Enabled Devices**

Configuration steps

You can configure these service parameters in the **System/Service Parameters** menu.

Select the cluster to be configured, and **Cisco CallManager service**.

In **Clusterwide Parameters (System - Location and Region)** box you will find codec specific parameters.

You can set these service parameters with the following values:

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

G.711 A-law Codec Enabled *	Enabled for All Devices ▼
G.711 mu-law Codec Enabled *	Enabled for All Devices ▼
G.722 Codec Enabled *	Enabled for All Devices Except Recording-Enabled Dev ▼
iLBC Codec Enabled *	Enabled for All Devices ▼
iSAC Codec Enabled *	Enabled for All Devices Except Recording-Enabled Dev ▼

Codec guidelines for Cisco network based recording

Overview

Verba supports all Cisco supported voice codecs (G.711, G.722, G.729, iLBC) [except iSAC](#).

However, when Cisco RTP-forking based central recording is used UCM and the phones might **drop call recording sessions and even calls** if transcoding is not properly configured.

The following call scenarios can trigger these events if **transcoding resources are not available**:

Scenario	Description	Example
Recorder and recorded phone are on different sites, WAN link bandwidth limitation requires low bitrate voice codec	In this case it is recommended to put the recorder into different UCM region, and set inter-region codec according to available bandwidth.	Phones at remote branch office are using G.722 /G.711 codec for internal calls. Between recorder and remote office G.729 codec would be preferred due to the office's upload bandwidth limitations.
Recorder and recorded phones are in different UCM regions	If the intra region codec bitrate (codec used in the "original" calls between phones/gateways in the same region) is higher than inter region codec between recorder and phone, then UCM is forced to insert a transcoder at the phone region to transcode the voice sent to the recorder, in order to match the inter-region codec bitrate.	original call bitrate is 64 kbps (G.711 or G.722), recorder - phone region relationship dictates 8 kbps G.729 (default inter-region codec in UCM).
Codec change in consultative transfer or joining a conference	If a different codec is involved in the consultation call leg, and after transfer/in conference leg UCM drops both the recording and original call session. This is a known Cisco issue, consultation and after consultation legs are recorded in the same session (from transferee or conferee point of view), when the phone starts a recording session using a certain codec, it gets "locked" into that codec. Verba supports mid-call codec change, but UCM does not support this in case of recorder calls. A transcoder can handle this situation, and UCM tries to insert it into the call to do transcoding between new call leg's codec and the "locked" codec.	Consultative transfer, Agent A calls recorded Agent B to transfer Customer C calling from PSTN. A->B internal call leg use G.722 codec, after transfer C->B gateway call leg switches to G.711. These call legs from B's point of view are handled in the same recording session by UCM, and due to locking the Built-in Bridge to G.722 causes to drop the second call leg.

Verify configuration

Verify region configuration

Step 1 - Open Cisco Unified CM administration

Step 2 - Select **System / Region** menu item

Step 3 - Select the Verba recorder's region

Step 4 - Check whether region relationship and inter-region codecs are configured according to your needs as described above

Region Information

Name*

Region Relationships

Region	Audio Codec Preference List	Maximum Audio Bit Rate	Maximum Session Bit Rate for Video Calls
Default	Use System Default (Factory Default low loss)	G.711	384
HQ - New Jersey	Use System Default (Factory Default low loss)	G.729	4096
Office - Dubai	Use System Default (Factory Default low loss)	G.729	2048
Office - Hong Kong	Use System Default (Factory Default low loss)	G.729	2048
Office - Stockholm	Use System Default (Factory Default low loss)	G.729	512
Recorders - New Jersey	Use System Default (Factory Default low loss)	G.729	4096

NOTE: Regions not displayed Use System Default Use System Default Use System Default

Modify Relationship to other Regions

Regions	Audio Codec Preference List	Maximum Audio Bit Rate	Maximum Session Bit Rate for Video Calls
<div style="border: 1px solid #ccc; padding: 2px;"> Default HQ - New Jersey Office - Dubai Office - Hong Kong Office - Stockholm </div>	<input type="text" value="Keep Current Setting"/>	<input type="text" value="8 kbps (G.729)"/>	<input type="radio"/> Keep Current Setting <input type="radio"/> Use System Default <input type="radio"/> None <input checked="" type="radio"/> <input type="text" value="512"/> kbps

Verify media resource configuration

Step 1 - Select the **System / Device** pool option

Step 2 - Select the recorded phones' pool(s)

Step 3 - Check whether valid transcoding resource is available in the **Media Resource Group List** if according to region relationships and other needs it might be required

Roaming Sensitive Settings

Date/Time Group*

Region*

Media Resource Group List

Errors in above codec and transcoding configurations can lead to **loss of recordings or dropped calls**.

Avoid unnecessary MTP insertion

In case of G.711 calls CUCM might insert MTP in the media path if the call passes a gateway without any real need. This can be avoided if a media resource group not containing any MTP is assigned to recorder trunk:

Step 1 - Under **Media Resources > Media Resource Group** select **Add New** and give it a name.

Step 2 - For **Selected Media Resources** add anything (announcer, cfb...) except MTP and hit the **Save** button.

Step 3 - Under **Media Resources > Media Resource Group List** select **Add New** and give it a name.

Step 4 - For **Selected Media Resource Groups** select the previously created Media Resource Group and hit the **Save** button.

Step 5 - Navigate to **Device > Trunk** and select your SIP Trunk which is created for the Verba Recorder server(s).

Step 6 - For **Media Resource Group List** select your previously created list. Hit the **Save** button and then hit the **Reset** button.

Known Cisco bugs affecting recording reliability

- [Cisco CallManager](#)
 - [Intermittent secure recording](#)
 - [Recording Tone options on phone page for 69x1 phones do not work](#)
 - [Call Redirect can fail when Call Recording Profile is enabled](#)
 - [Unable to record voice for SIP calls](#)
- [Cisco phone firmwares \(firmware versions!\)](#)
 - [Intermittent recording \(69xx/79xx\)](#)
 - [6921 sends one RTP stream to recorder, when sRTP is expected](#)
 - [Caller gets one-way audio after hold/resume when conf with recording](#)
 - [Recording Tone options on phone page for 69x1 phones do not work](#)
 - [6921 SCCP/SIP - Cannot turn off Recording Tone notification](#)

Cisco CallManager

Intermittent secure recording

<http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&bugId=CSCtu06601&from=summary>

Symptom: Secure recording failing intermittent with cause 57 403 forbidden

Work around: Put the agent phones on the same node as the sip trunk

First found: 8.5(1) (we experienced the same issue with 8.0 branch, upgrade to 9.0.1 solved it at customer)

Fixed: 8.6(2.98000.116), 8.6(2.98000.46), 9.0(1.10000.15), 9.0(1.10000.37)

Recording Tone options on phone page for 69x1 phones do not work

<http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&bugId=CSCtz31279&from=summary>

Symptom: Recording Tone parameters missing on phone page for 7911.

Work around: n/a

First found: 9.1(1)

Fixed: 9.0(0.98000.41), 9.0(0.98000.158), 8.6(3.98000.199), 8.6(4.10000.15), 9.0(1.10000.15), 9.0(1.10000.37)

Call Redirect can fail when Call Recording Profile is enabled

<http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&bugId=CSCtq87736&from=summary>

Symptom: When incoming call to UCCX being queue as all agents are busy, UCCX will record a call back number. If at a later time, an agent becomes available, UCCX will then call that agent, when agent answer the call, he will hear a menu prompt to press 1 to call the call back number, after that the UCCX will then call the call back number, currently after the agent press 1, the call get disconnected and it seems to mostly affect agent using extension mobility.

Work around: Remove Call Recording Profile.

First found: 7.1(2.31900.1), 8.5(1.11001.35)

Fixed: 8.6(1.98000.37), 8.6(1.98000.82), 8.5(1.12025.1), 8.0(3.23034.1), 8.6(1.21002.1), 8.6(2.10000.30), 7.1(5.34070.2)

Unable to record voice for SIP calls

<http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&bugId=CSCty15458&from=summary>

Symptom: Unable to record voice for some SIP calls. The issue will be encountered only during redirects over a SIPTrunk which looks at SIP URL in the Invite when the name/number got modified from the DA response after redirect request.

Work around: n/a

First found: 8.6(2)

Fixed: 9.0(0.98000.16), 9.0(0.99999.2242), 9.0(0.98000.55), 7.1(5.34091.1), 8.5(1.14060.1), 8.6(2.21900.5), 8.6(2.21021.1), 7.1(5.34900.7), 8.0(3.24047.1), 9.0(1.10000.15), 8.6(4.98000.10), 9.0(1.10000.37)

Cisco phone firmwares (firmware versions!)

Intermittent recording (69xx/79xx)

<http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&bugId=CSCtx84429&from=summary>

Symptom: Calls to 3rd party Recording Server via BIB are failing intermittently. CCM SDI Traces will show CUCM sending a BYE to the Recording Server with cause=47.

Work around: n/a

First found: 9.2.1 and higher

Fixed: 9.2(3)ES3, 9.2(3)MN1.16, 9.3(1)CT1.50 (we have experience with 9.3.1SR1, and can confirm it is fixed)

6921 sends one RTP stream to recorder, when sRTP is expected

<http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&bugId=CSCtj38017&from=summary>

Symptom: 6921 sends one RTP stream to recorder, when sRTP is expected. 9.2.1 firmware fixes the CSCtj38017 - SSRC field in RTP Stream Packet is always zero. However, the secure recording stream functionality is broken in 9.2.1 firmware. Downgrading to lower firmware version (9.1.1) would help in not running into the secure recording stream issue. However, the 6921 phone will be susceptible to CSCtj38017.

Work around: n/a

First found: 9.2(1)

Fixed: 9.2(1)SR1

Caller gets one-way audio after hold/resume when conf with recording

<http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&bugId=CSCtq76447&from=summary>

Symptom: Agents will get a one way audio after resume calls on hold/transfer This defect happen when RTL is act as call recoding agent and playing MMOH using multicast address. When customer resume this call. CUCM send skinny message StationStopMulticastMediaReceptionMessage to close MMOH media channel. But RTL call control do not clear multicast address properly. When CUCM trigger RTL to open RX/TX unicast media channel with customer. Call control open RX channel using the previous multicast address. Therefore, RTL cannot receive RX packets properly and play it out.

Work around: n/a

First found: 9.1(1.100)

Fixed: 9.2(2), 9.2(1)SR1

Recording Tone options on phone page for 69x1 phones do not work

<http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&bugId=CSCtq54881&from=summary>

Symptom: On the device phone page, enabling Recording Tone should play a tone for every call regardless of whether it is recorded or not. This does not play. Enabling the Recording Tone via Service Parameters does work for recorded calls, but the Recording Tone Volume options on the phone config page do not apply successfully.

Work around: n/a

First found: 9.1(1)

Fixed: 9.2(1)

6921 SCCP/SIP - Cannot turn off Recording Tone notification

<http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&bugId=CSCua57846&from=summary>

Symptom: Cannot disable the Recording Tone notification:

Work around: n/a

First found: 9.3(2)

Fixed: 9.3(1)ES1, 9.3(1)ES4

Configuring gateway preferred forking

Gateway requirements

- Supports both Voice gateways and Unified Border Elements (CUBE) as long as they interface with Unified CM using SIP and the Router platform supports the UC Services Interface (not supported for H323 or MGCP based calls)
- The word gateway is used interchangeably to refer to both Voice gateways and CUBE devices.
- The Gateway has to be directly connected to the Unified CM using a SIP trunk. No support for SIP Proxy servers
- ISR-G2 Gateways (29XX, 39XX Series) running release 15.3(3)M or later are supported. 15.3(3)M was released on CCO in July / 2013
- ASR-100X Gateways running release XE 3.10 or later are supported. XE 3.10 was released on CCO in July / 2013
- VG224 is not currently supported

Configuring the Cisco UCM

You need to mark the Gateway - CUCM trunk as recording enabled:

The screenshot shows two configuration sections. The first section, titled "Recording Information", has three radio button options: "None", "This trunk connects to a recording-enabled gateway" (which is selected and highlighted in yellow), and "This trunk connects to other clusters with recording-enabled gateways" (also highlighted in yellow). The second section, titled "Geolocation Configuration", contains two dropdown menus: "Geolocation" and "Geolocation Filter", both set to "< None >". Below these is a checkbox labeled "Send Geolocation Information" which is unchecked. At the bottom of the form are four buttons: "Save", "Delete", "Reset", and "Add New".

Follow the [Configuring Cisco UCM for central recording](#) guide to create them.

Configuring the Cisco gateway

Create xmf provider using the following commands to each CUCM subscriber node: (replace the example ip address to your Cisco UCM ip address(es))

```
//Configure HTTP connectivity for XMF API
Device(config)# http client connection idle timeout 600
Device(config)# ip http server
Device(config)# no ip http secure-server
Device(config)# ip http timeout-policy idle 600 life 86400 requests 86400
//Replace source-interface with GW's interface facing CUCM network
Device(config)# ip http client source-interface GigabitEthernet0/0/0
Device(config)# http client connection persistent
//Configure WSAPI XMF
Device(config)# uc wsapi
Device(config-uc-wsapi)# message-exchange max-failures 2
//Replace source-address with IP with GW's IP
Device(config-uc-wsapi)# source-address 10.30.110.2
Device(config-uc-wsapi)# probing interval negative 20
```

```
Device(config-uc-wsapi)# probing max-failures 5
Device(config-uc-wsapi)# provider xmf
Device(config-uc-wsapi)# no shutdown
//Replace URL with CUCM address
Device(config-uc-wsapi)# remote-url 1 http://192.168.111.111:8090/ucm\_xmf
Device(config-uc-wsapi)# remote-url 2 http://192.168.111.112:8090/ucm\_xmf
Device(config-uc-wsapi)# end

Device# show wsapi registration all
```

Provider XCC

=====

Provider XMF

=====

```
registration index: 1
id: 32EC5A98:VMF:Unified CM 10.5.0.99833-3:4
appUrl:http://192.168.111.111:8090/ucm\_xmf
appName: Unified CM 10.5.0.99833-3
provUrl: http://192.168.111.111:8090/xmf
prober state: STEADY
connEventsFilter: CREATED|DISCONNECTED
mediaEventsFilter:
```

Configuring call routing in Cisco UCM for recording

Create a new Route Group

Step 1 - Select **Call Routing / Route/Hunt / Route Group** menu item and click on the **Add New** button.

Step 2 - Add a name to the group in **Route Group Name**.

Step 3a - In case of Verba network-based or dial-in recording, set the **Distribution Algorithm** setting to **Top Down**.

Step 3b - In case of Verba proxy-based recording or the Announcement service, set the **Distribution Algorithm** setting to **Circular**. If the servers are in separate sites, and the load-balancing is not required, then set the **Distribution Algorithm** setting to **Top Down**.

Step 4 - Assign the previously created SIP trunk(s) to this route group at the **Find Device to Add to Route Group** pane. After selecting the desired SIP trunk(s), click on the **Add to Route Group** button.

The screenshot shows the configuration interface for a new Route Group. It is divided into three main sections:

- Route Group Information:** Contains a text field for "Route Group Name*" with the value "Recorder Router Group" and a dropdown menu for "Distribution Algorithm*" set to "Top Down".
- Route Group Member Information:** Contains a sub-section "Find Devices to Add to Route Group" with a search field "Device Name contains" (empty), a "Find" button, and a list of "Available Devices**" with "Recorder" selected. Below this is a "Port(s)" dropdown set to "None Available" and an "Add to Route Group" button.
- Current Route Group Members:** Contains a list of "Selected Devices***" with "Recorder (All Ports)" listed. To the right of this list are up and down arrow buttons. Below this is a list of "Removed Devices****" which is currently empty.

Step 5 Click on the **Save** button.

Create a new route list

Step 1 - Select **Call Routing / Route/Hunt / Route List** menu item and click on the **Add New** button. If you already have one, simply select it from the list.

Step 2 - Set a **Name** for the list.

Route List Information

Device is trusted

Name*

Description

Cisco Unified Communications Manager Group*

Step 3 - Select the appropriate **Cisco Unified Communications Manager Group** and click on the **Save** button.

Step 4 - Click on the **Add Route Group** button at the **Route List Member Information** panel.

Route List Member Information

Route Group*

Calling Party Transformations

Use Calling Party's External Phone Number Mask*

Calling Party Transform Mask

Prefix Digits (Outgoing Calls)

Calling Party Number Type*

Calling Party Numbering Plan*

Called Party Transformations

Discard Digits

Called Party Transform Mask

Prefix Digits (Outgoing Calls)

Called Party Number Type*

Called Party Numbering Plan*

Step 5 - Select the previously created route group at the **Route Group** setting, then click **Save**.

Route List Information

Name*

Description

Cisco Unified Communications Manager Group*

Enable this Route List (change effective on Save; no reset required)

Route List Member Information


Selected Groups**

▼
▲

▼ ▲

Removed Groups***

Route List Details


 [Recorder Route Group](#)

Step 6 - At the Route List Configuration page, click on the **Save** button.

Create a new route pattern

Step 1 Select **Call Routing / Route/Hunt / Route Pattern** menu item and click on the **Add New** button.

Step 2 Set the **Route Pattern** value.

-  In case, of **network-based, dial-in recording or announcement**, the Route Pattern value has to be a free directory number, not used by any other devices. Make sure it does not collide with your numbering plan. The routing of the entered number can be verified in the Call Routing / Route Plan Report menu.

 - In case of **proxy-based recording** see the instructions under **Stage Three** in Cisco UCM configuration example for proxy based recording

Step 3 Set the **Gateway/Route List** to the one created/modified in the previous step.

Step 4 Click on the **Save** button.

Pattern Definition

Route Pattern*	<input type="text" value="9999"/>
Route Partition	<input type="text" value=" < None >"/>
Description	<input type="text"/>
Numbering Plan	<input type="text" value="-- Not Selected --"/>
Route Filter	<input type="text" value=" < None >"/>
MLPP Precedence*	<input type="text" value="Default"/>
Resource Priority Namespace Network Domain	<input type="text" value=" < None >"/>
Gateway/Route List*	<input type="text" value="Recorder Route List"/> (Edit)
Route Option	<input checked="" type="radio"/> Route this pattern <input type="radio"/> Block this pattern <input type="text" value="No Error"/>
Call Classification*	<input type="text" value="OffNet"/>
<input type="checkbox"/> Allow Device Override <input checked="" type="checkbox"/> Provide Outside Dial Tone <input type="checkbox"/> Allow Overlap Sending <input type="checkbox"/> Urgent Priority	
<input type="checkbox"/> Require Forced Authorization Code	
Authorization Level*	<input type="text" value="0"/>
<input type="checkbox"/> Require Client Matter Code	

Create and configure a SIP Trunk

Create a new SIP Profile

Step 1 - Select the **Device / Device Settings / SIP Profile** menu item.

Step 2 - Create a new profile for the new recorder trunk by clicking on the **Add New** button.

Step 3 - Provide a **Name**

SIP Profile settings for proxy-based recording

If proxy-based recording is used, the following settings have to be set:

- **User-Agent and Server header information: Pass Through Received Information as User-Agent**
- **Early Offer support for voice and video calls: Best Effort (no MTP inserted)**
- **Allow Presentation Sharing using BFCP**
- **Allow iX Application Media**

SIP Profile settings for VoH/ViQ

If trunk is set for Video on Hold/Video in Queue, the following settings have to be set:

- **Early Offer support for voice and video calls: Best Effort (no MTP inserted)**
- **Allow Presentation Sharing using BFCP**

Step 4 - In the **Enable OPTIONS Ping** section turn on the **Enable OPTIONS Ping to monitor destination status for Trunks with Service Type "None (Default)"** setting.

SIP OPTIONS Ping	
<input checked="" type="checkbox"/> 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

Step 5 - Click on the **Save** button.

 It is allowed to use the same SIP Profile for multiple SIP Trunks.

Optional - Create a new SIP Trunk Security Profile

In special cases like **outbound announcement, secure SIP Trunk connection, or when multiple SIP Trunks going to connect to the same Verba server**, a new SIP Trunk Security Profile has to be created.

Step 1 - Select the **System / Security / SIP Trunk Security Profile** menu item.

Step 2 - Create a new profile for the new recorder trunk by clicking on the **Add New** button.

Step 3 - Provide a **Name**.

Step 4 - If **multiple SIP Trunks going to connect to the same Verba server**, then all of them should have a separate security profile with a different Incoming Port setting. If this is the case, then change the **Incoming Port** setting accordingly.

Step 5 - If the SIP Trunk going to be used for **outbound announcement**, then turn on the **Accept replaces header** setting.

Secure SIP Trunk connection

If secure SIP Trunk connection is used, the Verba server certificate has to be [uploaded to the CUCM first](#). In the SIP Trunk security profile, the following settings have to be set:

- **Device Security Mode: Encrypted**
- **Incoming Transport Type: TLS**
- **Outgoing Transport Type: TLS**
- **X.509 Subject Name: Recording Server certificate Subject value (after CN=), which is usually the FQDN of the Recording Server. You can check this attribute by opening the certificate file in Windows.**
- **Transmit Security Status**

Step 6 - Click **Save**.

Create a new SIP trunk

To provision a recorder as a SIP trunk device, a Unified CM administrator has to create a SIP trunk device from the device page.

Step 1 - Select the **Device / Trunk** menu item, and click on the **Add New** button.

Step 2 - Set the **Device Name** at the **Device Information** panel.

SIP Trunk setting for inbound announcement

If outbound announcement is used, the following settings have to be turned on:

- **PSTN Access**
- **Redirecting Diversion Header Delivery - Inbound**
- **Redirecting Diversion Header Delivery - Outbound**
- **Rerouting Calling Search Space:** must able to resolve the original callee as seen from Diversion header to transfer back the call to original callee after announcement

SIP Trunk setting for outbound announcement

If outbound announcement is used, the following settings have to be turned on:

- **PSTN Access**
- **Redirecting Diversion Header Delivery - Inbound**
- **Redirecting Diversion Header Delivery - Outbound**
- **Rerouting Calling Search Space:** must able to resolve the original callee as seen from Diversion header to replaces transfer /join the in and outbound call leg after announcement
- **Inbound calls/Calling Search Space:** must able to resolve the original callee as seen from Diversion header to initiate the outbound call leg between the service and callee in which the prompt is played

Step 3 - Set **Destination Address** value to match the recorder (or proxy in case of proxy-based recording) server local address.

Step 4 - Set **Destination Port** to **5060** (this value has to match the Verba Recording Server configuration).

Step 5 - Set **SIP Trunk Security Profile** to **Non Secure SIP Trunk Profile** or to the new profile created earlier.

Step 6 - Set the **SIP Profile** setting to the one created earlier.

Step 7 - Leave other parameters as default.

SIP Information

Destination

Destination Address is an SRV

	Destination Address	Destination Address IPv6	Destination Port	Status	Status Reason	Duration
1*	10.4.0.33		5060	down	local=2	Time Down: 0 day 23 hours 16 minutes

MTP Preferred Originating Codec* 711ulaw

BLF Presence Group* Standard Presence group

SIP Trunk Security Profile* Non Secure SIP Trunk Profile

Rerouting Calling Search Space < None >


Out-Of-Dialog Refer Calling Search Space < None >

SUBSCRIBE Calling Search Space < None >

SIP Profile* Verba SIP Profile [View Details](#)

DTMF Signaling Method* No Preference

Step 8 - Click on the **Save** button.

 After saving the changes, **reset** the trunk to apply the configuration on the trunk!

Configuring 2N Recording with Cisco CUBE Media Proxy

It is possible to set up 2N recording for Network-based recording using the Cisco CUBE Media Proxy feature. In that case, the phone device sends the forked media stream to the Cisco CUBE, which can forward the stream to multiple recorders.

For more information, and the configuration steps for the Cisco side, refer to the following site:

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/configuration/cube-book/voi-cube-media-proxy.html>

Configuring Verba for Cisco 2N Network-based Recording

Before the configuration steps, two servers have to be installed with the Verba Recording Server or Single Server role.

Once the configuration is done, both servers have to be configured for Network-based recording: [Configuring Verba for Cisco network-based recording](#)

While configuring, the following settings have to be made differently:

- At **Step 10**, only the "localhost:11200" value can be provided. The JTAPI connection between the servers cannot be cross-connected, all the servers need to have their own JTAPI connection.
- At **Step 14**, the CUBE IP address needs to be provided instead of the CUCM IP address.

Setting up one of the recorders as secondary

It is possible to mark one of the recorders as secondary, so the recordings made by this recorder will be hidden by default when using the Search.

Step 1 - In the Verba Web Interface go to **System \ Servers** menu, select your Recording (or Single) Server, then click on the **Change Configuration Settings** tab.

Step 2 - Set the **Unified Call Recorder \ Secondary Recorder Service** setting to **Yes**.

Step 3 - Save the changes by clicking on the



icon.

Step 17 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.



There are tasks to be executed regarding the configuration of this Verba Server.
If you would like to execute these tasks now, please [click here](#) .

Configuring the Cisco IP Phone Service

Overview

The Verba Phone Service enables you to use the Cisco IP phone XML capability in order to extend the functionality of the call recording system. Verba users are able to decide whether to record a call or not using this service. For detailed information about the available functions refer to [Using Verba form Cisco IP phones](#). In order to use this service, the Cisco Unified Communications Manager has to be configured.

Verba Phone Service modes

The Verba Phone Service supports four types of modes:

- **Verba Phone Service App** - Provides an interface for managing the existing recordings and on the ongoing call, like:
 - Marking as private
 - Marking as important
 - Adding a comment
 - Adding a marker
 - Emailing a link to the user or to the group supervisor
- **Recording control** - Provides an interface for starting / stopping the recording of the ongoing call.
- **Silent Monitoring** - Provides an interface for silent monitoring.
- **Quick actions** - Provides ability to execute actions on the ongoing call by pressing a single button, like:
 - Start recording
 - Stop recording
 - Keeping
 - Muting
 - Marking as protected.
 - Deleting
 - Marking as private
 - Marking as important
 - Adding a comment
 - Adding a marker
 - Emailing a link to the user or to the group supervisor

Authentication types

The Verba Phone Service supports four types of authentication:

- **Device name based** - Easiest to configure.
- **User ID based** - The username of the user is provided by a service parameter.
- **Device IP address based** - Recommended for passive recording.
- **Manual username and password provisioning** - Only available for the Verba Phone Service App and for silent monitoring.

Stage One: Creating a new Phone Service

Verba Phone Service

Individual features of the Verba Phone Service can be added to **line buttons** on the right side of the phone for quick access. E.g. a call can be marked important with a single press of a button.



Once subscribed to the Verba Phone Service, the service can be accessible by pressing the Phone Service button.

The following sections describes how to configure the Verba Phone Service based on authentication type.

i If multi-tenant system is being used, then an "eid" parameter also has to be added. See [Configuring the Verba Phone Service with user ID based authentication Step 9-14](#).

i Due to functional **limitations in Cisco UCM Express** based products, the Verba Phone Service has a simpler feature set. The [configuration steps are different](#) and the quick access mode cannot be used.

Configuring the Verba Phone Service with device name, IP address, or manual authentication

Step 1 - After authentication select the **Device / Device Settings / Phone Services** menu item.

Step 2 - Click on **Add New**.

Step 3 - Type in the **Service Name**: Verba (or what you would like to display)

Step 4 - Type in the **Service Description**: Verba Phone Service (or what you would like to display)

Step 5 - Provide the **Service URL** based on required function and authentication method:

▼ Service URLs for device name based authentication - Click to expand

Service URL	Description
http://verba_MR_address/verba/phoneservice.do?byDeviceOrIp=1&name=#DEVICENAME#	Enters to the Verba Phone Service App.
http://verba_MR_address/verba/phoneservice.do?byDeviceOrIp=1&name=#DEVICENAME#&manual=1	Enters to the recording control menu, where the user can start / stop the recording.
http://verba_MR_address/verba/phoneservicesm.do?byDeviceOrIp=1&name=#DEVICENAME#	Enters to the silent monitoring menu.
http://verba_MR_address/verba/ps_RecordByDeviceId.do?type=manualRecord&name=#DEVICENAME#	Quick action for starting the recording.
http://verba_MR_address/verba/ps_RecordByDeviceId.do?type=manualRecord&name=#DEVICENAME#&unmark=1	Quick action for stopping the recording.
http://verba_MR_address/verba/ps_RecordByDeviceId.do?name=#DEVICENAME#	Quick action for marking the recording for keeping.
http://verba_MR_address/verba/ps_ProtectByDeviceId.do?name=#DEVICENAME#	Quick action for marking the call as protected.
http://verba_MR_address/verba/ps_ProtectByDeviceId.do?name=#DEVICENAME#&unmark=1	Quick action for removing the protected mark.
http://verba_MR_address/verba/ps_DeleteByDeviceId.do?name=#DEVICENAME#	Quick action for stopping the recording, and delete it.
http://verba_MR_address/verba/ps_Mute.do?byDeviceOrIp=1&name=#DEVICENAME#	Quick action for muting the recording.

http://verba_MR_address/verba/ps_Unmute.do?byDeviceOrIp=1&name=#DEVICENAME#	Quick action for unmuting the recording.
http://verba_MR_address/verba/phoneservice.do?byDeviceOrIp=1&name=#DEVICENAME#&onLogin=Private	Quick action for marking the call as private.
http://verba_MR_address/verba/phoneservice.do?byDeviceOrIp=1&name=#DEVICENAME#&onLogin=Private&unmark=1	Quick action for removing the private mark.
http://verba_MR_address/verba/phoneservice.do?byDeviceOrIp=1&name=#DEVICENAME#&onLogin=Important	Quick action for marking the call as important.
http://verba_MR_address/verba/phoneservice.do?byDeviceOrIp=1&name=#DEVICENAME#&onLogin=Important&unmark=1	Quick action for removing the important mark.
http://verba_MR_address/verba/phoneservice.do?byDeviceOrIp=1&name=#DEVICENAME#&onLogin=AddTag	Quick action for adding a comment.
http://verba_MR_address/verba/phoneservice.do?byDeviceOrIp=1&name=#DEVICENAME#&onLogin=Marker	Quick action for adding a marker.
http://verba_MR_address/verba/phoneservice.do?byDeviceOrIp=1&name=#DEVICENAME#&onLogin=EmailMe	Quick action for emailing a link to the user.
http://verba_MR_address/verba/phoneservice.do?byDeviceOrIp=1&name=#DEVICENAME#&onLogin=EmailBoss	Quick action for emailing a link to the group supervisor.

▼ Service URLs for IP address based authentication - Click to expand

Service URL	Description
http://verba_MR_address/verba/phoneservice.do?byDeviceOrIp=1&name=#DEVICENAME#	Enters to the Verba Phone Service App.
http://verba_MR_address/verba/phoneservice.do?byDeviceOrIp=1&name=#DEVICENAME#&manual=1	Enters to the recording control menu, where the user can start / stop the recording.
http://verba_MR_address/verba/phoneservicesm.do?byDeviceOrIp=1&name=#DEVICENAME#	Enters to the silent monitoring menu.
http://verba_MR_address/verba/ps_RecordByIp.do?type=manualRecord	Quick action for starting the recording.
http://verba_MR_address/verba/ps_RecordByIp.do?type=manualRecord&unmark=1	Quick action for stopping the recording.
http://verba_MR_address/verba/ps_RecordByIp.do	Quick action for marking the recording for keeping.
http://verba_MR_address/verba/ps_ProtectByIp.do	Quick action for marking the call as protected.
http://verba_MR_address/verba/ps_ProtectByIp.do?unmark=1	Quick action for removing the protected mark.
http://verba_MR_address/verba/ps_DeleteByIp.do	Quick action for stopping the recording, and delete it.
http://verba_MR_address/verba/ps_MuteByIp.do	Quick action for muting the recording.
http://verba_MR_address/verba/ps_UnmuteByIp.do	Quick action for unmuting the recording.
http://verba_MR_address/verba/phoneservice.do?byDeviceOrIp=1&name=#DEVICENAME#&onLogin=Private	Quick action for marking the call as private.
http://verba_MR_address/verba/phoneservice.do?byDeviceOrIp=1&name=#DEVICENAME#&onLogin=Private&unmark=1	Quick action for removing the private mark.

http://verba_MR_address/verba/phoneservice.do? byDeviceOrIp=1&name=#DEVICENAME#&onLogin=Important	Quick action for marking the call as important.
http://verba_MR_address/verba/phoneservice.do? byDeviceOrIp=1&name=#DEVICENAME#&onLogin=Important&unmark=1	Quick action for removing the important mark.
http://verba_MR_address/verba/phoneservice.do? byDeviceOrIp=1&name=#DEVICENAME#&onLogin=AddTag	Quick action for adding a comment.
http://verba_MR_address/verba/phoneservice.do? byDeviceOrIp=1&name=#DEVICENAME#&onLogin=Marker	Quick action for adding a marker.
http://verba_MR_address/verba/phoneservice.do? byDeviceOrIp=1&name=#DEVICENAME#&onLogin=EmailMe	Quick action for emailing a link to the user.
http://verba_MR_address/verba/phoneservice.do? byDeviceOrIp=1&name=#DEVICENAME#&onLogin=EmailBoss	Quick action for emailing a link to the group supervisor.

▼ Service URLs for manual authentication - Click to expand

Service URL	Description
http://verba_MR_address/verba/phoneserviceauth.do	Brings up the login page, and after successful login enters to the Verba Phone Service App.
http://verba_MR_address/verba/phoneservicesmauth.do	Brings up the login page, and after successful login enters to the silent monitoring menu.

Step 6 - Set the **Service Category** setting to **XML Service**.

Step 7 - Set the **Service Type** setting to **Standard IP Phone Service**.

Step 8 - Turn on the **Enabled** setting.

Service Information

Service Name*

Service Description

Service URL*

Secure-Service URL

Service Category*

Service Type*

Service Vendor

Service Version

Enable

Step 9 - Click **Save**.

Configuring the Verba Phone Service with user ID based authentication

Step 1 - After authentication select the **Device / Device Settings / Phone Services** menu item.

Step 2 - Click on **Add New**.

Step 3 - Type in the **Service Name**: Verba (or what you would like to display)

Step 4 - Type in the **Service Description**: Verba Phone Service (or what you would like to display)

Step 5 - Provide the **Service URL** based on required function:

▼ Service URLs for user ID based authentication - Click to expand

Service URL for user ID based authentication	Description
http://verba_MR_address/verba/phoneservice.do	Enters to the Verba Phone Service App.
http://verba_MR_address/verba/phoneservice.do?manual=1	Enters to the recording control menu, where the user can start / stop the recording.
http://verba_MR_address/verba/phoneservicesm.do	Enters to the silent monitoring menu.
http://verba_MR_address/verba/phoneservice.do?type=manualRecord	Quick action for starting the recording.
http://verba_MR_address/verba/phoneservice.do?type=manualRecord&unmark=1	Quick action for stopping the recording.
http://verba_MR_address/verba/phoneservice.do?onLogin=Record	Quick action for marking the recording for keeping.
http://verba_MR_address/verba/phoneservice.do?onLogin=Protect	Quick action for marking the call as protected.
http://verba_MR_address/verba/phoneservice.do?onLogin=Protect&unmark=1	Quick action for removing the protected mark.
http://verba_MR_address/verba/phoneservice.do?onLogin=Delete	Quick action for stopping the recording, and delete it.
http://verba_MR_address/verba/phoneservice.do?onLogin=Mute	Quick action for muting the recording.
http://verba_MR_address/verba/phoneservice.do?onLogin=Unmute	Quick action for unmuting the recording.
http://verba_MR_address/verba/phoneservice.do?onLogin=Private	Quick action for marking the call as private.
http://verba_MR_address/verba/phoneservice.do?onLogin=Private&unmark=1	Quick action for removing the private mark.
http://verba_MR_address/verba/phoneservice.do?onLogin=Important	Quick action for marking the call as important.
http://verba_MR_address/verba/phoneservice.do?onLogin=Important&unmark=1	Quick action for removing the important mark.
http://verba_MR_address/verba/phoneservice.do?onLogin=AddTag	Quick action for adding a comment.
http://verba_MR_address/verba/phoneservice.do?onLogin=Marker	Quick action for adding a marker.
http://verba_MR_address/verba/phoneservice.do?onLogin=EmailMe	Quick action for emailing a link to the user.
http://verba_MR_address/verba/phoneservice.do?onLogin=EmailBoss	Quick action for emailing a link to the group supervisor.

Step 6 - Set the **Service Category** setting to **XML Service**.

Step 7 - Set the **Service Type** setting to **Standard IP Phone Service**.

Step 8 - Turn on the **Enabled** setting.

Step 9 - Add a new parameter by clicking on the **New Parameter** button. A new window opens.

Step 10 - Type **Parameter Name**: uname

Step 11 - Type in the **Parameter Display Name**: Login name of the user

Step 12 - Type in the **Parameter Description**: This parameter is equal to the Verba user login name. This parameter enables the service to identify the user that called the service from an IP phone.

Step 13 - Check the **Parameter is Required** option.

Service Parameter Information

Parameter Name*
uname

Parameter Display Name*
User name

Default Value

Parameter Description*
Verba user ID

Parameter is Required

Parameter is a Password (mask contents)

Step 14 - Press **Save And Close** button.

 If multi-tenant system is being used, then an "eid" parameter also has to be added.

Step 15 - Click **Save**.

Stage Two: Subscribing to the Verba Phone Service

After you have successfully configured the Verba Phone Service, you have to register the service for each IP phone device that needs access to the service.

Step 1 - Select the **Device / Phone** menu item.

Step 2 - Select the desired phone/device.

Step 3 - Select **Subscribe/Unsubscribe Services** link from the "Related links" dropdown list in the upper right corner.

Step 4 - In the new pop up window select the previously created phone service from the list box.

Service Information

Service Subscription: New

Select a Service*

Service Description

Verba Phone Service App

Step 5 - Press the **Next** button.

Step 6 - Provide the necessary parameters if required.

Service Information

Service Subscription: Verba

Service Name*

Environment ID [\(Description\)](#)

User Name [\(Description\)](#)

Step 7 - Press the **Subscribe** button.

If you have more than one line on a device and all of them are recorded, you do not have to configure different Verba Phone Services for them, because the service uses the device name / IP address or the user name for identifying calls related to a user, not extension numbers. If the user is properly configured in the Verba database, all calls are visible from the service, which are linked to the given user (calls are linked to a user through the station mapping).

Stage Three: Adding a new service button to the phone device

In order to utilize the quick access functions in the most efficient way, you can configure line buttons for it on certain IP phones. In this way a single button click on the phone can activate the given function. Follow the steps below to configure quick access functions on line buttons:

Step 1 - Select the **Device / Phone** menu item.

Step 2 - Select the desired phone/device.

Step 3 - In the left panel, click on the **Add a new SURL** link. A new window opens.

Step 4 - In the new window, select the previously subscribed phone service at the **Button Service** column, and provide a text to display at the **Label** column.

Service URL Settings on base Phone

	Button Service	Label
1	<input type="text" value="Verba"/>	<input type="text" value="Verba"/>

Step 5 - Click **Save**, then click **Close**.

Step 6 - Press the **Modify Button Items** button on the left side. A new window opens.

Step 7 - In the **Reorder Phone Button Configuration** window select the phone service item in the right list (Unassigned Associated Items) and move it to the left list (Associated Items). Make sure that the new SURL item will be visible on the given phone type considering the number of available items (line buttons).

Manage Button Associations.

Associated Items		Unassigned Associated Items
Line [1] - 2026 (no partition)- Fixed feature - button 1	↕	Line [2] - Add a new DN
Verba	↕	None
None		Add a new BLF SD
None		Add a new SD
None	➤	Add a new BLF Directed Call Park
None	↕	CallBack
None		Call Park
None		Call Pickup
None		Conference List
None		Conference

Step 8 - Press **Save**, then click **Close**.

Step 9 - Press the **Save** button in the Phone Configuration window, then click **Apply Config**.

Configure the IP Phone Service in UCM Express

Cisco Unified Communications Manager Express supports XML services but with limited functionality (e.g. phone level service parameters cannot be defined). Because of such kind of limitations, Verba Phone Service differs in some way from the original functionalities:

- **Access without authentication** - this mode originally requires a parameter provided by each phone in order to identify the given user. Since Unified Communications Manager Express does not support service parameters, the automatically provided device name (MAC address) is used to identify the users. The Verba Phone Service automatically recognizes the device name parameter and tries to find a matching extension record, which has a valid used mapping.
- **Access with authentication** - no difference from other Unified Communications Manager versions
- **Quick access** - cannot be used.

Configuring the Verba Phone Service without authentication

Step 1 - After authentication select t select the **Configure / IP Phone URLs** menu item.

Step 2 - Type in the **Service URL**:

`http://verba_media_repository_IP_address_or_hostname/verba/phoneservice.do`

Step 3 - Press the **Set** button.

Configuring the Verba Phone Service with authentication

Step 1 - After authentication select t select the **Configure / IP Phone URLs** menu item.

Step 2 - Type in the **Service URL**:

`http://verba_media_repository_IP_address_or_hostname/verba/phoneserviceauth.do`

Step 3 - Press the **Set** button.


Cisco UCCX Integration

Overview

The Verba Recording System supports direct **Cisco Unified Contact Center Express (UCCX)** integration as part of the **Verba Cisco JTAPI Service**. Using this integration the recording system provides access to Cisco UCCX specific call data.

Multiple new possibilities are available in your Verba Recording System based on the collection of UCCX information:


- **dialed number searches** - search for calls that came through a specific phone number
- **queue-based QM projects** - add all calls coming from a queue to a certain quality management project
- **identifying calls of an agent** - focus on the calls of a certain agent (no matter where they sit in the contact center)
- **search in IVR input** - search for IVR collected information, like customer IDs and zip codes
- **more CDR information** - get more insight into the history of your recorded calls

 The UCCX integration is only available when using Cisco **network-based** recording.

Collected UCCX parameters

- Application Name
- CSQ Name
- ANI
- DNIS
- Calling Device ID
- Called Device ID
- Called Agent ID
- Alerting Device ID
- Answering Device ID
- Answering Agent ID
- Dialed Number
- Last Redirect Device ID
- Connection Device ID
- CallVar1
- CallVar2
- CallVar3
- CallVar4
- CallVar5
- CallVar6
- CallVar7
- CallVar8
- CallVar9
- CallVar10

Configuring the Cisco Central Recording Service for UCCX integration

 In order to read the data of custom fields from UCCX, in the UCCX Metadata Template set the **UCCX Property Id** of *Call Variable X* to the identifier of the custom field (as shown in UCCX)

Cisco UCCX integration is built-in into your standard Verba Recording System solution.

Step 1 - The metadata is stored in a pre-configured metadata template. To use the built-in Cisco UCCX template, associate it with the desired Verba user group (the group where your UCCX agents and supervisors are) via the following web interface configuration page: **Users / Groups / <select a group> / Metadata Template Association**

Step 2 - On the Verba web interface, navigate to **System / Servers**, select the Recording Server where the **Verba Cisco JTAPI Service** is enabled.

Step 3 - Click on the **Change Configuration Settings** tab and expand the **Cisco JTAPI Configuration / Cisco UCCX Integration** section.


Step 4 - Type the IP addresses of your UCCX servers into the **Cisco UCCX IP Address(es)** field. Master and Slave UCCX servers should be listed in the same row separated by commas. Independent UCCX servers should be separated by new lines.

Step 5 - Click on the




icon to save your settings.

Step 6 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

 **There are tasks to be executed regarding the configuration of this Verba Server.**
If you would like to execute these tasks now, please [click here](#) .

After executing the steps above, UCCX related metadata is being collected for all new calls. Check [Call Details](#).

 You can show Cisco UCCX metadata as columns in your search results by modifying the [Conversation list layout](#).


Cisco UCCE Integration

Overview

The Verba Recording System supports direct **Cisco Unified Contact Center Enterprise (UCCE)** integration as part of the **Verba Cisco JTAPI Service**. Using this integration the recording system provides access to Cisco UCCE specific call data.

Multiple new possibilities are available in your Verba Recording System based on the collection of UCCE information:

- **dialed number searches** - search for calls that came through a specific phone number
- **queue-based QM projects** - add all calls coming from a queue to a certain quality management project
- **identifying calls of an agent** - focus on the calls of a certain agent (no matter where they sit in the contact center)
- **search in IVR input** - search for IVR collected information, like customer IDs and zip codes
- **more CDR information** - get more insight into the history of your recorded calls

 The UCCE integration is only available when using Cisco **network-based** recording.

Collected UCCE parameters

- Alerting Device ID
- ANI
- Answering Device ID
- Call Type
- Call Variable 1
- Call Variable 2
- Call Variable 3
- Call Variable 4
- Call Variable 5
- Call Variable 6
- Call Variable 7
- Call Variable 8
- Call Variable 9
- Call Variable 10
- Called Device ID
- Called Party Disposition
- Caller Entered Digits
- Calling Device ID
- Campaign ID
- Customer Account Number
- Customer Phone Number
- Dialed Number
- DNIS
- Last Redirect Device ID
- Line Handle
- Line Type
- Peripheral ID
- Peripheral Type
- Query Rule ID
- Service ID
- Service Number
- Skill Group ID
- Skill Group Number

- Skill Group Priority
- Trunk Group Number
- Trunk Number
- User Prompt
- UUI

Configuring the Cisco Central Recording Service for UCCE integration

The Cisco UCCE integration is built-in into your standard Verba Recording System solution.

Step 1 - The metadata is stored in a pre-configured metadata template. To use the built-in Cisco UCCE template, associate it with the desired Verba user group (the group where your UCCE agents and supervisors are) via the following web interface configuration page: **Users / Groups / <select a group> / Metadata Template Association**

✔ In order to read the data of custom fields from UCCE, in the UCCE Metadata Template set the **Property Id** of *Call Variable X* to the identifier of the custom field (as shown in UCCE)

Step 2 - On the Verba web interface, navigate to **System / Servers**, select the Recording Server where the **Verba Cisco JTAPI Service** is enabled.

Step 3 - Click on the **Change Configuration Settings** tab and expand the **Cisco JTAPI Configuration / Cisco UCCE Integration** section.

Step 4 - Fill out the configuration fields according to the table below.


Parameter name	Description																						
Cisco UCCE PG CTI Server IP(s) and port(s)	After clicking on the gear icon at the end of the line, the following fields can be configured: <ul style="list-style-type: none"> • Master IP Address • Master Port • Slave IP Address • Slave Port 																						
CTI Server Protocol Version	<p>Using a higher protocol version than the highest supported by the CTI Server will cause communication failures. However, using a lower version than the highest supported, the CTI Server has to reencode every message.</p> <p>Protocol versions based on UCCE version:</p> <table border="1" style="margin-left: 20px;"> <thead> <tr> <th>UCCE Version</th> <th>Protocol Version</th> </tr> </thead> <tbody> <tr><td>UCCE Version 10.0</td><td>18-19</td></tr> <tr><td>UCCE Version 9.0</td><td>16-17</td></tr> <tr><td>UCCE Version 8.5</td><td>15</td></tr> <tr><td>UCCE Version 8.0</td><td>14</td></tr> <tr><td>ICM Version 7.0</td><td>10-13</td></tr> <tr><td>ICM Version 5.0</td><td>9</td></tr> <tr><td>ICM Version 4.6</td><td>8</td></tr> <tr><td>ICM Version 4.5</td><td>7</td></tr> <tr><td>ICM Version 4.1</td><td>6</td></tr> <tr><td>ICM Version 4.0</td><td>5</td></tr> </tbody> </table>	UCCE Version	Protocol Version	UCCE Version 10.0	18-19	UCCE Version 9.0	16-17	UCCE Version 8.5	15	UCCE Version 8.0	14	ICM Version 7.0	10-13	ICM Version 5.0	9	ICM Version 4.6	8	ICM Version 4.5	7	ICM Version 4.1	6	ICM Version 4.0	5
UCCE Version	Protocol Version																						
UCCE Version 10.0	18-19																						
UCCE Version 9.0	16-17																						
UCCE Version 8.5	15																						
UCCE Version 8.0	14																						
ICM Version 7.0	10-13																						
ICM Version 5.0	9																						
ICM Version 4.6	8																						
ICM Version 4.5	7																						
ICM Version 4.1	6																						
ICM Version 4.0	5																						
Peripheral ID	If only a specific Peripheral should be monitored, then set this setting to that Peripheral ID. Otherwise, leave this setting on 999999999, and the system will monitor every Peripheral.																						

Step 5 - Click on the




icon to save your settings.

Step 6 - The system will notify you that the changes need to be applied to the server by restarting the involved services or rereading the new configuration. Execute the required tasks.

 There are tasks to be executed regarding the configuration of this Verba Server.
If you would like to execute these tasks now, please [click here](#) .

After executing the steps above, UCCE related metadata will be collected for all new calls. Check [Call Details](#).

 You can show Cisco UCCE metadata as columns in your search results by modifying the [Conversation list layout](#).

Configuring Cisco Unified IM and Presence 8.x, 9.x and Verba for Jabber IM recording

Add Verba as a compliance server in Cisco Unified IM and Presence server 8.x, 9.x

In order to record Cisco Jabber IM conversations, there are some configuration steps that need to be performed in the **Cisco Unified IM and Presence console**. This paragraph provides a detailed step by step guide on how to add a **Verba Recording Server as a third-party compliance server** in Cisco Unified IM and Presence.

Follow the steps below to add a Verba Recording Server as a third-party compliance server in the CUPS configuration console. You can find more details in the official Cisco documentation at [Instant Messaging Compliance for IM and Presence Service on Cisco Unified Communications Manager, Release 9.0\(1\), Integration with Third-Party Compliance Servers](#).

Step 1 Log into the **CUPS administration console**.

Step 2 From the top menu select **Messaging > External Server Setup > Third party compliance servers**

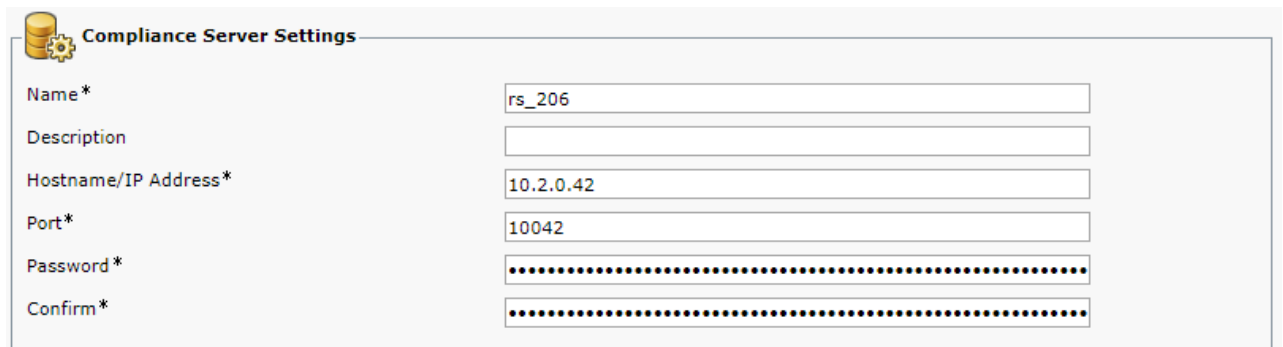
Step 3 Click **Add New**

Step 4 Fill out the name and (optionally) description fields.

Step 5 Provide the **IP address of the Verba Recording Server and Port (10042 by default)**

Step 6 Provide a **password** for authentication. This **has to match the password in the Verba Recording Server's configuration**.

Step 7 Click **Save**.



Compliance Server Settings	
Name *	rs_206
Description	
Hostname/IP Address *	10.2.0.42
Port *	10042
Password *
Confirm *

Step 8 From the top menu select **Messaging > Compliance**

Step 9 Select '**Third-Party Compliance Server**', then find and **select the previously configured Verba Compliance Server** from the drop-down list.

Step 10 Click **Save**.

Compliance Settings

Save

Status

Status: Ready

Compliance Settings

Select a compliance server type. A compliance server can be used to log and archive all instant messaging traffic.

Compliance Server Selection

Not Configured
 Message Archiver
 Third-Party Compliance Server (selected)

Third Party Server Assignment	
Node	Compliance Server
CUPS91	rs_206

Save

⚠ After changing the Compliance Settings, the XCP Router Service has to be restarted for the changes to take effect.

Configuring Cisco IM and P connections in Verba

Step 1 - In the Verba Web Interface go to **System > Servers > Select your Recording (or Single) Server > Click on the Service Activation** tab.

Step 2 - Activate the **Verba Cisco Compliance Service** by clicking on the



icon.

Step 3 - Click on the **Change Configuration Settings** tab.

Step 4 - Expand the **Cisco Compliance Service \ General** node. Set the **Cisco IM&P Server Version** setting to **Cisco IM&P 9.x and below**.

Step 5 - To configure a connection, in the next line click on the




icon.

Step 6 - At the right panel, set the **Component Name** setting the following way: open-compliance.node_name


The node name can be found by going to the **Messaging \ Compliance \ Compliance Settings** menu in the IM&P server.

ⓘ If your node name has dots (.) in it, for example, cups11.domain.com, then in your component name the dots should be removed and dashes should be added like this: open-compliance.cups11-domain-com

Compliance Settings

 Save

Status

 Status: Ready


Compliance Settings

Select a compliance server type. A compliance server can be used to log and archive all instant messaging traffic.

Compliance Server Selection

Not Configured
 Message Archiver
 Third-Party Compliance Server **(selected)**

Third Party Server Assignment	
Node	Compliance Server
CUPS91	rs_206

 Save

The **Port** and **Password** should be the same as what previously set in the Compliance Profile that is assigned to this node in the IM&P servers.

Presence Servers

Component Name	<input type="text" value="open-compliance.cups21"/>
Port	<input type="text" value="10042"/>
Password	<input type="password" value="*****"/>



Click **Save**.


Step 7 - Expand the **IM Recording** node, and set the **Enable Recorder** setting to **Yes**, and set the **Internal Doman, Number Pattern** setting according to the internal SIP domains.

Cisco Compliance Service

General

Cisco IM&P Server Version: Cisco IM&P 9.x and below

Cisco Unified CM IM&P Connections: open-compliance.cups21|10042|1vcYm2yq7Fr5WuO3yi9oQQ==  
 +

Work Folder: C:\Program Files (x86)\Verba\work\ciscocompliance 

IM Recording

Enable Recorder: Yes

Internal Domain, Numbers Pattern: .*@contoso.com

Enable Notification Message Inside Domains: No

Notification Subject Inside Domains: Verba System Message

Notification Message Inside Domains: Conversation is recorded.

Enable Notification Message Between Domains: No

Notification Subject Between Domains: Verba System Message

Notification Message Between Domains: Conversation is recorded.

Duplicate Recording If Both Parties Are Recorded: Yes

Call Timeout (seconds): 300

Persistent Chat Segment Length (minutes): 1440


Create Transcript and Metadata XML Files: No

Step 8 - Save the changes by clicking on the



icon.

Step 9 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

 There are tasks to be executed regarding the configuration of this Verba Server. If you would like to execute these tasks now, please [click here](#) .

Step 10 - Click on the **Service Control** tab.

Step 11 - Start the **Verba Cisco Compliance Service** by clicking on the



icon.

Step 12 - Repeat the steps on all Recording servers if there are multiple.

Restarting the XCP Router Service

For the Compliance server settings to take effect, the **XCP Router Service** has to be restarted. To do that, follow the steps below:

Step 1 From the list in the top right corner of the CUPS management interface select **Cisco Unified IM and Presence Serviceability** and click Go.

Step 2 From the top menu select **Tools > Control Center > Network Services**

Step 3 From the server list select **CUCM IM and Presence** and click Go.

Step 4 Select the **Cisco XCP Router** service and click **Restart**. The process can take several minutes to complete.

Configure extensions

After finalizing the configuration of the recording services, make sure you have added the SIP URIs you want to record to the Verba extension list. This can be done manually ([Extension list](#)) or using [Active Directory Synchronization](#).

Configuring Cisco Unified IM and Presence 10.x, 11.x, 12.x and Verba for Jabber IM recording

Add Verba as a compliance server in Cisco Unified IM and Presence server 10.x, 11.x, 12.x

In order to record Cisco Jabber IM conversations, there are some configuration steps that need to be performed in the **Cisco Unified IM and Presence console**. This paragraph provides a detailed step by step guide on how to add a **Verba Recording Server as a third-party compliance server** in Cisco Unified IM and Presence.

Follow the steps below to add a Verba Recording Server as a third-party compliance server in the CUPS configuration console. You can find more details in the official Cisco documentation at [Instant Messaging Compliance for IM and Presence Service on Cisco Unified Communications Manager, Release 10.0\(1\), Integration with Third-Party Compliance Servers](#).

Step 1 Log into the **CUPS administration console**.

Step 2 From the top menu select **Messaging > External Server Setup > Third party compliance servers**

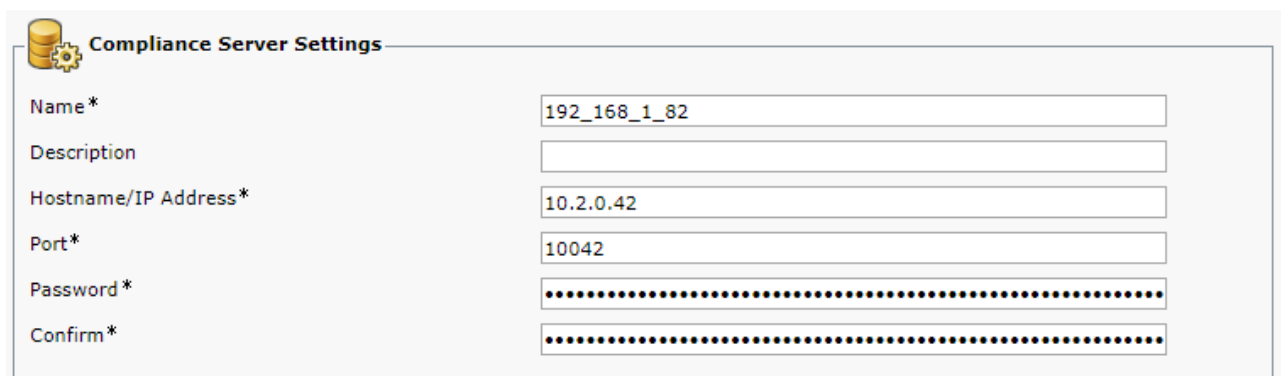
Step 3 Click **Add New**

Step 4 Fill out the name and (optionally) description fields.

Step 5 Provide the **IP address of the Verba Recording Server and Port (10042 by default)**

Step 6 Provide a **password** for authentication. This **has to match the password in the Verba Recording Server's configuration**.

Step 7 Click **Save**.



Compliance Server Settings

Name *	<input type="text" value="192_168_1_82"/>
Description	<input type="text"/>
Hostname/IP Address *	<input type="text" value="10.2.0.42"/>
Port *	<input type="text" value="10042"/>
Password *	<input type="password" value="....."/>
Confirm *	<input type="password" value="....."/>

Step 8 From the top menu select **Messaging > Compliance > Compliance Settings**

Step 9 Select **'Third-Party Compliance Server'**.

Step 10 Find the **previously configured compliance server in the list below**, then **select the CUPS server you want to be recorded from drop-down list under 'Node'**.

Step 11 In the **same row**, set the **Compliance Profile to SystemDefaultComplianceProfile**.

Step 12 Take note of the **'Open-port Component name'** as this will be needed when configuring the Verba Recording Server.

Step 13 Click **Save**.

Compliance Settings Related Links: [Go to Routing Priority](#)

Status
 Status: Ready

Compliance Settings
 Select a compliance server type. A compliance server can be used to log and archive all instant messaging traffic.

Compliance Server Selection

Not Configured
 Message Archiver
 Third-Party Compliance Server **(selected)**

Third-Party Compliance Server and Compliance Profile Assignment
 Compliance is a cluster-wide configuration. All nodes in the cluster are subject to compliance logging.

Third-Party Compliance Server and Compliance Profile Assignment			
Compliance Server	Node	Compliance Profile	Open-port Component Name
192_168_1_209	-- Unassigned --	-- Unassigned --	
192_168_1_82	cups10	SystemDefaultComplianceProfile	op-192_168_1_82.cups10

⚠ After changing the Compliance Settings, the XCP Router Service has to be restarted for the changes to take effect.

Configuring Cisco IM and P connections in Verba

Step 1 - In the Verba Web Interface go to **System > Servers > Select your Recording (or Single) Server > Click on the Service Activation** tab.

Step 2 - Activate the **Verba Cisco Compliance Service** by clicking on the



icon.

Step 3 - Click on the **Change Configuration Settings** tab.

Step 4 - Expand the **Cisco Compliance Service \ General** node. Set the **Cisco IM&P Server Version** setting to **Cisco IM&P 10.x and above**.

Step 5 - To configure a connection, in the next line click on the



icon.

Step 6 - At the right panel, set the **Component Name** setting. The component name will be the **Open-port Component Name** that is shown in the IM&P servers under **Messaging \ Compliance \ Compliance Settings** menu as shown in the picture below.

ⓘ When you copy the Open-port Component Name please make sure that you delete any space characters from the end. This is a common mistake.

Compliance Settings

Select a compliance server type. A compliance server can be used to log and archive all instant messaging traffic.

Compliance Server Selection

Not Configured
 Message Archiver
 Third-Party Compliance Server (**selected**)

Third-Party Compliance Server and Compliance Profile Assignment

Compliance is a cluster-wide configuration. All nodes in the cluster are subject to compliance logging.

Third-Party Compliance Server and Compliance Profile Assignment			
Compliance Server	Node	Compliance Profile	Open-port Component Name
rsew	cups1061	VerbaEthicalWallProfile	op-rsew.cups1061

The **Port** and **Password** should be the same as what previously set in the Compliance Profile that is assigned to this node in the IM&P servers.

Presence Servers

Component Name:

Port:

Password:

Click **Save**.

Step 7 - Expand the **IM Recording** node, and set the **Enable Recorder** setting to **Yes**, and set the **Internal Doman, Number Pattern** setting according to the internal SIP domains.

Cisco Compliance Service

General

Cisco IM&P Server Version: Cisco IM&P 10.x and above

Cisco Unified CM IM&P Connections:

op-rsew.cups1061 10042 1vcYm2yq7Fr5WuO3yi9oQQ==		
op-rsew_2.cups1061 10043 1vcYm2yq7Fr5WuO3yi9oQQ==		

Work Folder: C:\Program Files (x86)\Verba\work\ciscocompliance

IM Recording

Enable Recorder: Yes

Internal Domain, Numbers Pattern: .*@contoso.com

Enable Notification Message Inside Domains: No

Notification Subject Inside Domains: Verba System Message

Notification Message Inside Domains: Conversation is recorded.

Enable Notification Message Between Domains: No

Notification Subject Between Domains: Verba System Message

Notification Message Between Domains: Conversation is recorded.

Duplicate Recording If Both Parties Are Recorded: Yes

Call Timeout (seconds): 300

Persistent Chat Segment Length (minutes): 1440

Create Transcript and Metadata XML Files: No

Step 8 - Save the changes by clicking on the



icon.

Step 9 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

There are tasks to be executed regarding the configuration of this Verba Server.
 If you would like to execute these tasks now, please [click here](#) .

Step 10 - Click on the **Service Control** tab.

Step 11 - Start the **Verba Cisco Compliance Service** by clicking on the



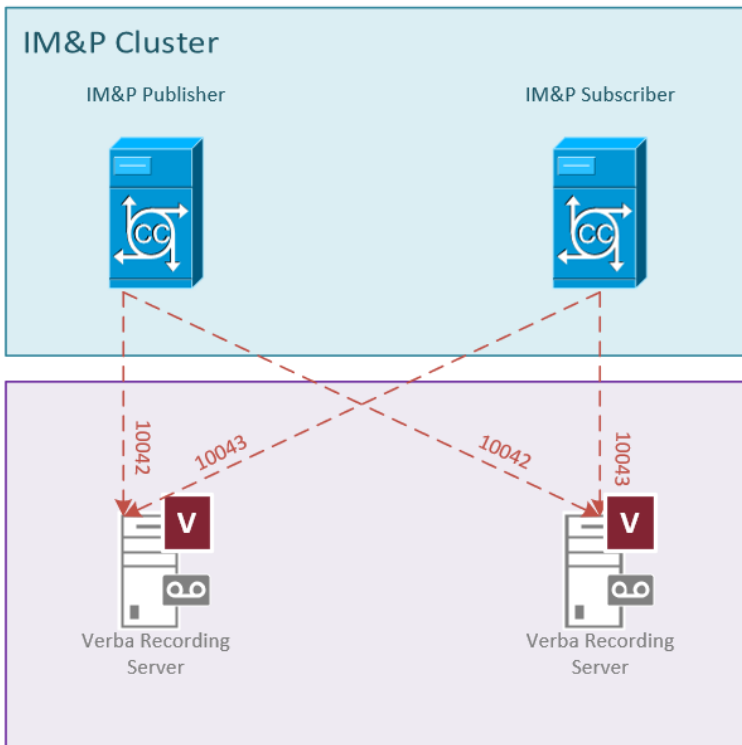
icon.

Step 12 - Repeat the steps on all Recording servers if there are multiple.

Configuring High Availability

In order to ensure that Cisco Jabber communications are not disrupted, it is best practice to deploy Recording Servers in a resilient fashion. Multiple Recording Servers should be configured to receive the XMPP events for processing.

Recording Servers are deployed as active components and IM&P Nodes are load-balancing between the Recording Servers using a modulo algorithm and the IM&P nodes are handling the fail over scenarios. If a recording service fails (e.g. service or server crash, network failure) during the recording of an ongoing conversation, the Cisco IM&P service which is the host of the recorded conversation, detects the failure and reassigns the conversation to another connected Recording Server.



Each recording server can be added using the process above, the main consideration to make is to ensure that each IM&P node connection has an unique port on the recorder server

Restarting the XCP Router Service

For the Compliance server settings to take effect, the **XCP Router Service** has to be restarted. To do that, follow the steps below:

- Step 1** From the list in the top right corner of the CUPS management interface select **Cisco Unified IM and Presence Serviceability** and click Go.
- Step 2** From the top menu select **Tools > Control Center > Network Services**
- Step 3** From the server list select **CUCM IM and Presence** and click Go.
- Step 4** Select the **Cisco XCP Router** service and click **Restart**. The process can take several minutes to complete.

Configure extensions

After finalizing the configuration of the recording services, make sure you have added the SIP URIs you want to record to the Verba extension list. This can be done manually ([Extension list](#)) or using [Active Directory Synchronization](#).

Configuring Verba for Cisco Jabber File Transfer recording

Prerequisites

Enable Managed File Transfer

The files shared can be recorded only if the Managed File Transfer is enabled and configured at the Cisco IM&P side. For the configuration, refer to the following article:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/im_presence/configAdminGuide/10_5_2/CUP0_BK_CEB3E82E_00_config-admin-guide-imp-1052/CUP0_BK_CEB3E82E_00_config-admin-guide-imp-1052_chapter_010110.html

Create a User

An End User has to be created on the Cisco side, which going to be used by the Verba Recording Server. No special right needed.

Configuring Verba for Cisco Jabber File Transfer recording

Step 1 - In the Verba Web Interface go to **System > Servers > Select your Recording (or Single) Server > Click on the Service Activation** tab.

Step 2 - Activate the **Verba Cisco Compliance Service** by clicking on the



icon.

Step 3 - Click on the **Change Configuration Settings** tab.

Step 4 - Expand the **Cisco Compliance Service \ XMPP Client** node.

Step 5 - Set the **Enable XMPP Client** setting to **Yes**.

Step 6 - Provide the **Cisco IM&P Server Address** setting. This should be the **IP address** of the IM&P publisher.

Step 7 - Provide the details of the end user created for Verba at the IM&P side in the **XMPP Domain**, **Jabber Login ID**, and **Jabber Password** settings.


▲ Cisco Compliance Service		
▶ General		
▶ IM Recording		
▶ Communication Policies		
▲ XMPP Client		
Enable XMPP Client:	<input checked="" type="checkbox"/>	Yes ▼
Cisco IM&P Server Address:	<input checked="" type="checkbox"/>	192.168.1.22
Cisco IM&P Server XMPP Port:	<input type="checkbox"/>	5222
XMPP Domain:	<input checked="" type="checkbox"/>	contoso.com
Jabber Login ID:	<input checked="" type="checkbox"/>	verbauser
Jabber Password:	<input checked="" type="checkbox"/>	*****
Jabber Client resource:	<input type="checkbox"/>	verba-xmpp-client

Step 8 - Save the changes by clicking on the



icon.

Step 9 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

 There are tasks to be executed regarding the configuration of this Verba Server.
If you would like to execute these tasks now, please [click here](#) .

Step 10 - Click on the **Service Control** tab.

Step 11 - Start the **Verba Cisco Compliance Service** by clicking on the



icon.

Configure extensions

After finalizing the configuration of the recording services, make sure you have added the SIP URIs you want to record to the Verba extension list. This can be done manually ([Extension list](#)) or using [Active Directory Synchronization](#).

Configuring Verba for Cisco proxy based recording

The Cisco proxy based recording option in Verba allows recording voice/video calls forked at the Verba proxy server. This recording option requires custom call routing configuration.

Cisco UCM side configuration for proxy based recording

In the proxy-based recording model all recorded calls have to be routed to the Verba Proxy Server(s). This requires custom routing configuration in the Cisco environment. Please contact Verba support for information on the UCM side configuration details and possible impact.

Internal Article

If the customer requests information about the Cisco side config, then this article can be exported then sent:

[Cisco UCM configuration example for proxy based recording](#)

Verba side configuration for proxy based recording

Stage One: Configure the Verba Media Collector and Proxy service for RTP Proxy based recording

Follow the steps below to configure the Verba Media Collector and Proxy service to operate in Proxy mode.

 Stages One and Two take place on the same server's configuration page if the Recorder and Proxy Servers are co-located.

Step 1 - In the Verba web interface go to **System / Servers**, select the Recording (or separate Proxy) Server and click on the **Service Activation** tab.

Step 2 - Activate the **Verba Media Collector and Proxy Service** by clicking on the



icon.

Step 3 - Click on the **Change Configuration Settings** tab. Expand the **Media Collector and Proxy** section.

Step 4 - Under **General / Recorder Connection**, configure the authentication credentials for the connections with the recording service. Define the **Authentication User** and **Authentication Passwords** values. These credentials will be used later when configuring the connections in the recorder service.

Step 5 - In the **General** section set the **Internal Domain, Numbers Pattern** setting. This has to be a regex which matches to all internal line numbers and SIP domains.

Media Collector and Proxy

General

Recorder connection

Announcement Service Uri:	<input type="checkbox"/>	
Assign Call To Recorder only on First RTP:	<input type="checkbox"/>	Yes
Call Timeout (sec):	<input type="checkbox"/>	600
SIP Uri Modification:	<input type="checkbox"/>	Remove domain part for numbers only
Enable RTP over TCP Support:	<input type="checkbox"/>	Yes
Record video calls as audio only:	<input type="checkbox"/>	No
Recorder Groups and Priorities:	<input type="checkbox"/>	
Default Recorder Group Priority:	<input type="checkbox"/>	0
Internal Domain, Numbers Pattern:	<input checked="" type="checkbox"/>	\d{4}.*@contoso.com
Record SfB/Lync Application Sharing (RDP):	<input type="checkbox"/>	Yes
Record SfB/Lync File Transfer:	<input type="checkbox"/>	Yes
Enable Performance Based Loadbalancing for Recorders:	<input type="checkbox"/>	No
Use Overloaded Recorder as Last Effort:	<input type="checkbox"/>	Yes

Step 6 - In **RTP Proxy** section set **Enabled** to **Yes**.

Media Collector and Proxy

General

Remote Capture

Lync Connector

RTP Proxy

Advanced

Enabled:	<input checked="" type="checkbox"/>	Yes
Relay video streams:	<input type="checkbox"/>	Yes
A/V Port Range Begin:	<input type="checkbox"/>	16384
A/V Port Range End:	<input type="checkbox"/>	65535
Separated Video Port Range Begin:	<input type="checkbox"/>	0
Separated Video Port Range End:	<input type="checkbox"/>	0

Step 7 - In **RTP Proxy / Advanced** section set the **Enforce ACL on Relay Sessions** to **Yes**.

Media Collector and Proxy

- General
- Remote Capture
- Lync Connector

RTP Proxy

Advanced

Enforce ACL on Relay Sessions:	<input checked="" type="checkbox"/>	Yes
Enforce ACL Modalities on Relay Sessions:	<input type="checkbox"/>	Yes
Relay Media from Public Address:	<input type="checkbox"/>	Yes
Advanced Relay Mode:	<input type="checkbox"/>	No
Drop Unsolicited Packets:	<input type="checkbox"/>	No
Support RTCP Mux:	<input type="checkbox"/>	No
Support Late Media Negotiation:	<input type="checkbox"/>	No

Step 8 - In **SIP Proxy** section set **'Enabled'** to **Yes**.

Media Collector and Proxy

- General
- Remote Capture
- Lync Connector
- RTP Proxy

SIP Proxy

Enabled:	<input checked="" type="checkbox"/>	Yes
Listening Ports:	<input type="checkbox"/>	5060 outboundproxy Ogrwt4OfRps=

Step 9 - Click on the



icon in order to edit the preconfigured incoming SIP connection.

Step 10 - At the left panel, change the **Mode** setting to **SIP Router**. If necessary, change the Port, or provide the certificate settings if secure SIP connection is used. Click **Save**.

Proxy SIP Port

SIP Port	5060
Mode	SIP Router
TLS Certificate	
TLS CA	
TLS Key	
TLS Key Password	

Step 11 (Optional) - Add additional incoming SIP connections if there are multiple incoming connections, by clicking on the



icon.

Secure SIP Trunk Connection

If secure SIP Trunk connection is required, the following settings have to be set:

TLS Certificate: The thumbprint of the Verba server certificate being used for the connection. This has to be the same certificate which was upload to the CUCM.

TLS CA: The thumbprint of the CUCM server certificate, or the thumbprint of the CA certificate which issued the CUCM server certificate. Alternatively, "*" can be used. In this case, every certificate going to be trusted, whose CA certificate can be found in under the Trusted Root Certificate Authorities folder. If left empty, every certificate going to be trusted.


Alternatively, .crt/.cer and .key files can be used. In this case, UNC paths can be provided in the TLS Certificate and the TLS Key settings, and the TLS Key Password has to be provided.


Step 12 - Save the changes by clicking on the



icon.

Step 13 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

 There are tasks to be executed regarding the configuration of this Verba Server. If you would like to execute these tasks now, please [click here](#) .

 Changes can be execute at once at the end. In that case don't forget to click on **'Check All'**.

Step 14 - Click on the **Service Control** tab

Step 15 - Start the **Verba Media Collector and Proxy Service** by clicking on the



icon.

Repeat these steps for each Proxy Server in your system.

For more information about the Verba Media Collector and Proxy Service see [Verba Media Collector and Proxy Service Reference](#).

Stage Two: Configure the Verba Passive Recorder service for RTP Proxy based recording

Follow the steps below to configure the Verba Passive Recorder service for Proxy based recording:

 Stages One and Two take place on the same server's configuration page if the Recorder and Proxy Servers are co-located.

Step 1 - In the Verba web interface go to **System / Servers**, select the Recording Server and click on the **Service Activation** tab.

Step 2 - Activate the **Verba Passive Recorder Service** by clicking on the



icon.

Step 3 - Click on the **Change Configuration Settings** tab. Expand the **Passive Recorder** section.

Step 4 - Under **Basics** add your Proxy Servers and Media Collectors by clicking on the



next to **Recorder Proxy**.

Step 5 - At the right panel select the Proxy Server from the drop-down list at the **Host**. Provide the username and password configured in the **Verba Media Collector and Proxy Service** above for the connections. If there are multiple proxy servers, then set the **Recorder Weight** to **1** to enable equal-weight load balancing. Click **Save**.

Recorder Proxy

Host: TESTPROXY1.VERBATEST.LOCAL

Port: 11112

User: verba

Password:

Compress Connection Stream:

Recorder Weight: 1

Secure:

Recorder Group:

Step 6 - Repeat Steps 4-5 for every Proxy Server in your system.

Step 7 - Set the **Internal Domain, Numbers Pattern** setting. This has to be a regex which matches to all internal line numbers and SIP domains.

Step 8 (Optional) - If the video recording required then set the **Record Video Call As Audio Call** setting **No** under the **Advanced** node.

Passive Recorder

Basics

Recording Interface: +

Media Collector and Proxies:

TESTPROXY1.VERBATEST.LOCAL 11112 verba 1vcYm2yq7Fr5WuO3yI9oQQ== 0 1 1		
TESTPROXY2.VERBATEST.LOCAL 11112 verba 1vcYm2yq7Fr5WuO3yI9oQQ== 0 0 1		
EDGE1.VERBATEST.LOCAL 11112 verba 1vcYm2yq7Fr5WuO3yI9oQQ== 0 1 1		

Audio Format: Microsoft GSM-Fullrate (LPC-RPE) in WAV

Video Format: Verba RTP Dumped Media Format

Bidirectional/Stereo Recording: No

Automatic Gain Control Enabled: Yes

Conference Resources IP Addresses:

Experimental H.323 Support Enabled: No

SIP Support Enabled: Yes

Skinny Support Enabled: Yes

Call Timeout (seconds): 600

Voice Activity Statistics: No

Secondary Recording Server: No

Internal Domain, Numbers Pattern: \d{5}.*@contoso.com


Step 9 - Save the changes by clicking on the



icon.

Step 10 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

Changes can be executed at once at the end. In that case don't forget to click on **'Check All'**.

 There are tasks to be executed regarding the configuration of this Verba Server. If you would like to execute these tasks now, please [click here](#) .

Step 11 - Click on the **Service Control** tab

Step 12 - Start the **Verba Passive Recorder Service** by clicking on the



icon.

Repeat these steps for each Recorder Server in your system.

Final Stage: Configure extensions

After finalizing the configuration of the recording services, make sure you have added the extensions you want to record to the Verba extension list. This can be done manually ([Extension list](#)) or using [Active Directory Synchronization](#).

Recording redundancy, load balancing, and failover

For the configuration see: [Recorder load balancing and failover design](#)

Verba Media Collector and Proxy Service Reference

Verba Proxy Recorder service consists of the following modules:

- **Remote Capture** - This module allows to remotely capture network traffic. When the service is enabled on a server, Verba Recording Servers - deployed on other servers - can get access to the network traffic of the local network interfaces on the server. The application is primarily used in Microsoft Lync recording, where the remote capture service is able to identify the recorded call related streams and send them to the Recording Server for processing. The remote capture service receives signaling information for the Lync Filter applications, installed on Front End servers and SBAs and SBS. Signaling information is used to identify the relevant streams and only fork streams related to recorded interactions.
- **RTP Proxy** - This module acts as a standard RTP proxy, allowing to reroute any RTP stream through the application and provide access to media streams for recording. You can use the RTP proxy in any standard SIP environment together with SIP Proxy module, and in Lync environment together with Lync Filter applications installed on frontends, SBA and SBSs.
- **SIP Proxy** - It is a standard bypass SIP proxy server implementation. You can reroute SIP calls through the proxy server in order to get access to media streams for recording, and insert into the calls the RTP proxy module. The proxy server can act as SIP outbound proxy and as SIP router, in this case calls based on called pattern are rerouted to intended next hop in the route. The proxy supports TLS so secure SIP and SRTP in the RTP proxy is supported as well.

You can use any of these modules in the service, you can also combine them on a single server.

General settings

Configuration Parameter Name	Description	Sample Value
Recorder connection \ Listening Port	API port used with the Verba passive recording service.	11111
Recorder connection \ Secure Listening Port	API port over TLS used with the Verba passive recording service.	11112
Recorder connection \ Certificate File Path	Path to the certificate file used by the recorder proxy service to establish the TLS connection with the passive recorder service. Supported file format: X.509. You can use your own, self-signed certificate.	c:\verba.crt
Recorder connection \ Certificate Authority Certificate File Path	Path to the Certificate Authority (CA) certificate file. Supported file format: X.509. If you do not have this type of CA certificate, you can use your own, self-signed certificate; in this case leave this setting empty.	
Recorder connection \ Private Key File Path	Path to the private key file used by the recorder proxy service to establish the TLS connection with the passive recorder service. Supported file format: X.509.	c:\verba.key
Recorder connection \ Private Key File Password	Password for the private key file used by the recorder proxy service to establish the TLS connection with the passive recorder service.	
Recorder connection \ Authentication User	User account name to authenticate the passive recorder service accessing the proxy service.	verba
Recorder connection \ Authentication Password	Password for the user account.	
Announcement Service Uris		
Assign Call To Recorder only on First RTP	If enabled, calls will only be forked to the recording service when the proxy service receives the first RTP packet. If set to No and there is no RTP for the recorded call, the call will not be recorded at all.	No

Call Timeout (sec)	Defines the call timeout value in seconds, which is used to terminate the call recording automatically if the last RTP packet is received before this value.	60
SIP Uri Modification	Allows to define SIP address manipulation before applying the recording rules. The following valid values apply: <ul style="list-style-type: none"> Do not modify SIP addresses - this option does not update/manipulate the addresses at all Remove domain part - removes the domain part from addresses Remove domain part for numbers only - removes the domain from addresses only for addresses containing numbers 	Remove domain part for numbers only
Enable RTP over TCP Support		Yes
Record video calls as audio only	Sets whether the video modality is going to be recorded.	No
Recorder Groups and Priorities	The recorder groups and the corresponding priorities. For more information see Lync recorder load balancing and failover design	1 Group1 2 Group2
Default Recorder Group Priority	The default priority of the recorder groups if no priority configured.	0
Internal Domain, Numbers Pattern		
Record SfB/Lync Application Sharing (RDP)	Enables the recording of application and screen sharing.	Yes
Record SfB/Lync File Transfer	Enables the recording of file transfer.	Yes
Enable Performance Based Loadbalancing for Recorders		No
Use Overloaded Recorder as Last Effort		Yes

Remote Capture settings

Configuration Parameter Name	Description	Sample Value
Enabled	Enable or disable the remote capture module in the service.	Yes
Interfaces	Interface name of the Ethernet port where recording will be done. Click on the button on the right to select the interface. In the interface selection window you can also check the actual status of the interface regarding the number of RTP and signaling messages captured, so you can select the right interface easily.	
Capture Buffer Size (megabytes)	Ethernet-level capture buffer size in megabytes.	90

Skinny Support Enabled	Turns on SCCP/Skinny support. By enabling this settings, you can record any type of calls using SCCP signaling.	Yes
SIP Support Enabled for Recording	Enable or disable SIP signaling support for the service.	Yes
RTP Address Translation Enabled	Enable or disable RTP address translation hint to detect the address of translated RTP streams.	Yes
Use RTP source address in call - RTP mapping	Allows to use RTP source address in internal stream map tables.	No
SIP Capture Filter	Capcure filter for SIP packets	ip[2]<5120 and (ip[6:2]&0x3F!=0 or (tcp[0:2]=5060 or tcp[2:2]=5060 or udp[0:2]==5060 or udp[2:2]==5060))
Skinny Capture Filter	Capcure filter for Skinny packets	ip[2]<1024 and (tcp[0:2]=2000 or tcp[2:2]=2000)
Media Capture Filter	Capcure filter for RTP packets	ip[2]<2048 and (udp and ip[6:2]&0x3F!=0 or tcp src port 443 or ((udp[8:2]=0x0115 and udp[24:4]=0x00000000) or (udp[8:2]=0x0004 and udp[12:4]=0x2112a442)) or (udp[8]&0xC0=0x80 and (udp[9]&0x7f <35 or udp[9]&0x7f >95)))
TCP Media Capture Filter	Capcure filter for TCP Media packets	(tcp dst portrange 1024-65535 or tcp port 443)
Base Capture Filter		

Lync Connector settings

Configuration Parameter Name	Description	Sample Value
Connection \ Listening Port	API port number used by the Lync Filter services.	10201
Connection \ Certificate File Path	Path to the certificate file used by the recorder proxy service to establish the TLS connection with the Lync filter service. Supported file format: X.509. You can use your own, self-signed certificate.	C:\Program Files (x86)\Verba\bin\recordercert.crt
Connection \ Certificate Authority Certificate File Path	Path to the Certificate Authority (CA) certificate file. Supported file format: X.509. If you do not have this type of CA certificate, you can use your own, self-signed certificate; in this case leave this setting empty.	
Connection \ Private Key File Path	Path to the private key file used by the recorder proxy service to establish the TLS connection with the Lync filter service. Supported file format: X.509.	C:\Program Files (x86)\Verba\bin\recorderkey.key
Connection \ Private Key File Password	Password for the private key file used by the recorder proxy service to establish the TLS connection with the Lync filter service.	

Enabled	Enable or disable the Lync Filter connection. This setting needs to be enabled when Lync recording is used.	Yes
Act as RTP Proxy	If enabled, call setup messages - sent by the Lync Filter services - are updated to include the proxy server as the only available media route option between the participants.	Yes
Legacy Mode		No
Enable Luware LUCS Integration		No
Contact Center UCMA B2B Agents		RTCC/5.0.0.0 ACE RTCC/5.0.0.0 ICH RTCC/5.0.0.0 ICH-1.0.0.0 RTCC/5.0.0.0 TM-ICH RTCC/6.0.0.0 UCC

RTP Proxy settings

Configuration Parameter Name	Description	Sample Value
Advanced \ Enforce ACL on Relay Sessions		No
Advanced \ Enforce ACL Modalities on Relay Sessions		Yes
Advanced \ Relay Media from Public Address		Yes
Advanced \ Advanced Relay Mode		No
Advanced \ Drop Unsolicited Packets		No
Advanced \ Support RTCP Mux		No
Advanced \ Support Late Media Negotiation		No
Advanced \ Banned IP Subnets		
Advanced \ Codecs To Remove From Media Offer		
Advanced \ Crypto To Remove From Media Offer		
Advanced \ Redirect SfB/Lync Application Sharing Streams (RDP)		Yes
Advanced \ Redirect SfB/Lync File Transfer		Yes
Advanced \ Force Non-Secure RTP		No
Advanced \ Try To Avoid Double-Edge Relaying		No
Advanced \ Enable Address Translation for NAT Traversing		No
Advanced \ Merge B2B Call Legs to One Relay Session		Yes
Advanced \ Enable relaying of TCP sessions		Yes
Enabled	Enable or disable the RTP proxy module in the service.	Yes

Relay video streams	Enables the relaying of the video streams.	Yes
A/V Port Range Begin	RTP port range starting number to receive media streams.	16384
A/V Port Range End	RTP port range ending number to receive media streams.	65535
Separated Video Port Range Begin		0
Separated Video Port Range End		0
Appshare Port Range Begin		42000
Appshare Port Range End		44999
Filetransfer Port Range Begin		45000
Filetransfer Port Range End		49999
Block the calls if there is no online recorder		No
Proxy pool name		

SIP Proxy settings

Configuration Parameter Name	Description	Sample Value
Connection \ Listening Port	SIP listening port.	5060
Connection \ Secure Listening Port	Secure SIP listening port.	5061
Connection \ Certificate File Path	Path to the certificate file used by the recorder proxy service to establish the SIP TLS connection with the communication server (e.g. Cisco UCM). Supported file format: X.509. You can use your own, self-signed certificate.	c:\verba.crt
Connection \ Certificate Authority Certificate File Path	Path to the certificate file used by the recorder service to establish the SIP TLS connection with the communication server (e.g. Cisco UCM). Supported file format: X.509. You can use your own, self-signed certificate.	
Connection \ Private Key File Path	Path to the private key file used by the recorder service to establish the SIP TLS connection with the communication server (e.g. Cisco UCM). Supported file format: X.509.	c:\verba.key
Connection \ Private Key File Password	Password for the private key file used by the recorder service to establish the SIP TLS connection with the communication server (e.g. Cisco UCM).	
Enabled	Enable or disable SIP Proxy module in the service.	Yes
Operation mode	The following valid values apply: <ul style="list-style-type: none"> Outbound Proxy - the SIP proxy server acts as a standard outbound proxy. SIP Router - the SIP proxy server uses its own routing rules to route calls. 	Outbound Proxy

Overload Thresholds

Configuration Parameter Name	Description	Sample Value
Concurrent Calls	Maximum concurrent calls threshold.	1250
Concurrent Media Relay Sessions	Maximum media relay sessions threshold. Every call consists of multiple relay sessions	1250
CPU (%)	Maximum CPU utilization threshold.	75
Network (%)	Maximum network utilization threshold.	75

Create and Associate Calling Search Spaces and Route Partitions

Phone devices with a specific Calling Search Space configured can call only numbers which are associated to a corresponding Route Partition.


Create Route Partition

Step 1 - Go to the **Call Routing / Class of Control / Partition** menu.


Step 2 - Click on the **Add New** button.

Step 3 - Provide a **Name**.

Step 4 - Click **Save**.

 Save


- Status


 Status: Ready

- Partition Information

To enter multiple partitions, use one line for each partition entry. You can enter up to 75 partitions; the names and descriptions can have up to a total of 1475 characters. The partition name cannot exceed 50 characters. Use a comma (,) to separate the partition name and description on each line. If a description is not entered, Cisco Unified Communications Manager uses the partition name as the description. For example:
<< partitionName >> , << description >>
CiscoPartition, Cisco employee partition
DallasPartition

Name*

 Save

 *- indicates required item.

Create Calling Search Space

Step 1 - Go to the **Call Routing / Class of Control / Calling Search Space** menu.

Step 2 - Click on the **Add New** button.

Step 3 - Provide a **Name**.

Step 4 - Click **Save**.

Associate Route Partition(s) with Calling Search Space

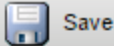
Step 1 - Go to the **Call Routing / Class of Control / Calling Search Space** menu.

Step 2 - Select the Calling Search Space.


Step 3 - Under the **Route Partitions for this Calling Search Space** section select the Route Partition(s) from the **Available Partitions** box.

Step 4 - Add the selected Route Partition(s) with the down arrow.

Step 5 - Click **Save**.



- Status

 Status: Ready

- Calling Search Space Information

Name*

Description


- Route Partitions for this Calling Search Space


Available Partitions**


- AnalogPorts
- Directory URI
- Global Learned Enterprise Patterns
- VerbaDev-SfB
- Global Learned E164 Numbers

Selected Partitions

- Lab-Internal
- VerbaDev-Cisco



 *- indicates required item.

 **Selected Partitions are ordered by highest priority

Configuring Central Silent Monitoring and Whisper Coaching

This procedure consists of multiple steps:


Configure phones for silent monitoring

For each phone, which you would like to silently monitor, you have to enable the built-in-bridge in the device configuration. This will allow to utilize the RTP forking feature of the device. For supported phone models, see [Supported Cisco environment](#).

Step 1 Select **Device / Phone** menu item and select the desired phone.

Step 2 On the configuration page enable the **Built In Bridge**.

Step 3 Click on the **Save** button.

 You need to **reset every phone you configure** for silent monitoring.

Configure supervisor line/directory number

The central - RTP forking based - silent monitoring feature requires the phone of the supervisor. When a silent monitoring session is initiated, a new call is made to the supervisor's line, which must include the monitored agent or device partition to allow monitoring the agent.

Step 1 - Select **Device / Phone** menu item and select the desired supervisor phone.

Step 2 - Select the line you would like to use for silent monitoring.

Step 3 - On the directory number configuration page set the proper **Monitoring Calling Search Space**.

Step 4 - Click on the **Save** button.

Create an application user for the JTAPI application

Step 1 - Navigate to **User Management / Application User / Add New** menu item.

Step 2 - Fill out all necessary fields and make a note of the **User ID** and **Password** fields, because you will have to set them in the Verba Recording System.

Step 3 - Add the devices, you would like to silently monitor, to the user by selecting them from the upper pane at the **Device Information** panel and move them to the **Controlled Devices** list.

Step 4 - Add the devices, you would like to use for silent monitoring (phones, which will be used to receive the silent monitoring session, in a contact center environment, these phones are usually used by the supervisors) to the user by selecting them from the upper pane at the **Device Information** panel and move them to the **Controlled Devices** list.

Step 5 - Navigate to **User Management / User Group** menu item.

Step 6 - Put the user to **Standard CTI Enabled** group by selecting this group from the list, then click **Add Application Users to Group** and select the previously created user.

Step 7 - Put the user to **Standard CTI Allow Call Monitoring** group by selecting this group from the list, then click **Add Application Users to Group** and select the previously created user.

Step 8 - If you are planning to use Cisco 89xx or 99x SIP phones, you have to also put the user to **Standard CTI Allow Control of Phones supporting Connected Xfer and conf** group by selecting this group from the list, then click **Add Application Users to Group** and select the previously created user.

Enable Cisco Silent Monitoring in Verba

Step 1 - Open the Verba Web Interface and go to the **System \ Servers** menu.

Step 2 - Select the Media Repository (or Single) server from the list, then go to the **Service Activation** tab.

Step 3 - Activate the **Verba Cisco Central Silent Monitoring Service** by clicking on the



icon.

Step 4 - Go to the **Change Configuration Settings** tab.

Step 5 - Expand the **Cisco Central Silent Monitoring Configuration \ Features** node.

Step 6 - Set the **Silent Monitoring Enabled** and/or the **Whisper Coaching Enabled** setting(s) to **Yes**, based on your needs.

Step 7 - Under the Settings node, provide the **Cisco UCM IP Address(es)**, the **JTAPI User Name** and the **JTAPI Password**.

▲ Central Cisco Silent Monitoring Configuration

▲ Features

Silent Monitoring Enabled:	<input checked="" type="checkbox"/>	Yes	▼
Whisper Coaching Enabled:	<input checked="" type="checkbox"/>	Yes	▼

▲ Settings

Cisco UCM IP Address(es):	<input checked="" type="checkbox"/>	10.4.1.20	
JTAPI User Name:	<input checked="" type="checkbox"/>	VerbaJTAPI	
JTAPI User Password:	<input checked="" type="checkbox"/>	*****	
Play Tone:	<input type="checkbox"/>	No tone play	▼
Work Folder:	<input type="checkbox"/>	C:\Program Files\Verba\work\ciscocentralsm	
API Port:	<input type="checkbox"/>	10013	

Step 8 - Click on the



icon.

Step 9 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

There are tasks to be executed regarding the configuration of this Verba Server. If you would like to execute these tasks now, please [click here](#) .

Step 10 - Go to the **Service Control** tab.


Step 11 - Start the **Verba Cisco Central Silent Monitoring Service** by clickin on the



icon.

Configuring Cisco UC Gateway for recording

In order to take advantage of the Cisco UC gateway RTP forking method and use the Verba Recording System's Cisco UC Gateway Recording method, configuration of the voice gateway(s) are required. This technology e.g. allows you to recording Jabber mobile calls, even if they do not enter your network.

 This recording method requires **Cisco UC ISR G2 routers** with **Cisco IOS Release 15.2(2)T or newer**. The WSAPI makes possible recording calls where at least one leg is SIP or TDM.

Configuration steps in gateway's IOS

Step 1 - Enter terminal configuration mode

1. enable
2. configure terminal

Step 2 - Enable HTTP server module

1. ip http server: enter HTTP configuration mode
2. ip http max-connection value (optional): Sets the maximum number of concurrent connections to the HTTP sever that will be allowed. The default value is 5.
3. ip http timeout-policy idle seconds life seconds requests value (optional): Sets the characteristics that determine how long a connection to the HTTP server should remain open. The default values are: idle 600 life 86400 requests 86400.
4. http client persistent (**required**): Enables HTTP persistent connections.
5. http client connection idle timeout seconds (optional): Sets the number of seconds that the client waits in the idle state until it closes the connection. The default value is 600.

Step 3 - Enable gateway API


1. uc wsapi: enter GW API configuration mode
2. message-exchange max-failures number (optional): Configures the maximum number of failed message exchanges between the application and the provider before the provider stops sending messages to the application. Range is 1 to 3. Default is 1.
3. probing max-failures number (optional): Configures the maximum number of failed probing messages before the router unregisters the application. Range is 1 to 5. Default is 3.
4. probing interval keepalive seconds (optional): Configures the interval between probing messages, in seconds. Default is 120 seconds.
5. probing interval negative seconds (optional): Configures the interval between negative probing messages, in seconds.
6. source-address ip-address (**required**): Configures the IP address (hostname) as the source IP address for the UC IOS service.

Step 4 - Enable XCC API service

1. uc wsapi: enter GW API configuration mode
2. provider xcc: enter Call Control API configuration mode
3. remote-url url: specifies recorder server's URL. It is used to contact the recorder and IP : Port part authenticates Register requests from recorder. **Please note that resource part must be cisco_xcc, for example: http://192.168.1.150:8090 /cisco_xcc**
4. no shutdown: enabled API
5. exit
6. end

Configuration example

```
....  
ip http server  
http client persistent  
....  
uc wsapi  
source-address router_ip  
provider xcc  
remote-url http://verba\_rec:8090/cisco\_xcc  
no shutdown
```

 If you are using IP access list, you should allow HTTP connection from/to the recorder on the defined port, and allow RTP flow from GW to the recorder in the given UDP port range. The WSAPI module listens on TCP 8090 for HTTP api requests.

Configuring Verba Cisco Recording Announcement for Inbound Calls

Overview

Verba uses Cisco External Call Control (ECC) to trigger prompts for the calls controlled by CUCM.

For more information on ECC, click [here](#).

The Cisco ECC feature relies on an external application (hosted on Verba servers in this case) that responds to external call control requests configured on various trigger points, such as translation patterns, route patterns, lines, etc. Cisco UCM provides an XML/HTTP API for ECC request, called Cisco Unified Routing Rules XML Interface (CURRI).

Inbound call flow

1. External person calls an internal number.
2. ECC is triggered on the called directory number.
3. CUCM sends a routing request to the Verba Announcement service (XML/HTTP API)
4. The Verba Announcement service decides based on the announcement configuration what to do with the call, or if the call can be established without an announcement. It returns an appropriate routing decision to the CUCM.
5. CUCM based on CURRI response redirects the call to the Verba Announcement server/SIP trunk.
6. The Verba Announcement service accepts caller's call and plays the announcement prompt
7. The Verba Announcement service blind transfers the call back to the original callee

Prerequisites

A [new SIP Trunk](#) pointing to the Verba Announcement server has to be created.

❗ The SIP Trunk used for the recording cannot be used; this has to be a separate SIP Trunk. Note that it requires a custom SIPTrunkSecurityProfile, since it needs a separate incoming port at the UCM side. The same SIP Trunk can be used for inbound and outbound announcement.

❗ The SIP trunk should deliver Diversion header and use the appropriate redirection CSS to be able to handle the redirected calls properly. Diversion header should deliver callee in a routable form (translation issues) and rerouting CSS should resolve this number to successfully blind transfer the call back to original callee after announcement played. See more under SIP trunk settings.

Configuring Cisco for Recording Announcement

Creating routing to the Announcement Service:

[Configuring call routing in Cisco UCM for recording](#)

Inbound Announcement and Proxy-based Recording

In case of proxy-based recording, the number of the announcement service has to be proxied.

Creating the External Call Control Profile:

i If the outbound announcement is configured already, then the existing External Call Control Profile can be used, so Step 1-5 can be skipped.

Step 1 - Open the Cisco Unified Call Manager web interface and go to the **Call Routing \ External Call Control Profile** menu.

Step 2 - Click on the **Add New** button.

Step 3 - Provide a **Name**, and set the **Primary Web Service** setting the following way: http://verba_server_hostname:10205/ciscoannouncement

Optionally, the announcement service can redirect the call to multiple trunks and announcement service can terminate multiple trunks.

In large deployments it might be necessary to use different CSSs for outbound announcement's outbound leg or for resolving original callee at redirection CSS.

This would also require to setup different ECCs routing the call to the desired trunk (route pattern) and assign it to the desired triggering point(s) (lines/translation patterns/route patterns).

In this case the trunk's phone number where the calls to be announced should be redirected should be set in the web service URL with ?redirectto=trunks_number.

For example, redirecting calls to 989898 can be specified by setting the url to: http://verba_server_hostname:10205/ciscoannouncement?redirectto=989898.

If not specified, then the redirection will happen to the number set in the Announcement server's config handling the CURRI request

Step 4 - Set the **Call Treatment on Failures** setting to **Block Calls**.

External Call Control Information	
Name *	<input type="text" value="announcement"/>
Primary Web Service *	<input type="text" value="http://testmr4.verbatest.local:10205/ciscoannouncement/"/>
Secondary Web Service	<input type="text"/>
<input type="checkbox"/> Enable Load Balancing	
Routing Request Timer	<input type="text"/>
Diversion Rerouting Calling Search Space	< None > ▼
Call Treatment on Failures *	Allow Calls ▼

Step 5 - Click on the **Save** button.

Assigning the External Call Control Profile to the Directory Number(s):

Step 1 - Go to the **Device \ Phone** menu, and search for the phone device.

Step 2 - Select the phone device, then on the left side click on the directory number.

Step 3 - Set the **External Call Control Profile** setting to the one created earlier.

External Call Control Profile ▼

Step 4 - Click on **Save** button then on the **Apply Config**.

Step 5 - Repeat Step 1-4 at all phone devices where the inbound announcement si required.

Inbound Announcement and Proxy-based Recording

In case of proxy-based recording, the External Call Control Profile has to be set on the patterns (which are matching to the outside numbers) pointing to the Verba Proxy server.

Configuring Verba for Cisco Recording Announcement

Step 1 - On the Verba web interface, navigate to **System > Servers > Select the server which is hosting the Announcement service > Click on the Service Activation** tab.

Step 2 - Activate the **Verba Cisco Announcement Service** by clicking on the



icon.

Step 3 - Click on the **Change Configuration Settings** tab. Expand the **Cisco Recording Announcement** section.

Step 4 - Add a new SIP port by clicking on the



icon at the **SIP Ports** setting.

Step 5 - At the right panel, provide the **SIP Port number**. This has to be port the SIP Trunk connecting to the Verba server on.

Secure SIP Ports	
Port	<input type="text" value="5060"/>
SSL/TLS Certificate	<input type="text"/>
SSL/TLS Key	<input type="text"/>
SSL/TLS Key Password	<input type="text"/>
SSL/TLS Trust List	<input type="text"/>

Secure SIP Trunk Connection

If secure SIP Trunk connection is required, the following settings have to be set:

SSL/TLS Certificate: The thumbprint of the Verba server certificate being used for the connection. This has to be the same certificate which was uploaded to the CUCM.

SSL/TLS Trust List: The thumbprint of the CUCM server certificate, or the thumbprint of the CA certificate which issued the CUCM server certificate. Alternatively, "*" can be used. In this case, every certificate going to be trusted, whose CA certificate can be found in under the Trusted Root Certificate Authorities folder. If left empty, every certificate going to be trusted.

Alternatively, .crt/.cer and .key files can be used. In this case, UNC paths can be provided in the SSL/TLS Certificate and the SSL/TLS Key settings, and the SSL/TLS Key Password has to be provided.







Step 6 - Provide the announcement service SIP trunk number at the **Service's Phone Number** setting. (see more at ECC profile setup Step 3)

Step 7 - Set the **Internal Number Pattern** setting. This has to be a regex which matches to all internal line numbers.

Step 8 - If multiple announcement services are configured for redundancy, enumerate the CURRI listener address/URL of all announcement servers in **Announcement Servers (URL)** setting. Make sure firewall will allow this communication.

The services shares with each other what calls they are dealing with to ensure CURRI will not redirect already redirected calls again if related call legs were handled on different servers

Cisco Recording Announcement


CURRI Listening Port:	<input type="checkbox"/>	10205
CURRI TLS Certificate:	<input type="checkbox"/>	
CURRI TLS Key:	<input type="checkbox"/>	
CURRI TLS Key Password:	<input type="checkbox"/>	*****
RTP Port Range Start:	<input type="checkbox"/>	16384
RTP Port Range End:	<input type="checkbox"/>	65535
SIP Ports:	<input checked="" type="checkbox"/>	5060  
		
SIP Uri Modification:	<input type="checkbox"/>	Remove domain part for numbers only 
Service's Phone Number:	<input checked="" type="checkbox"/>	8888
Internal Number/Domains Pattern:	<input checked="" type="checkbox"/>	Vd{4}
Enable Service Alerts:	<input type="checkbox"/>	Yes 
Diversion Context TTL (seconds):	<input type="checkbox"/>	5
Ringing timeout (seconds):	<input type="checkbox"/>	600
Transfer delay (milliseconds):	<input type="checkbox"/>	1500
Announcement/VOH Prompt Path:	<input type="checkbox"/>	
Enabled Audit Log:	<input type="checkbox"/>	No 
Announcement Servers (URLs):	<input checked="" type="checkbox"/>	<pre>http://dev-ciscoann1.verba1abs.com:10205 http://dev-ciscoann2.verba1abs.com:10205</pre>

Step 9 - Save the changes by clicking on the



icon.

Step 10 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

 There are tasks to be executed regarding the configuration of this Verba Server. If you would like to execute these tasks now, please [click here](#) .

Step 11 - Click on the **Service Control** tab.

Step 12 - Start the **Verba Cisco Announcement Service** by clicking on the



icon.


Setting up Extensions for Inbound Announcement

Step 1 - In the Verba web interface, go to **Users > Users** menu.

Step 2 - Select the user from the list.

Step 3 - Under the Cisco Recording Announcement section set the **Play Notification for Inbound Calls** setting.


Cisco Recording Announcement

Play Notification for Inbound Calls Media Resource ID for Inbound Calls This_Call_Is_Being_Recorded.wma 

Play Notification for Outbound Calls

Step 4 - Click the **Save**.

Step 5 - A notification banner will appear on the top. Click on the **click here** link, and you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

 There are tasks to be executed regarding the configuration of this Verba Server.
If you would like to execute these tasks now, please [click here](#) .

Configuring custom prompts for users (optional)

Step 1 - Login to the **Announcement server**, and go to the **C:\Program Files\Verba\resources\announcement** folder. It is possible to configure custom notification sounds on a per user basis. To achieve this follow these steps:

Step 2 - Copy the .wma files to the **conference**, **inbound** and **outbound** folders.

Step 3 - Open the Verba web interface, click on the **System / Servers** and select the Media Repository server, or select the appropriate Configuration Profile at **System / Configuration Profiles**.

Step 4 - Click on the **Change Configuration Settings** tab. Expand the **Web Application** section.

Step 5 - Expand the **Lync recording Announcement** node, and add the names of the .wma files to the **PSTN Inbound Announcement Prompt Files** and the **Conference Announcement Prompt Files**, one in a line.

Step 6 - Click the



icon to save your settings.

Step 7 - The system will notify you that the changes need to be applied to the server by restarting the involved services. Execute the required tasks.

Step 8 - Repeat the steps on each Media Repository server.

To configure the custom prompt for the users please see the [User Configuration](#) configuration.

Configuring Verba Cisco Recording Announcement for Inbound Calls (CUCM based)

The Verba system allows configuring audio prompts for inbound PSTN calls to Cisco systems. The feature is available with any Cisco recording technology.

- [Overview](#)
 - [Inbound call flow](#)
- [Prerequisites](#)
- [Configuring Cisco for Recording Announcement](#)
- [Configuring Verba for Cisco Recording Announcement](#)
- [Setting up Extensions for Inbound Announcement](#)

Overview

Verba uses Cisco External Call Control (ECC) to trigger prompts for the calls controlled by CUCM.

For more information on ECC, click [here](#).

The Cisco ECC feature relies on an external application (hosted on Verba servers in this case) that responds to external call control requests configured on various trigger points, such as translation patterns, route patterns, etc. Cisco UCM provides an XML/HTTP API for ECC request, called Cisco Unified Routing Rules XML Interface (CURRI).

Inbound call flow

1. Internal or external person calls a regulated user
2. ECC is triggered on the line/directory number of the regulated users
3. CUCM sends a routing request to the Verba Announcement service (XML/HTTP API)
4. The Verba Announcement service decides based on the announcement configuration which notification should be played, or if the call can be established without an announcement. It returns an appropriate routing decision to the CUCM.
5. CUCM plays the selected announcement and establishes the call with the original called party.

Prerequisites


In order to play recording announcement, the SIP Profile of the SIP Trunk connecting to the Gateway has to be configured. The SIP Profiles can be found in the **Device \ Device Settings \ SIP Profile** menu. CUCM uses Early Media for the announcement. The following settings are required:

- **SIP Rel1XX Options: Send PRACK for all 1xx Messages**
- **Early Offer support for voice and video calls: Mandatory (insert MTP if needed)**

The second prerequisite is the **Cisco IP Voice Media Streaming App**. The services can be configured in the **Cisco Unified Serviceability**, in the **Tools \ Control Center - Feature Services** menu.

Configuring Cisco for Recording Announcement

Create the External Call Control Profile:

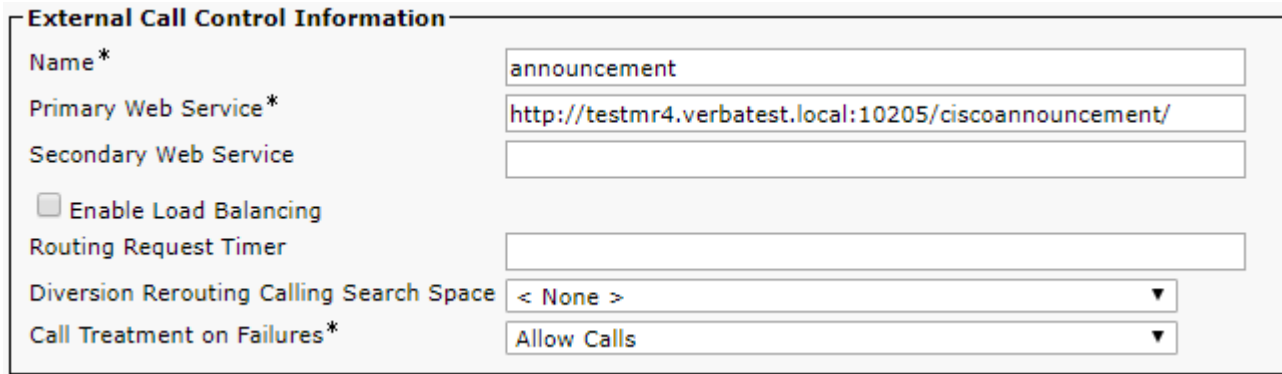
 If the outbound announcement is configured already, then the existing External Call Control Profile can be used, so the following steps can be skipped

Step 1 - Go to the **Call Routing \ External Call Control Profile** menu.

Step 2 - Click on the **Add New** button.

Step 3 - Provide a **Name**, and set the **Primary Web Service** setting the following way: http://verba_server_hostname:10205/ciscoannouncement/

Step 4 - Set the **Call Treatment on Failures** setting to **Block Calls**.



External Call Control Information

Name *	announcement
Primary Web Service *	http://testmr4.verbatest.local:10205/ciscoannouncement/
Secondary Web Service	
<input type="checkbox"/> Enable Load Balancing	
Routing Request Timer	
Diversion Rerouting Calling Search Space	< None >
Call Treatment on Failures *	Allow Calls

Step 5 - Click on the **Save** button.

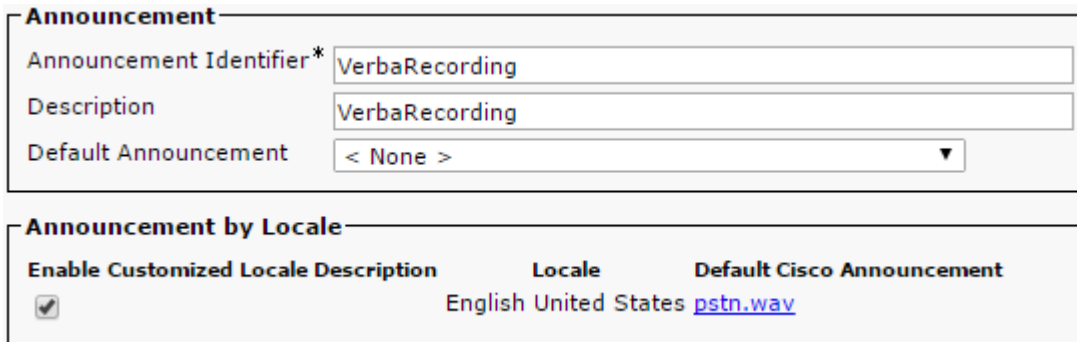
Create a new Media Resource:

Step 1 - Open the Cisco Unified Call Manager web interface and go to the **Media Resources \ Announcement** menu.

Step 2 - Click on the **Add New** button.

Step 3 - Provide a name at the **Announcement Identifier** setting, then click **Save**.

Step 4 - Click on the **Upload File** button, then upload an announcement file in .wav format.



Announcement

Announcement Identifier *	VerbaRecording
Description	VerbaRecording
Default Announcement	< None >

Announcement by Locale

Enable Customized Locale Description	Locale	Default Cisco Announcement
<input checked="" type="checkbox"/>	English United States	pstn.wav

Configuring Verba for Cisco Recording Announcement

Step 1 - On the Verba web interface, navigate to **System > Servers > Select the server which is hosting the Announcement service > Click on the Service Activation** tab.

Step 2 - Activate the **Verba Cisco Announcement Service** by clicking on the



icon.

Step 3 - Click on the **Change Configuration Settings** tab. Expand the **Cisco Recording Announcement** section.

Step 4 - Set the **Internal Number Pattern** setting. This has to be a regex which matches to all internal line numbers.

Cisco Recording Announcement


CURRI Listening Port:	<input type="checkbox"/>	10205
CURRI TLS Certificate:	<input type="checkbox"/>	
CURRI TLS Key:	<input type="checkbox"/>	
CURRI TLS Key Password:	<input type="checkbox"/>	
RTP Port Range Start:	<input type="checkbox"/>	16384
RTP Port Range End:	<input type="checkbox"/>	65535
SIP Ports:	<input type="checkbox"/>	+
SIP Uri Modification:	<input type="checkbox"/>	Remove domain part for numbers only ▼
Service's Phone Number:	<input type="checkbox"/>	
Internal Number/Domains Pattern:	<input checked="" type="checkbox"/>	\d{4}
Enable Service Alerts:	<input type="checkbox"/>	Yes ▼

Step 5 - Save the changes by clicking on the



icon.

Step 6 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

 There are tasks to be executed regarding the configuration of this Verba Server.
If you would like to execute these tasks now, please [click here](#) .

Step 7 - Click on the **Service Control** tab.

Step 8 - Start the **Verba Announcement Service** by clicking on the



icon.

Step 9 - On the Verba web interface, navigate to **System > Servers > Select the Media Repository (or Combo) server > Click on the Change Configuration Settings** tab.

Step 10 - Under the **Web Application \ Lync Recording Announcement** section, provide the previously set Announcement Identifier at the **Inbound Announcement Cisco Media Resource IDs** setting.

- ▾ Web Application
 - ▶ Network
 - ▶ Password Policy
 - ▶ User Lockout Policy
 - ▶ Authentication
 - ▶ Reporting
 - ▶ Active Directory Synchronization
 - ▶ Media Utility Service
- ▾ Lync Recording Announcement

PSTN Inbound Announcement Prompt Files:	<input type="checkbox"/>	This_Call_Is_Being_Recorded.wma
PSTN Outbound Announcement Prompt Files:	<input type="checkbox"/>	This_Call_Is_Being_Recorded.wma
Conference Announcement Prompt Files:	<input type="checkbox"/>	This_Meeting_Is_Being_Recorded.wma
Inbound Announcement Cisco Media Resource IDs:	<input checked="" type="checkbox"/>	VerbaRecording
Outbound Announcement Cisco Media Resource IDs:	<input type="checkbox"/>	

Step 11 - Save the changes by clicking on the



icon.

Step 12 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

⚠ There are tasks to be executed regarding the configuration of this Verba Server. If you would like to execute these tasks now, please [click here](#) .

Step 13 - Log into the Media Repository (or Combo) server and **restart** the **Verba Web Application service** in the Services console.

Setting up Extensions for Inbound Announcement

Step 1 - Open the Cisco Unified Call Manager web interface and go to the **Call Routing \ Directory Number** menu.

Step 2 - Select the Directory Number from the list.

Step 3 - Set the **External Call Control Profile** setting to the one created earlier.

External Call Control Profile

Step 4 - Click on **Save** button then on the **Apply Config**.

Outbound Announcement and Proxy-based Recording

In case of proxy-based recording, the External Call Control Profile has to be set to on the Route Pattern which is the same as the Directory Number.

Step 5 - In the Verba web interface, go to **Users > Users** menu.

Step 6 - Select the user from the list.

Step 7 - Under the Cisco Recording Announcement section set the Play Notification for Inbound Calls setting.


Cisco Recording Announcement

Play Notification for Inbound Calls Media Resource ID for Inbound Calls

Play Notification for Outbound Calls

Step 8 - Click the **Save**.

Step 9 - A notification banner will appear on the top. Click on the **click here** link, and you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

 There are tasks to be executed regarding the configuration of this Verba Server.
If you would like to execute these tasks now, please [click here](#) .

Configuring Verba Cisco Recording Announcement for Outbound PSTN Calls

Overview

Verba uses Cisco External Call Control (ECC) to trigger prompts for the calls controlled by CUCM.

For more information on ECC, click [here](#).


The Cisco ECC feature relies on an external application (hosted on Verba servers in this case) that responds to external call control requests configured on various trigger points, such as translation patterns, route patterns, lines, etc. Cisco UCM provides an XML/HTTP API for ECC request, called Cisco Unified Routing Rules XML Interface (CURRI).


Outbound call flow

1. Internal person calls an external number.
2. ECC is triggered on the called translation/route pattern number.
3. CUCM sends a routing request to the Verba Announcement service (XML/HTTP API)
4. The Verba Announcement service decides based on the announcement configuration what to do with the call, or if the call can be established without an announcement. It returns an appropriate routing decision to the CUCM.
5. CUCM based on CURRI response redirects the call to the Verba Announcement server/SIP trunk.
6. The Verba Announcement service accepts caller's call and plays ringback tone
7. The Verba Announcement service initiates an outbound call to the original callee
8. Once original callee:
 1. refuses the call, or outbound call leg fails: busy tone is played to the caller and inbound call is terminated
 2. accepts the call: recording prompt is played to callee
9. Recording prompt ends, the in and outbound call leg is replaces referred/transferred/joined together and announcement service leaves

Prerequisites

A [new SIP Trunk](#) pointing to the Verba Announcement server has to be created.

 The SIP Trunk used for the recording cannot be used; this has to be a separate SIP Trunk. Note that it requires a custom SIPTrunkSecurityProfile, since it needs a separate incoming port at the UCM side. The same SIP Trunk can be used for inbound and outbound announcement.

 The SIP trunk should deliver Diversion header and use the appropriate inbound and redirection CSS to be able to handle the redirected calls properly. Diversion header should deliver callee in a routable form (translation issues) and inbound, rerouting CSS should resolve this number to successfully call the callee and join/replaces transfer the in and outbound call legs after announcement played. See more under SIP trunk settings.

Configuring Cisco for Recording Announcement

Creating routing to the Announcement Service:

[Configuring call routing in Cisco UCM for recording](#)

Outbound Announcement and Proxy-based Recording

In case of proxy-based recording, the number of the announcement service has to be proxied.

Creating the External Call Control Profile:

i If the inbound announcement is configured already, then the existing External Call Control Profile can be used, so Step 1-5 can be skipped.

Step 1 - Open the Cisco Unified Call Manager web interface and go to the **Call Routing \ External Call Control Profile** menu.

Step 2 - Click on the **Add New** button.

Step 3 - Provide a **Name**, and set the **Primary Web Service** setting the following way: http://verba_server_hostname:10205/ciscoannouncement

Optionally, the announcement service can redirect the call to multiple trunks and announcement service can terminate multiple trunks.

In large deployments it might be necessary to use different CSSs for outbound announcement's outbound leg or for resolving original callee at redirection CSS.

This would also require to setup different ECCs routing the call to the desired trunk (route pattern) and assign it to the desired triggering point(s) (lines/translation patterns/route patterns).

In this case the trunk's phone number where the calls to be announced should be redirected should be set in the web service URL with ?redirectto=trunks_number.

For example, redirecting calls to 989898 can be specified by setting the url to: http://verba_server_hostname:10205/ciscoannouncement?redirectto=989898.

If not specified, then the redirection will happen to the number set in the Announcement server's config handling the CURRI request

Step 4 - Set the **Call Treatment on Failures** setting to **Block Calls**.

External Call Control Information	
Name *	<input type="text" value="announcement"/>
Primary Web Service *	<input type="text" value="http://testmr4.verbatest.local:10205/ciscoannouncement/"/>
Secondary Web Service	<input type="text"/>
<input type="checkbox"/> Enable Load Balancing	
Routing Request Timer	<input type="text"/>
Diversion Rerouting Calling Search Space	< None > ▼
Call Treatment on Failures *	Allow Calls ▼

Step 5 - Click on the **Save** button.

Assigning the External Call Control Profile to the Route Pattern(s):

Step 1 - Go to the **Call Routing \ Route/Hunt \ Route Pattern** menu.

Step 2 - Select the Route Pattern pointing to the Gateway or to the Route List / SIP Trunk pointing outside.

Step 3 - Set the **External Call Control Profile** setting to the one created earlier.

External Call Control Profile

Step 4 - Click on **Save** button then on the **Apply Config**.

Step 5 - Repeat Step 1-4 on all outgoing Route Patterns.

Outbound Announcement and Proxy-based Recording

In case of proxy-based recording, the External Call Control Profile has to be set on the patterns (which are matching to the outside numbers) pointing to the Verba Proxy server.

Configuring Verba for Cisco Recording Announcement

Step 1 - On the Verba web interface, navigate to **System > Servers > Select the server which is hosting the Announcement service > Click on the Service Activation** tab.

Step 2 - Activate the **Verba Cisco Announcement Service** by clicking on the



icon.

Step 3 - Click on the **Change Configuration Settings** tab. Expand the **Cisco Recording Announcement** section.

Step 4 - Add a new SIP port by clicking on the



icon at the **SIP Ports** setting.

Step 5 - At the right panel, provide the **SIP Port number**. This has to be port the SIP Trunk connecting to the Verba server on.

Secure SIP Ports	
Port	<input type="text" value="5060"/>
SSL/TLS Certificate	<input type="text"/>
SSL/TLS Key	<input type="text"/>
SSL/TLS Key Password	<input type="text"/>
SSL/TLS Trust List	<input type="text"/>

Secure SIP Trunk Connection

If secure SIP Trunk connection is required, the following settings have to be set:

SSL/TLS Certificate: The thumbprint of the Verba server certificate being used for the connection. This has to be the same certificate which was uploaded to the CUCM.

SSL/TLS Trust List: The thumbprint of the CUCM server certificate, or the thumbprint of the CA certificate which issued the CUCM server certificate. Alternatively, "*" can be used. In this case, every certificate going to be trusted, whose CA certificate can be found in under the Trusted Root Certificate Authorities folder. If left empty, every certificate going to be trusted.

Alternatively, .crt/.cer and .key files can be used. In this case, UNC paths can be provided in the SSL/TLS Certificate and the SSL/TLS Key settings, and the SSL/TLS Key Password has to be provided.




Step 6 - Provide the announcement service SIP trunk number at the **Service's Phone Number** setting. (see more at ECC profile setup Step 3)

Step 7 - Set the **Internal Number Pattern** setting. This has to be a regex which matches to all internal line numbers.

Step 8 - If multiple announcement services are configured for redundancy, enumerate the CURRI listener address/URL of all announcement servers in **Announcement Servers (URL)** setting. Make sure firewall will allow this communication.

The services shares with eachother what calls they are dealing with to ensure CURRI will not redirect already redirected calls again if related call legs were handled on different servers

Cisco Recording Announcement


CURRI Listening Port:	<input type="checkbox"/>	10205
CURRI TLS Certificate:	<input type="checkbox"/>	
CURRI TLS Key:	<input type="checkbox"/>	
CURRI TLS Key Password:	<input type="checkbox"/>	*****
RTP Port Range Start:	<input type="checkbox"/>	16384
RTP Port Range End:	<input type="checkbox"/>	65535
SIP Ports:	<input checked="" type="checkbox"/>	5060  
		
SIP Uri Modification:	<input type="checkbox"/>	Remove domain part for numbers only
Service's Phone Number:	<input checked="" type="checkbox"/>	8888
Internal Number/Domains Pattern:	<input checked="" type="checkbox"/>	Vd{4}
Enable Service Alerts:	<input type="checkbox"/>	Yes
Diversion Context TTL (seconds):	<input type="checkbox"/>	5
Ringing timeout (seconds):	<input type="checkbox"/>	600
Transfer delay (milliseconds):	<input type="checkbox"/>	1500
Announcement/VOH Prompt Path:	<input type="checkbox"/>	
Enabled Audit Log:	<input type="checkbox"/>	No
Announcement Servers (URLs):	<input checked="" type="checkbox"/>	<pre>http://dev-ciscoann1.verba1abs.com:10205 http://dev-ciscoann2.verba1abs.com:10205</pre>

Step 9 - Save the changes by clicking on the



icon.

Step 10 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

 There are tasks to be executed regarding the configuration of this Verba Server. If you would like to execute these tasks now, please [click here](#) .

Step 11 - Click on the **Service Control** tab.

Step 12 - Start the **Verba Announcement Service** by clicking on the



icon.

Setting up Extensions for Outbound Announcement

Step 1 - In the Verba web interface, go to **Users > Users** menu.

Step 2 - Select the user from the list.

Step 3 - Under the Cisco Recording Announcement section set the **Play Notification for Outbound Calls** setting.

Cisco Recording Announcement


Play Notification for Inbound Calls

Play Notification for Outbound Calls Media Resource ID for Outbound Calls

This_Call_Is_Being_Recorded.wma

Step 4 - Click the **Save**.

Step 5 - A notification banner will appear on the top. Click on the **click here** link, and you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

 There are tasks to be executed regarding the configuration of this Verba Server. If you would like to execute these tasks now, please [click here](#) .

Configuring custom prompts for users (optional)

Step 1 - Login to the **Announcement server**, and go to the **C:\Program Files (x86)\Verba\resources\announcement** folder. It is possible to configure custom notification sounds on a per user basis. To achieve this follow these steps:

Step 2 - Copy the .wma files to the **conference, inbound** and **outbound** folders.

Step 3 - Open the Verba web interface, click on the **System / Servers** and select the Media Repository server, or select the appropriate Configuration Profile at **System / Configuration Profiles**.

Step 4 - Click on the **Change Configuration Settings** tab. Expand the **Web Application** section.

Step 5 - Expand the **Lync recording Announcement** node, and add the names of the .wma files to the **PSTN Inbound Announcement Prompt Files** and the **Conference Announcement Prompt Files**, one in a line.

Step 6 - Click the



icon to save your settings.

Step 7 - The system will notify you that the changes need to be applied to the server by restarting the involved services. Execute the required tasks.


Step 8 - Repeat the steps on each Media Repository server.

To configure the custom prompt for the users please see the [User Configuration](#) configuration.

Genesys contact center integration in Cisco environment

Overview

The Verint Verba platform is capable to gather and stores Genesys contact center metadata. The integration is two-way, Verint Verba sends Verba Conversation ID to the Genesys platform. The solution is based on CTI integration with Genesys T-Server and supports resilient Genesys T-Server configurations.

 The Genesys contact center integration is available only for Cisco network-based recording with JTAPI integration. Tested and verified with Genesys T-Server v8.1.

Pre-installed metadata template for Genesys

A new metadata template is available for Genesys and selective recording is available based on Genesys meta information

Administrators can add any number of new fields can be added, including user-defined Genesys fields by referencing the names.

Metadata Template Configuration

[Add New Metadata Template Field](#)
[Add New Metadata Template](#)
[Back to Previous Metadata Template List](#)

Metadata Template: Genesys Template

[Metadata Template Data](#)

[Metadata Template Fields](#)

?

13 items found, displaying all items.

Display Name ↕	Enable API Access ↕	Editable ↕	Private ↕	Type ↕
ANI	Yes	No	No	Text
DNIS	Yes	No	No	Text
Call Type	Yes	No	No	Text
This Party	Yes	No	No	Text
This Party Role	Yes	No	No	Text
This Party Queue	Yes	No	No	Text
This Party Trunk	Yes	No	No	Text
Other Party	Yes	No	No	Text
Other Party Role	Yes	No	No	Text
Other Party Queue	Yes	No	No	Text
Other Party Trunk	Yes	No	No	Text
Call UUID	Yes	No	No	Text
UserData.GSIP_REC_FN	Yes	No	No	Text

13 items found, displaying all items.

Export options: [Excel](#) | [CSV](#) | [PDF](#)

✔ You can show Genesys metadata as columns in your search results by modifying the [Conversation list layout](#).

Sending Verba Conversation IDs to Genesys

In addition to gathering information from Genesys to Verint Verba, a field can be configured to store the Verba Conversation Identifier in Genesys.

Genesys Integration

Genesys T-Server IP(s):	<input checked="" type="checkbox"/>	<input type="text" value=":Ogrwt4OfRps=@genesys"/>	<input type="button" value="🗑"/>	<input type="button" value="⚙"/>
		<input style="border: 1px solid #ccc; width: 20px; height: 20px; text-align: center; line-height: 20px; margin: 2px 0;" type="button" value="+"/>		
Target Genesys Field for Verba Call ID:	<input checked="" type="checkbox"/>	<input type="text" value="VerbaCallID"/>		

Selective recording rules based on Genesys metadata

 Selective recording rules are only available for [Cisco Network-Based Recording](#) deployments with JTAPI integration.

When the Genesys integration is used, Recording Rules can be created that refer to Genesys metadata fields.

See an example below:

Recording Rule Configuration

[Add New Recording Rule](#)
[Back to Previous Page](#)

Recording Rule

ID 1

Name * Verint Verba Record

Description

Rule Sections

[Move Up](#) [Move Down](#) [Remove Section](#)

ID 12

Name Record if ShouldRecord flag is true

Action Record

CTI Triggered Recording

Filters

Genesys Field | UserData ShouldRecord | Simple | true

[Add New Filter](#)

[Move Up](#) [Move Down](#) [Remove Section](#)

ID 11

Name Otherwise Do not Record

Action Do not Record

CTI Triggered Recording

Filters

[Add New Filter](#)



[Save](#) [Delete](#)

Available metadata fields in a Recording Rule are: Caller Party, Called Party and all Genesys Fields.

After a Recording Rule is created, it can be applied to any Extension on the [Extension Configuration page](#):

Extension Configuration

[Add New Extension](#)
[Back to Previous List](#)



Extension Data

Synchronized by Active Directory

Extension*

Phone number ('1234') or address ('user@company.com')

User

If a user is missing from the list, please verify the Valid Until and Valid From fields of that user.

Type*

Update user information on existing conversations

Apply on: new conversations unassigned conversations all conversations
 Update conversations within the user's validity period only

Description

Recording Settings

Recording Mode*

Recording Rule

For Cisco JTAPI based selective recording integrations only

Voice


Instant Messaging

You can automate the assignment of Recording Rules to Extensions by referring to the name of the rule in [Active Directory synchronization](#).

Genesys integration for Cisco network based recording

Overview

The Verba Recording System supports **Genesys CTI** integration as part of the **Verba Cisco JTAPI Service**. Using this integration the recording system provides access to Genesys specific call data.

-  The Genesys CTI integration is only available when using Cisco **network-based** recording with JTAPI.
The Verba system supports Genesys active recording, see [Genesys](#).

Collected Genesys parameters (configurable)


- ANI
- DNIS
- Call Type
- This Party
- This Party Role
- This Party Queue
- This Party Trunk
- Other Party
- Other Party Role
- Other Party Queue
- Other Party Trunk
- Call UUID
- UserData.GSIP_REC_FN


Configuring the Cisco JTAPI Service for Genesys integration

The Cisco Genesys integration is built into your standard Verba solution.

Step 1 - The metadata is stored in a pre-configured metadata template. To use the built-in Cisco Genesys template, associate it with the desired Verba user group (the group where your Genesys agents and supervisors are) via the following web interface configuration page: **Users / Groups / <select a group> / Metadata Template Association**

The collected data is configurable in the Metadata Template, thus if you change the Property Id of the fields or add new fields to the template, the system will start collecting that data as well.

-  In order to read the data of custom attached user fields from Genesys, in the Genesys Metadata Template use the "UserData." prefix in the **Property Id**. For example: UserData.MyField

-  After a Genesys Metadata Template changed, the affected Verba Cisco JTAPI Service(s) have to be restarted on the Recording Server(s).

Step 2 - On the Verba web interface, navigate to **System / Servers**, select the Recording Server where the **Verba Cisco JTAPI Service** is enabled.

Step 3 - Click on the **Change Configuration Settings** tab and expand the **Cisco JTAPI Configuration / Cisco Genesys Integration** section.

Step 4 - Fill out the configuration fields according to the table below.


Parameter name	Description
Genesys T-Server IP(s)	After clicking on the gear icon at the end of the line, the following fields can be configured: <ul style="list-style-type: none">• User• Password• IP Address(es) and ports the port should be separated by a (pipe) character, the default port is 9020
Target Genesys Field for Verba Call ID	Verba will attach the Verba Call ID to this Genesys User Data Field.

Step 5 - Click on the




icon to save your settings.

Step 6 - The system will notify you that the changes need to be applied to the server by restarting the involved services or rereading the new configuration. Execute the required tasks.

 **There are tasks to be executed regarding the configuration of this Verba Server.**
If you would like to execute these tasks now, please [click here](#) .

After executing the steps above, Genesys related metadata will be collected for all new calls. Check [Call Details](#).

 You can show Cisco Genesys metadata as columns in your search results by modifying the [Conversation list layout](#).

Configuring Cisco Expressway for recording through Mobile and Remote Access (MRA)

Overview

The Expressway supports Built-in-Bridge (BiB) recording over Mobile and Remote Access (MRA). This recording method can be used to record the audio portion of calls that are made or received by users working off-premises.

Prerequisites

To utilize recording Cisco endpoints that support BiB through MRA, Expressway X8.11.1 or newer is required. Additionally, to record Jabber BiB for iOS and Android over Expressway MRA with JTAPI CTI, CUCM 12.5.1 or newer is required. For more information on the prerequisites and the list of compatible devices, see https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/config_guide/X12-5/exwy_b_mra-expressway-deployment-guide/exwy_b_mra-expressway-deployment-guide_chapter_01000.html#reference_F246F8721664A45638A98B9E9A9B2919.

Configure Cisco Unified Call Manager for Network-based recording

To configure the CUCM and the endpoints, complete the tasks in the following article: [Configuring Cisco UCM for network-based recording](#)

Configure Verba for network-based recording

On configuring Verba for Cisco Network-Based recording, visit [Configuring Verba for Cisco network-based recording](#)

Configure Cisco Expressway

Step 1 - On the Cisco Expressway-C, go to Configuration > Unified Communications > Configuration.

Step 2 - Set SIP Path headers to On.

Step 3 - Go to Configuration > Unified Communications > Unified CM servers.

Step 4 - Click Refresh servers.

Configuring the Verba Cisco MediaSense connector

[Skip to end of metadata](#)

- [Page restrictions apply](#)
- [Attachments:4](#)

Added by [Verba Support](#), last edited by [Verba Support](#) on Sep 24, 2012

[\(view](#)

[change\)](#)

[Go to start of metadata](#)

Prerequisites - PBX side configuration

First, you should configure Cisco UCM [and Cisco MediaSense](#) to enable central recording API with the dedicated Verba server(s).

Step 1 - Activate the Cisco MediaSense Services

Step 1 - In the Verba Web Interface go to **System > Servers > Select your Recording (or Single) Server > Click on the Service Activation** tab.

Step 2 - Activate the **Verba Cisco Media Sense Connector Service** by clicking on the



icon.

Step 3 - Activate the **Verba Cisco JTAPI Service** by clicking on the



icon.

Step 2 - Configure the Central Cisco Recorder Database Service

Step 1 - Click on the **Change Configuration Settings** tab.

Step 2 - Expand the **Cisco JTAPI Configuration \ Basics** node. The IP address(es) of the CUCM(s) have to be provided at the **Cisco UCM IP Address(es)** setting, and the JTAPI username and password at the **JTAPI User Name** and **JTAPI User Password** setting.

▲ Cisco JTAPI Configuration

▲ Basics


Cisco UCM IP Address(es):	<input checked="" type="checkbox"/>	10.4.1.20
JTAPI User Name:	<input checked="" type="checkbox"/>	VerbaJTAPI
JTAPI User Password:	<input checked="" type="checkbox"/>	*****

Step 3 - After making your changes click on the



icon in the top right corner of the configuration tree.

Step 4 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

 There are tasks to be executed regarding the configuration of this Verba Server.
If you would like to execute these tasks now, please [click here](#) .

Step 5 - Click on the **Service Control** tab.

Step 6 - Start the **Verba Cisco JTAPI Service** by clicking on the



icon.

Step 3 - Configure the Cisco MediaSense Connector Service

Step 1 - Click on the **Change Configuration Settings** tab.

Step 2 - Expand the **Cisco Media Sense \ Basics** node.

Step 3 - Set the **Scheduled offline call import interval start time** and **end time**. If start and end time is equal, import is done continuously. The polling interval can be set at the **Advanced \ MediaSense Polling interval** setting. This import feature affects calls recorded during connector is down.

Step 4 (Optional) - Modify the **Call event listening port** if necessary (the HTTPS port on which MediaSense connects to send call event notifications after connector successfully subscribed on events). Firewall must allow connection to this port.

Step 5 - Under the **MediaSense Cluster** node, set the **Frontend(s)** setting. It is a list of comma-separated list of the MediaSense frontend addresses. By default port 443 is assumed, but port can be specified explicitly inip:port format.

Step 6 - Set the **User** setting. It's the same JTAPI username as configured previously.

Step 7 - Set **JTAPI User Password** configured previously.


Cisco MediaSense	
Basics	
Automatic Gain Control Enabled:	<input type="checkbox"/> Yes
Audio Format:	<input type="checkbox"/> Microsoft GSM-Fullrate (LPC-RPE) in WAV
Bidirectional/Stereo Recording:	<input type="checkbox"/> No
Call event listening port:	<input type="checkbox"/> 10104
Scheduled offline call import interval start time (hh:mm):	<input checked="" type="checkbox"/> 21:00
Scheduled offline call import interval end time (hh:mm):	<input checked="" type="checkbox"/> 05:00
Central Recorder DB Service address:	<input type="checkbox"/> 127.0.0.1
Central Recorder DB Service port:	<input type="checkbox"/> 11200
MediaSense Cluster	
Frontends:	<input checked="" type="checkbox"/> 192.168.1.192
User:	<input checked="" type="checkbox"/> VerbaJTAPI
Password:	<input checked="" type="checkbox"/>

Step 8 - Save the changes by clicking on the



icon.

Step 9 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

 There are tasks to be executed regarding the configuration of this Verba Server.
If you would like to execute these tasks now, please [click here](#) .

Step 10 - Click on the **Service Control** tab.

Step 11 - Start the **Verba Cisco Media Sense Connector Service** by clicking on the



icon.

If the services start properly, you can start making **test calls** from your configured endpoints and verify them by searching for phone calls.

Configuring Cisco MediaSense for Verba integration

In order to take advantage of Cisco MediaSense and Verba integration, the configuration of the Cisco Unified Communication Manager and the recorded devices is required.

✔ We recommend that you **keep this page open** while you are configuring Cisco UCM and open each step in a new window.

Cisco UCM configuration

The initial Cisco UCM configuration includes the following steps:


- Step 1** - Activate and start Cisco AXL web service. MediaSense uses AXL for administration and configuration tasks
- Step 2** - Create or modify an application super user to grant AXL access permission. Application user should have Standard CCM Super Users group rights
- Step 3** - Create Media Sense API user (standard End user, no special rights required), Verba is going to use the user to connect MediaSense
- Step 4** - [Create and configure the SIP trunk](#) pointing to the MediaSense server(s). Default listening port is 5060, SIP over TLS, and encrypted call recording is not supported currently by Media Sense.
- Step 5** - [Create a recording profile](#) used by the recorded lines / extensions
- Step 6** - [Configure call routing](#) that let the Cisco UCM to direct calls to the MediaSense cluster
- Step 7** - [Create an application user for the JTAPI connection](#) that provides recording control and detailed CDR information. Verba is extending available CDR information for real-time calls via JTAPI
- Step 8** - [Disable the unsupported iSAC and G.722 codec](#) if you use devices supporting iSAC (89xx, 99xx family) or G.722 (**only** applicable above CUCM 8.5(1)SU1)
- Step 9** - [Verify if transcoding is required and available](#) (recommended)
- Step 10** - [Configure a recording notification tone](#) (optional)

Cisco MediaSense configuration

The initial Cisco MediaSense configuration includes the following steps:

- Step 1** - In the configuration wizard or Administration/Unified CM configuration menu provide the AXL service provider. It should be the primary node in your CUCM cluster, and user should be an application super user having AXL API access role
- Step 2** - In the configuration wizard or Administration/MediaSense API user configuration menu add the end user to be used for API access
- Step 3** - In the configuration wizard or Administration/Prune policy menu configure the desired data pruning policy


After these steps you can start adding extensions.

 The codec configuration in UCM is important for recording, since Cisco phones do not support codec changes of the secondary recording call. You might have to deploy transcoding resources to handle all scenarios, for more information read [Codec guidelines for Cisco Central Recording](#).

Adding and removing extensions

Follow the steps below to add and remove extensions to/from central recording in Cisco UCM:

- [Add new extensions](#) to central recording (follow these steps to [add extensions with Extension Mobility](#))
- [Remove extensions](#) from central recording

 When you use RTP-forking based Cisco central recording, the system can record only those extensions that are properly configured in the Cisco UCM. It is not enough to add extensions in the Verba Recording System.

Configuring Verba for Skype for Business and Lync recording

This guide describes the necessary configuration steps for Microsoft Skype for Business / Lync voice, video and application share call recording.

Prerequisites

Before deploying the solution, select the right deployment option and recording method based on the requirements. The Verba system can be deployed in [multiple ways](#), supporting various recording methods.

Before the starting the configuration, every Verba server and component have to be installed. For more information: [Microsoft Skype for Business](#)

Configuring Voice, Video and Application share recording

There are different methods for Skype for Business / Lync recording:

- The **Proxy-based SfB / Lync recording** option allows recording **all types of call scenarios** including inbound, outbound, internal, conference, federated and external calls. For the configuration steps see [Configuring Verba for RTP Proxy based recording](#).
- The **Mediation / AVMCU based SfB / Lync recording** option allows recording **inbound and outbound PSTN calls and/or conferences**. For the configuration steps see [Configuring Verba for Mediation - AVMCU based recording](#).

Each recording methods can be extended with the **recording of the federated calls, calls of users logged in remotely and application shares**. For that, a Media Collector and Proxy component have to installed and configured on the Edge server. For configuration steps see [Configuring Media Collector on Edge servers](#)

Load balancing, failover, and geographical routing configuration

- [SfB - Lync proxy load balancing and failover design](#)
- [Recorder load balancing and failover design](#)

Configuring IM recording

Verba supports the recording of both peer to peer chat sessions and persistent chat rooms.

- For the **P2P IM recording** configuration steps, see [Configuring Verba for Skype for Business / Lync IM recording](#).
- For the **persistent chat room recording** configuration steps, see [Configuring persistent chat room recording for SfB and Lync](#).

Configuring Archive Importing

Several modalities cannot be recorded directly, but they can be imported from the Skype for Business / Lync archive. The following meeting contents are archived:

- Whiteboard
- Polls and Q&A
- Files shared on the meeting
- Powerpoint shared on the meeting

For the configuration steps see [Configuring SfB - Lync archive import](#).

Configuring advanced features for Skype for Business / Lync recording

After the recording configuration, additional features can be configured. Most of these features are crucial for compliance.

Recording Announcement

Recording announcement can be added for inbound and outbound PSTN and federated calls and conferences. For the configuration steps see [Installing and configuring the Verba SfB - Lync Announcement service](#).

Call Blocking

There are cases when recording of a call is more important than the ability to establish the call itself because of compliance reasons. If there are no online proxy or recorder services then Verba can block the call establishment. For the configuration steps see [Configuring Lync call blocking on recording failure](#)

Dual-Relaying

In a multi-site environment where there are multiple SfB / Lync pools present, by default the calls between the pools recorded only on the caller side. It's possible to record the calls at both ends by configuring Dual-Relaying. For the configuration steps see [Configuring Verba for Dual-Relaying](#)

Final configuration: Configuring extensions and media file upload

After finalizing the configuration of the recording services, make sure you have added the extensions you want to record to the Verba extension list. This can be done manually ([Extension list](#)) or using [Active Directory Synchronization](#).

If the Recorder Server is not co-located with the Media Repository or there are multiple Recorder Servers, then the media files have to be uploaded to a single location. For the upload options see [Configuring media file upload](#).

Configuring Verba recording announcement service

The service is installed on Media Repository & Recording Server, Media Repository, Recording Server and Announcement Server roles. The service requires UCMA 4.0 runtime on the server. You can download the runtime at <https://www.microsoft.com/en-us/download/details.aspx?id=34992>.

Once you have activated the service, you go to the **Change Configuration Settings** tab and configure the following parameters under the **Lync Recording Announcement** node. The highlighted ones always have to be configured:

Configuration Parameter Name	Description
Service FQDN	Fully Qualified Domain Name (FQDN) of the server running the application. It has to match the value entered during the application pool registration.
Service Port	Service port number used by the UCMA library to communicate with the Front End servers. It has to match the value entered during the trusted application pool registration.
Lync Pool FQDN	Fully Qualified Domain Name (FQDN) of the Front End pool where the application is registered.
Lync Port	SIP port on the Front End pool.
Service certificate	Friendly name of the certificate used to establish trusted connection between the UCMA application and the Front End pool. You can obtain the name by locating the installed certificate under application host computer's Console Root\Certificates (Local Computer)\Personal\Certificates folder, and checking the certificate details.
Service certificate password	The password of the certificate used to establish trusted connection between the UCMA application and the Front End pool. Required only if it was exported from an other server then imported to the store.
Application URI	SIP address of the announcement service endpoint created by the New-CsTrustedApplicationEndpoint command. To check the address run the Get-CsTrustedApplicationEndpoint command and look for the SipAddress parameter.
Application GRUU	Computer Routable User Agent URI (GRUU) of the announcement application. Run the following command in a Lync Management Shell, where the the FQDN of the trusted application pool is 'verbaapps.contoso.com' and the application 'verbaAppID'. You can check these parameters by simply running the Get-CsTrustedApplication command: <pre>\$a = Get-CsTrustedApplication -identity "verbaapps.contoso.com/urn:application:verbaAppID" \$a.ComputerGruus</pre> More information: http://msdn.microsoft.com/en-us/library/office/hh347323(v=office.14).aspx
HTTP API URL	Recorder API address and port number. Use * to enable the API on all local network interfaces. The service uses this API to communicate with the recorder service(s) to obtain events like call recording getting started/stopped.
IM notification message	The instant messaging text displayed when recording is started by one of the participants in the conference. The message is displayed in the group chat when recording is started. If a new participant joins the conference, the message is not displayed again.
Default Voice prompt for conference calls	The audio prompt played when recording is started by one of the participants in the conference. If a new participant joins the conference, the service automatically plays the announcement privately to the new participant. Existing participants will hear the prompt again.

Enable voice announcement for inbound and outbound calls	Enable voice announcement for inbound and outbound calls.
Default voice prompt for inbound calls	The audio prompt played when receiving an inbound call.
Default voice prompt for outbound calls	The audio prompt played when making an outbound call.
Enable caller impersonation for outbound calls	
On hold prompt for outbound calls	The audio played to the caller when making an outbound call.
Announcement Prompt Store Path	The store of the audio files used for announcement.
Voice Prompt Delay for PSTN Conference Joiners (msec)	The delay for the conference announcement for PSTN joiners.

When the configuration is done, click on the save



button, then execute the changes.

Configuring Remote Capture on Lync servers

This chapter describes the necessary steps required to configure the Verba Proxy Server and the Remote Capture module to identify and capture recorded call related media streams on the Lync servers such as Mediation, Edge and AVMCU.

The remote capture component can be installed on the Lync Edge, Mediation and AVMCU server. It is part of the Verba RTP proxy server.

Steps of configuring Remote Capture component

Step 1 Go To 'Administration/Verba Servers' and select the Lync server where the Verba Proxy server is.

Step 2 Select 'Change Configuration Settings' and select the 'Recorder Proxy' node from the configuration tree.

Recorder Proxy

General

Remote Capture

Enabled:	Yes	▼
Interfaces:	ice\WPRO_41_1742_{F21D14A2-96F7-4705-8E64-2388083E5A22}	🗑️ ⚙️
	+	
Capture Buffer Size (megabytes):	90	
Skinny Support Enabled:	Yes	▼
RTP Address Translation Enabled:	Yes	▼
Use RTP source address in call - RTP mapping:	No	▼

Lync Connector

RTP Proxy

SIP Proxy

Step 3 Open 'Remote Capture' node and set the fields by the following way:

Step 1 Set 'Enabled' to **Yes**

Step 2 Set the desired interfaces for recording by clicking on the interfaces row's gear icon. The interfaces can be applied one by one.

Choose Recording Interface


Host: Port:

User: Password:

Interface Name	SCCP	SIP	RTP	Total	IP Address
Ethernet 3	46	32	111	6004	fe80::1d60:df06:165f:17e3 192.168.1.44
Ethernet 2	0	0	0	0	fe80::61a6:653a:da72:bdf3 86.101.183.134
Ethernet	46	32	111	5928	fe80::792a:af67:64e1:5b2b 192.168.1.203

Select the desired server first at the host field. If a remote capture server is selected, proper user credentials are also required. After that, select the recording interface from the available network interfaces by clicking on the proper table row. You can also view the interface statistics, which helps to find the right interface. Click the Refresh button below to update the statistics.

If you selected one of the localhost's interfaces hit the 'Save' button.

 Please note that all configuration changes need restarting of the services or just a reread of configuration by the running service. The Verba Web Application puts notification on the top of the configuration form about the required tasks.

Configuring Lync conference call invitation

This feature in the Verba Web Application allows to receive Lync conference call invites and parse the available metadata in the invitation and store the information in the database along with the conference call recordings. The application is able to detect the subject of the conference call, the meeting ID, and the participants are also stored in the Verba system. If a call recording is started with a meeting ID which was previously received in an invitation, the system automatically attach the mentioned metadata to the call. The system uses a built-in custom metadata template to store the information.

The related configuration options are accessible on the web interface: open the Media Repository server's configuration and open Web Application / Conference Share Invitation item in the tree.

Meeting processing currently is a custom feature in Verba. In order to match the recordings with the invitations, the following SQL script has to be executed in the database: invitation-create-share-trigger.sql

Configuration Parameter Name	Description	Sample Value																
Email Protocol	POP3 or IMAP	POP3																
Email Server	Host name or IP address of the POP3 or IMAP server.	pop.mailserver.com																
Email Server Folder for Invites	Logical name of the Inbox folder. Usually it should be set to INBOX.	INBOX																
Email Account User Name	User name of the email server account.	verba_account																
Email Account Password	Password for the email server account.	secret_pwd																
Authentication Required for Email Account	If the email server requires authentication, this should be set to Yes.	Yes																
Email Server Port Number	Default ports: <ul style="list-style-type: none"> • POP3: 110 • POP3+SSL: 995 • IMAP: 143 • IMAP+SSL: 993 	110																
SSL Required for Email Server	If the email server requires the use of SSL, this should be set to Yes.	No																
Archive Invites in Folder	Verba puts a flag on each processed email message. If processed messages should be moved to a specific folder (because there are too many), here you can set the target folder name.	PROCESSED																
Delete Invites After (days)	Invitation emails can be left on the email server for debugging purposes. Emails will be deleted after the configured value in days. If emails should be deleted immediately after processing, this should be set to 0.	0																
Meeting URLs in Invites	Verba parses the invitation email and tries to find a Meeting ID in the body of the email. This setting lets the system know where to look for the Meeting ID. For example, if the meeting URL looks like "https://meet.mycompany.com/myuser/QOP2XV3S", then set this setting to "meet.mycompany.com". Multiple values separated by new lines are accepted.	meet.mycompany.com																
Store Invite Message Bodies	For debugging purposes the invitation message body can be stored in the database. Requires more storage but can be handy if anything went wrong.	No																
Check for New Invites Period (sec)	Frequency of email server polling.	15																
Send Notification Emails	If it is set to "Yes", Verba will send an email after each recording to the meeting organizer and participants.	Yes																
Email Subject	The subject of the notification email sent by Verba. Available reference strings: <table border="1" data-bbox="236 1601 829 1892"> <thead> <tr> <th>Reference</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>\${MEETING_ID}</td> <td>Meeting ID parsed from the meeting URL.</td> </tr> <tr> <td>\${CONFERENCE_ID}</td> <td>Conference ID found in the meeting email after "Conference ID:"</td> </tr> <tr> <td>\${MEETING_SUBJECT}</td> <td>Subject of the invitation email.</td> </tr> <tr> <td>\${USER_NAME}</td> <td>Name of the user the email will be sent to.</td> </tr> <tr> <td>\${ORGANIZER_NAME}</td> <td>Name of the meeting organizer.</td> </tr> <tr> <td>\${ORGANIZER_EMAIL}</td> <td>Email address of the meeting organizer.</td> </tr> <tr> <td>\${LINK}</td> <td>Direct access link to the recording (pointing to Verba web application)</td> </tr> </tbody> </table>	Reference	Description	\${MEETING_ID}	Meeting ID parsed from the meeting URL.	\${CONFERENCE_ID}	Conference ID found in the meeting email after "Conference ID:"	\${MEETING_SUBJECT}	Subject of the invitation email.	\${USER_NAME}	Name of the user the email will be sent to.	\${ORGANIZER_NAME}	Name of the meeting organizer.	\${ORGANIZER_EMAIL}	Email address of the meeting organizer.	\${LINK}	Direct access link to the recording (pointing to Verba web application)	Meeting (\${MEETING_SUBJECT} - \${CONFERENCE_ID} - \${MEETING_ID}) recording available
Reference	Description																	
\${MEETING_ID}	Meeting ID parsed from the meeting URL.																	
\${CONFERENCE_ID}	Conference ID found in the meeting email after "Conference ID:"																	
\${MEETING_SUBJECT}	Subject of the invitation email.																	
\${USER_NAME}	Name of the user the email will be sent to.																	
\${ORGANIZER_NAME}	Name of the meeting organizer.																	
\${ORGANIZER_EMAIL}	Email address of the meeting organizer.																	
\${LINK}	Direct access link to the recording (pointing to Verba web application)																	

Email Body for Attendees	The body of the notification email sent by Verba to all of the participants except the one who recorded the call. Available reference strings are the same as for the Email Subject setting. Verba sends the email in HTML format so it has to be valid HTML.	Dear \${USER_NAME}, The recorded media of your Lync Meeting (\${MEETING_SUBJECT} - \${CONFERENCE_ID} - \${MEETING_ID}), organized by \${ORGANIZER_NAME} (\${ORGANIZER_EMAIL}) is now shared with you on the following link: \${LINK} You can also access it by looking for it under the Sharing / View Shared Items menu. Sincerely, Verba Recording System
Email Body for Organizer	The body of the notification email sent by Verba to the user who recorded the call. Available reference strings are the same as for the Email Subject setting. Verba sends the email in HTML format so it has to be valid HTML.	Dear \${USER_NAME}, The recorded media of your Lync Meeting (\${MEETING_SUBJECT} - \${CONFERENCE_ID} - \${MEETING_ID}) is now available on the following link: \${LINK} You can also access it by looking for it under the Search menu. Sincerely, Verba Recording System
Share Recordings to Participants	If it is "Yes", Verba will automatically create a so called Shared Item and adds the participants to it so they will have access to the recording. Note that the recording is owned by the user who started the recording and normally only the owner has access to a recording.	

Configuring Verba for Skype for Business / Lync IM recording

Prerequisites

The [Verba Sfb / Lync Filtler](#) component have to be installed on **all Front-End servers**. The **Verba Sfb / Lync IM Filter service have to be registered** in the Lync pool.

For the recording and the web access at least a [Single Server](#) have to be installed. The roles also can be separated by installing a separate [Media Repository](#) and a [Recording Server](#). If high availability or load balancing is required, then additional Recording Servers can be installed.

Firewall configuration

Refer to [Firewall configuration for Skype for Business - Lync deployments](#) for more information.

Stage One: Configuring the Verba Sfb/Lync IM Recorder component

Follow the steps below to configure the Verba Sfb/Lync IM Recorder service

Step 1 - In the Verba web interface go to **System > Servers > Select your Recording Server > Click on the Service Activation** tab.

Step 2 - Activate the **Verba Sfb/Lync IM Recorder Service** by clicking on the



icon.

Step 3 - Click on the **Change Configuration Settings** tab. Expand the **Sfb/Lync IM Recorder** section.

Step 4 - Under the **General** section set the '**Internal Domain, Numbers Pattern**' setting by entering the **recorded SIP domains** separated by '|' character. (example: contoso.com|adatum.com)


Step 5 (Optional) - Set the '**Create Transcript and Metadata XML Files**' setting to **Yes** in order to write the IM recordings to the disk. (By default the IM recordings are stored only in the database.)


Step 6 - **Save** the changes by clickin on the



icon.

Step 7 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

 There are tasks to be executed regarding the configuration of this Verba Server. If you would like to execute these tasks now, please [click here](#) .

 Changes can be execute at once at the end. In that case don't forget to click on '**Check All**'.

Step 8 - Click on the **Service Control tab** tab.

Step 9 - Start the **Verba Sfb/Lync IM Recorder Service** by clicking on the



icon.

Repeat these steps for each Recorder Server in your system.

Stage Two: Configuring the Verba SfB/Lync IM Filter component

Step 1 - In the Verba web interface go to **System > Servers > Select your Front-End Server > Click on the Service Activation** tab.

Step 2 - Activate the **Verba SfB/Lync IM Filter Service** by clicking on the



icon.

Step 3 - Click on the **Change Configuration Settings** tab. Expand the **SfB/Lync IM Filter** section.

Step 4 - Under the **General** section set the '**Internal Domain, Numbers Pattern**' setting by entering the **recorded SIP domains** separated by '|' character. (example: [contoso.com](#)|[adatum.com](#))

Step 5 - Set the **Server Version** setting according to the SfB / Lync environment version.

Step 6 - The **Verba Lync Chat Recorder Servers** field has to contain the list of the servers where the IM Recorder service installed. Enter every server with the correct port (**FQDN:10220**), one at each line.

▲ SfB/Lync IM Filter

▲ General


Filter Pool Name:	<input type="checkbox"/>	verbaim
Internal Domain, Numbers Pattern:	<input checked="" type="checkbox"/>	\d{5}\. *@contoso.com
Server Version:	<input checked="" type="checkbox"/>	Skype for Business ▼
Enable Notification Message Between Domains:	<input type="checkbox"/>	No ▼
Enable Notification Message Inside Domains:	<input type="checkbox"/>	No ▼
Enable Notification Message for Conferences:	<input type="checkbox"/>	No ▼
Notification Message Text:	<input type="checkbox"/>	
Verba Lync Chat Recorder Servers:	<input checked="" type="checkbox"/>	TESTRS1.VERBATEST.LOCAL:10220 TESTRS2.VERBATEST.LOCAL:10220
Enable Performance Based Load Balancing for IM Recorders:	<input type="checkbox"/>	Yes ▼

Step 7 - Save the changes by clicking on the



icon.

Step 8 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

 **There are tasks to be executed regarding the configuration of this Verba Server.**
If you would like to execute these tasks now, please [click here](#) .

Step 9 - Click on the **Service Control tab** tab.

Step 10 - Start the **Verba SfB/Lync IM Filter Service** by clicking on the



icon.


Repeat these steps for each Front-End Server in your system.

Final Stage: Configuring extensions

After finalizing the configuration of the recording services, make sure you have added the extensions you want to record to the Verba extension list. This can be done manually ([Extension list](#)) or using [Active Directory Synchronization](#).

Configuring Verba for Mediation - AVMCU based recording

This article provides a detailed step by step guide on how to configure the Verba Recording System for RTP Proxy based recording in a Microsoft Lync environment.

 Mediation / AVMCU based recording will **only record incoming and outgoing PSTN calls and/or conferences** which pass through the Mediation / AVMCU server. Internal and external Lync to Lync calls will not be recorded. If you need to record calls other than PSTN or Conference calls, [configure RTP Proxy based recording instead](#).

When using Mediation / AVMCU based recording, **calls are not rerouted**, the call media path is not altered by Verba in any way. Media Collectors installed on the Lync Mediation / AVMCU servers are responsible for sending call media streams to the Recording Servers.

- [Important note on terminology](#)
- [Preparation](#)
 - [Firewall configuration](#)
- [Stage One: Configure the Verba Media Collector and Proxy for Mediation / AVMCU based recording \(Remote Capture / Media Collector mode\)](#)
- [Stage Two: Configure the Verba Lync Filter for Mediation based recording](#)
- [Stage Three: Configure the Verba Passive Recorder service for Mediation based recording](#)
- [Final Stage: Configure extensions](#)

Important note on terminology

Traffic collection is managed by the **Verba Recorder Proxy service operating in Remote Capture mode**.

When configured this way, the service is not an active part of the call media path. **It only captures the media streams that normally pass through its location** (in this case the Mediation / AVMCU Server).

Preparation


Before starting to configure Verba for Lync recording, **every Verba server and component have to be installed**. For more information about the required servers and components see [Call recording for Microsoft Lync and Skype for Business](#).

Firewall configuration

Refer to [Firewall configuration for Skype for Business - Lync deployments](#) for more information.

Stage One: Configure the Verba Media Collector and Proxy for Mediation / AVMCU based recording (Remote Capture / Media Collector mode)

Follow the steps below to configure the Verba Recorder Proxy service for Media Collector mode operation on the Mediation Server.

 Stages One and Two take place on the same server's configuration page if the Mediation / AVMCU Servers are co-located on your Front End servers.

Step 1 - In the Verba web interface go to **System / Servers**, select the Mediation / AVMCU server where the Media Collector and Proxy service is installed and click on the **Service Activation** tab.

Step 2 - Activate the **Verba Media Collector and Proxy Service** by clicking on the



icon.

Step 3 - Click on the **Change Configuration Settings** tab. Expand the **Media Collector and Proxy** section.

Step 4 - Under **General / Recorder Connection**, configure the authentication credentials for the connections with the recording service. Define the **Authentication User** and **Authentication Passwords** values. These credentials will be used later when configuring the connections in the recorder service.

Step 5 - In the **General** section set the **Internal Domain, Numbers Pattern** setting. This have to be a regex which matches to all internal line numbers and SIP domains.

Step 6 - Under **Remote Capture** set the **Enabled** field to **Yes**.

Step 7 - At **Interfaces** add the Mediation server's network interface for listening by clicking on the



button.

Step 8 - At the right panel select an interface from the list, then click '**Save**'.

Choose Recording Interface

Host	<input type="text" value="localhost"/>	Port	<input type="text"/>		
User	<input type="text"/>	Password	<input type="text"/>		
Interface Name	SCCP	SIP	RTP	Total	IP Address
Ethernet	0	0	0	0	fe80::31e0:9628:94fb:6f12 10.4.0.42
Ethernet 2	0	0	0	0	fe80::f45f:f332:190e:40d 192.168.167.65

Step 9 - Repeat the steps 7-8 until every interface is added to the configuration.

Step 10 - Under **Lync Connector** section set the **Enabled** setting to **Yes**.

Media Collector and Proxy

General

Recorder connection

Announcement Service Uri:	<input type="checkbox"/>	
Assign Call To Recorder only on First RTP:	<input type="checkbox"/>	Yes
Call Timeout (sec):	<input type="checkbox"/>	600
SIP Uri Modification:	<input type="checkbox"/>	Remove domain part for numbers only
Enable RTP over TCP Support:	<input type="checkbox"/>	Yes
Record video calls as audio only:	<input type="checkbox"/>	No
Recorder Groups and Priorities:	<input type="checkbox"/>	
Default Recorder Group Priority:	<input type="checkbox"/>	0
Internal Domain, Numbers Pattern:	<input checked="" type="checkbox"/>	ld(5).*@contoso.com
Record SfB/Lync Application Sharing (RDP):	<input type="checkbox"/>	Yes
Record SfB/Lync File Transfer:	<input type="checkbox"/>	Yes
Enable Performance Based Loadbalancing for Recorders:	<input type="checkbox"/>	No
Use Overloaded Recorder as Last Effort:	<input type="checkbox"/>	Yes

Remote Capture

Enabled:	<input checked="" type="checkbox"/>	Yes									
Interfaces:	<input checked="" type="checkbox"/>	<table border="1"><tr><td>DeviceNPF_{1DA95C96-2C3E-44DD-9615-0A00F58173A0}</td><td><input type="checkbox"/></td><td><input type="checkbox"/></td></tr><tr><td>DeviceNPF_{6E3FCD20-5D25-42D8-B432-B020A0E7F904}</td><td><input type="checkbox"/></td><td><input type="checkbox"/></td></tr><tr><td colspan="3" style="text-align: center;">+</td></tr></table>	DeviceNPF_{1DA95C96-2C3E-44DD-9615-0A00F58173A0}	<input type="checkbox"/>	<input type="checkbox"/>	DeviceNPF_{6E3FCD20-5D25-42D8-B432-B020A0E7F904}	<input type="checkbox"/>	<input type="checkbox"/>	+		
DeviceNPF_{1DA95C96-2C3E-44DD-9615-0A00F58173A0}	<input type="checkbox"/>	<input type="checkbox"/>									
DeviceNPF_{6E3FCD20-5D25-42D8-B432-B020A0E7F904}	<input type="checkbox"/>	<input type="checkbox"/>									
+											
Capture Buffer Size (megabytes):	<input type="checkbox"/>	90									
Skinny Support Enabled:	<input type="checkbox"/>	Yes									
SIP Support Enabled:	<input type="checkbox"/>	Yes									
RTP Address Translation Enabled:	<input type="checkbox"/>	Yes									
Use RTP source address in call - RTP mapping:	<input type="checkbox"/>	No									
SIP Capture Filter:	<input type="checkbox"/>	ip[2]<5120 and (ip[6:2]&0x3F!=0 or (tcp[0:2]=5060 or tcp[2:2]=5060 or udp[0:2]==5060 or udp[2:2]==5060)									
Skinny Capture Filter:	<input type="checkbox"/>	ip[2]<1024 and (tcp[0:2]=2000 or tcp[2:2]=2000)									
Media Capture Filter:	<input type="checkbox"/>	ip[2]<2048 and (udp and ip[6:2]&0x3F!=0 or tcp src port 443 or ((udp[8:2]=0x0115 and udp[24:4]=0x0000)									
TCP Media Capture Filter:	<input type="checkbox"/>	(tcp dst portrange 1024-65535 or tcp port 443)									
Base Capture Filter:	<input type="checkbox"/>										

Lync Connector

Connection

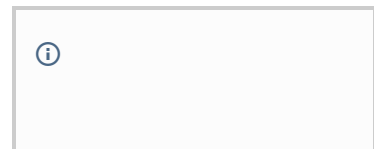
Enabled:	<input checked="" type="checkbox"/>	Yes
Act as RTP Proxy:	<input type="checkbox"/>	No
Legacy Mode:	<input type="checkbox"/>	No
Enable Luvare LUCS Integration:	<input type="checkbox"/>	No

Step 11 - Save the changes by clickin on the



icon.

Step 12 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.





There are tasks to be executed regarding the configuration of this Verba Server. If you would like to execute these tasks now, please [click here](#).

Changes can be execute at once at the end. In that case don't forget to click on **'Check All'**.

Step 13 - Click on the **Service Control tab** tab.

Step 14 - Start the **Verba Media Collector and Proxy Service** by clicking on the



icon.

Step 15 - Repeat these steps for each Mediation / AVMCU servers in your system.

Stage Two: Configure the Verba Lync Filter for Mediation based recording

Follow the steps below to configure the Verba Lync Filters located on the Lync Front End servers. The Verba Lync Filter is responsible for capturing and modifying the signaling messages to alter the media path to include the Proxy Server.

i Stages One and Two take place on the same server's configuration page if the Mediation / AVMCU Servers are co-located on your Front End servers.

Step 1 - In the Verba web interface go to **System / Servers**, select the Front End server running the Verba Lync Filter and click on the **Service Activation** tab.

Step 2 - Activate the **Verba SfB/Lync Call Filter Service** by clicking on the



icon.

Step 3 - Click on the **Change Configuration Settings** tab. Expand the **SfB/Lync Call Filter** section.

Step 4 - In the **General** section set the **Internal Domain, Numbers Pattern** setting. This have to be a regex which matches to all internal line numbers and SIP domains.

Step 5 - Set the **Server version** to the version of the Lync Platform you are using.

Step 6 (Optional) - If the Conference Only recording mode required, then set the **Record Conference Calls Only** setting to **Enable**.

Step 7 - Under the **Signaling Information Target Settings** section add your Mediation / AVMCU Servers by clicking on the



button next to **Media Collector(s)**.

Step 8 - At the right panel select the Mediation / AVMCU Server from the drop down list at the **Host**. Click **Save**.

Signaling Information Target Media Collectors

Host

TESTFE1SFB.VERBATEST.LOCAL



Port

Public IP

Step 9 - Repeat Steps 7-8 for every Mediation / AVMCU Server in your system.

▲ Sfb/Lync Call Filter

▲ General

Filter Pool Name:	<input type="checkbox"/>	verba
Internal Domain, Numbers Pattern:	<input checked="" type="checkbox"/>	ld{5}.*@contoso.com
Server Version:	<input checked="" type="checkbox"/>	Skype for Business ▼
Relaying Mode:	<input checked="" type="checkbox"/>	Reroute/relay recorded calls through Verba Proxy server(s) ▼
Record Conference Calls Only:	<input type="checkbox"/>	Disable ▼

▲ Signaling Information Target Settings

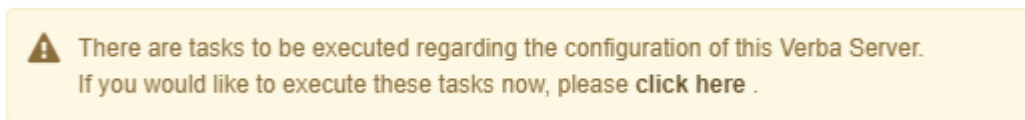
Media Collector(s):	<input checked="" type="checkbox"/>	TESTFE1SFB.VERBATEST.LOCAL:10201		
	<input checked="" type="checkbox"/>	TESTFE2SFB.VERBATEST.LOCAL:10201		

Step 10 - Save the changes by clicking on the



icon.

Step 11 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.



Step 12 - Click on the **Service Control tab** tab.

Step 13 - Start the **Verba Sfb/Lync Call Filter Service** by clicking on the



icon.

Step 14 - Repeat these steps for every Lync Front End / Filter in your system.

Stage Three: Configure the Verba Passive Recorder service for Mediation based recording

Follow the steps below to configure the Verba Passive Recorder service for Mediation based recording:

Step 1 - In the Verba web interface go to **System / Servers**, select the Recording Server and click on the **Service Activation** tab.

Step 2 - Activate the **Verba Passive Recorder Service** by clicking on the



icon.

Step 3 - Click on the **Change Configuration Settings tab**. Expand the **Passive Recorder** section.

Step 4 - Under **Basics** add your **Mediation / AVMCU Servers** by clicking in the



next to **Recorder Proxy**.

Step 5 - Select the Mediation / AVMCU Server from the drop down list. Provide the username and password configured in the **Verba Media Collector and Proxy Service** above for the connections. Click **Save**.

Recorder Proxy

Host	TESTFE1SFB.VERBATEST.LOCAL
Port	11112
User	verba
Password	*****
Compress Connection Stream	<input type="checkbox"/>
Recorder Weight	1
Secure	<input checked="" type="checkbox"/>
Recorder Group	

Step 6 - Repeat Steps 4-5 for every Mediation / AVMCU Server in your system.

Step 7 - Set the **Internal Domain, Numbers Pattern** setting. This have to be a regex which matches to all internal line numbers and SIP domains.

Step 8 (Optional) - If the video recording required then set the **Record Video Call As Audio Call** setting **No** under the **Advanced** node.

Passive Recorder

Basics


Recording Interface:	<input type="checkbox"/>	+	
Media Collector and Proxies:	<input checked="" type="checkbox"/>		TESTFE2SFB.VERBATEST.LOCAL 11112 verba 1vcYm2yq7Fr5WuO3yi9oQQ== 0 1 1
Audio Format:	<input type="checkbox"/>		Microsoft GSM-Fullrate (LPC-RPE) in WAV
Video Format:	<input type="checkbox"/>		Verba RTP Dumped Media Format
Bidirectional/Stereo Recording:	<input type="checkbox"/>		No
Automatic Gain Control Enabled:	<input type="checkbox"/>		Yes
Conference Resources IP Addresses:	<input type="checkbox"/>		
Experimental H.323 Support Enabled:	<input type="checkbox"/>		No
SIP Support Enabled:	<input type="checkbox"/>		Yes
Skinny Support Enabled:	<input type="checkbox"/>		Yes
Call Timeout (seconds):	<input type="checkbox"/>		600
Voice Activity Statistics:	<input type="checkbox"/>		No
Secondary Recording Server:	<input type="checkbox"/>		No
Internal Domain, Numbers Pattern:	<input checked="" type="checkbox"/>		ld(5].*@contoso.com

Step 9 - Save the changes by clicking on the



icon.

Step 10 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

 There are tasks to be executed regarding the configuration of this Verba Server.
If you would like to execute these tasks now, please [click here](#) .

Step 11 - Click on the **Service Control tab** tab.

Step 12 - Start the **Verba Passive Recorder Service** by clicking on the



icon.

Step 12 - Repeat these steps for each Recorder Server in your system.

Final Stage: Configure extensions

After finalizing the configuration of the recording services, make sure you have added the extensions you want recorded to the Verba extension list. This can be done manually ([Extension list](#)) or using [Active Directory Synchronization](#).

Recorder load balancing and failover design


 This feature is available in version 8 and later.

Table of Contents

- [Overview](#)
 - [Media Collectors and Recording Servers](#)
 - [Routing concepts and configuration](#)
 - [Recording routing decision](#)
- [Configuring High Availability](#)
 - [On Verba Recording Servers](#)
 - [On Verba Media Collectors](#)
- [Configuration examples](#)
 - [Example 1 - Three recording servers with load balancing](#)
 - [Example 2 - Dual recording with failover](#)
 - [Example 3 - Two sites dual recording with site-failover to each-other](#)

Overview

Verba Recording Servers can be used as a standalone recording solution, or in cooperation with Verba Media Collectors.

When Verba Media Collectors are used, you can build a 2 layer recording architecture, where:

- a **media collector layer** collects all necessary media
- a **recorder layer** that processes and records media

Complex load balancing and failover configurations are possible between the media collector and the recorder layer.

Media Collectors and Recording Servers

Verba Media Collectors on the media collector layer are able to collect media from

- network traffic recorded from a network port (e.g. calls with unencrypted SIP, Skinny signaling)
- network traffic recorded from a network port, extended with signaling from an external source (e.g. signaling from Lync filters)
- the built-in media proxy, an RTP proxy that terminates media streams and forwarded them to a target (e.g. Lync proxy recording mode, where the Media Collector acts as a middleman in the media stream)
- the built-in SIP proxy (e.g. a SIP trunk can be routed through a Media Collector).

In turn, the **Verba Recording Servers** are able to:

- receive and process media and signaling from Verba Media Collectors
- create and send call detail records to the database
- compress and write recorded media to disk
- upload recordings directly to Media Repositories or external compliance stores

Verba Media Collectors have a **very low CPU and disk I/O** requirements, while the Verba Recording Servers need **more CPU and disk I/O** to process and store calls.

In all cases, the Verba Media Collector can send media to:

- a single recorder
- multiple recorders at the same time (redundancy)
- multiple recorders in a load balanced way (load balancing)

The Verba Media Collector makes a recording routing decisions based on the redundancy configuration of the deployed platform.

Routing concepts and configuration

The following concepts are used on the redundancy configuration of a Verba system:

- **Server Weight** - defines the relative processing power of a Recording Server, to be used when a weighted load balancing algorithm is used to distribute recordings to Recording Servers. The **weight** counts when we are load balancing Recorder Servers with the same priority. We distribute the traffic between the Recorder Servers in the ratio of their weight: if there are three Recorder Servers joined to a Verba Proxy with the weight of 1, 2 and 3 then the first will get 1/6 the second will get 2/6 and the third will get 3/6 number of calls. In case of the weight is set to 0 then the Recorder Server will only get calls when there are no other ones online. If there are multiple Recorder Servers with the weight of 0 then the last connected one will get all the calls. If that one goes offline then the second last connected will get all the calls.
- **Recorder Group** - list of Recording Servers belonging to the same Recorder group are receiving the same recordings **at the same time**
- **Recorder Group Priority** - the priority of a Recorder Group

Recording routing decision

The following steps are used by a Media Collector when a recording routing decision is made:

1. it selects the Recorder Group (or groups) with the highest Recorder Group priority
2. lists the servers included in the group(s)
3. (if there are no servers, it goes back to step 1 and continues with lower Recorder Group priorities)
4. it randomly selects a recorder using the server weight (only using servers with the same Recorder Group priority)
5. it sends recordings to the selected server AND to all other servers in the same Recorder Group

Configuring High Availability

On Verba Recording Servers


On Verba Recording Servers you have to define the

- list of Media Collectors, this recorder accepts recordings from
- the weight of this Recording Server as advertised to each Media Collector
- the Recorder Group of this Recording Server as advertised to each Media Collector

The Verba server configuration tool provides a tool to configure the Media Collector list:

Example configuration (with the parameters seen in the screenshot):

```
PETER-PC | 11112 | verba | 1vcYm2yq7Fr5WuO3yi9oQQ== | 0 | 1 | 1 | GRPA1
```

 Different Media Collectors can get different weight, however, for easier understanding, it is highly recommended to advertise the same weight for all Media Collectors. One Recording Server could belong to multiple groups, but only one group can be advertised to a certain Media Proxy.

On Verba Media Collectors

On **Verba Media Collectors** you have to define the


- list of Recorder Groups and
- associated priorities for each Recorder Group.

Syntax:

<Recorder Group priority>|<Recorder Group name>

Example configuration:

```
10 | GROUP1
10 | GROUP2
1 | GROUP3
```

 Different Media Collectors can be configured with different Recorder Group lists in order to configure e.g. more complex load balancing designs

Configuration examples

Example 1 - Three recording servers with load balancing

Requirements

MC1 should load balanced recordings to R1, R2 and R3

Configuration overview

List of Recorder Groups on MC1:	1 MGR1 1 MGR2 1 MGR3 (each server belongs to a separate Recorder Group and all groups
List of Media Collectors on R1:	MC1:5, MGR1
List of Media Collectors on R2:	MC1:5, MGR2
List of Media Collectors on R3:	C1:5, MGR3

Explanation

As all recorders belong to different Recorder Groups, all recordings will only be sent once and the weight of the servers are used for load balancing.

Example 2 - Dual recording with failover

Requirements

- MC1 should send recordings to both R1 and R2 at the same time,
- however, if none of them are available it should send to R3.

Configuration overview

List of Recorder Groups on MC1:	2 MGR1 1 MGR2 (MGR1 has higher priority than MGR2)
List of Media Collectors on R1:	MC1:5, MGR1
List of Media Collectors on R2:	MC1:5, MGR1
List of Media Collectors on R3:	C1:5, MGR2 (note: this server is not in MGR1, but in MGR2)

Explanation

R1 and R2 servers are part of MGR1, therefore will get the same recordings at the same time. MGR1 is also higher priority than MGR2, therefore MGR2 will only get recordings if MGR1 is no server from MGR1 is available.

Example 3 - Two sites dual recording with site-failover to each-other

Requirements

- MCA and MCB are Media Collectors in two separate data centers (A and B). RA1, RA2 recorders are on site A, while RB1 and RB2 are on site B
- The sites are running in an active-active setup with calls passing by both Media Collectors, those should send recordings to both servers on the same site
- however, if none of the local servers are available, recordings should be sent to the other site
- When recordings are sent to the other site, only one copy should be sent to lower bandwidth

Configuration overview

List of Recorder Groups on MCA:	10 MGRA 1 MGR-RB1 1 MGR-RB2 (MGRA consists of the local servers, so it is higher priority) (MGRB-R1 and MGRB-R2 will consist only one server, and since their priority is the same, they will be load balanced)
List of Recorder Groups on MCB:	MGR-RA1, 1 MGR-RA2, 1 MGRB, 10 (configuration on the other site is reversed)
List of Media Collectors on RA1:	MCA:1, MGRA MCB:1, MGR-RA1 (Note how different groups are advertised to different Media Collectors)
List of Media Collectors on RA2:	MCA:1, MGRA MCB:1, MGR-RA2
List of Media Collectors on RB1:	MCA:1, MGR-RB2 MCB:1, MGRB

List of Media Collectors on RB2:	MCA:1, MGR-RB2 MCB:1, MGRB (note: this server is not in MGR1, but in MGR2)
----------------------------------	--

Explanation

From the perspective of MCA, local servers belong to a single group, remote servers belong to two groups. MCB has the same list reversed. On both MCA and MCB the group with the two local servers have higher priority, while the servers on the other site are listed as Recorder Groups, that have the same priority and only hold a single server.

By advertising different groups to different Media Collectors, the recording servers achieve that the local recorders will be preferred until at least one of them is up, otherwise, the recordings will be load balanced to one of the two remote servers.

Port range and QoS settings for proxy based recording

Media port range

Verba Proxy Servers use a predefined UDP port range for media relaying. These ports are not constantly open for listening as they are allocated on-demand as the relay service needs them. The number of ports required to relay a call depends on a number of factors:

- Every established voice call requires minimum 4 ports (2 RTP, 2 RTCP).
- Every established video call requires minimum 8 ports (4 RTP, 4 RTCP).
- During call setup, endpoints use additional ports during ICE negotiation. These ports are only allocated for a few seconds.
 - If an endpoint has 1 wired and 1 wireless connection, it will require 2x4=8 ports on the relay server during call setup and ICE negotiation (first ~10sec).
 - For RGS and simulring call scenarios, Lync tries to allocate ports for each and every possible endpoint (RGS members, targets). If a team has 20 members, the system will try to allocate 20x4 ports at once during call setup and ICE negotiation (first ~10sec).

If the media port range is not configured properly, and there is not enough port available, the call setup will fail.

QoS configuration

The Verba Proxy Servers are subject to Quality of Service (QoS) design as the media streams will go through these servers. More information on QoS design in Lync: <https://technet.microsoft.com/en-us/library/gg405409.aspx>

If you want to apply QoS policies, follow the guidelines of this article: <https://technet.microsoft.com/en-us/library/jj204681.aspx>. It is about the internal interface of the Edge Server, which is identical to the Verba relay server concept. The port range defined in the QoS policy must match the range configured for the proxy server.

Configuring Lync call blocking on recording failure

Available in version 8.7 and later

For a general overview of this feature refer to the [Call Blocking on Recording Failure](#) article.

Configuring Call Blocking

You have to enable the call blocking feature on both Verba Proxy and Verba Lync Filter components.

Step 1 - Navigate to **System / Servers**. Select your server running the proxy service.

Step 2 - Go to **Change Configuration Settings / Media Collector and Proxy / RTP Proxy** and enable "Block the calls if there is no online recorder".

▲ RTP Proxy	
▶ Advanced	
Enabled:	<input checked="" type="checkbox"/> Yes
Relay video streams:	<input type="checkbox"/> Yes
A/V Port Range Begin:	<input type="checkbox"/> 16384
A/V Port Range End:	<input type="checkbox"/> 65535
Separated Video Port Range Begin:	<input type="checkbox"/> 0
Separated Video Port Range End:	<input type="checkbox"/> 0
Appshare Port Range Begin:	<input type="checkbox"/> 42000
Appshare Port Range End:	<input type="checkbox"/> 44999
Filetransfer Port Range Begin:	<input type="checkbox"/> 45000
Filetransfer Port Range End:	<input type="checkbox"/> 49999
Block the calls if there is no online recorder:	<input checked="" type="checkbox"/> Yes
Proxy pool name:	<input type="checkbox"/>

Step 3 - Click the **Save** icon to save your settings.

Step 4 - The system will notify you that the changes need to be applied to the server by restarting the necessary services. Execute the required tasks.

Step 5 - Navigate to **System / Servers**. Select your server running the Lync Filter plugin.





Step 6 - Go to **Change Configuration Settings / Lync Filter / Call Blocking** and set the "**Block the calls if there is no online proxy**" and the "**Block the calls if media collector fails**" settings to **Yes**.

▲ Call Blocking	
Block the calls if there is no online proxy:	<input checked="" type="checkbox"/> Yes
Block the calls if media collector fails:	<input checked="" type="checkbox"/> Yes

Step 7 - Go to **Change Configuration Settings / Lync Filter / Signaling Information Target Settings** and add the public addresses of the edge servers with a '|' separator in the Recording Server(s) section.

▲ Signaling Information Target Settings

Media Collector(s):

<input type="checkbox"/>	EDGE1.VERBATEST.LOCAL:10201 publicIP		
<input checked="" type="checkbox"/>	EDGE2.VERBATEST.LOCAL:10201 publicIP		
<input data-bbox="742 324 774 358" type="button" value="+"/>			

Step 8 - Click the **Save** icon to save your settings.

Step 9 - The system will notify you that the changes need to be applied to the server by restarting the necessary services. Execute the required tasks.

Configuring persistent chat room recording for SfB and Lync

The Persistent Chat Endpoints belongs to FE pools. One endpoint can handle more than one persistent chat room. Therefore it cannot be used in recorded extension configuration. The message traffic of the endpoints should be recorded in their home SfB pool because that is the place where the messages are centralised.

The chat rooms are identified by the ChatRoomUri attribute, which needs to be configured as an extension in Verba.

Prerequisites

The [Verba SfB / Lync Filtler](#) component have to be installed on **all Front-End servers**. The **Verba SfB / Lync IM Filter service have to be registered** in the Lync pool.

For the recording and the web access at least a [Single Server](#) have to be installed. The roles also can be separated by installing a separate [Media Repository](#) and a [Recording Server](#). If high availability or load balancing is required, then additional Recording Servers can be installed.

Firewall configuration

Refer to [Firewall configuration for Skype for Business - Lync deployments](#) for more information.

Stage One: Configuring the Verba SfB/Lync IM Recorder component

Follow the steps below to configure the Verba SfB/Lync IM Recorder service

Step 1 - In the Verba web interface go to **System > VServers > Select your Recording Server > Click on the Service Activation** tab.

Step 2 - Activate the **Verba SfB/Lync IM Recorder Service** by clicking on the



icon.

Step 3 - Click on the **Change Configuration Settings** tab. Expand the **SfB/Lync IM Recorder** section.

Step 4 - Under the **General** section set the '**Internal Domain, Numbers Pattern**' setting by entering the **recorded SIP domains** separated by '|' character. (example: [contoso.com](#)|[adatum.com](#))


Step 5 (Optional) - Set the '**Create Transcript and Metadata XML Files**' setting to **Yes** in order to write the IM recordings to the disk. (By default the IM recordings are stored only in the database.)


Step 6 - **Save** the changes by clickin on the



icon.

Step 7 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

 There are tasks to be executed regarding the configuration of this Verba Server. If you would like to execute these tasks now, please [click here](#) .

 Changes can be execute at once at the end. In that case don't forget to click on '**Check All**'.

Step 8 - Click on the **Service Control** tab.

Step 9 - Start the **Verba SfB/Lync IM Recorder Service** by clicking on the



icon.

Repeat these steps for each Recorder Server in your system.

Stage Two: Configuring the Verba SfB/Lync IM Filter component

Step 1 - Login to the **Lync Front End Server**

Step 2 - Open the Management Shell and execute the **Get-CsPersistentChatEndpoint** command in order to get the Persistent Chat Endpoint SIP address.

Step 3 - Copy the **SipAddresses** which belongs to the recorded pool. (For example: if the filters are installed in the fepool.verbalabs.com FE pool then you will need to copy the SIP addresses which belongs to that pool.)

```
Administrator: Lync Server Management Shell
Priority      : 13
Uri          : http://www.verba.com/LyncChatRecorder
Name         : LyncChatRecorder
Enabled      : True
Critical     : False
ScriptName   :
Script       :

PS C:\Users\administrator.VERBALABS> Get-CsPersistentChatEndpoint

Identity     : CN={4e6ee463-be2e-4e0a-bb12-8a1e59cd2b0f},CN=Application
              Contacts,CN=RTC Service,CN=Services,CN=Configuration,DC=V
              ERBALABS,DC=COM
SipAddress    : sip:GC-1-PersistentChatService-31@verbalabs.com
RegistrarPool : repool.verbalabs.com
DisplayName   : Persistent Chat Service
CreatedByActivation : True
Enabled       : True

PS C:\Users\administrator.VERBALABS>
```

Step 4 - In the Verba web interface go to **System > Servers > Select your Front-End Server > Click on the Service Activation** tab.

Step 5 - Activate the **Verba SfB/Lync IM Filter Service** by clicking on the



icon.

Step 6 - Click on the **Change Configuration Settings** tab. Expand the **SfB/Lync IM Filter** section.

Step 7 - Under the **General** section set the '**Internal Domain, Numbers Pattern**' setting by entering the **recorded SIP domains** separated by '|' character. (example: contoso.com|adatum.com)

Step 8 - Set the **Server Version** setting according to the SfB / Lync environment version.

Step 9 - The **Verba Lync Chat Recorder Servers** field has to contain the list of the servers where the IM Recorder service installed. Enter every server with the correct port (**HOSTNAME:10220**), one at each line.

Step 10 - Under the **Persistent Chat** section provide the previously Persistent Chat Endpoint SIP address at the **Persistent Chat UrIs** setting. If there are multiple recorded endpoints, then one can be provided in each line.

▲ SfB/Lync IM Filter
 ▲ General

Filter Pool Name:	<input type="checkbox"/>	verbaim
Internal Domain, Numbers Pattern:	<input checked="" type="checkbox"/>	ld(5).*@contoso.com
Server Version:	<input checked="" type="checkbox"/>	Skype for Business ▼
Enable Notification Message Between Domains:	<input type="checkbox"/>	No ▼
Enable Notification Message Inside Domains:	<input type="checkbox"/>	No ▼
Enable Notification Message for Conferences:	<input type="checkbox"/>	No ▼
Notification Message Text:	<input type="checkbox"/>	
Verba Lync Chat Recorder Servers:	<input checked="" type="checkbox"/>	TESTRS1.VERBATEST.LOCAL:10220 TESTRS2.VERBATEST.LOCAL:10220
Enable Performance Based Load Balancing for IM Recorders:	<input type="checkbox"/>	Yes ▼

▲ Persistent Chat


Persistent Chat Uri:	<input checked="" type="checkbox"/>	sip:GC-1-PersistentChatService-31@verbalabs.com
----------------------	-------------------------------------	---

Step 11 - Save the changes by clicking on the



icon.

Step 12 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.


There are tasks to be executed regarding the configuration of this Verba Server.
 If you would like to execute these tasks now, please [click here](#) .

Step 13 - Click on the **Service Control tab** tab.

Step 14 - Start the **Verba SfB/Lync IM Filter Service** by clicking on the



icon.

Repeat these steps for each Front-End Server in your system.

Stage Three: Setup a recorded chat room

Step 1 - Login to the **Lync Persistent Chat Server**.

Step 2 - Open the Management Shell and execute the **Get-CsPersistentChatRoom** command.

Step 3 - Find a room which will be recorded and copy the **ChatRoomUri** attribute.

```
Administrator: Lync Server Management Shell
Invitations : Inherit
Members     : {}
Managers    : {}
Presenters  : {}
Disabled    : False

Identity    : PCHAT.verbalabs.com\TestRoom
Name        : TestRoom
Description :
Category    : Test Category
CategoryUri : ma-cat://verbalabs.com/4c950e46-14ad-458d-bb0f-f9978c457b21
ChatRoomUri : ma-chan://verbalabs.com/b1416b88-d65e-4bf5-86ce-856f23e62c33
Type        : Normal
Addin       :
Privacy     : Open
Invitations : Inherit
Members     : {}
Managers    : {sip:bajzat@verbalabs.com}
Presenters  : {}
Disabled    : False

PS C:\Program Files\Microsoft Lync Server 2013> _
```

Step 4 - Login to the **Verba Web Interface**.

Step 5 - Go to the **Users / Extensions** menu.

Step 6 - Click on the **Add New Extension** link.


Step 7 - Paste the **ChatRoomUri** attribute to the **Extension** field.

Step 8 - Change the type of the extension to **Persistent Chat Room**.

Step 9 - Check the **Instant Messaging** check box at the **Recording Settings**.

Step 10 - Click on the **Save** button.

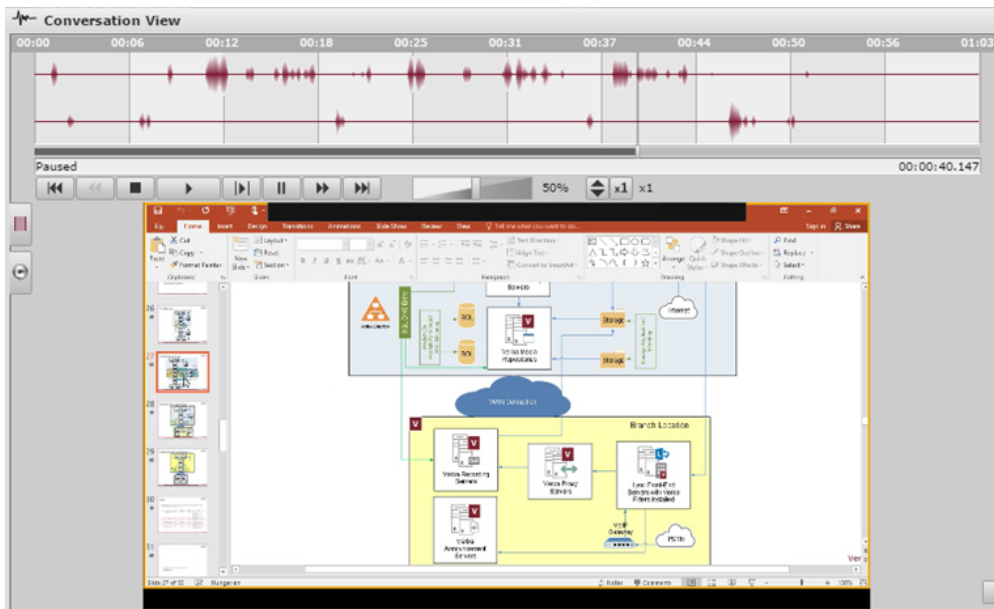
Step 11 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

 There are tasks to be executed regarding the configuration of this Verba Server. If you would like to execute these tasks now, please [click here](#) .

Configuring Lync - SfB Screen and Application Share recording

It is possible to record the Screen/Application Share sessions in Lync/SfB environments. The solution works for all call scenarios, including internal, external, conference calls.

An example of what this looks like in the Verba player can be seen in the picture below.



Screen or Application Share recording cannot be controlled separately as in essence they are the same feature.

There is no extra configuration required in the system (on top of voice recording) to start recording screen sharing sessions.

- ✔ To see how to install and configure Lync voice recording, refer to the [Installing the Verba Skype for Business - Lync Filter](#) and the [Configuring Verba for RTP Proxy based recording](#) articles.

To enable recording for this traffic, follow the steps below.

Step 1 - Navigate to the extension configuration page of an extension. In the Verba menu, this is found under **Administration -> Extension -> Select an extension**

Step 2 - Check the checkbox for **Screen/Application Share**

Step 3 - (Optional) By default all directions are recorded for this extension for this type of traffic. Optionally, **define which directions** should be recorded.

Step 4 - Repeat steps 1-3 for **all extensions** where this feature is to be used.

Extension Data

Synchronized by Active Directory

Extension*
Phone number ('1234') or address ('user@company.com')

User x

If a user is missing from the list, please verify the Valid Until and Valid From fields of that user.

Type* ▼

Update user information on existing conversations
Apply on: new conversations unassigned conversations all conversations
 Update conversations within the user's validity period only

Description

Recording Settings

Recording Mode* ▼

Voice

Instant Messaging

Video

Desktop Screen

Screen & Application Share

Whiteboard

Poll / Q&A

File Share

Support of modalities depends on the recorded platform, more information [here](#).

Recorded Directions All
 Internal PSTN In PSTN Out External Federated In Federated Out Conference

Record Calls Answered by 3rd Party All
 Forwarded Transferred Team Call Delegated

Only available for Sfb/Lync recording

Configuring Verba for RTP Proxy based recording

This article provides a detailed step by step guide on how to configure the Verba Recording System for RTP Proxy based recording in a Microsoft Lync environment.

❗ Configuring RTP Proxy based recording is only necessary (and should only be done) if **internal Lync calls** need to be recorded. Using this method will result in calls (for recorded extensions) being **rerouted through the Verba Proxy Server(s)**. The proxy server is an active part of the call media path and it can introduce additional network latency and jitter, if it goes down for any reason, ongoing recorded calls will be terminated.
If recording the internal calls is not required, please configure [Mediation Server server-based recording](#) instead.

- [Important note on terminology](#)
- [Preparation](#)
 - [Firewall configuration](#)
- [Stage One: Configure the Verba Media Collector and Proxy service for RTP Proxy based recording](#)
- [Stage Two: Configure the Verba Lync Filter for RTP Proxy based recording](#)
- [Stage Three: Configure the Verba Passive Recorder service for RTP Proxy based recording](#)
- [Final Stage: Configure extensions](#)

This guide does not cover:

- [Recorder load balancing and failover design](#)
- [Port range and QoS settings for proxy based recording](#)

Important note on terminology

The **Verba Media Collector and Proxy Service** can operate in two modes:

- **RTP Proxy mode:** the service acts as an RTP Proxy and is inserted into the altered recorded call media path. The recorders connect to the service in order to capture the media streams there.
- **Remote capture / Media collector mode:** used on Edge and/or Mediation servers to capture the call media streams on their normal (unaltered) route. The recorders connect to the service in order to capture the media streams there.

The same service is responsible for carrying out both of these tasks, **based on location and configuration**. This guide will reference a **Verba Media Collector Proxy service operating in RTP Proxy Mode** (either deployed on a Recording Server or on a separate machine) as a **Proxy Server**.

A **Verba Media Collector and Proxy operating in Remote Capture / Media collector mode** (deployed on Edge and/or Mediation servers) will be referenced as a **Media Collector**.

Preparation

Before starting to configure Verba for Lync recording, **every Verba server and component have to be installed**. For more information about the required servers and components see [Microsoft Skype for Business](#).

Firewall configuration

Refer to [Firewall configuration for Skype for Business - Lync deployments](#) for more information.

Stage One: Configure the Verba Media Collector and Proxy service for RTP Proxy based recording

Follow the steps below to configure the Verba Media Collector and Proxy service to operate in RTP Proxy mode.

 Stages One and Three take place on the same server's configuration page if the Recorder and Proxy Servers are co-located.

Step 1 - In the Verba web interface go to **System / Servers**, select the Recording (or separate Proxy) Server and click on the **Service Activation** tab.

Step 2 - Activate the **Verba Media Collector and Proxy Service** by clicking on the



icon.

Step 3 - Click on the **Change Configuration Settings** tab. Expand the **Media Collector and Proxy** section.

Step 4 - Under **General / Recorder Connection**, configure the authentication credentials for the connections with the recording service. Define the **Authentication User** and **Authentication Passwords** values. These credentials will be used later when configuring the connections in the recorder service.

Step 5 - In the **General** section set the **Internal Domain, Numbers Pattern** setting. This has to be a regex which matches to all internal line numbers and SIP domains.

Step 6 - In the **Lync Connector** section, set both **Enabled** and **Act as RTP Proxy** to **Yes**.

Step 7 - In **RTP Proxy** section set '**Enabled**' to **Yes**.

Media Collector and Proxy

General

Recorder connection

Announcement Service Uri:	<input type="checkbox"/>	
Assign Call To Recorder only on First RTP:	<input type="checkbox"/>	Yes
Call Timeout (sec):	<input type="checkbox"/>	600
SIP Uri Modification:	<input type="checkbox"/>	Remove domain part for numbers only
Enable RTP over TCP Support:	<input type="checkbox"/>	Yes
Record video calls as audio only:	<input type="checkbox"/>	No
Recorder Groups and Priorities:	<input type="checkbox"/>	
Default Recorder Group Priority:	<input type="checkbox"/>	0
Internal Domain, Numbers Pattern:	<input checked="" type="checkbox"/>	ld{5}.*@contoso.com
Record SfB/Lync Application Sharing (RDP):	<input type="checkbox"/>	Yes
Record SfB/Lync File Transfer:	<input type="checkbox"/>	Yes
Enable Performance Based Loadbalancing for Recorders:	<input type="checkbox"/>	No
Use Overloaded Recorder as Last Effort:	<input type="checkbox"/>	Yes

Remote Capture

Lync Connector

Connection

Enabled:	<input checked="" type="checkbox"/>	Yes
Act as RTP Proxy:	<input checked="" type="checkbox"/>	Yes
Legacy Mode:	<input type="checkbox"/>	No
Enable Luware LUCS Integration:	<input type="checkbox"/>	No
Contact Center UCMA B2B Agents:	<input type="checkbox"/>	RTCC/5.0.0.0 ACE RTCC/6.0.0.0 ACE RTCC/5.0.0.0 ICH RTCC/5.0.0.0 ICH-1.0.0.0 RTCC/5.0.0.0 TM-ICH

RTP Proxy

Advanced

Enabled:	<input checked="" type="checkbox"/>	Yes
Relay video streams:	<input type="checkbox"/>	Yes
A/V Port Range Begin:	<input type="checkbox"/>	16384
A/V Port Range End:	<input type="checkbox"/>	65535

Step 8 - Save the changes by clicking on the



icon.

Step 9 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

i Changes can be execute at once at the end. In that case don't forget to click on **'Check All'**.



There are tasks to be executed regarding the configuration of this Verba Server. If you would like to execute these tasks now, please [click here](#).

Step 10 - Click on the **Service Control** tab.

Step 11 - Start the **Verba Media Collector and Proxy Service** by clicking on the



icon.

Repeat these steps for each Proxy Server in your system.

For more information about the Verba Media Collector and Proxy Service see [Verba Media Collector and Proxy Service Reference](#).

Stage Two: Configure the Verba Lync Filter for RTP Proxy based recording

Follow the steps below to configure the Verba Lync Filters located on the Lync Front End servers. The Verba Lync Filter is responsible for capturing and modifying the signaling messages to alter the media path to include the Proxy Server.

Step 1 - In the Verba web interface go to **System / Servers**, select the Front End server running the Verba Lync Filter and click on the **Service Activation** tab.

Step 2 - Activate the **Verba SfB/Lync Call Filter Service** by clicking on the



icon.

Step 3 - Click on the **Change Configuration Settings** tab. Expand the '**SfB/Lync Call Filter**' section.

Step 4 - In the **General** section set the **Internal Domain, Numbers Pattern** setting. This have to be a regex which matches to all internal line numbers and SIP domains.

Step 5 - Set the **Server Version** to the version of the Lync Platform you are using.

Step 6 - Set the **Relaying mode** to **Reroute/relay recorded calls through Verba Proxy server(s)**.

Step 7 - Under the **Proxy Server Based Relay Settings** section add your Proxy Servers by clicking on the



next to **Verba Proxy Servers**.

Step 8 - At the right panel select the Proxy Server from the drop down list at the **Proxy Host**. Click **Save**.

Verba Proxy Servers	
Type	Does not belong to pool ▼
Proxy Host	TESTPROXY1.VERBATEST.LOCAL ▼
Proxy Port	10201
Priority or Subnets	
Pool Name	

Step 9 - Repeat Steps 7-8 for every Proxy Server in your system.

▲ SfB/Lync Call Filter

▲ General

Filter Pool Name:	<input type="checkbox"/>	verba
Internal Domain, Numbers Pattern:	<input checked="" type="checkbox"/>	ld{5}.*@contoso.com
Server Version:	<input checked="" type="checkbox"/>	Skype for Business
Relaying Mode:	<input checked="" type="checkbox"/>	Reroute/relay recorded calls through Verba Proxy server(s)
Record Conference Calls Only:	<input type="checkbox"/>	Disable

▶ Signaling Information Target Settings

▶ Edge Server Based Relay Settings

▲ Proxy Server Based Relay Settings

Verba Proxy Servers:	<input checked="" type="checkbox"/>	TESTPROXY1.VERBATEST.LOCAL:10201		
	<input checked="" type="checkbox"/>	TESTPROXY2.VERBATEST.LOCAL:10201		
		<input type="text" value=""/>		

Call Timeout(seconds):	<input type="checkbox"/>	14400
------------------------	--------------------------	-------

Step 10 - Save the changes by clicking on the



icon.

Step 11 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

There are tasks to be executed regarding the configuration of this Verba Server. If you would like to execute these tasks now, please [click here](#).

Step 12 - Click on the **Service Control** tab.

Step 13 - Start the **Verba SfB/Lync Call Filter Service** by clicking on the



icon.

Repeat these steps for every Lync Front End / Filter in your system.

Stage Three: Configure the Verba Passive Recorder service for RTP Proxy based recording

Follow the steps below to configure the Verba Passive Recorder service for RTP Proxy based recording:

Stages One and Three take place on the same server's configuration page if the Recorder and Proxy Servers are co-located.

Step 1 - In the Verba web interface go to **System / Servers**, select the Recording Server and click on the **Service Activation** tab.

Step 2 - Activate the **Verba Passive Recorder Service** by clicking on the



icon.

Step 3 - Click on the **Change Configuration Settings** tab. Expand the **Passive Recorder** section.

Step 4 - Under **Basics** add your Proxy Servers and Media Collectors by clicking on the



next to **Media Collector and Proxies**.

Step 5 - At the right panel select the Proxy Server from the drop down list at the **Host**. Provide the username and password configured in the **Verba Media Collector and Proxy Service** above for the connections. If there are multiple proxy servers, then set the **Recorder Weight** to **1** so there will be load-balancing. Click **Save**.

Recorder Proxy	
Host	TESTPROXY1.VERBATEST.LOCAL
Port	11112
User	verba
Password	*****
Compress Connection Stream	<input type="checkbox"/>
Recorder Weight	1
Secure	<input checked="" type="checkbox"/>
Recorder Group	

Step 6 - Repeat Steps 4-5 for every Proxy Server in your system.

Step 7 - Set the **Internal Domain, Numbers Pattern** setting. This has to be a regex which matches to all internal line numbers and SIP domains.


Passive Recorder	
Basics	
Recording Interface:	<input type="checkbox"/> +
Media Collector and Proxies:	<input type="checkbox"/> TESTPROXY1.VERBATEST.LOCAL 11112 verba 1vcYm2yq7Fr5WuO3yi9oQQ== 0 1 1
	<input checked="" type="checkbox"/> TESTPROXY2.VERBATEST.LOCAL 11112 verba 1vcYm2yq7Fr5WuO3yi9oQQ== 0 0 1
	<input type="checkbox"/> EDGE1.VERBATEST.LOCAL 11112 verba 1vcYm2yq7Fr5WuO3yi9oQQ== 0 1 1
	+ <input type="checkbox"/>
Audio Format:	<input type="checkbox"/> Microsoft GSM-Fullrate (LPC-RPE) in WAV
Video Format:	<input type="checkbox"/> Verba RTP Dumped Media Format
Bidirectional/Stereo Recording:	<input type="checkbox"/> No
Automatic Gain Control Enabled:	<input type="checkbox"/> Yes
Conference Resources IP Addresses:	<input type="checkbox"/>
Experimental H.323 Support Enabled:	<input type="checkbox"/> No
SIP Support Enabled:	<input type="checkbox"/> Yes
Skinny Support Enabled:	<input type="checkbox"/> Yes
Call Timeout (seconds):	<input type="checkbox"/> 600
Voice Activity Statistics:	<input type="checkbox"/> No
Secondary Recording Server:	<input type="checkbox"/> No
Internal Domain, Numbers Pattern:	<input checked="" type="checkbox"/> \d{5}.*@contoso.com

Step 8 - Save the changes by clicking on the



icon.

Step 9 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

 There are tasks to be executed regarding the configuration of this Verba Server.
If you would like to execute these tasks now, please [click here](#) .

Step 10 - Click on the **Service Control** tab.

Step 11 - Start the **Verba Passive Recorder Service** by clicking on the



icon.

Repeat these steps for each Recorder Server in your system.

Final Stage: Configure extensions

After finalizing the configuration of the recording services, make sure you have added the extensions you want to record to the Verba extension list. This can be done manually ([Extension list](#)) or using [Active Directory Synchronization](#).

Configuring Verba for Dual-Relaying

In a multi-site environment, it is possible to use a proxy server at each site so the call can be recorded on both ends. To achieve this we can configure dual relaying mode.

Lync Filter configuration

Step 1 In the Verba web interface go to **System > Servers > Select your Front End server containing the Verba Lync Filter > Click on the Change configuration settings** tab. Expand the 'Lync Filter' section.

Step 2 Under the **Proxy Server Based Relay Settings** node add a new Proxy by clicking on the plus icon, or modify the existing one by clicking on the gear icon.

Verba Proxy Servers	
Type	Belongs to pool ▼
Proxy Host	DEV-PROXY1 ▼
Proxy Port	10201
Priority or Subnets	1
Pool Name	pool1

Step 3 Set the **Type** property to "**Belongs to pool**" and fill the **Pool Name** textbox.

Step 4 Save the changes.

Step 5 Repeat the steps above for all Frontend servers at the same site. For the Frontend servers at the other site choose another pool name.

Proxy configuration

Step 1 In the Verba web interface go to **System > Servers > Select your Recording (or separate Proxy) Server > Click on the Change configuration settings** tab. Expand the **Media Collector and Proxy** section.

▲ RTP Proxy

▶ Advanced

Enabled:	<input checked="" type="checkbox"/>	Yes
Relay video streams:	<input type="checkbox"/>	Yes
A/V Port Range Begin:	<input type="checkbox"/>	16384
A/V Port Range End:	<input type="checkbox"/>	65535
Separated Video Port Range Begin:	<input type="checkbox"/>	0
Separated Video Port Range End:	<input type="checkbox"/>	0
Appshare Port Range Begin:	<input type="checkbox"/>	42000
Appshare Port Range End:	<input type="checkbox"/>	44999
Filetransfer Port Range Begin:	<input type="checkbox"/>	45000
Filetransfer Port Range End:	<input type="checkbox"/>	49999
Block the calls if there is no online recorder:	<input type="checkbox"/>	No
Proxy pool name:	<input checked="" type="checkbox"/>	pool1

Step 2 Under the **RTP Proxy** node you can find the **Proxy pool name** property. Fill it with the pool name you added at the Lync Filter config in the same site.

Step 3 Save the changes.

Step 4 Repeat the steps above for the proxy server(s) at the other site

Configuring Media Collector on Edge servers

The Proxy and the Mediation-based recording methods can be extended with the recording of the federated calls, calls of users logged in remotely and application share recording. For that, a Media Collector and Proxy component have to be installed and configured on the Edge server.

Prerequisites

The Media Collector and Proxy component have to be installed on all Edge servers. For the installation guide see: [Installing the Verba Media Collector and Proxy component](#)

Firewall configuration

Refer to [Firewall configuration for Skype for Business - Lync deployments](#) for more information.

Stage One: Configure the Verba Media Collector and Proxy service for capturing

Follow the steps below to configure the Verba Recorder Proxy service to operate in Media Collector mode.

Step 1 - In the Verba web interface go to **System / Servers**, select the Edge server where the Media Collector and Proxy service is installed and click on the **Service Activation** tab.

Step 2 - Activate the **Verba Media Collector and Proxy Service** by clicking on the



icon.

Step 3 - Click on the **Change Configuration Settings** tab. Expand the **Media Collector and Proxy** section.

Step 4 - Under **General / Recorder Connection**, configure the authentication credentials for the connections with the recording service. Define the **Authentication User** and **Authentication Passwords** values. These credentials will be used later when configuring the connections in the recorder service.

Step 5 - In the **General** section set the **Internal Domain, Numbers Pattern** setting. This has to be a regex which matches to all internal line numbers and SIP domains.

Step 6 - Under **Remote Capture** set the **Enabled** field to **Yes**.

Step 7 - At **Interfaces** add the server's own network interface for listening by clicking on the



button.

Step 8 - At the right panel select an interface from the list, then click **Save**.

Choose Recording Interface

Host	localhost	▼	Port		
User			Password		
Interface Name	SCCP	SIP	RTP	Total	IP Address
Ethernet	0	0	0	0	fe80::31e0:9628:94fb:6f12 10.4.0.42
Ethernet 2	0	0	0	0	fe80::f45f:f332:190e:40d 192.168.167.65

Step 9 - Repeat the steps 7-8 until every interface is added to the configuration.

Step 10 - Under **Lync Connector** section set the **Enabled** setting to **Yes**.

Media Collector and Proxy

General

Recorder connection

Announcement Service Uri:	<input type="checkbox"/>	
Assign Call To Recorder only on First RTP:	<input type="checkbox"/>	Yes
Call Timeout (sec):	<input type="checkbox"/>	600
SIP Uri Modification:	<input type="checkbox"/>	Remove domain part for numbers only
Enable RTP over TCP Support:	<input type="checkbox"/>	Yes
Record video calls as audio only:	<input type="checkbox"/>	No
Recorder Groups and Priorities:	<input type="checkbox"/>	
Default Recorder Group Priority:	<input type="checkbox"/>	0
Internal Domain, Numbers Pattern:	<input checked="" type="checkbox"/>	ld(5).*@contoso.com
Record SfB/Lync Application Sharing (RDP):	<input type="checkbox"/>	Yes
Record SfB/Lync File Transfer:	<input type="checkbox"/>	Yes
Enable Performance Based Loadbalancing for Recorders:	<input type="checkbox"/>	No
Use Overloaded Recorder as Last Effort:	<input type="checkbox"/>	Yes

Remote Capture

Enabled:	<input checked="" type="checkbox"/>	Yes									
Interfaces:	<input checked="" type="checkbox"/>	<table border="1"><tr><td>DeviceNPF_{1DA95C96-2C3E-44DD-9615-0A00F58173A0}</td><td><input type="checkbox"/></td><td><input type="checkbox"/></td></tr><tr><td>DeviceNPF_{6E3FCD20-5D25-42D8-B432-B020A0E7F904}</td><td><input type="checkbox"/></td><td><input type="checkbox"/></td></tr><tr><td colspan="3" style="text-align: center;">+</td></tr></table>	DeviceNPF_{1DA95C96-2C3E-44DD-9615-0A00F58173A0}	<input type="checkbox"/>	<input type="checkbox"/>	DeviceNPF_{6E3FCD20-5D25-42D8-B432-B020A0E7F904}	<input type="checkbox"/>	<input type="checkbox"/>	+		
DeviceNPF_{1DA95C96-2C3E-44DD-9615-0A00F58173A0}	<input type="checkbox"/>	<input type="checkbox"/>									
DeviceNPF_{6E3FCD20-5D25-42D8-B432-B020A0E7F904}	<input type="checkbox"/>	<input type="checkbox"/>									
+											
Capture Buffer Size (megabytes):	<input type="checkbox"/>	90									
Skinny Support Enabled:	<input type="checkbox"/>	Yes									
SIP Support Enabled:	<input type="checkbox"/>	Yes									
RTP Address Translation Enabled:	<input type="checkbox"/>	Yes									
Use RTP source address in call - RTP mapping:	<input type="checkbox"/>	No									
SIP Capture Filter:	<input type="checkbox"/>	ip[2]<5120 and (ip[6:2]&0x3F!=0 or (tcp[0:2]=5060 or tcp[2:2]=5060 or udp[0:2]==5060 or udp[2:2]==5060)									
Skinny Capture Filter:	<input type="checkbox"/>	ip[2]<1024 and (tcp[0:2]=2000 or tcp[2:2]=2000)									
Media Capture Filter:	<input type="checkbox"/>	ip[2]<2048 and (udp and ip[6:2]&0x3F!=0 or tcp src port 443 or ((udp[8:2]=0x0115 and udp[24:4]=0x0000)									
TCP Media Capture Filter:	<input type="checkbox"/>	(tcp dst portrange 1024-65535 or tcp port 443)									
Base Capture Filter:	<input type="checkbox"/>										

Lync Connector

Connection

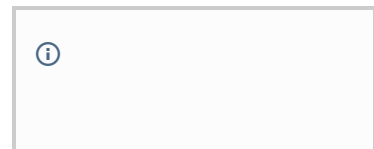
Enabled:	<input checked="" type="checkbox"/>	Yes
Act as RTP Proxy:	<input type="checkbox"/>	No
Legacy Mode:	<input type="checkbox"/>	No
Enable Luvare LUCS Integration:	<input type="checkbox"/>	No


Step 11- Save the changes by clicking on the



icon.

Step 12 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.



 There are tasks to be executed regarding the configuration of this Verba Server. If you would like to execute these tasks now, please [click here](#) .

Changes can be execute at once at the end. In that case don't forget to click on '**Check All**'.

Repeat these steps for each Edge servers in your system.

Stage Two: Configure the Verba Lync Filter for Edge based recording

Follow the steps below to configure the Verba Lync Filters located on the Lync Front End servers. The Verba Lync Filter is responsible for capturing and modifying the signaling messages to alter the media path to include the Proxy Server.

Step 1 - In the Verba web interface go to **System / Servers**, select the Front End server running the Verba Lync Filter and click on the **Service Activation** tab.

Step 2 - Activate the **Verba SfB/Lync Call Filter Service** by clicking on the



icon.

Step 3 - Click on the **Change Configuration Settings** tab. Expand the **SfB/Lync Call Filter** section.

Step 4 - Under the **Signaling Information Target Settings** section add your Edge Servers by clicking on the



button next to **Media Collector(s)**.

Step 5 - At the right panel select the Edge Server from the drop down list at the **Host**. Click **Save**.


Step 6 - Repeat Steps 4-5 for every Edge Server in your system.

Step 7 - Save the changes by clicking on the



icon.

Step 8 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

 There are tasks to be executed regarding the configuration of this Verba Server. If you would like to execute these tasks now, please [click here](#) .

Step 9 - Repeat these steps for every Lync Front End / Filter in your system.

Stage Three: Configure the Verba Passive Recorder service for Edge based recording

Follow the steps below to configure the Verba Passive Recorder service for Mediation based recording:

Step 1 - In the Verba web interface go to **System / Servers**, select the Recording Server and click on the **Service Activation** tab.

Step 2 - Activate the **Verba Passive Recorder Service** by clicking on the



icon.

Step 3 - Click on the **Change Configuration Settings tab**. Expand the **Passive Recorder** section.

Step 4 - Under **Basics** add your **Media Collectors** by clicking in the



next to **Recorder Proxy**.

Step 5 - At the right panel, select the Edge server from the drop down list. Provide the username and password. Click **Save**.

Recorder Proxy	
Host	TESTFE1SFB.VERBATEST.LOCAL ▼
Port	11112
User	verba
Password
Compress Connection Stream	<input type="checkbox"/>
Recorder Weight	1 ▼
Secure	<input checked="" type="checkbox"/>
Recorder Group	

Step 6 - Repeat **Steps 4-5** for every Edge servers in your system.


Step 7 - Set the **Internal Domain, Numbers Pattern** setting. This have to be a regex which matches to all of the internal line numbers and SIP domains.

Step 8 - Save the changes by clicking on the



icon.

Step 9 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

 There are tasks to be executed regarding the configuration of this Verba Server.
If you would like to execute these tasks now, please [click here](#) .

Step 10 - Repeat these steps for each Recorder Server in your system.

Configuring Lync - SfB P2P File Transfer Recording

It is possible to record the P2P File Transfers in Lync/SfB environments. The solution works for internal and federated P2P transfers. It does not work for conferences.

There is no extra configuration required in the system (on top of voice recording) to start recording screen sharing sessions.

✔ To see how to install and configure Lync voice recording, refer to the [Installing the Verba Skype for Business - Lync Filter](#) and the [Configuring Verba for RTP Proxy based recording](#) articles.

To enable recording for this traffic, follow the steps below.

Step 1 - Navigate to the extension configuration page of an extension. In the Verba menu, this is found under **Administration -> Extension -> Select an extension**

Step 2 - Check the checkbox for **File Share**

Step 3 - (Optional) By default all directions are recorded for this extension for this type of traffic. Optionally, **define which directions** should be recorded.

ⓘ File Transfers in conference are recorded by importing from the native Lync Archive. The conference direction selection enables importing from the archive, the other directions enable P2P file transfer recording.

Step 4 - Repeat steps 1-3 for **all extensions** where this feature is to be used.

The screenshot displays the configuration page for an extension, divided into two main sections: 'Extension Data' and 'Recording Settings'.

Extension Data:

- Synchronized by Active Directory:**
- Extension*:** 1914 (Phone number ('1234') or address ('user@company.com'))
- User:** Micheal Cohen (micheal)
- Type*:** Number/Address
- Update user information on existing conversations:** Apply on: new conversations, unassigned conversations, all conversations. Update conversations within the user's validity period only.
- Description:** (Empty text area)

Recording Settings:

- Recording Mode*:** Full
- Voice:**
- Instant Messaging:**
- Video:**
- Desktop Screen:**
- Screen & Application Share:**
- Whiteboard:**
- Poll / Q&A:**
- File Share:**

Recorded Directions: Support of modalities depends on the recorded platform, more information [here](#).

- All
- Internal PSTN In PSTN Out External Federated In Federated Out Conference

Record Calls Answered by 3rd Party: All Forwarded Transferred Team Call Delegated

Only available for SfB/Lync recording

Installing and configuring the Verba SfB - Lync Announcement service

For a general overview of the function refer to the [Announcement](#) article.

- [Prerequisites](#)
- [Installation and service activation](#)
 - [Verba Announcement Server installation](#)
 - [Enabling the Verba SfB/Lync Announcement service](#)
- [Configuring the Verba SfB/Lync Announcement Service](#)
- [Configuring Verba components for announcement](#)
 - [Configuring the Verba SfB/Lync Call Filter for announcement](#)
 - [Configuring the Verba Media Collector and Proxy for announcement](#)
 - [Configuring the Verba Passive Recorder for conference call announcement](#)
- [Configuring custom prompts for users \(optional\)](#)
- [Configuring announcement transfer hiding \(optional\)](#)
- [Configuring redirect on failed transfer \(optional\)](#)

Prerequisites

The Verba Announcement service is available in the following server roles:

- Media Repository & Recording Server
- Media Repository
- Recording Server
- Announcement Server

To enable the service, the following tasks need to be executed on all Verba servers where the service needs to be enabled:

Step 1 - Add the Windows user account used during installation to the following groups:

- CSAdministrator
- Local Administrator
- RTCUniversalServerAdmins

Step 2 - Install the following features on the server(s) if they are not installed already.

- Microsoft .NET Framework 3.5
- Microsoft .NET Framework 4.0/4.5
- Media Foundation (Windows Server 2012 or newer) / Desktop Experience (Windows Server 2008 R2)

Step 3 - Install the [Microsoft UCMA Runtime 4.0](#) on the UCMA application servers

Step 4 - [Configure your firewalls](#)

Step 5 - [Create a Trusted Application Pool/Server](#) in your Skype for Business / Lync environment

Step 6 - [Request / assign a certificate](#) for/to the Announcement Server

Step 7 - If there are multiple announcement servers, create a new DNS entry for each server using the pool FQDN.

Installation and service activation

Verba Announcement Server installation

If you want to run the service separately, you need to install a Verba Announcement Server role on dedicated server(s).

Follow the guidelines at [Installing a Verba Announcement Server](#)

Enabling the Verba SfB/Lync Announcement service

If you already have the desired server role installed, you just need to enable the service.

Step 1 - Using the web application, navigate to the **System / Servers** page and select the server.

Step 2 - Click on the **Service Activation** tab.

Step 3 - Click on the



button for the **Verba SfB/Lync AnnouncementService** to activate the service.

Configuring the Verba SfB/Lync Announcement Service

When the above steps are completed, the Verba Announcement service can be configured as any other server component in the system using the Verba web interface.

For more information see [Configuring Verba recording announcement service](#).

Configuring Verba components for announcement

Configuring the Verba SfB/Lync Call Filter for announcement

Step 1 - Open the Verba web interface, click on the **System / Servers** and select the SfB/Lync Front-End / SBA / SBS server, or select the appropriate Configuration Profile at **System / Configuration Profiles**.

Step 2 - Go to the **Change Configuration Settings** tab, then expand the **SfB/Lync Call Filter / Recording Announcement** node.

Step 3 - Configure the following settings:

Configuration Parameter Name	Description	Sample Value
Recording announcement	Enable the announcement feature	Yes
Recording announcement for incoming PSTN calls	Enable voice announcement for incoming PSTN calls.	Yes
Enable Announcement for Outgoing PSTN calls	Enable voice announcement for outgoing PSTN calls.	Yes
Enable Announcement for Incoming Federated calls	Enable voice announcement for incoming Federated calls.	Yes

Enable Announcement for Outgoing Federated calls	Enable voice announcement for outgoing Federated calls.	Yes
Apply announcement to forwarded calls	Enable voice announcement for forwarded calls.	Yes
Enable announcement for Team calls	Sets whether the announcement should be played in the case of all users in the team, or to none of them.	Yes
Remove route information from SIP INVITE messages		Yes
Verba Announcement URI	The SIP addresses of the announcement service. If there are multiple announcement service pools, then all SIP addresses have to be provided, separated by a new line.	sip: VerbaAnnouncement@yourDomain.com
Internal Number Pattern	Defines the internal numbers	^(((4-9)[0-9]{3}) [\+]?[0-9]{5})\$
Internal SIP Domains	Defines the internal SIP domains. One at each line.	yourDomain.com
Verba Announcement services	Configure the installed announcement services	announcementserver: 10210 ComputerGRUU
Lync/SfB Contact Center UCMA B2B Agents	List of user agents where the announcement should not be played, separated by a new line.	RTCC/5.0.0.0 ACE RTCC/6.0.0.0 ACE RTCC/5.0.0.0 ICH RTCC/5.0.0.0 ICH-1.0.0.0 RTCC/5.0.0.0 TM-ICH RTCC/6.0.0.0 UCC RTCC/6.0.0.0 LUCS-ICH RTCC/4.0.0.0 ice RTCC/5.0.0.0 ice RTCC/6.0.0.0 ice

Step 4 - Click the



icon to save your settings.

Step 5 - The system will notify you that the changes need to be applied to the server by restarting the involved services. Execute the required tasks.

Step 6 - Repeat the steps on each Front-End / SBA / SBS server.

Configuring the Verba Media Collector and Proxy for announcement

Step 1 - Open the Verba web interface, click on the **System / Servers** and select the Verba Media Collector and Proxy (Proxy Server, Edge Server or Mediation server in case of mediation based recording), or select the appropriate Configuration Profile at **System / Configuration Profiles**.

Step 2 - Go to the **Change Configuration Settings** tab. Expand the **Media Collector and Proxy** node.

Step 3 - Under the **General** section provide the SIP URI of the announcement service(s) at the **Announcement Service Uris** setting.

Step 4 - Click the



icon to save your settings.

Step 5 - The system will notify you that the changes need to be applied to the server by restarting the involved services. Execute the required tasks.

Step 6 - Repeat the steps on each Proxy Server, Edge server or Mediation server in case of mediation based recording.

Configuring the Verba Passive Recorder for conference call announcement

Step 1 - Open the Verba web interface, click on the **System / Servers** and select the Recorder Server, or select the appropriate Configuration Profile at **System / Configuration Profiles**.

Step 2 - Go to the **Change Configuration Settings** tab, then expand the **Passive Recorder / Recording Announcement for Lync Conference** node.

Step 3 - Configure the following settings:

Configuration Parameter Name	Description	Sample Value
------------------------------	-------------	--------------

<p>Announcement Service Urls</p>	<p>Conference call announcement settings in the following format:</p> <p>https://announcement_server_IP_or_hostname:12222 Priority or List of IP addresses of FE/AVMCU servers</p> <ul style="list-style-type: none"> • Priority: The recorder service will balance the load amongst the announcement services with the same priority. • FE / AVMCU Preference: The recorder service selects the announcement service based on the IP address of the SfB/Lync FE / AVMCU used of the conference call in order to ensure that the same announcement service is selected by different recording services (even different recording services in different Verba clusters). In this case, there is no dynamic load balancing, and the FE / AVMCU IP addresses have to be split across multiple announcement servers manually in the configuration. <p>✓ Configuration for large multi-site deployments The configuration should consist of two parts:</p> <ul style="list-style-type: none"> • In the first part, the frontend IPs has to be assigned to the announcement servers. Each line represents an announcement server. Every announcement server has to be represented only once. Multiple IPs can be assigned to the same announcement server, but an individual IP can be assigned to only one announcement server (so an IP should show up only in one line). This part represents the primary announcement servers for each frontend. This part should be the same at all recorder configuration, regardless the site! Example: https://announcement1:12222 FE_IP1,FE_IP2 https://announcement2:12222 FE_IP3,FE_IP4,FE_IP5 https://announcement3:12222 FE_IP6 https://announcement4:12222 FE_IP7,FE_IP8 • The second part represents the failover announcement servers. This part can vary per site, based on the nearest announcement server. At this part, the priority should be set instead of the list of the IPs. For example: Site1: https://announcement2:12222 3 https://announcement3:12222 2 https://announcement4:12222 1 Site2: https://announcement1:12222 3 https://announcement3:12222 2 https://announcement4:12222 1 Site3: https://announcement1:12222 3 https://announcement2:12222 2 https://announcement3:12222 1 <p>So for example, the final configuration for Site1 should be something like this: https://announcement1:12222 FE_IP1,FE_IP2 https://announcement2:12222 FE_IP3,FE_IP4,FE_IP5 https://announcement3:12222 FE_IP6 https://announcement4:12222 FE_IP7,FE_IP8 https://announcement2:12222 3 https://announcement3:12222 2 https://announcement4:12222 1</p>	<p>Load balancing and failover configuration with priorities (2 announcement servers per datacenter):</p> <p>https://192.168.1.166:12222 0 https://192.168.1.167:12222 0 https://192.168.2.166:12222 1 https://192.168.2.167:12222 1</p> <p>Load balancing and failover configuration with FE / AVMCU preference (1 announcement server per data center):</p> <p>https://192.168.1.166:12222 192.168.1.210,192.168.1.211,192.168.1.217 https://192.168.1.167:12222 192.168.1.123,192.168.1.124</p>
---	--	--

Announcement Service Uri	The SIP addresses of the announcement service, one in a line. Required for hiding transfer information in metadata.	VerbaAnnouncement1@yourDomain.com VerbaAnnouncement2@yourDomain.com
---------------------------------	---	--

Step 4 - Click the



icon to save your settings.

Step 5 - The system will notify you that the changes need to be applied to the server by restarting the involved services. Execute the required tasks.

Step 6 - Repeat the steps on each Recording Server.

Configuring custom prompts for users (optional)

Available in version 8.3 and later

It is possible to configure custom notification sounds on a per user basis. To achieve this follow these steps:

Step 1 - Login to the **Announcement server**, and go to the **C:\Program Files\Verba\resources\announcement** folder.

Step 2 - Copy the .wma files to the **conference**, **inbound** and **outbound** folders.

Step 3 - Open the Verba web interface, click on the **System / Servers** and select the Media Repository server, or select the appropriate Configuration Profile at **System / Configuration Profiles**.

Step 4 - Click on the **Change Configuration Settings** tab. Expand the **Web Application** section.

Step 5 - Expand the **Lync recording Announcement** node, and add the names of the .wma files to the **PSTN Inbound Announcement Prompt Files** and the **Conference Announcement Prompt Files**, one in a line .

Step 6 - Click the



icon to save your settings.

Step 7 - The system will notify you that the changes need to be applied to the server by restarting the involved services. Execute the required tasks.

Step 8 - Repeat the steps on each Media Repository server.

To configure the custom prompt for the users please see the [User Configuration](#) configuration.

Configuring announcement transfer hiding (optional)

Available in version 8.3 and later

It is possible to hide the announcement transfer information using Verba Announcement service. To achieve this follow these steps:

Step 1 - Open the Verba web interface, click on the **System / Servers** and select the SfB/Lync Front-End / SBA / SBS server, or select the appropriate Configuration Profile at **System / Configuration Profiles**.

Step 2 - Go to the **Change Configuration Settings** tab, then expand the **SfB/Lync Call Filter / Recording Announcement** node.

Step 3 - Set **Hide transfer information from Announcement service** to **Yes**.

Step 4 - Click the



icon to save your settings.

Step 5 - The system will notify you that the changes need to be applied to the server by restarting the involved services. Execute the required tasks.

Step 6 - Repeat steps 1-5 on each SfB/Lync Front-End / SBA / SBS servers.

Step 7 - Navigate to **System / Servers** and select the Recording Server, or select the appropriate Configuration Profile at **System / Configuration Profiles**.

Step 8 - Click on the **Change Configuration Settings** tab. Expand the **Passive Recorder / Recording Announcement for Lync Conference** section.

Step 9 - At **Announcement Service Uris**, enter the SIP address of your announcement services.

Step 10 - Click the



icon to save your settings.

Step 11 - The system will notify you that the changes need to be applied to the server by restarting the involved services. Execute the required tasks.

Step 12 - Repeat steps 7-11 on each Recording Servers.

Configuring redirect on failed transfer (optional)

Available in version 9.0 and later

In the case of the incoming calls, it is possible to also play announcement when the callee is not available actually. In the cases like this, an alternative destination has to be specified where the incoming call will terminate instead of the original callee.

Step 1 - Open the Verba web interface, click on the **System / Servers** and select the Announcement server, or select the appropriate Configuration Profile at **System / Configuration Profiles**.

Step 2 - Go to the **Change Configuration Settings** tab, then expand the **SfB/Lync Recording Announcement / Advanced** node.

Step 3 - Redirect targets can be configured at the "**Redirect Targets for Failed Transfers**" setting. The format is the following:
sip_ui_or_line_number|response_code

One can be provided in each line. If the transfer fails, the service will try to redirect the call to the target with the matching response code. Wildcard (x) can be used in the response code.

Example

```
john_doe@adatum.com | 486  
peter_parker@adatum.com | 408  
bruce_wayne@adatum.com | 4xx
```

In this example, if the callee returns a busy (486) response, then the incoming call will be transferred to john_doe@adatum.com.

If the callee doesn't answer the call, just returns a timeout (408), then the incoming call will be transferred to peter_parker@adatum.com.

In the case of all other response codes starting with 4, the service will try to transfer the call to bruce_wayne@adatum.com, since it matching to all response codes starting with 4.

For the list of the response codes, see: https://en.wikipedia.org/wiki/List_of_SIP_response_codes

Step 4 - Click the



icon to save your settings.

Step 5 - The system will notify you that the changes need to be applied to the server by restarting the involved services. Execute the required tasks.

Step 6 - Repeat steps 1-5 on each Recording Servers.

Creating a Trusted Application Pool for the Verba Announcement Service

Create a Pool of Trusted Application Servers

All computers the application runs on must be added to the Lync / Skype for Business topology document. It is recommended that you create a separate computer pool for a trusted application instead of running the application in the same pool where other Lync / Skype for Business services are running. This step involves creating a new pool and adding application servers to it.

You can create the pool for the trusted application servers with the Lync / Skype for Business Server Topology Builder.

Step 1. On the Lync Frontend server open the **Lync Server Topology Builder**.

Step 2. Select the **Download Topology from existing deployment**.

Step 3. Right click on the **Trusted application servers** node and select the **New Trusted Application Pool** option.

Step 4. If you want to install only one Announcement Server select the **Single computer pool** and enter the **FQDN for your Announcement Server**, otherwise select the **Multiple computer pool** and enter the **FQDN of you new trusted application pool**. Click on the **Next**.

Step 5. If you selected the Multiple computer pool, add the **FQDNs of you Announcement Servers**. Click on the **Next**.

Step 6. Enable the **Associate next hop pool** checkbox and select your Lync pool where you creating the the Trusted Application Pool from the dropdown list. Click on the **Finish**.

Step 7. Click on the **Action -> Topology -> Publish** menu, and click **Next** for publishing the changes.

Optionally the Pool of Trusted Application Servers can be created using PowerShell Cmdlets

Step 1. As a Lync / Skype for Business Administrator launch **Lync / Skype for Business Server Management Shell** on a computer where it is installed.

Step 2. Create the application pool by running the **New-CsTrustedApplicationPool** cmdlet. In the following example, the FQDN of the pool of trusted application computers is 'verbaannouncement.contoso.com'. The Registrar pool FQDN is 'sfbpool1.contoso.com', Central Management Store replication is set to 'false', and the site ID is 'contoso'. The **ComputerFqdn** parameter specifies the FQDN of the first server in the trusted application pool. FQDN of this server is 'server1.contoso.com'.

```
New-CsTrustedApplicationPool -Identity verbaannouncement.contoso.com -RegistrarFqdn sfbpool1.contoso.com -CentralManagementStoreReplication false -SiteId contoso -ComputerFqdn server1.contoso.com
```

The FQDN of the application server should appear in the list of replicas.

Step 3. (Optional) If you want to deploy the recording announcement application on multiple servers, additional servers have to be added to the trusted application pool. Run the **New-CsTrustedApplicationComputer** cmdlet. In the following example, a new server with an FQDN of 'server2.contoso.com' is added to the trusted application pool whose FQDN is 'verbaannouncement.contoso.com'.

```
New-CsTrustedApplicationComputer -Identity server2.contoso.com -TrustedApplicationPool verbaannouncement.contoso.com
```

Step 4. Run the **Enable-CsTopology** cmdlet to create the appropriate trusted service entries in Active Directory for interoperability with Microsoft Office Communications Server 2007 R2.

```
Enable-CsTopology
```

Add a Trusted Service Port for the Application

To perform the steps of the following procedure, you must be in the Lync Server / Skype for Business Administrator role on the computer where Lync / Skype for Business Server Management Shell is installed. To add a trusted service port for the application:

Step 1. Launch **Lync / Skype for Business Server Management Shell** on a server where it is installed.

Step 2. Add your application to the application pool.

The following PowerShell cmdlet adds an application to the 'verbaannouncement.contoso.com' application pool, using port 6000, with application ID 'verbaannouncementapplication'. The provided pool name at the TrustedApplicationPoolFqdn have to match to the pool previously created. The application ID can be anything. If using a port other than 6000, then that also have to be configured in the Verba Announcement service configuration.

```
New-CsTrustedApplication -ApplicationId verbaannouncementapplication -TrustedApplicationPoolFqdn
```

Step 3. Run the **Enable-CsTopology** cmdlet to create the appropriate trusted service entries in Active Directory for interoperability with Microsoft Office Communications Server 2007 R2.

```
Enable-CsTopology
```

Using Microsoft Lync Server 2010 Control Panel you can view the application name, trusted application pool FQDN, and application port.

Create Active Directory Contact Object

The Active Directory contact object is similar to an Active Directory user object. This contact object gives the application a virtual identity in the form of a SIP URI or phone number. To create an Active Directory contact object, carry out the following steps. To perform the steps of the following procedure, you must be in the Lync Server Administrator role or Trusted Application Operator role, on a computer on which Lync Server Management Shell is installed. To create Active Directory contact objects:

Step 1. Launch **Lync / Skype for Business Server Management Shell** on a server where it is installed.

Step 2. Add an endpoint for the trusted application. In the following example, a new trusted application endpoint is added to the trusted application with an ID of 'verbaannouncementapplication', running on the trusted application pool whose FQDN is 'verbaannouncement.contoso.com'. The endpoint is assigned a SIP URI of 'sip:verbaannouncement@yoursipdomain.com' and a display name of 'Announcement Service'. The provided pool name at the TrustedApplicationPoolFqdn and the provided application ID have to match to the pool and application previously created. The SIP URI and the display name can be anything.

```
New-CsTrustedApplicationEndpoint -SipAddress sip:verbaannouncement@yoursipdomain.com -DisplayNan
```

(Optional) Assign dial plan and voice policy for the application endpoint in order to allow transfer calls to PSTN.

You can use one of the following commands to assign a new dial plan to the application endpoint:

```
Grant-CSDialplan -Identity "sip:verbaannouncement@yoursipdomain.com" -PolicyName "dial plan dis
```

You can use one of the following commands to assign a new voice policy to the application endpoint:

```
Grant-CsVoicePolicy -Identity "sip:verbaannouncement@yoursipdomain.com" -PolicyName "voice polic
```


Configuring SfB - Lync archive import

Overview

The Verba is able to import the archived conference/meeting content into Verba from the Skype for Business / Lync archives. It allows archiving the following meeting content:

- Whiteboard
- Polls and Q&A
- Files shared on the meeting
- Powerpoint shared on the meeting

This is done by the **Verba Import Service**.

Prerequisites

Step 1 - Verify the SfB/Archiving configuration to ensure that the meeting/conference content is properly archived using the Skype for Business storage option. For more information: <https://technet.microsoft.com/en-us/library/dn951419.aspx>

Step 2 - Make sure the server is part of the same domain where the SfB/Lync is deployed

Step 3 - If not domain user being used, then **create a new domain user account** for the Verba Import Service (e.g. svcverbaimport). This account can be the same as the one used at the other Verba servers.

Step 4 - Add the service user to the following groups:

- **CSArchivingAdministrator** on domain level
- **Local Administrators** on server level

Step 5 - Install [SfB/Lync Server Management Shell](#) on the **Media Repository server**.

Firewall configuration

Refer to [Firewall configuration for Skype for Business - Lync deployments](#) for more information.

Service activation

Follow the steps below to activate the required service on the Verba Media Repository Server.

Step 1 - Using the web application, navigate to the **Administration / Verba Servers** page and select the Media Repository (or Single) Server.

Step 2 - Click on the **Service Activation** tab.

Step 3 - **Activate** the **Verba CDR and Archived Content Importer Service** using the



(Activate this service) button.

Configuring Verba for archive import

Step 1 - Go to the **Data | Import Sources** menu.

Step 2 - Click on the **Add New Import Source** menu in the upper right corner.

Step 3 - Provide a **name** for the new data source and select **Lync/SfB Archive** at the **Type** setting.

Step 4 - Provide the **Archive Server FQDN** and specify the **Server Type** according to the SfB/Lync version. Provide a **Work Folder** for the data source (recommended: C:\Program Files\Verba\work\archive_importer), then click **Save**.

Name *	<input type="text" value="SfB Archive"/>
Type *	<input type="text" value="Lync/SfB Archive"/>

Archive Server FQDN	<input type="text" value="testsfbsql.verbatest.local"/>
Work Folder	<input type="text" value="C:\Program Files\Verba\work\archive_importer"/>
Server Type	<input type="text" value="Skype for Business"/>

Step 5 - Go to the **Data \ Data Management Policies** menu.

Step 6 - Click on the **Add New Data Management Policy** menu in the upper right corner.

Step 7 - Provide a **name** for the new data policy and select **Data Import** at the **Action** setting.

Step 8 - Add the import source previously created from the **Available Import Sources** by clicking on the **Add** button.

Name*

Enabled*

Priority*
Higher priority policies are processed first when the 'older than' dates are equal.

Action*

Import Source Type*

Available Import Sources

Import Sources*

Selected Import Sources

SfB Archive (Lync/SfB Archive) - Archive Server: testsfbsql.verbatest.local, Work Folder: C:\Prograr

Enable Recording Rules

Execute Only on Selected Servers

TESTMR1.VERBATEST.LOCAL

Custom Schedule

Step 9 - Click **Save**.

Configuring extensions

After finalizing the configuration of the recording services, make sure you have added the extensions you want to record to the Verba extension list. This can be done manually ([Extension list](#)) or using [Active Directory Synchronization](#).

SfB - Lync proxy load balancing and failover design

Overview

Verba Media Collector and Proxy service can be used as a standalone proxy, or multiple Media Collector and Proxy services can be set up as a proxy for load balancing, failover or for geographic routing.

Configuring High Availability and Geographic Routing

On Verba SfB / Lync Call Filter services the following can be configured:

- priority of the proxy servers
- endpoint subnets assigned to the proxy servers

The configuration can be provided in the Verba SfB / Lync Filter configuration, at the **SfB/Lync Call Filter \ Proxy Server Based Relay Settings \ Verba Proxy Servers** setting. The configuration tool can be opened by clicking on the



icon at the existing connections, or by adding a new proxy connection with the



icon.

The configuration can be provided at the **Priority or Subnets** settings. There can be provided priority only, subnet only, or both with the subnet|priority format.

Configuration examples

Example 1 - Three proxies with load-balancing

Requirements

In the proxy connection configurations, either no priority or the same priority at all proxies can be provided. No priority means priority 0.

Configuration overview

Proxy connection 1 setting	1
Proxy connection 2 setting	1
Proxy connection 3 setting	1

Example 2 - Three proxies with three-level failover

Requirements

Different priorities should be provided in the proxy connection configurations.

Configuration overview

Proxy connection 1 setting	3
Proxy connection 2 setting	2

Proxy connection 3 setting	1
----------------------------	---

Example 3 - Two proxies for manual subnet-based load-balancing or for geographical routing

Requirements

The endpoint subnets should be provided at the proxy connections. Multiple subnets can be provided, separated by a comma.

 If multiple proxies are provided with the same subnet configuration, then there will be failover only between the proxies.


Configuration overview

Proxy connection 1 setting	192.168.1.0/24,192.168.2.0/24
Proxy connection 2 setting	10.0.0.0/8

Example 4 - Combining priorities and subnets for geographical routing in large deployments

Requirements

The subnets of the branch sites should be provided with higher priority at the branch site proxy connections. The proxy connection of the central site (where most of the users are located, and there are plenty of subnets) should be provided with lower priority, without subnets.

 If subnet-based filtering is used with a specific priority, then the subnet-based filtering have to be used at the other proxy connections also on the same priority.

Proxy connection 1 setting	192.168.1.0/24,192.168.2.0/24 2
Proxy connection 2 setting	192.168.3.0/24,192.168.4.0/24 2
Proxy connection 3 setting	1

Configuring Microsoft Teams Recording

For the general overview of the Microsoft Teams recording refer to the [Microsoft Teams](#) article.

Prerequisites

Before starting the deployment of the Verba system for Microsoft Teams, the following prerequisites has to be met:

- **Virtual machines** have to be created in Azure with Recording Server roles which will host the Verba Microsoft Teams Bot service and the Unified Call Recorder service. It is recommended to have the servers in the same region as the Teams tenant. The servers need to have a **public IP address**.
- For resilient and/or high volume configurations, multiple virtual machines (running the Recording Server role) has to be deployed. In order to distribute the load across multiple Verba Microsoft Teams Bot services, an **Azure Application Gateway** has to be deployed in front of the VMs.
- A **new CNAME entry** has to be created in a public domain, pointing to the Verba virtual machines in Azure.
- A **publicly signed certificate** is required for the virtual machines. **Only CSP** certificates are supported (CNG/KSP certificates are not supported). The SAN configuration of the certificate must include the virtual machines (with the public domain). Using asterisk in the SAN is accepted. The **private key** of the certificate has to be **exportable**.
- Configure the **firewall rules** both on the operating system and the Azure virtual machine level.
- The Microsoft Graph Communications Calling SDK does not support FIPS 140-2 validation. Make sure the validation is disabled on the server. Please refer to this documentation on how to disable [FIPS 140-2 Validation](#)

The following permissions and roles required to configure the system:

- Azure: Application Administrator or Global administrator
- Office 365 / Teams: Global Administrator
- Windows: Local Administrator
- Verba: System Administrator

Creating the Microsoft Teams Recording Bot

Step 1 - [Registering the Bot](#)

Step 2 - [Whitelisting the App](#)

Step 3 - [Creating a Compliance Policy](#)

Configuring Verba for Microsoft Teams recording

Step 4 - [Configuring the Verba Microsoft Teams Bot and Unified Call Recorder Services](#)

Adding Users for Recording

In order to enable recording for the users, first, the previously created compliance policy has to be assigned to the user. For the configuration steps, see [Administering Compliance Policy for Microsoft Teams Users](#).

Once the compliance policy is set, create the **users** and the **extensions** on the Verba side. This can also be done via [Active Directory Synchronization](#). The extensions have to match the Azure AD object ID of the users (not the User Principal Name or email address).

Selective recording rules can only also be applied to record calls/meetings where there is an external participant or the meeting was scheduled, etc. For more information see [Microsoft Teams selective recording settings](#).

Controlling recording using the Teams Application

The Verint Capture for Microsoft Teams - Recording Controls Application, is a native Microsoft Teams Application that allows privileged Microsoft Teams users to control compliance recording, by starting and or stopping the VFC Compliance Recorder. For more information, see [Microsoft Teams Application](#).

Adding a Verba Tab to Microsoft Teams

For adding a Verba tab to the Microsoft Teams client, see [Adding Verba Tab to a Microsoft Teams Channel](#).

If SSO is being used, then it is required to modify the settings of the web application to make it working in the Microsoft Teams client. This will lower the security of the web application. For the configuration steps, see [Enabling the Verba Web Application in 3rd Party Frame](#).

Recording Meeting Subjects as Metadata

The Verba Microsoft Teams Bot service checks several Graph API calls in order to gather the meeting subjects. In order to make sure that the Bot has the ability to gather this information, besides the Calendars.Read permission, additional policy settings may be required.

For the configuration steps, see: [Configuring Access Policy for Meeting Metadata](#)

Adding Verba Tab to a Microsoft Teams Channel

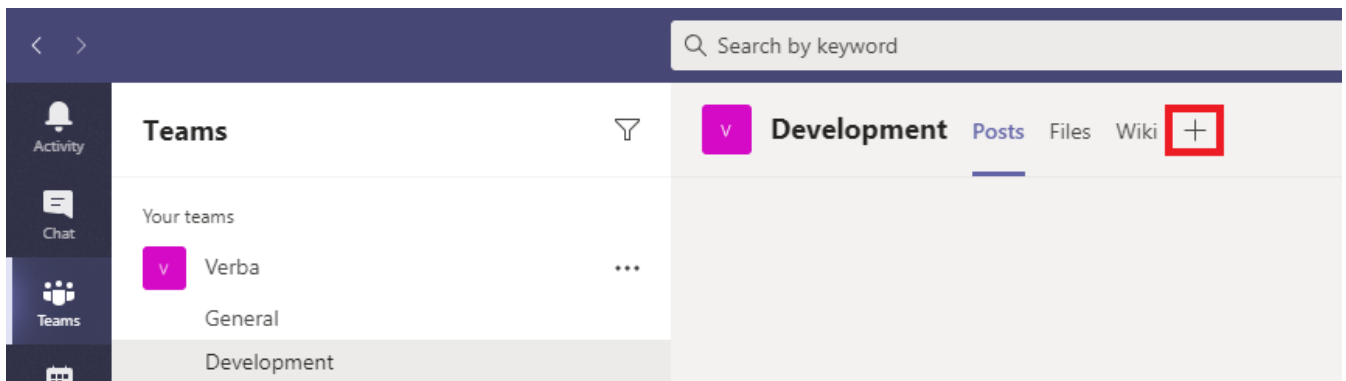
It is possible to embed the Verba Web Application into the Microsoft Teams client.

If SSO is being used, then it is required to modify the settings of the web application to make it working in the Microsoft Teams client. This will lower the security of the web application. For the configuration steps, see: [Enabling the Verba Web Application in 3rd Party Frame](#)

Step 1 - Log into Microsoft Teams.

Step 3 - Go to Teams, and select a channel.

Step 4 - On the top, click on the + icon to add a new tab.



Step 5 - Select the Website option.



Website

Step 6 - Provide a Tab name (it can be anything), then provide the URL of the Verba Web Application.



Website

About ×

Tab name

Verba



URL*

https://verba.contoso.com



*Make sure you're only linking to sites that start with 'https://' and contain trustworthy web content. That way, you and your team can stay secure.



Post to the channel about this tab

Back

Save

Step 7 - Click **Save**.

Administering Compliance Policy for Microsoft Teams Users

In order to complete the steps below, you must have a Teams Service Administrator role.

In the case of Microsoft Teams, the invitation of the Verba Microsoft Teams Bot and the recording is triggered based on the compliance policy assignment of the users.

The registration consists of the following steps:

- [Prerequisites](#)
- [Accessing the tenant via PowerShell](#)
- [Assigning a Compliance Policy to a user](#)
- [Removing the Compliance Policy from a user](#)

Prerequisites

Step 1 - Download and install [PowerShell 5.1](#).

Step 2 - Open PowerShell as administrator.


Step 3 - Install the NuGet package provider module by running the following command:

```
Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force
```

Step 4 - Install the Microsoft Teams module by running the following command:

```
Install-Module MicrosoftTeams
```

Accessing the tenant via PowerShell

 **Separate Azure tenants for the recording provider (bot) and for the Teams environment to record**
In the case when the recorded Teams environment and the recording bot are in separate Azure tenants, the following steps have to be done in the Teams tenant.

Follow the steps below to assign a compliance policy to a user:

Step 1 - Open **PowerShell** as administrator.

Step 2 - Execute the following command:

```
Connect-MicrosoftTeams
```

Step 3 - A login prompt will show up. Provide the user credentials.

Assigning a Compliance Policy to a user

Step 4 - Execute the following command. Replace the <User's UPN> part with the recorded user's UPN. Replace the <PolicyName> part with the name of the compliance policy (Whitelisting the App and Creating the Compliance Policy - Step 9)

```
Grant-CsTeamsComplianceRecordingPolicy -Identity '<User's UPN>' -PolicyName '<PolicyName>'
```

Once the compliance policy is assigned to the user, it may take some time to take effect. The policy assignment of the user can be checked with the following command. Replace the <User's UPN> part with the recorded user's UPN.

```
Get-CsOnlineUser -Identity '<User's UPN>' | Select-Object -ExpandProperty 'TeamsComplianceRecordi
```

Removing the Compliance Policy from a user

Follow the steps below to remove the compliance policy from a user:

Step 5 - Execute the following command. Replace the <User's UPN> part with the recorded user's UPN. Leave PolicyName empty to remove the policy.

```
Grant-CsTeamsComplianceRecordingPolicy -Identity '<User's UPN>' -PolicyName ''
```

It may take some time to take effect. The policy assignment of the user can be checked with the following command. Replace the <User's UPN> part with the recorded user's UPN.

```
Get-CsOnlineUser -Identity '<User's UPN>' | Select-Object -ExpandProperty 'TeamsComplianceRecordi
```

Configuring the Verba Microsoft Teams Bot and Unified Call Recorder Services

In order to complete the steps below, you must have System Administrator role in Verba.

It is recommended to co-locate the Verba Microsoft Teams Bot service and the Verba Unified Call Recorder service on the same Azure virtual machine.

The registration consists of the following steps:

- [Enabling the services](#)
- [Configuring the Verba Microsoft Teams Bot service](#)
- [Configuring the Verba Unified Call Recorder service](#)
- [Starting the services](#)
 - [Updating the Server Certificate for Microsoft Teams Bot](#)
- [Configuration reference](#)

Enabling the services

Step 1 - Log in to the Verba web interface and go to **System \ Servers** menu.

Step 2 - Select your Recording (Bot) Server from the list, then click on the **Service Activation** tab.

Step 3 - Activate the **Verba Microsoft Teams Bot Service** and the **Verba Unified Call Recorder Service** by clicking on the



icon.

Configuring the Verba Microsoft Teams Bot service

Step 4 - Click on the **Change Configuration Settings** tab.

Step 5 - Expand the **Microsoft Teams Bot** node.

Step 6 - Under **General**, provide a regex pattern at the **Internal Tenant IDs, Numbers Pattern** setting. This pattern should cover all the internal numbers and domains.

Step 7 - Under **General / Recorder Connection**, configure the authentication credentials for the connections with the recording service. Define the **Authentication User** and **Authentication Passwords** values. These credentials will be used later when configuring the connections in the recorder service.

Step 8 - Under **Microsoft Teams**, configure the following settings (see configuration reference for more details):

Setting Name	Description
Bot Service DNS Name	The FQDN of the virtual machine
Bot Service Public CName	The CNAME DNS entry created for the server
Service Certificate	The thumbprint of the publicly signed certificate used previously for binding the ports
Bot Application ID	The App ID of the bot (see related step at Registering the Microsoft Teams Bot in Azure)
Bot Application Secret	The secret created for the bot (see related step at Registering the Microsoft Teams Bot in Azure)

Microsoft Teams Tenant ID	The ID of the Azure tenant where the bot was created (see related step at Registering the Microsoft Teams Bot in Azure)
Query Hosting Tenant's Azure AD	Defines if the bot service will query the Azure Active Directory for User Principal Names (UPN)
Public IP Address	The public IP address of the virtual machine

Microsoft Teams

Bot Service DNS Name:	<input checked="" type="checkbox"/>	verbateamsbot.westeurope.cloudapp.azure.com
Bot Service Public CNAME:	<input checked="" type="checkbox"/>	verbateamsbot.verba.com
Service Certificate:	<input checked="" type="checkbox"/>	136CCF6CCF27080AC155F0298E08E4ADA749BD08
Service Certificate Key File:	<input type="checkbox"/>	
Service Certificate Key File Password:	<input type="checkbox"/>	*****
Bot Application ID:	<input checked="" type="checkbox"/>	a3dfe84e-6ad3-4074-9f61-b3ebf98bec9f
Bot Application Secret:	<input checked="" type="checkbox"/>	*****
Bot Application Authentication Certificate:	<input type="checkbox"/>	
Authentication Certificate Key File:	<input type="checkbox"/>	
Authentication Certificate Key File Password:	<input type="checkbox"/>	*****
Microsoft Teams Tenant ID:	<input checked="" type="checkbox"/>	df530937-2dd6-44ed-8ae9-77a9db3f82d8
Query Hosting Tenant's Azure AD:	<input checked="" type="checkbox"/>	Yes
Public IP Address:	<input checked="" type="checkbox"/>	52.142.217.198
Bot Service Port:	<input type="checkbox"/>	9440
Call Control Port:	<input type="checkbox"/>	10100
Media Control Port:	<input type="checkbox"/>	8445
Media Port Range Begin:	<input type="checkbox"/>	16384
Media Port Range End:	<input type="checkbox"/>	65535
Recording Notification:	<input type="checkbox"/>	Yes

Configuring the Verba Unified Call Recorder service

Step 9 - Expand the **Unified Call Recorder \ Media Recorder \ Microsoft Teams** node.

Step 10 - At the **Teams Bot Servers** setting, click on the



icon to add a new connection.




Step 11 - In the right panel, provide the username and password configured in the **Verba Microsoft Teams Bot Service** above for the connections. At the **Host** setting, select the Verba Recording (Bot) server from the dropdown menu. Set the **Port** to **10501**.

Remote Media Recording Servers

Protocol	<input type="text" value="vrp"/>
User	<input type="text" value="verba"/>
Password	<input type="password" value="*****"/>
Host	<input type="text" value="verbateamsbot"/>
Port	<input type="text" value="10501"/>
Priority	<input type="text"/>

Step 12 - Click on the **Save** button at the bottom. You will see the bot connection added to the configuration.

- Unified Call Recorder
 - Media Recorder
 - Incoming Connection
 - Microsoft Teams


Teams Bot Servers:   

Step 13 - Save the changes by clicking on the



icon.

Step 14 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

 There are tasks to be executed regarding the configuration of this Verba Server.
If you would like to execute these tasks now, please [click here](#) .

Starting the services

Step 15 - Click on the **Service Control** tab.

Step 16 - Start the **Verba Microsoft Teams Bot Service** and the **Verba Unified Call Recorder Service** by clicking on the



icon.

Updating the Server Certificate for Microsoft Teams Bot

Manual binding of certificates

Prior to v9.5.3.5973 (2020 June) certificates had to be manually bound to HTTPS ports. While this does not affect normal operation, during the renewal process the old binding must be removed, otherwise, the old certificate will be used.

The service automatically binds and unbinds the certificate, in order to check if the certificate is manually bound follow these steps:

Step 1 - Log in to the Verba Bot virtual machine in Azure, and open an administrator command prompt.

Step 2 -Stop the Verba Microsoft Teams service and Verba System Monitor service

Step 3 - Run the following command in the command prompt, replace the ip_address part with the public IP address of the server

```
show sslcert ipport=ip_address
```

The binding can be deleted by following these steps:

Step 1 - Log in to the Verba Bot virtual machine in Azure, and open an administrator command prompt.

Step 2 -Stop the Verba Microsoft Teams service and Verba System Monitor service

Step 3 - Remove the bound certificate to the TCP ports 9440 and 10100 with the following command. Replace the ip_address part with the public IP address of the server

```
netsh http delete sslcert ipport=ip_address:port
```

Configuration reference

	Setting Name	Description
General /Recorder Connection	Recording Director Listening Port	The TCP/TLS port where the bot service is listening for the Recording Director connections from the Verba Recorder Service
	Media Recorder Listening Port	The TCP/TLS port where the bot service is listening for the Media Recorder connections from the Verba UI Service.
	Authentication User	Username for authenticating with the Verba Unified Call Recorder Service.
	Authentication Password	Password for authenticating with the Verba Unified Call Recorder Service.
General	Internal Tenant IDs, Numbers Pattern	<p>A regular expression that defines the internal Microsoft Teams tenant IDs or phone numbers to identify the recorded calls properly.</p> <p>E.g.:</p> <pre>^(b6fd8d51-3271-4896-bb8b-4d7390b51784 f4552cc7-3685-4ffb-bf68-79bb0ab4b007)([0-9]{5})\$</pre> <p>This regular expression considers two tenants (b6fd8d51-3271-4896-bb8b-4d7390b51784, f4552cc7-3685-79bb0ab4b007) and every 5 digit numbers that is starting with 1 to 4 as internal.</p> <p>For more information, see Conversation direction detection using internal domain and number patterns.</p>
	Record Non-configured Extensions	Defines if the bot service has to record non-configured extensions.
	Compress RAW audio to G.711	Defines if the bot service transcodes the original PCM audio stream to G.711 before sending the data to the recorder.

Bidirectional /Stereo Recording	Defines if the bot service subscribes for unmixed audio stream in the Microsoft Teams call.	
Number of Recorded Video Participants	Defines how many video streams are recorded per call, including the video streams of the recorded user.	
Preferred Video Resolution	The video resolution used when the bot subscribes to the video streams of the participants. Microsoft Teams video up to the resolution requested during the subscription. The resolution can be lower based on network/capacity.	
Preferred Screen Share Resolution	The video resolution used when the bot subscribes to the screen share streams of the participants. Microsoft Teams video up to the resolution requested during the subscription. The resolution can be lower based on network/capacity.	
Separated Screen Share Record	Defines if a separated record is created for the screen share modality. The separate call includes the audio and video streams of the participants.	
Start Recording After Recorded User Joined	<p>Defines if the bot waits for the join event of the recorded user before it starts recording a meeting. This setting is for meetings, for P2P and PSTN calls, the bot always waits for the recorded user join event.</p> <p>If the configuration is set to 'Yes', the bot will start the recording when it identifies the recorded user on the call. Also, the bot will start streaming media to the recorder after the recorded user is identified in the call.</p> <p>If the configuration is set to 'No', the bot will trigger recording after it processed the first participant of the call. The service will also stream every media packet to the recorder without waiting for the recorded user to join the call.</p>	
Block Calls when Recording Server Unavailable	If there is no available recorder, the bot will not join the call. If the Microsoft Teams recording policy is in strict mode, it will prevent the establishment of the call. If the bot cannot fail-over to another recorder mid-call, the bot will disconnect from the call.	
Number of Tries to Find a New Recorder for an Ongoing Call	Defines the number of tries after a recorder disconnects from the bot service, and the bot service tries to find another online Unified Call Recorder service/server.	
Interval between Tries to Find a New Recorder for an Ongoing Call	Defines the interval between tries when a recorder disconnects from the bot service, and the bot service tries to find another online Unified Call Recorder service/server.	
Microsoft Teams	Bot Service DNS Name	The FQDN of the virtual machine hosting the bot service.
	Bot Service Public CNAME	CNAME entry on the public trusted domain which points to the public IP (ILPIP) of the virtual machine hosting the bot service.
	Service Certificate	The thumbprint or the file path of the public domain's certificate. If the certificate is in the WCS, it has to have a private key. Only CSP certificates are supported (CNG/KSP certificates are not supported!)

Service Certificate Key File	The key file if the certificate is files based.
Service Certificate Key File Password	Password for the key file
Bot Application ID	The Application ID generated during the bot registration. Format: GUID
Bot Application Secret	The Application secret generated during the bot registration.
Bot Application Authentication Certificate	The authentication certificate uploaded on the Certificates and Secrets page of the Azure AD App registration application secret is ignored.
Authentication Certificate Key File	The key file if the certificate is files based
Authentication Certificate Key File Password	Password for the key file
Microsoft Teams Tenant ID	The ID of the Microsoft Teams Tenant where the bot is hosted. Format: GUID
Query Hosting Tenant's Azure AD	Defines if the bot will query the Azure Active Directory of the tenant for additional user information such as Name.
Public IP Address	The public IP address assigned to the virtual machine hosting the bot service.
Bot Service Port	HTTPS port where the bot is listening for call invites from Microsoft Teams.
Call Control Port	HTTPS port where the bot is listening for call control messages from Microsoft Teams.
Media Control Port	HTTPS port used by the Microsoft Media SDK for media control messages.
Media Port Range Begin	Beginning of the UDP port range for the media streams.
Media Port Range End	End of the UDP port range for the media stream.
Recording Notification	Global notification setting, if turned off, the user settings won't be taken into account.

	Bot Grouping	<p>Turns on Microsoft Teams Bot Grouping capability. If enabled, the bot service answers the call with the cc capacity. Based on the capacity, Microsoft Teams will invite the recording bot for the recorded meeting o number of capacity if the recorded users share the same compliance recording policy.</p> <p>When the bot grouping is enabled, the following features are not supported for the user handled by the b</p> <ul style="list-style-type: none"> • Video/ Screen Share recording • Controlled recording • Never record (recording mode) • record only if external user is participating • record video only for external participants • record only scheduled meeting
	Bot Group Participant Capacity	Defines the capacity of the bot grouping feature
Advanced	Microsoft API Endpoint	Base URL of the Microsoft Graph API. All API messages from the bot are sent to the URL.

Creating a Microsoft Teams Compliance Policy

In order to complete the steps below, you must have Global Administrator or Teams Service Administrator role.

At least one compliance policy has to be created in Teams which is then assigned to recorded users. Multiple policies can be configured and assigned to different bots.

For more information on policies, see <https://docs.microsoft.com/en-us/powershell/module/skype/set-csteamscompliancepolicy>

The policy configuration consists of the following steps:

- [Prerequisites](#)
- [Creating a Teams Compliance Recording Policy](#)
- [Changing the Compliance Recording Policy settings](#)

Prerequisites

Step 1 - Download and install [PowerShell 5.1](#).

Step 2 - Open PowerShell as administrator.

Step 3 - Set the security protocol to TLS 1.2 with the following command:

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
```


Step 4 - Install the NuGet package provider module by running the following command:

```
Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force
```

Step 5 - Install the Microsoft Teams module by running the following command:

```
Install-Module MicrosoftTeams
```

Accessing the tenant via PowerShell

 **Separate Azure tenants for the recording provider (bot) and for the Teams environment to record**
In the case when the recorded Teams environment and the recording bot are in separate Azure tenants, the following steps have to be done in the Teams tenant.

Step 1 - Open **PowerShell** as administrator.

Step 2 - Execute the following command:

```
Update-Module MicrosoftTeams
```

Step 3 - Execute the following command:

```
Connect-MicrosoftTeams
```

Step 4 - A login prompt will show up. Provide the user credentials.

Creating a Teams Compliance Recording Policy

Step 5 - Execute the following command. At the <Policy Description> part, provide some description. At the <PolicyName> part, provide a name.

```
New-CsTeamsComplianceRecordingPolicy -Enabled $true -Description '<Policy Description>' -Identity
```

Step 6 - Execute the following command. Replace the <PolicyName> parts with the name provided in the previous command. Replace the <ObjectId> part with the Object ID gathered at the previous part of the configuration (Whitelisting the Microsoft Teams Bot App - Step 6).

```
Set-CsTeamsComplianceRecordingPolicy -Identity '<PolicyName>' -ComplianceRecordingApplications @(
```

Step 7 (Optional - 2N recording) - If 2N recording will be used, then execute the following command. Replace the <ObjectId> part with the ID from the results of the previous command and the <ObjectId_of_Bot2> part with the ID from the result of **Step 8** here: [Whitelisting the Microsoft Teams Bot App](#).

```
Set-CsTeamsComplianceRecordingApplication -Identity 'Tag:<PolicyName>/<ObjectId>' -ComplianceReco
```

Changing the Compliance Recording Policy settings

The Teams Compliance Recording Policy allows the following configuration options:

Name	Description	Default Setting
RequiredBeforeMeetingJoin	Defines if the bot has to join the call before the recorded user can join the meetings	1 (On)
RequiredBeforeCallEstablishment	Defines if the bot has to join the call before the recorded user can place or receive calls	1 (On)
RequiredDuringMeeting	Defines if the recorded user will be disconnected from the meetings if the recorder bot connection is lost	1 (On)
RequiredDuringCall	Defines if the recorded user will be disconnected from the call if the recorder bot connection is lost	1 (On)

⚠ It is strongly recommended to **use the default settings (strict mode)** for the compliance recording policies. The default settings ensure that if, for some reason, the bot cannot join or disconnects from the call/meeting, the recorded user will be disconnected automatically to avoid compliance issues. There is no failover or automatic retry mechanism implemented on the Teams side.

Follow the steps below to change the settings:

Step 8 - Execute the following command to get the ID of the compliance recording application and the name of the compliance recording policy. It will return the name of the compliance recording policy in the **Identity** field. Take note of the value of the **Identity** field (after the Tag: part). It also returns the compliance recording application ID. Take a note of the identifier which is displayed after **ComplianceRecordingApplications : {Id=**.


```
Get-CsTeamsComplianceRecordingPolicy
```

```
PS C:\Users\Janos.Bodnar> Get-CsTeamsComplianceRecordingPolicy
Identity                : Global
ComplianceRecordingApplications : {}
Enabled                 : False
WarnUserOnRemoval      : True
Description             :
Identity                : Tag:Norbi_Test
```

```
ComplianceRecordingApplications : {Id=7042623d-1111-11e1-905e-000000000000; RequiredBeforeMeetingJoin=True;
RequiredBeforeCallEstablishment=True; RequiredDuringMeeting=True; Required
DuringCall=True; ConcurrentInvitationCount=1}
Enabled : True
WarnUserOnRemoval : True
Description :
```

Step 9 - Execute the following commands to change the compliance recording policy options. Replace the <PolicyName> and the <ComplianceApplicationId> parts with the values received in the previous command. This example below turns off all restrictions.

```
Set-CsTeamsComplianceRecordingApplication -Identity '<PolicyName>/<ComplianceApplicationId>' -Req
```

 Changing these parameters of an existing compliance recording policy that is already granted to a recorded user might take hours to take effect on the user's calls & meetings. As an alternative, we recommend creating a new compliance recording policy (see Step 7) with all the parameters having the same values as before, except the PolicyName that should be different; setting the new policy's parameters using the Set-CsTeamsComplianceRecordingApplication command; then granting this policy to the recorded user (see [Administering Compliance Policy for Microsoft Teams Users](#)) that takes effect almost immediately. Of course, if you have a policy already set up with the desired parameter values, it's enough to grant that policy to the user, no need to create another one with the same settings.

Enabling the Verba Web Application in 3rd Party Frame

Because of the default security settings of the Verba Web Application, displaying the webapp in a 3rd party frame is not allowed. The following steps describe how to turn off this security feature.

Step 1 - Log in to the Verba Media Media Repository (or Single) server.

Step 2 - Go to the `[APPLICATION_FODLER]\tomcat\conf` folder.

Step 3 - Open the `web.xml` file for editing.

Step 4 - Remove or comment out the following lines:

```
<filter>
  <filter-name>httpHeaderSecurity</filter-name>
  <filter-class>org.apache.catalina.filters.HttpHeaderSecurityFilter</filter-class>
  <async-supported>true</async-supported>
  <init-param>
    <param-name>antiClickJackingOption</param-name>
    <param-value>SAMEORIGIN</param-value>
  </init-param>
</filter>
```

Step 5 - Remove or comment out the following lines too:

```
<filter-mapping>
  <filter-name>httpHeaderSecurity</filter-name>
  <url-pattern>/*</url-pattern>
  <dispatcher>REQUEST</dispatcher>
</filter-mapping>
```

Step 6 - Save the changes.

Step 7 - Restart the **Verba Web Application** service in the Services console.

Registering the Microsoft Teams Bot in Azure

In order to complete the steps below, you must have Application Administrator or Global administrator role in Azure.

The registration consists of the following steps:

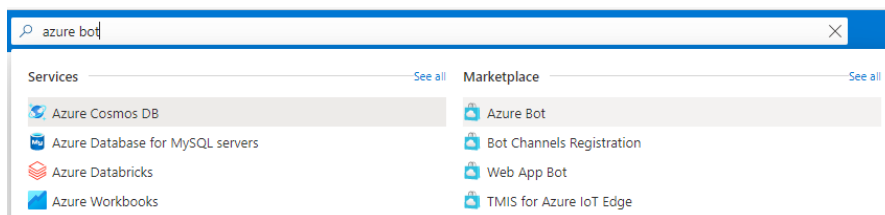
- [Creating a bot channel registration](#)
- [Adding a Teams Channel to the Bot Service](#)
- [Configuring authentication for the bot](#)
- [Configuring permissions to the bot](#)
- [Granting admin consent to the permissions](#)
 - [Multi-Tenant configuration:](#)
- [2N Recording](#)
- [Protected API Access for Chat Recording](#)

The following steps have to be done only once per bot. Once it's done, the bot can be used in multiple Azure tenants.

Creating a bot channel registration

Step 1 - Log in to the [Azure portal](#).

Step 2 - Search for **Azure Bot** in the search box on the top, then click on the link under the **Marketplace** section.



Step 3 - In the left panel, provide a unique name at the **Bot handle**, then select the **Subscription**, the **Resource group**. Set the **Type of App** to either **Single Tenant** or **Multi Tenant**. If the Bot will be used by multiple tenants, then select Multi Tenant.

Registering the Microsoft Teams Bot using Azure CLI and PowerShell

The Microsoft Teams Bot can be also registered using Azure CLI and PowerShell commands.

Step 1 - Download and install the [Azure CLI](#).

Step 2 - Open PowerShell and log in to Azure using the [az login](#) command. For example:

```
az login -u "[user_UPN]" -p
```

Step 3 - Create the App registration using the [az ad app create](#) command. Provide an **App secret** also. When it is done, take a note of the **App Id**; it will be needed in the later commands, in Verba configuration, and in the Teams recording policy.

```
$app = az ad app create --c  
$appID = $app.appId  
echo $appID
```

Step 4 (Optional) - Assign an user to the App registration as owner using the [az ad app owner add](#) command:

```
az ad app owner add --id $a
```

Step 5 - Add permissions to the App registration using the [az ad app permission add](#) command:

```
az ad app permission add --
```

Step 6 (Optional) - If the same App Registration will be used for Chat

Basics Tags Review + create

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Bot handle * ⓘ

Subscription * ⓘ

Resource group * ⓘ [Create new](#)

Pricing

Select a pricing tier for your Azure Bot resource. You can change your selection later in the Azure portal's resource management. Learn more about available options, or request a pricing quote, by visiting the [Azure Bot Services pricing](#)

Pricing tier * **Standard** [Change plan](#)

Microsoft App ID

A Microsoft App ID is required to create an Azure Bot resource. If your bot app doesn't need to access resources outside of its home tenant and if your bot app will be hosted on an Azure resource that supports Managed Identities, then choose option User-Assigned Managed Identity so that Azure takes care of managing the App credentials for you. Otherwise, depending on whether your bot will be accessing resources only in its home tenant or not, choose either Single tenant or Multi tenant option respectively.

Type of App

Step 4 - Click on the **Review + Create** button and if the configuration is correct the **Create** button again. Creating the Azure Bot may take some seconds. Azure will actually create an App Registration and a Bot Service assigned to it.

recording also, then add the following permissions also:

```
az ad app permission add --
```

Step 7 - Grant admin consent using the [az ad app permission admin-consent](#) command:

```
az ad app permission admin-
```

Step 8 - Create the Bot channels registration using the [az bot create](#) command:

```
az bot create -n "[bot_char
```

Step 9 - Add the Teams channel to the Bot channels registration using the [az bot msteams create](#) command:

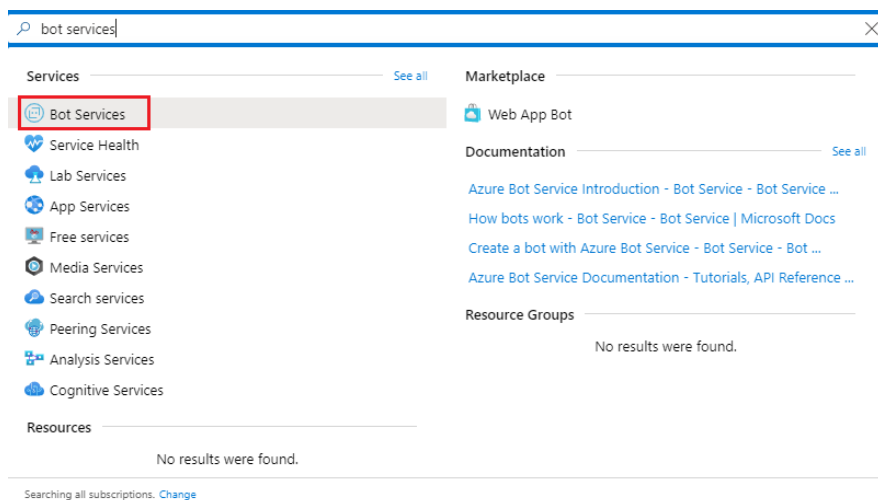
```
az bot msteams create -n "[
```

Step 10 (Optional) - If the Chat recording will be used, the prteted API access has to be requested. See **Protected API Access for Chat Recording** section at the bottom.

Adding a Teams Channel to the Bot Service

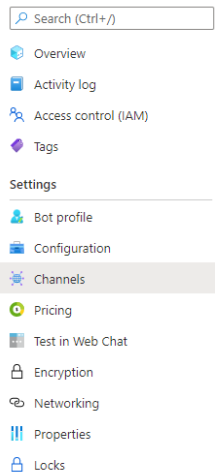
Step 5 - Once the Bot Channels Registration is completed, search for **Bot Services** in the search box on the top, then click on the Bot Services link under the **Services** section.

(Alternatively, the Bot Services can be also found by opening the **hamburger menu** in the upper right corner, then selecting **All services**, then the **AI + machine learning** category.)



Step 6 - Select the Bot Service from the list that was created previously using the name provided at Step 3 (Bot handle).

Step 7 - In the second left panel, under the **Settings** section, click on the **Channels** menu.



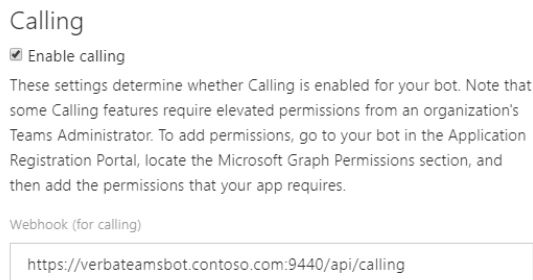
Step 8 - Under the **Available channels** section select **Microsoft Teams** option.

Step 9 - Accept the terms of service, select the **Microsoft Teams Commercial** option, then click **Apply**.

Step 10 - Select the **Calling** tab, then tick the **Enable calling** checkbox.

Step 11 - At the **Webhook (for calling)** setting, provide the following URL:
https://verba_bot_vm.domain.com:9440/api/calling

Replace the verba_bot_vm part with the hostname of the Azure virtual machine which will host the Verba Bot service. At the domain part, use the domain of the Teams tenant (also specified in the SSL certificate).

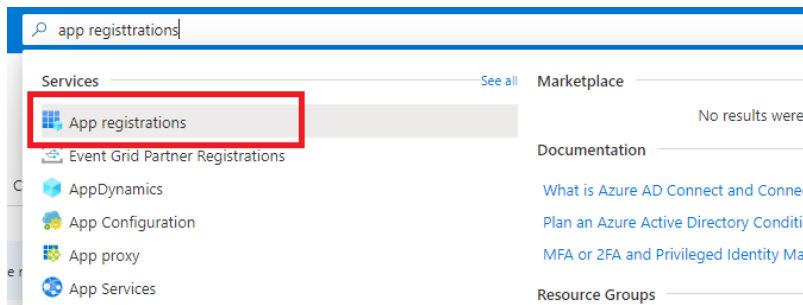


Step 12 - Click on the **Apply** button.

Configuring authentication for the bot

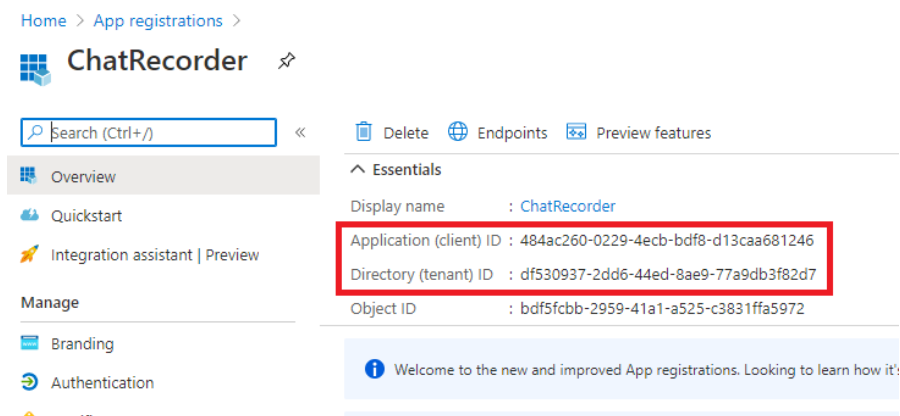
Step 13 - Search for **App registrations** in the search box on the top, then click on the **App registrations** link under the **Services** section.

(Alternatively, the App registrations can be also found by opening the **hamburger menu** in the upper right corner, then selecting the **Azure Active Directory**, then selecting **App registrations** in the left panel.)

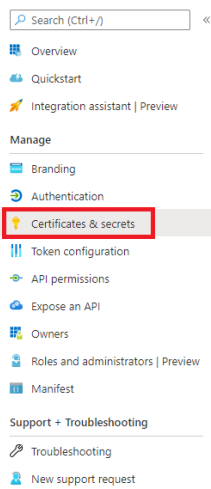


Step 14 - Select the App Registration from the list that was created previously using the name provided at Step 3 (Bot handle).

Step 15 - Take a note of the **Application (client) ID** and the **Directory (tenant) ID**. They will be needed later.



Step 16 - Select the **Certificates & secrets** menu in the left panel.



Step 17 - Under the Client secrets section, click on the **New Client Secret** button.

Step 18 - Provide a **Description**, set when the secret **Expires**, then click on the **Add** button.

Add a client secret

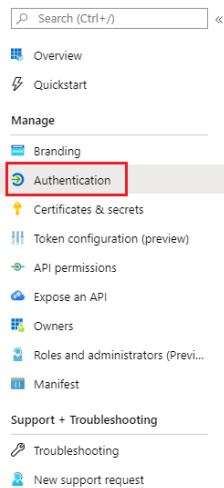
Description

Expires

- In 1 year
- In 2 years
- Never

Step 19 - Take a note of the new **Client secret**. It will be needed later.

Step 20 - In the left panel, under the **Manage** section, click on the **Authentication** menu.

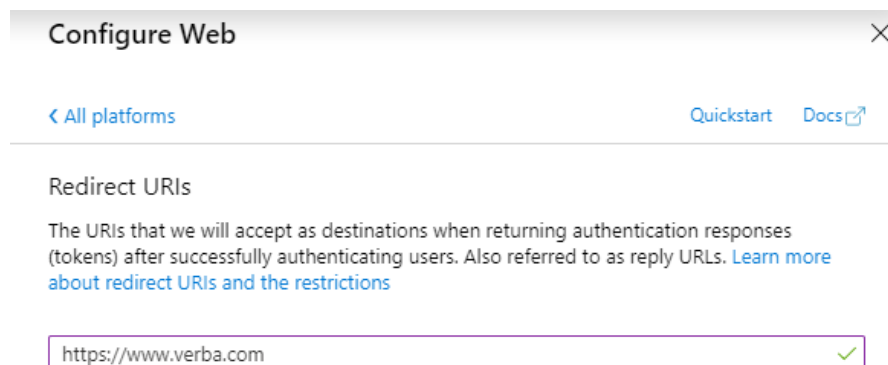


Step 21 - Under the **Platform configuration** sections, click on the **Add a platform** button.

Step 22 - In the right panel, select **Web**.

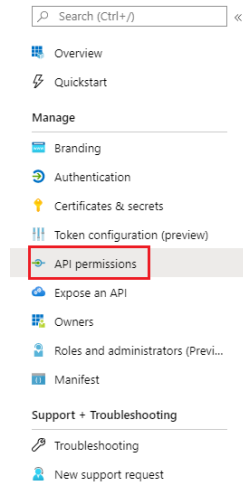
Step 23 - Provide a **Redirect URI**. It can be any website. Take a note of the URI provided, it will be needed later.

Step 24 - Click on the **Configure** button in the bottom.



Configuring permissions to the bot

Step 25 - In the left panel, under the **Manage** section, click on the **API permissions** menu.



Step 26 - Click on the **Add a permission** button.

Step 27 - Select Microsoft Graph, then select **Application permissions**.

Step 28 - Select the following permissions:

- Calendars.Read
- Calls.AccessMedia.All
- Calls.JoinGroupCall.All
- Calls.JoinGroupCallAsGuest.All
- OnlineMeetings.Read.All
- User.Read.All



Using the same App Registration for Chat Recording also

The same App Registration can be used for the chat recording. In that case, add the following permissions also:

- Group.Read.All
- Chat.Read.All
- ChannelMessage.Read.All
- ChannelMember.Read.All
- Directory.Read.All
- Files.Read.All
- Sites.Read.All

If the Chat recording will be used, the protected API access has to be requested. See **Protected API Access for Chat Recording** section at the bottom.

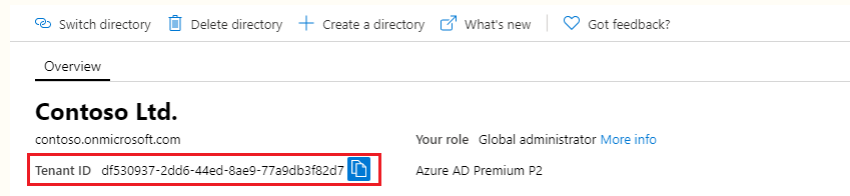
Step 29 - Click on the **Add permissions** button.

Granting admin consent to the permissions



Separate Azure tenants for the recording provider (bot) and for the Teams environment to record

In the case when the recorded Teams environment and the recording bot are in separate Azure tenants, the following steps have to be done using the Tenant ID of the Azure tenant where the Teams environment to record resides, and also using a user that has the Teams Service Admin or Global Admin role in that tenant. In order to gather the Tenant ID for Step 29, you have to log in to the [Azure portal](#) of that tenant, then go to the **Azure Active Directory**.



Multi-Tenant configuration:

If the same bot is being used in multiple tenants, then the following steps have to be done for each tenants using the guidelines above.

Step 30 - Build the consent URL. The format is the following:

```
https://login.microsoftonline.com/{tenant_id}/adminconsent?client_id={microsoft_app_id}&state=12
```

Replace the {tenant_id} part with the Directory (tenant) ID and the {microsoft_app_id} part with the Application (client) ID from **Step 14**. Replace {redirect_uri} part with the URI from **Step 22**.

Step 31 - Copy the previously created consent URL into the browser, then hit enter. Log in with a **Teams Service Admin** or **Global Admin** user of the Azure tenant where the Teams environment to record resides. Click on the Accept button. The page will redirect to the webpage provided in the Redirect URI setting.

2N Recording

Step 32 (Optional) - In the case of 2N recording, all the steps above have to be done twice. Take a note of the second **Application (client) ID** also at **Step 14**. It will be needed in the next part of the configuration guide.

Protected API Access for Chat Recording

Step 33 (Optional) - If the same App Registration will be used for Chat recording also, then the following form has to be sent:

<https://aka.ms/teamsgraph/requestaccess>

At the **Data Retention** setting select **“It is obvious to any admin installing this app that it will make a copy of Microsoft Teams messages”**. On the second page, leave the URLs empty.

Whitelisting the Microsoft Teams Bot App

In order to complete the steps below, you must have Global Administrator role.

The same Bot can be whitelisted in multiple Azure tenants, and can be used for multiple compliance policies.

The registration consists of the following steps:

- [Prerequisites](#)
- [Accessing the tenant via PowerShell](#)
- [Registering the bot as a Teams application](#)

Prerequisites

Step 1 - Download and install [PowerShell 5.1](#).

Step 2 - Open PowerShell as administrator.

Step 3 - Set the security protocol to TLS 1.2 with the following command:

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
```


Step 4 - Install the NuGet package provider module by running the following command:

```
Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force
```

Step 5 - Install the Microsoft Teams module by running the following command:

```
Install-Module MicrosoftTeams
```

Accessing the tenant via PowerShell

 **Separate Azure tenants for the recording provider (bot) and for the Teams environment to record**
In the case when the recorded Teams environment and the recording bot are in separate Azure tenants, the following steps have to be done in the Teams tenant.

Step 1 - Open **PowerShell** as administrator.

Step 2 - Execute the following command:

```
Update-Module MicrosoftTeams
```

Step 3 - Execute the following command:

```
Connect-MicrosoftTeams
```

Step 4 - A login prompt will show up. Provide the user credentials.

Registering the bot as a Teams application

Step 5 - Execute the following command. At the <UPN> part, provide a unique UPN for the recording bot, for example, verbabot@contoso.com. Provide something at the <displayName> part, it can be anything. Replace the <botAppId> part with the application ID from the previous section (Creating the Microsoft Teams Recording Bot - Step 13).

```
New-CsOnlineApplicationInstance -UserPrincipalname <UPN> -DisplayName '<displayName>' -Applicatio
```

Step 6 - In the command results, take note of the **ObjectId**. It will be needed later.

Step 7 - Execute the following command. Replace the <ObjectId> part with the ID from the results of the previous command.

```
Sync-CsOnlineApplicationInstance -ObjectId <ObjectId>
```

Step 8 (Optional - 2N recording) - If 2N recording will be configured, then **repeat the steps 5-7** for the second bot registration also. Take a note of the second ObjectId.

Configuring Access Policy for Meeting Metadata

Prerequisites

Step 1 - Download and install [PowerShell 5.1](#).

Step 2 - Open PowerShell as administrator.


Step 3 - Install the NuGet package provider module by running the following command:

```
Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force
```

Step 4 - Install the Microsoft Teams module by running the following command:

```
Install-Module MicrosoftTeams
```

Accessing the tenant via PowerShell

 **Separate Azure tenants for the recording provider (bot) and for the Teams environment to record**
In the case when the recorded Teams environment and the recording bot are in separate Azure tenants, the following steps have to be done in the Teams tenant.

Follow the steps below to assign a compliance policy to a user:

Step 1 - Open **PowerShell** as administrator.

Step 2 - Execute the following command:

```
Connect-MicrosoftTeams
```

Step 3 - A login prompt will show up. Provide the user credentials.

Creating Application Access Policy

Step 4 - Execute the following command. Replace the <Policy Name> part with a unique name for the policy. Replace the <Bot App ID> part with the Application (Client) ID of the App Registration of the Bot. Replace the <Description> with a description.

```
New-CsApplicationAccessPolicy -Identity "<Policy Name>" -AppIds "<Bot App ID>" -Description "<Des
```

Step 5 - Execute the following command. Replace the <Policy Name> part with the name provided in the previous command.

```
Grant-CsApplicationAccessPolicy -PolicyName "<Policy Name>" -Global
```


Installing and configuring Microsoft Teams custom announcement

For a general overview of the function refer to the [Announcement](#) article.

- [Installation](#)
- [Prerequisites](#)
 - [Disable the built-in audio notification for P2P PSTN Calls](#)
 - [Audio file](#)
- [Configuring custom announcements for the Verba Microsoft Teams Bot Service](#)
- [Configuring custom prompts for users](#)

Installation

The custom announcement capability is built into the Verba Microsoft Teams Bot Service, there is no additional installation step required.

Prerequisites

Disable the built-in audio notification for P2P PSTN Calls

Disabling the built-in audio notification is required because, in the case of the custom audio announcements, both the bot service and the Teams notification service play a prompt for P2P PSTN calls.

Step 1 - Open **PowerShell** as administrator.

Step 2 - Execute the following command:

```
Connect-MicrosoftTeams
```

Step 3 - A login prompt will show up. Provide the user credentials.

Step 4 - Execute the following command. Replace the <PolicyName> part with the name of the compliance policy

```
Set-CsTeamsComplianceRecordingPolicy -Identity '<PolicyName>' -DisableComplianceRecordingAudioNot
```

Audio file

The Verba Microsoft Teams Bot service is using the Graph Communications Bot Media SDK which supports **16 kHz PCM** Wave audio files as input.

Configuring custom announcements for the Verba Microsoft Teams Bot Service

Follow the steps below to configure custom announcement-related settings for the Verba Microsoft Teams Bot Service:

Step 1 - Open the Verba web interface, click on the **System / Servers** and select the Recording Server where the bot service is deployed, or select the appropriate Configuration Profile at **System / Configuration Profiles**.

Step 2 - Go to the **Change Configuration Settings** tab, then expand the **Microsoft Teams Bot / General** node.

Step 3 - Configure the following settings:

Configuration Parameter Name	Description	Sample Value
Apply User's Recording Announcement Configuration	Global notification setting, if turned off, the user settings won't be taken into account.	Yes
Audit Log for Customisable Announcement	Audit log for the customizable audio announcement, If turned on the bot service inserts audit log entries through the Web Application's HTTP API to the database.	Yes

Step 4 - Click the



icon to save your settings.

Step 5 - The system will notify you that the changes need to be applied to the server by restarting the involved services. Execute the required tasks.

Step 6 - Repeat the steps on each server.



Limitation

In 2N recording configurations, where 2 separate bots join a call, both bots will play the announcement. As a workaround, the custom announcement feature can be disabled on one of the 2N lanes.

Configuring custom prompts for users

It is possible to configure custom notification sounds on a per-user basis. To achieve this follow these steps:

Step 1 - Login to the **Recording Server** which runs the bot service, and go to the **C:\Program Files\Verba\resources\announcement** folder.

Step 2 - Copy the .wav files to the **internal, inbound** and **outbound** folders.

Step 3 - Open the Verba web interface, click on the **System / Servers** and select the Media Repository server, or select the appropriate Configuration Profile at **System / Configuration Profiles**.

Step 4 - Click on the **Change Configuration Settings** tab. Expand the **Web Application** section.

Step 5 - Expand the **Recording Announcement** node, and add the names of the .wav files to the **Teams Internal Calls Prompt Files, Teams PSTN/Federated Inbound Prompt Files, and Teams PSTN/Federated Outbound Files** settings, one in a line.

Step 6 - Click the



icon to save your settings.

Step 7 - The system will notify you that the changes need to be applied to the server by restarting the involved services. Execute the required tasks.

Step 8 - Repeat the steps on each Media Repository server.

To configure the custom prompt for the users please see the [User Configuration](#) configuration.

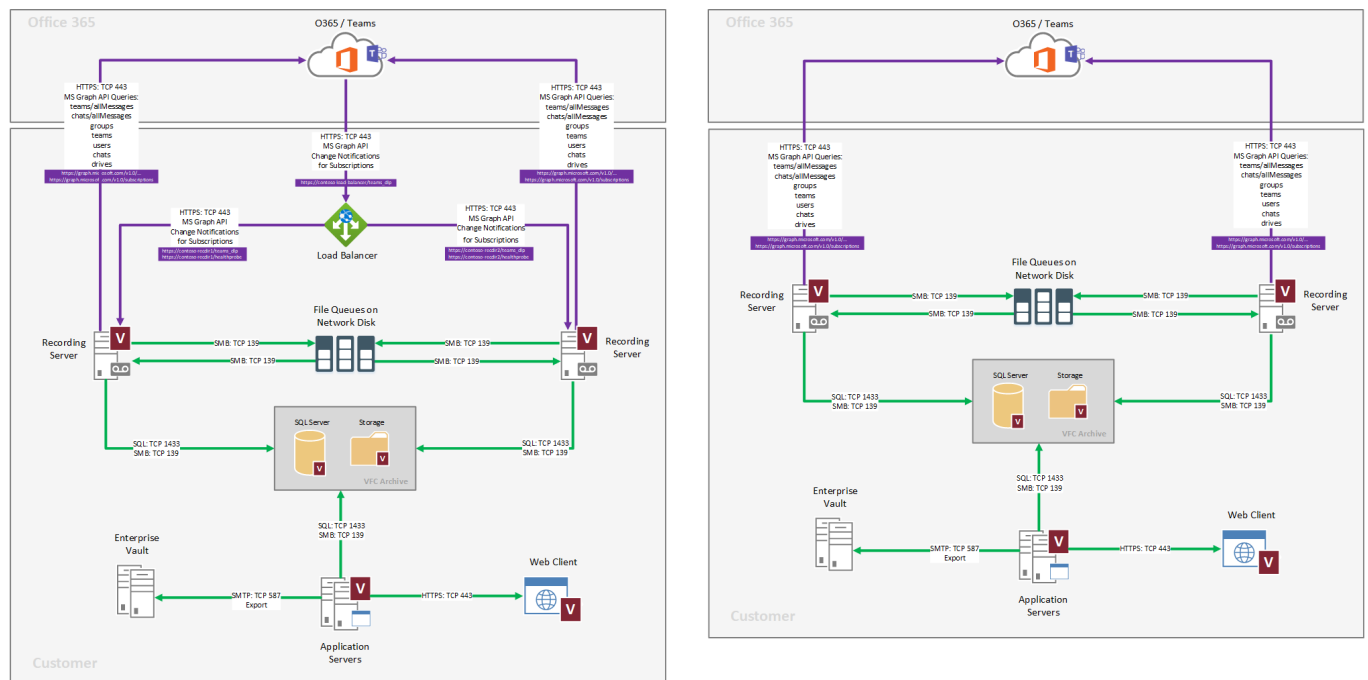
Configuring Microsoft Teams Chat and Channel Archiving

In order to complete the steps below, you must have a System Administrator role in Verba.

- [Architecture](#)
 - [File Queue Setup for Load-balancing and Failover](#)
- [Configuration](#)
 - [Prerequisites](#)
 - [Assigning a Public IP Address \(Webhook/DLP API only\)](#)
 - [Creating an App Registration in Azure](#)
 - [Creating the File Queue folder](#)
 - [Assigning Certificates \(Webhook/DLP API only, optional\)](#)
 - [Configuring Microsoft Teams chat and channel archiving with Webhook/DLP API](#)
 - [Configuring Microsoft Teams chat and channel archiving with Export API](#)
 - [Configuring Separated Recording Director and Media Recorder roles](#)
 - [Configuring multi tenant Microsoft Teams chat and channel archiving](#)
 - [Adding users for chat and channel archiving](#)
 - [Chat archiving](#)
 - [Channel archiving](#)

Architecture

The following diagrams show the connections in a highly available Microsoft Teams chat and channel archiving environment when using the Webhook/DLP API (left), and Export API (right).



File Queue Setup for Load-balancing and Failover

When there is only a single recorder, the value of the "Number of Processing Queues Owned by Recorder Role" and the "Number of Receiving Queues Owned by Director Role" settings will be the same, and it will be equal to the total number of cores of the server multiplied by two.

When there are multiple Recording Servers, and there is load-balancing between them, then the value of these settings will be different.

The "**Number of Receiving Queues Owned by Director Role**" setting has to be the same on all Recording Servers (Recording Directors). This setting has to be the same as the total **active** Recording Server (Media Recorder) cores multiplied by two.

Number of Receiving Queues Owned by Director Role = Total Active Recording Server cores * 2
or
Number of Receiving Queues Owned by Director Role = Number of Processing Queues Owned by Recorder

The "**Number of Processing Queues Owned by Recorder Role**" setting also has to be the same on all Recording Servers (Media Recorder). But instead of the total active cores, this setting is always equal to the number of CPU cores of the **individual** Recording Servers (Media Recorders) multiplied by two.

Number of Processing Queues Owned by Recorder Role = Individual Recording Server cores * 2

For example, if there are two Recording Servers with 4 CPU cores each, then the "Number of Processing Queues Owned by Recorder Role" setting will be 8 on each servers (Media Recorders), and the "Number of Receiving Queues Owned by Director Role" setting will be 16 on each servers (Recording Directors).

If there are three Recording Servers with 4 CPU cores each, and one of them is standby (N+1), then the numbers will be the same. The "Number of Processing Queues Owned by Recorder Role" setting will be 8 on each server (Media Recorder), and the "Number of Receiving Queues Owned by Director Role" setting will be 16 on each server (Recording Director).

Configuration

Prerequisites

Assigning a Public IP Address (Webhook/DLP API only)

For a single non-HA setup, the Recording Server (Recording Director) needs to have a public IP address. In the case of a highly-available setup, the public IP address has to be assigned to the load-balancer.

Creating an App Registration in Azure

Before configuring the Verba Recording Server(s) for Microsoft Teams Chat recording, an App Registration has to be created in Azure. For the configuration steps, see:

[Registering an App for Microsoft Teams Chat Recording in Azure](#)

Creating the File Queue folder

A root folder has to be created for the processing queues. In the case of a **single-recorder** setup, this folder can be created on the **local disk** of the server (recommended path: [APPLICATION_FOLDER]\processing_queue). In the case of a HA setup, the processing queue folder cannot be created on the local disk of the Recording Server. Instead, it has to be created on a separate **network location** accessible from all servers.

Assigning Certificates (Webhook/DLP API only, optional)

For the connection encryption certificate, both publicly signed and locally generated certificate works. **Only CSP** certificates are supported (CNG/KSP certificates are not supported). The SAN configuration of the certificate must include the public address of the Recording Server, or the load-balancer in the case of multiple Recording Servers. Using an asterisk in the SAN is accepted. The **private key** of the certificate has to be **exportable**.

Configuring Microsoft Teams chat and channel archiving with Webhook/DLP API

The configuration steps for the Webhook/DLP API can be found here:


[Configuring the Verba Unified IM Recorder Service for Microsoft Teams chat and channel archiving with DLP/Webhook API](#)

Configuring Microsoft Teams chat and channel archiving with Export API

The configuration steps for the Export API can be found here:

[Configuring the Verba Unified IM Recorder Service for Microsoft Teams chat and channel archiving with Export API](#)

Configuring Separated Recording Director and Media Recorder roles

 Separating the Recording Director and Media Recorder roles is not recommended.

In the case of the Webhook/DLP API, it is possible to separate the Recording Server roles.

The following configuration steps need to be done when the Recording Director and the Media Recorder roles are separated:

Step 1 - [Configuring the Verba Unified IM Recorder Service on the Recording Director Servers](#)

Step 2 - [Configuring the Verba Unified IM Recorder Service on the Media Recorder Servers](#)

Configuring multi tenant Microsoft Teams chat and channel archiving

To configure Microsoft Teams chat and channel archiving in a multi tenant system:

[Configuring multi tenant Microsoft chat and channel archiving](#)

Adding users for chat and channel archiving

Chat archiving

For both DLP/Webhook and Export API based integrations, in order to enable chat archiving for specific users, create the [users](#) and the [extensions](#) on the Verba side. This can also be done via [Active Directory Synchronization](#). The extensions have to match the Azure AD object ID of the users (not the User Principal Name or email address).

Channel archiving

For the DLP/Webhook integration, in order to enable channel archiving for specific users, create the [users](#) and the [extensions](#) on the Verba side. This can also be done via [Active Directory Synchronization](#). The extensions have to match the Azure AD object ID of the users (not the User Principal Name or email address).

For the Export API integration, in order to enable channel archiving, the Microsoft Teams teams have to be added as recorded extension. Due to limitations in the Microsoft Export API, it is not possible to archive channel based on users, only based on teams. The extensions have to match the Azure AD object ID of the teams. The system allows importing the teams manually under **Users / Import Teams/Channels**.

Registering an App for Microsoft Teams chat and channel archiving in Azure

In order to complete the steps below, you must have Application Administrator or Global administrator role in Azure.

The registration consists of the following steps:

- [Creating an App Registration](#)
- [Configuring permissions to the App](#)
- [Granting admin consent to the permissions](#)
 - [Multi-Tenant configuration:](#)
- [Protected API Access for Chat Recording](#)

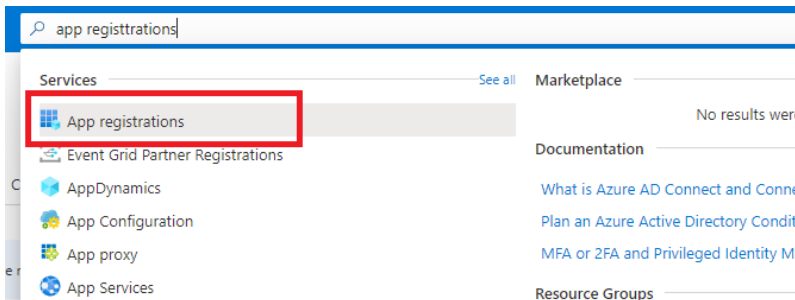
If Chat recording and Voice recording will be used at the same time for Microsoft Teams, then a single app can be used for both. In that case, use the configuration steps described in the [Registering the Microsoft Teams Bot in Azure](#) article.

Creating an App Registration

Step 1 - Log in to the [Azure portal](#).

Step 2 - Search for **App registrations** in the search box on the top, then click on the **App registrations** link under the **Services** section.

(Alternatively, the App registrations can be also found by opening the **hamburger menu** in the upper right corner, then selecting the **Azure Active Directory**, then selecting **App registrations** in the left panel.)



Step 3 - Click on **New Registration**.

Step 4 - Provide a name for the App, then at the "Who can use this application or access this API?" section select the "**Accounts in any organizational directory (Any Azure AD directory - Multitenant)**" option.

* Name
The user-facing display name for this application (this can be changed later).

Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (Verba Technologies Ltd. only - Single tenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- Personal Microsoft accounts only

Step 5 - Click **Register**.

Registering the App using Azure CLI and PowerShell

The Microsoft Teams Bot can be also registered using Azure CLI and PowerShell commands.

Step 1 - Download and install the [Azure CLI](#).

Step 2 - Open PowerShell and log in to Azure using the [az login](#) command. For example:

```
az login -u "[user_UPN]" -p
```

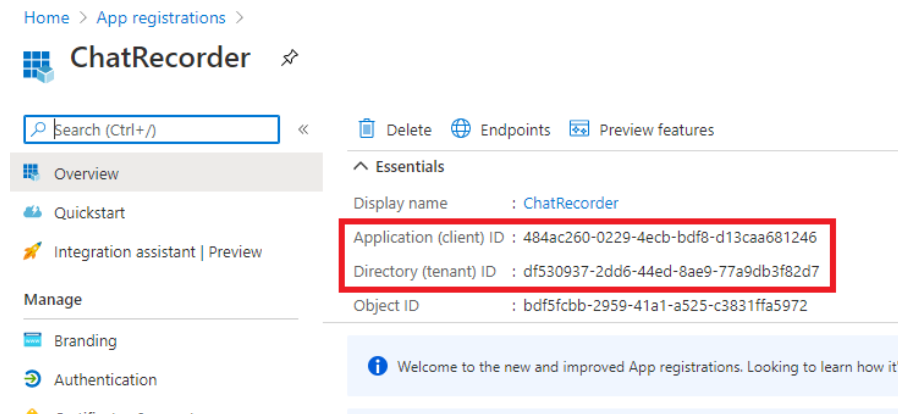
Step 3 - Create the App registration using the [az ad app create](#) command. Provide an **App secret** also. When it is done, take a note of the **App Id**; it will be needed in the later commands, in Verba configuration, and in the Teams recording policy.

```
$app = az ad app create --c  
$appID = $app.appId  
echo $appID
```

Step 4 (Optional) - Assign an user to the App registration as owner using the [az ad app owner add](#) command:

```
az ad app owner add --id $a
```

Step 6 - Take a note of the **Application (client) ID** and the **Directory (tenant) ID**. They will be needed later.



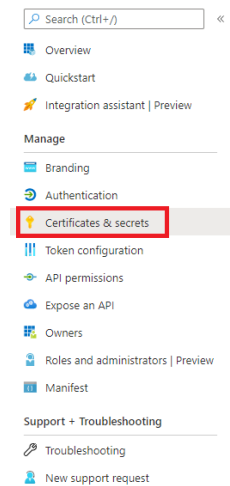
Step 5 - Add permissions to the App registration using the [az ad app permission add](#) command:

```
az ad app permission add --
```

Step 6 - Grant admin consent using the [az ad app permission admin-consent](#) command:

```
az ad app permission admin-
```

Step 7 - Select the **Certificates & secrets** menu in the left panel.



Step 7 - The protected API access has to be requested. See **Protected API Access for Chat Recording** section at the bottom

Step 8 - Under the Client secrets section, click on the **New Client Secret** button.

Step 9 - Provide a **Description**, set when the secret **Expires**, then click on the **Add** button.

Add a client secret

Description

Expires

In 1 year

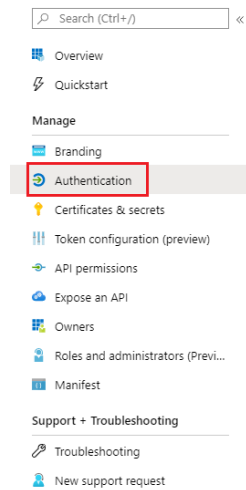
In 2 years

Never

Add Cancel

Step 10 - Take a note of the new **Client secret**. It will be needed later.

Step 11 - In the left panel, under the **Manage** section, click on the **Authentication** menu.

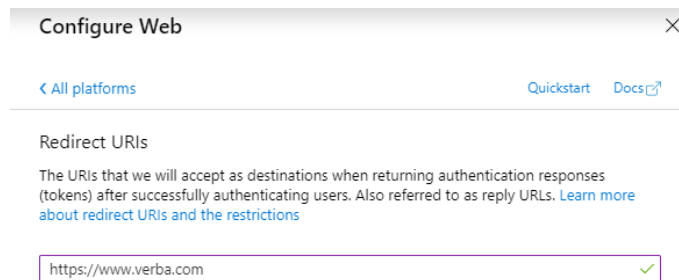


Step 12 - Under the **Platform configuration** sections, click on the **Add a platform** button.

Step 13 - In the right panel, select **Web**.

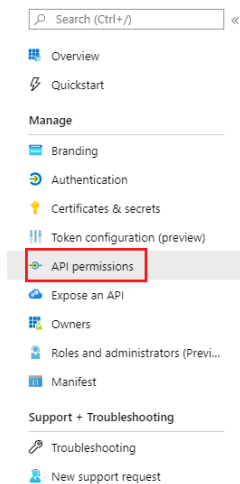
Step 14 - Provide a **Redirect URI**. It can be any website. Take a note of the URI provided, it will be needed later.

Step 15 - Click on the **Configure** button in the bottom.



Configuring permissions to the App

Step 16 - In the left panel, under the **Manage** section, click on the **API permissions** menu.



Step 17 - Click on the **Add a permission** button.

Step 18 - Select Microsoft Graph, then select **Application permissions**.

Step 19 - Select the following permissions:

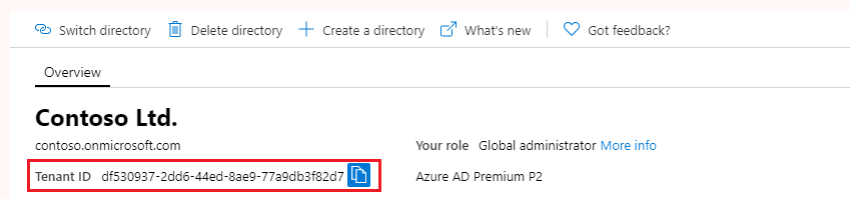
- User.Read.All
- Group.Read.All
- Chat.Read.All
- ChannelMessage.Read.All
- ChannelMember.Read.All
- Directory.Read.All
- Files.Read.All
- Sites.Read.All

Step 20 - Click on the **Add permissions** button.

Granting admin consent to the permissions

⚠ Separate Azure tenants for the recording provider (App) and for the Teams environment to record

In the case when the recorded Teams environment and the recording bot are in separate Azure tenants, the following steps have to be done using the Tenant ID of the Azure tenant where the Teams environment to record resides, and also using a user that has the Teams Service Admin or Global Admin role in that tenant. In order to gather the Tenant ID for Step 29, you have to log in to the [Azure portal](#) of that tenant, then go to the **Azure Active Directory**.



Multi-Tenant configuration:

If the same bot is being used in multiple tenants, then the following steps have to be done for each tenants using the guidelines above.

Step 21 - Build the consent URL. The format is the following:

`https://login.microsoftonline.com/{tenant_id}/adminconsent?client_id={microsoft_app_id}&state=12`

Replace the {tenant_id} part with the Directory (tenant) ID and the {microsoft_app_id} part with the Application (client) ID from **Step 6**. Replace {redirect_uri} part with the URI from **Step 14**.

Step 22 - Copy the previously created consent URL into the browser, then hit enter. Log in with a **Teams Service Admin** or **Global Admin** user of the Azure tenant where the Teams environment to record resides. Click on the Accept button. The page will redirect to the webpage provided in the Redirect URI setting.

Protected API Access for Chat Recording

If the same App Registration will be used for Chat recording also, then the following form has to be sent:

<https://aka.ms/teamsgraph/requestaccess>

At the **Data Retention** setting select **“It is obvious to any admin installing this app that it will make a copy of Microsoft Teams messages”**. On the second page, leave the URLs empty.

Configuring the Verba Unified IM Recorder Service for Microsoft Teams chat and channel archiving with DLP/Webhook API

This configuration guide describes how to configure the Verba Unified IM Recorder service on a Recording Server in the case of a single-recorder environment, or in the case of a highly-available environment where the Recording Director and the Media Recorder roles are co-located.

In order to complete the steps below, you must have the System Administrator role in Verba.

The configuration consists of the following steps:

- [Enabling the service](#)
- [Configuring the Verba Unified IM Recorder Service](#)
- [Starting the service](#)

Enabling the service

Step 1 - Log in to the Verba web interface and go to **System \ Servers** menu.

Step 2 - Select your Recording Server from the list, then click on the **Service Activation** tab.

Step 3 - Activate the **Verba Unified IM Recorder Service** by clicking on the



icon.

Configuring the Verba Unified IM Recorder Service

Step 4 - Click on the **Change Configuration Settings** tab.

Step 5 - Expand the **Unified IM Recorder \ General** node.

Step 6 - Set the **Role** setting to **Director + Recorder**.

Step 7 - Expand the **Processing Queues** node.

Step 8 - Provide the **Number of Processing Queues Owned by Recorder Role** and the **Number of Receiving Queues Owned by Director Role** settings. In the case of the single-recorder setup, the values of these two settings have to be the same.

The **Number of Processing Queues Owned by Recorder Role** setting determines the number of processing threads on the Recording Server. In a highly-available setup, this has to be the same on all Recording Servers.

In the case of a highly-available setup, the **Number of Receiving Queues Owned by Director Role** settings can be calculated the following way:

"Number of Processing Queues Owned by Recorder Role" setting value * Number of Recording servers

Step 9 - Provide the location of the processing queue root folder at the **SMB Queues Path** setting. The folder is not allowed to be configured under the media folder Audio Path.

In the case of the single-recorder setup, this folder is preferably on the local disk of the server (e.g.: [APPLICATION_FOLDER] \unifiedimrec\processing_queue). In a HA setup, this is an SMB path.

Step 10 (HA) - Provide a windows domain user credential at the **SMB Credential, User** and the **SMB Credential, Password** settings. The service will use this user when accessing the folder provided at the **SMB Queues Path** setting.

Step 11 - Expand the **Recording Providers \ Microsoft Teams** node.

Step 12 - At the **Microsoft Teams** setting, click on the



icon to add a new connection.

Step 13 - In the left panel, provide the following settings:

Setting Name	Description
Application (Client) ID	The ID of the App Registration (Registering an App for Chat Recording in Azure - Step 6 or Registering the Microsoft Teams Bot in Azure - Step 13)
Application (Client) Secret	The secret created for the App Registration (Registering an App for Chat Recording in Azure - Step 10 or Registering the Microsoft Teams Bot in Azure - Step 17)
Directory (Tenant) ID	The ID of the Azure tenant where the App Registration was created (Registering an App for Chat Recording in Azure - Step 6 or Registering the Microsoft Teams Bot in Azure - Step 29)
Notification URL	The notification URL of the Unified IM Recorder service. The format is the following: <code>https://server_CNNAME.domain.com:3333/msteams</code> . <i>Note: in case you're using any kind of network element that accepts incoming messages from Microsoft Teams servers and forwards it to your recorder(s), here you should use the port opened on that network element (not necessarily 3333). The port the recorder awaits messages on is configured in the next field.</i> The Microsoft Graph API limits the subscriptions to resources on the same Tenant and AppID to 1. Because of this, the only correct way to create a highly available configuration with 2 Recording Directors is to configure recorders with the same Notification URL and Connection Encryption Certificate , and set the notification URL for a load balancer that distributes incoming requests between the running recorders. If configurations differ and multiple recorders are set up for the same Tenant and AppID, because of the Microsoft API limit of 1 subscription, each recorder will constantly delete other recorders' subscriptions and create their own.
Event Listener Port	The event listener port of the Unified IM Recorder service. Set it to 3333.
Connection Encryption Certificate	The thumbprint of the certificate that is used for the connection. The certificate has to reside in the Windows Certificate Store. The same certificate has to be used for all Teams connections on all the servers. Alternatively, a certificate file can be used instead of the Windows Certificate Store. In this case, the path to the .crt file has to be provided.
Connection Encryption Key file	If the file path is provided at the Connection Encryption Certificate setting, then the path to the .key file has to be provided here.
Connection Encryption Key file password	If the file path is provided at the Connection Encryption Certificate setting, then the password of the .key file has to be provided here.
Connection Encryption trust list	The thumbprint of the incoming connection certificates that should be trusted, or the thumbprint of the CA certificates whose certificates should be trusted. If left empty, all certificates will be trusted.
Disable P2P /Group Chat Subscription	Sets whether the P2P or group chats should be recorded or not.

Disable Team /Channel Chat Subscription	Sets whether the Team or Channel chats should be recorded or not.
Forward Proxy Address	If a forward proxy is being used for the outgoing connection, then the proxy address has to be provided here.
Forward Proxy Port	The port of the forward proxy connection.
Forward Proxy User	The user of the forward proxy connection. Required, if the proxy requires authentication.
Forward Proxy Password	The password of the forward proxy connection. Required, if the proxy requires authentication.
Licensing Model	<p>The licensing model that is used for the chat archiving integration. The following licensing models are available:</p> <ul style="list-style-type: none"> • A: Applications performing a security or compliance function, and requires a supported license. This is the default licensing model. • B: Applications that do not perform a security or compliance function. • Evaluation Mode: enables access to APIs with limited usage per requesting application for evaluation purposes. <p>More information: Licensing and payment requirements - Microsoft Graph</p>



Microsoft Teams IM

Application (Client) ID	EB17D4E0-CA1C-45D8-9356-DA0BF96BB55F
Application (Client) Secret
Directory (Tenant) ID	9F39980E-6E41-4399-BE16-060F8A99F73F
Notification URL	https://imrecorder.contoso.com:3333
Event Listener Port	3333
Connection Encryption Certificate	6E8A7E9FDD294CD4BD3A91124F35419E
Connection Encryption Key file	
Connection Encryption Key file password	
Connection Encryption trust list	
Disable P2P/Group Chat Subscription	No
Disable Team/Channel Chat Subscription	No
Forward Proxy Address	
Forward Proxy Port	
Forward Proxy User	
Forward Proxy Password	
License Model	A

Step 14 - Click **Save**.

Step 15 - Repeat steps 12-14 for every Microsoft Teams connection.

- Recording Providers
 - Microsoft Teams


Microsoft Teams: 484ac260-0229-4ecb-bdf8-d13caa681246|sSkV8aqywDe8tE3B6zqDcEEyOA3lt  

Step 16 - Save the changes by clicking on the



icon.

Step 17 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

 There are tasks to be executed regarding the configuration of this Verba Server. If you would like to execute these tasks now, please [click here](#) .

Starting the service

Step 18 - Click on the **Service Control** tab.

Step 19 - Start the **Verba Unified IM Recorder Service** by clicking on the



icon.

Configuring the Verba Unified IM Recorder Service for Microsoft Teams chat and channel archiving with Export API

This configuration guide describes how to configure the Verba Unified IM Recorder service on a Recording Server in the case of a single-recorder environment, or in the case of a highly-available environment where the Recording Director and the Media Recorder roles are co-located.

In order to complete the steps below, you must have the System Administrator role in Verba.

The configuration consists of the following steps:

- [Enabling the service](#)
- [Configuring the Verba Unified IM Recorder Service](#)
- [Starting the service](#)

Enabling the service

Step 1 - Log in to the Verba web interface and go to **System \ Servers** menu.

Step 2 - Select your Recording Server from the list, then click on the **Service Activation** tab.

Step 3 - Activate the **Verba Unified IM Recorder Service** by clicking on the



icon.

Configuring the Verba Unified IM Recorder Service

Step 4 - Click on the **Change Configuration Settings** tab.

Step 5 - Expand the **Unified IM Recorder \ General** node.

Step 6 - Set the **Role** setting to **Director + Recorder**.

Step 7 - Expand the **Processing Queues** node.

Step 8 - Provide the **Number of Processing Queues Owned by Recorder Role** and the **Number of Receiving Queues Owned by Director Role** settings. In the case of the single-recorder setup, the values of these two settings have to be the same.

- The **Number of Processing Queues Owned by Recorder Role** setting determines the number of processing threads on the Recording Server. The value of this setting is equal to the number of cores of the Recording Server multiplied by two. In a highly-available setup, this has to be the same on all Recording Servers.
- In the case of a highly-available setup, the **Number of Receiving Queues Owned by Director Role** settings can be calculated the following way:

"Number of Processing Queues Owned by Recorder Role" setting value * Number of Recording servers

Step 9 - Provide the location of the processing queue root folder at the **SMB Queues Path** setting. The folder is not allowed to be configured under the media folder Audio Path.

In the case of the single-recorder setup, this folder is preferably on the local disk of the server (e.g.: [APPLICATION_FOLDER] \unifiedimrec\processing_queue). In a HA setup, this is an SMB path.

Step 10 (HA) - Provide a windows domain user credential at the **SMB Credential, User** and the **SMB Credential, Password** settings. The service will use this user when accessing the folder provided at the **SMB Queues Path** setting.

Step 11 - Expand the **Recording Providers \ Microsoft Teams** node.

Step 12 - At the **Microsoft Teams Export API Connection** setting, click on the







icon to add a new connection.

Step 13 - In the left panel, provide the following settings:

Setting Name	Description
Application (Client) ID	The ID of the App Registration (Registering an App for Chat Recording in Azure - Step 6 or Registering the Microsoft Teams Bot in Azure - Step 13)
Application (Client) Secret	The secret created for the App Registration (Registering an App for Chat Recording in Azure - Step 10 or Registering the Microsoft Teams Bot in Azure - Step 17)
Directory (Tenant) ID	The ID of the Azure tenant where the App Registration was created (Registering an App for Chat Recording in Azure - Step 6 or Registering the Microsoft Teams Bot in Azure - Step 29)
Disable P2P/Group Chat Subscription	Sets whether the P2P or group chats should be recorded or not.
Disable Team/Channel Chat Subscription	Sets whether the Team or Channel chats should be recorded or not.
Forward Proxy Address	If a forward proxy is being used for the outgoing connection, then the proxy address has to be provided here.
Forward Proxy Port	The port of the forward proxy connection.
Forward Proxy User	The user of the forward proxy connection. Required, if the proxy requires authentication.
Forward Proxy Password	The password of the forward proxy connection. Required, if the proxy requires authentication.
Licensing Model	The licensing model that is used for the chat archiving integration. The following licensing models are available: <ul style="list-style-type: none"> • A: Applications performing a security or compliance function, and requires a supported license. This is the default licensing model. • B: Applications that do not perform a security or compliance function. • Evaluation Mode: enables access to APIs with limited usage per requesting application for evaluation purposes. More information: Licensing and payment requirements - Microsoft Graph
Message Polling time (seconds)	The polling interval for downloading the chats in seconds.
Message batch size	The page size used in the API connection.
Initial date importing from	The date from where the import should start. If empty, then the first messages will be imported only from the point when the service started.



Microsoft Teams IM Export API

Application (Client) ID	6C8A7202-D168-4983-8161-B0581AE3FF25
Application (Client) Secret
Directory (Tenant) ID	0C88C147-0377-4CEC-9B55-B28728D717F3
Disable P2P/Group Chat Subscription	No 
Disable Team/Channel Chat Subscription	No 
Forward Proxy Address	
Forward Proxy Port	
Forward Proxy User	
Forward Proxy Password	
License Model	A 
Message Polling time (seconds)	600
Message batch size	250
Initial date importing from	

Step 14 - Click **Save**.

Step 15 - Repeat steps 12-14 for every Microsoft Teams Export API connection.

Recording Providers

- Microsoft Teams
 - Microsoft Teams Webhooks: 
 - Microsoft Teams Export API Connections: 6C8A7202-D168-4983-8161-B0581AE3FF25jzCqpdZLUVDCxSxN5INDbpHIKs8yezv  
 - 

Step 16 (Optional) - Set the additional Export API query settings:

Setting	Description
Export API Batch Length in Hours	The number of hours of chat queried retroactively.
Export API Query Delay Timer (seconds)	The time delay used in the chat queries. This delay is required because the file attachments are usually not available immediately for download.

Step 17 - Save the changes by clicking on the



icon.

Step 18 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

Starting the service

Step 19 - Click on the **Service Control** tab.

Step 20 - Start the **Verba Unified IM Recorder Service** by clicking on the



icon.

Configuring the Verba Unified IM Recorder Service on the Media Recorder Servers

This configuration guide describes how to configure the Verba Unified IM Recorder service on a Recording Server (Media Recorder) in the case of a highly available environment.

In order to complete the steps below, you must have the System Administrator role in Verba.

The configuration consists of the following steps:

- [Enabling the service](#)
- [Configuring the Verba Unified IM Recorder Service as Media Recorder](#)
- [Starting the service](#)

Enabling the service

Step 1 - Log in to the Verba web interface and go to **System \ Servers** menu.

Step 2 - Select your **Recording Server (Media Recorder)** from the list, then click on the **Service Activation** tab.

Step 3 - Activate the **Verba Unified IM Recorder Service** by clicking on the



icon.

Step 4 - Repeat Steps 1-3 for all Media Recorder servers.

Configuring the Verba Unified IM Recorder Service as Media Recorder

Step 5 - Click on the **Change Configuration Settings** tab.

Step 6 - Expand the **Unified IM Recorder \ General** node.

Step 7 - Set the **Role** setting to **Recorder Only**.

Step 8 - Expand the **Processing Queues** node.

Step 9 - Provide the **Number of Processing Queues Owned by Recorder Role** setting. This setting determines the number of processing threads on the Media Recorder. This has to be the same on all Media Recorder servers.

Step 10 - Provide the network path of the processing queue root folder at the **SMB Queues Path** setting.

Step 11 - Provide a windows domain user credential at the **SMB Credential, User** and the **SMB Credential, Password** settings. The service will use this user when accessing the folder provided at the **SMB Queues Path** setting.

Step 12 - Expand the **Recording Providers \ Microsoft Teams** node.

Step 13 - At the **Microsoft Teams** setting, click on the



icon to add a new connection.

Step 14 - In the left panel, provide the following settings:

Setting Name	Description
--------------	-------------

Application (Client) ID	The ID of the App Registration (Registering an App for Chat Recording in Azure - Step 6 or Registering the Microsoft Teams Bot in Azure - Step 13)
Application (Client) Secret	The secret created for the App Registration (Registering an App for Chat Recording in Azure - Step 10 or Registering the Microsoft Teams Bot in Azure - Step 17)
Directory (Tenant) ID	The ID of the Azure tenant where the App Registration was created (Registering an App for Chat Recording in Azure - Step 6 or Registering the Microsoft Teams Bot in Azure - Step 29)
Notification URL	The notification URL of the Unified IM Recorder service. The format is the following: https://server_CNAME.domain.com:3333/msteams . <i>Note: in case you're using any kind of network element that accepts incoming messages from Microsoft Teams servers and forwards it to your recorder(s), here you should use the port opened on that network element (not necessarily 3333). The port the recorder awaits messages on is configured in the next field.</i> The Microsoft Graph API limits the subscriptions to resources on the same Tenant and AppID to 1. Because of this, the only correct way to create a highly available configuration with 2 Recording Directors is to configure recorders with the same Notification URL and Connection Encryption Certificate , and set the notification URL for a load balancer that distributes incoming requests between the running recorders. If configurations differ and multiple recorders are set up for the same Tenant and AppID, because of the Microsoft API limit of 1 subscription, each recorder will constantly delete other recorders' subscriptions and create their own.
Event Listener Port	The event listener port of the Unified IM Recorder service. Set it to 3333.
Connection Encryption Certificate	The thumbprint of the certificate that is used for the connection. The certificate has to reside in the Windows Certificate Store. The same certificate has to be used for all Teams connections on all the servers. Alternatively, a certificate file can be used instead of the Windows Certificate Store. In this case, the path to the .crt file has to be provided.
Connection Encryption Key file	If the file path is provided at the Connection Encryption Certificate setting, then the path to the .key file has to be provided here.
Connection Encryption Key file password	If the file path is provided at the Connection Encryption Certificate setting, then the password of the .key file has to be provided here.
Connection Encryption trust list	The thumbprint of the incoming connection certificates that should be trusted, or the thumbprint of the CA certificates whose certificates should be trusted. If left empty, all certificates will be trusted.
Disable P2P /Group Chat Subscription	Sets whether the P2P or group chats should be recorded or not.
Disable Team /Channel Chat Subscription	Sets whether the Team or Channel chats should be recorded or not.
Forward Proxy Address	If a forward proxy is being used for the outgoing connection, then the proxy address has to be provided here.

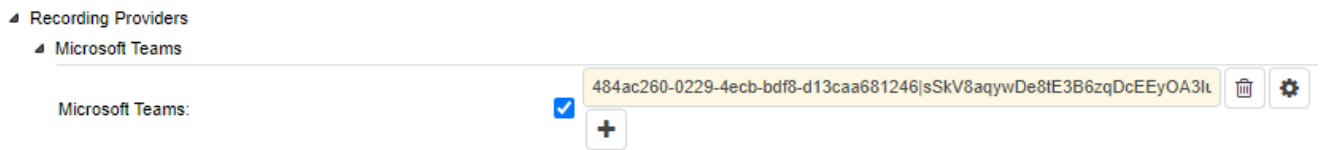
Forward Proxy Port	The port of the forward proxy connection.
Forward Proxy User	The user of the forward proxy connection. Required, if the proxy requires authentication.
Forward Proxy Password	The password of the forward proxy connection. Required, if the proxy requires authentication.
Licensing Model	<p>The licensing model that is used for the chat archiving integration. The following licensing models are available:</p> <ul style="list-style-type: none"> • A: Applications performing a security or compliance function, and requires a supported license. • B: Applications that do not perform a security or compliance function. • Evaluation Mode (default): enables access to APIs with limited usage per requesting application for evaluation purposes. <p>More information: Licensing and payment requirements - Microsoft Graph</p>

Microsoft Teams IM

Application (Client) ID	<input type="text" value="EB17D4E0-CA1C-45D8-9356-DA0BF96BB55F"/>
Application (Client) Secret	<input type="password" value="....."/>
Directory (Tenant) ID	<input type="text" value="9F39980E-6E41-4399-BE16-060F8A99F73F"/>
Notification URL	<input type="text" value="https://imrecorder.contoso.com:3333"/>
Event Listener Port	<input type="text" value="3333"/>
Connection Encryption Certificate	<input type="text" value="6E8A7E9FDD294CD4BD3A91124F35419E"/>
Connection Encryption Key file	<input type="text"/>
Connection Encryption Key file password	<input type="text"/>
Connection Encryption trust list	<input type="text"/>
Disable P2P/Group Chat Subscription	<input type="text" value="No"/> ▼
Disable Team/Channel Chat Subscription	<input type="text" value="No"/> ▼
Forward Proxy Address	<input type="text"/>
Forward Proxy Port	<input type="text"/>
Forward Proxy User	<input type="text"/>
Forward Proxy Password	<input type="password"/>
License Model	<input type="text" value="A"/> ▼

Step 15 - Click **Save**.

Step 16 - Repeat steps 13-15 for every Microsoft Teams connection.




Step 17 - Save the changes by clicking on the



icon.

Step 18 - Repeat Steps 5-17 for all Media Recorder servers.

Step 19 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

 There are tasks to be executed regarding the configuration of this Verba Server. If you would like to execute these tasks now, please [click here](#) .

Starting the service

Step 20 - Click on the **Service Control** tab.

Step 21 - Start the **Verba Unified IM Recorder Service** by clicking on the



icon.

Step 22 - Repeat Step 21 for all Media Recorder servers.

Configuring the Verba Unified IM Recorder Service on the Recording Director Servers

This configuration guide describes how to configure the Verba Unified IM Recorder service on a Recording Server (Recording Director) in the case of a highly available environment.

In order to complete the steps below, you must have the System Administrator role in Verba.

The configuration consists of the following steps:

- [Enabling the service](#)
- [Configuring the Verba Unified IM Recorder Service as Recording Director](#)
- [Starting the service](#)

Enabling the service

Step 1 - Log in to the Verba web interface and go to **System \ Servers** menu.

Step 2 - Select your **Recording Server (Recording Director)** from the list, then click on the **Service Activation** tab.

Step 3 - Activate the **Verba Unified IM Recorder Service** by clicking on the



icon.

Step 4 - Repeat Steps 1-3 for all Recording Director servers.

Configuring the Verba Unified IM Recorder Service as Recording Director

Step 5 - Click on the **Change Configuration Settings** tab.

Step 6 - Expand the **Unified IM Recorder \ General** node.

Step 7 - Set the **Role** setting to **Director Only**.

Step 8 - Expand the **Processing Queues** node.

Step 9 - Provide the **Number of Receiving Queues Owned by Director Role** setting. In the case of a highly-available setup, this setting can be calculated the following way:

"Number of Processing Queues Owned by Recorder Role" setting value on the Media Recorders * Numbe

Step 10 - Provide the network path of the processing queue root folder at the **SMB Queues Path** setting.

Step 11 - Provide a windows domain user credential at the **SMB Credential, User** and the **SMB Credential, Password** settings. The service will use this user when accessing the folder provided at the **SMB Queues Path** setting.

Step 12 - Expand the **Recording Providers \ Microsoft Teams** node.

Step 13 - At the **Microsoft Teams** setting, click on the



icon to add a new connection.

Step 14 - In the left panel, provide the following settings:

Setting Name	Description
Application (Client) ID	The ID of the App Registration (Registering an App for Chat Recording in Azure - Step 6 or Registering the Microsoft Teams Bot in Azure - Step 13)
Application (Client) Secret	The secret created for the App Registration (Registering an App for Chat Recording in Azure - Step 10 or Registering the Microsoft Teams Bot in Azure - Step 17)
Directory (Tenant) ID	The ID of the Azure tenant where the App Registration was created (Registering an App for Chat Recording in Azure - Step 6 or Registering the Microsoft Teams Bot in Azure - Step 29)
Notification URL	<p>The notification URL of the Unified IM Recorder service. The format is the following: https://server_CNAME.domain.com:3333/msteams. <i>Note: in case you're using any kind of network element that accepts incoming messages from Microsoft Teams servers and forwards it to your recorder(s), here you should use the port opened on that network element (not necessarily 3333). The port the recorder awaits messages on is configured in the next field.</i></p> <p>The Microsoft Graph API limits the subscriptions to resources on the same Tenant and AppID to 1. Because of this, the only correct way to create a highly available configuration with 2 Recording Directors is to configure recorders with the same Notification URL and Connection Encryption Certificate, and set the notification URL for a load balancer that distributes incoming requests between the running recorders. If configurations differ and multiple recorders are set up for the same Tenant and AppID, because of the Microsoft API limit of 1 subscription, each recorder will constantly delete other recorders' subscriptions and create their own.</p>
Event Listener Port	The event listener port of the Unified IM Recorder service. Set it to 3333.
Connection Encryption Certificate	<p>The thumbprint of the certificate that is used for the connection. The certificate has to reside in the Windows Certificate Store. The same certificate has to be used for all Teams connections on all the servers.</p> <p>Alternatively, a certificate file can be used instead of the Windows Certificate Store. In this case, the path to the .crt file has to be provided.</p>
Connection Encryption Key file	If the file path is provided at the Connection Encryption Certificate setting, then the path to the .key file has to be provided here.
Connection Encryption Key file password	If the file path is provided at the Connection Encryption Certificate setting, then the password of the .key file has to be provided here.
Connection Encryption trust list	The thumbprint of the incoming connection certificates that should be trusted, or the thumbprint of the CA certificates whose certificates should be trusted. If left empty, all certificates will be trusted.
Disable P2P /Group Chat Subscription	Sets whether the P2P or group chats should be recorded or not.
Disable Team /Channel Chat Subscription	Sets whether the Team or Channel chats should be recorded or not.

Forward Proxy Address	If a forward proxy is being used for the outgoing connection, then the proxy address has to be provided here.
Forward Proxy Port	The port of the forward proxy connection.
Forward Proxy User	The user of the forward proxy connection. Required, if the proxy requires authentication.
Forward Proxy Password	The password of the forward proxy connection. Required, if the proxy requires authentication.
Licensing Model	<p>The licensing model that is used for the chat archiving integration. The following licensing models are available:</p> <ul style="list-style-type: none">• A: Applications performing a security or compliance function, and requires a supported license. This is the default licensing model.• B: Applications that do not perform a security or compliance function.• Evaluation Mode: enables access to APIs with limited usage per requesting application for evaluation purposes. <p>More information: Licensing and payment requirements - Microsoft Graph</p>



Microsoft Teams IM

Application (Client) ID	<input type="text" value="EB17D4E0-CA1C-45D8-9356-DA0BF96BB55F"/>
Application (Client) Secret	<input type="password" value="....."/>
Directory (Tenant) ID	<input type="text" value="9F39980E-6E41-4399-BE16-060F8A99F73F"/>
Notification URL	<input type="text" value="https://imrecorder.contoso.com:3333"/>
Event Listener Port	<input type="text" value="3333"/>
Connection Encryption Certificate	<input type="text" value="6E8A7E9FDD294CD4BD3A91124F35419E"/>
Connection Encryption Key file	<input type="text"/>
Connection Encryption Key file password	<input type="password"/>
Connection Encryption trust list	<input type="text"/>
Disable P2P/Group Chat Subscription	<input type="text" value="No"/>
Disable Team/Channel Chat Subscription	<input type="text" value="No"/>
Forward Proxy Address	<input type="text"/>
Forward Proxy Port	<input type="text"/>
Forward Proxy User	<input type="text"/>
Forward Proxy Password	<input type="password"/>
License Model	<input type="text" value="A"/>

Step 15 - Click **Save**.

Step 16 - Repeat steps 13-15 for every Microsoft Teams connection.

- Recording Providers
 - Microsoft Teams

Microsoft Teams:  


Step 17 - Save the changes by clicking on the



icon.

Step 18 - Repeat Steps 5-17 for all Recording Director servers.

Step 19 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

 There are tasks to be executed regarding the configuration of this Verba Server.
If you would like to execute these tasks now, please [click here](#) .

Starting the service

Step 20 - Click on the **Service Control** tab.

Step 21 - Start the **Verba Unified IM Recorder Service** by clicking on the



icon.

Step 22 - Repeat Step 21 for all Recorder Director servers.

Configuring multi tenant Microsoft chat and channel archiving

In order to deploy Microsoft Teams chat and channel archiving in a multi tenant environment, follow the instructions below:

Step 1 - Create an app registration in the service/hosting provider tenant. For more information, see [Registering an App for Microsoft Teams chat and channel archiving in Azure](#)

Step 2 - Configure the Microsoft O365/M365 tenant ID for the Verba environment for each tenant under **System / Multi-tenant Administration / Environments / Teams tab / Teams Tenant ID**.

Step 3 - Configure the Azure User Object IDs (and/or team IDs for Export API based channel archiving) as recorded extensions for each tenant. For more information, see [Configuring Microsoft Teams Chat and Channel Archiving](#).

Step 4 - Configure a separate Recording Provider for each tenant. For more information,

- for DLP/Webhook, see [Configuring the Verba Unified IM Recorder Service for Microsoft Teams chat and channel archiving with DLP /Webhook API](#) and,
- for Export API, see [Configuring the Verba Unified IM Recorder Service for Microsoft Teams chat and channel archiving with Export API](#).

You can use the same app registration, as long as you have the admin consent for the tenant, but the **Directory (tenant) ID** must be the one configured for the Environment. Otherwise, you will need to have a separate app registration in each tenant. In the case of using the DLP/Webhook based integration, the **Notification URL** and the **Event Listener Port** must be unique for each tenant, otherwise, the service will not be able to assign the messages to the right tenant/environment.

Configuring IPC Unigy recording

For more information on the integration with IPC Unigy, see [IPC Unigy](#)

The configuration consists of:

Step 1 - [Configuring turrets for recording](#)

Step 2 - [Configuring secure communication between Unigy and Verba](#)

Step 3 - [Configuring Verba Unified Recorder service](#)

Step 4 - [Provision turret users for recording](#)

Step 5 - [Configure search layout to extend with IPC specific custom metadata](#)

Secure Recording

Configuring secure communication is required to record turrets which are configured to use secure connections/media encryption


Provisioning recorded agents

Agents/traders are identified by Unigy End User's personal extension. This should be added as Agent Id type extension

Configuring secure recorder communication for IPC Unigy

Unigy authenticates the recorder service via TLS, ie. the recorder service must provide a certificate trusted by Unigy at TLS handshake. This step describes how Unigy can sign a certificate request, so how to create the required certificate.

Step 1 - Create a Certificate Signing Request.

 Certificate's CN/Subject must be the IP of the recorder

The following command can be used to generate the CSR with OpenSSL

```
openssl req -new -newkey rsa:2048 -nodes -out c:\verba_ipc.csr -keyout c:\verba_ipc.key -subj "/C
```

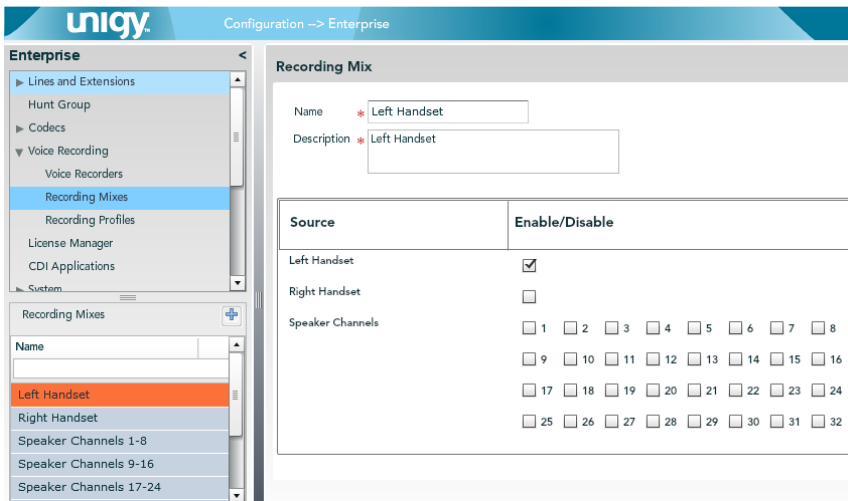
Step 2 - Post the CSR to Unigy and download the signed certificate by clicking on Generate signed certificate (Enterprise\Security\PKI\Device Certificates, 3rd party Integration tab)

Configuring turrets for recording

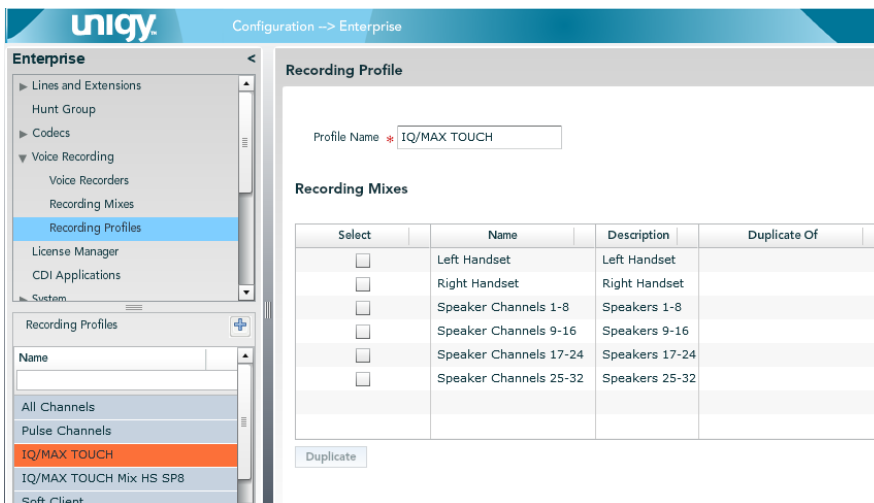
The configuration consists of defining recording mixes, assigning mixes to recording profile and assigning recorder profile to users.

Recording mix defines which audio sources are added to a recording channel

Step 1 - Create/modify recording mixes (Enterprise\Voice Recording\Recording Mixes)



Step 2 - Create/modify recording profile. Assign previously created mixes (Enterprise\Voice Recording\Recording Profiles)



Step 3 - If 2N recording is desired, define duplication for the relevant mixes in the profile. The duplicated channels will go to the secondary recorder as well

Recording Mixes

Select	Name	Description	Duplicate Of
<input checked="" type="checkbox"/>	All Channels	All Channels	
<input type="checkbox"/>	DUPLICATE - All Channels	All Channels	All Channels
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			

Duplicate

Step 4 - Assign recording profile to the users (System Designer/End User Configuration)

System Designer --> End User Configuration

Powered by

Turret type → IQ/MAX & Edge

User: Vtest3

Trad... Face ... Spea... Privi... Audio Displ... Soft... Pers... OCS Pulse CDI ... CU ... Snap... Sp

HFM Transmit Volume * 26

HFM Transmit Noise Reduce Mode * Low

HFM Transmit Auto Gain Control Mode * Off

HFM Receive Equalization * Off

Recording

Record Mix Profile IQ/MAX TOUCH

Number of Recording Licenses for the User: 2 and the number of Recording Channels: 2

IP Record Output Gain (dB) * 0

IP Record Handset Microphone Mix Gain (dB) * 0

IP Record Speaker Microphone Mix Gain (dB) * 0

Recording protocol * IP

Miscellaneous

Acoustic Feedback Reduction

Revert S

For each recorded user select the appropriate recording profile.

Step 5 - Set the Recording protocol to IP and save the configuration



Please note this is a device specific setting and so on right top corner the device type should be selected

Configuring Verba for IPC Unigy recording

The Verba Unified Recorder service should be enabled and configured for IPC Unigy recording as follows.

- [Active the Unified Call Recorder service on the Recording Servers](#)
- [Configure the Recording Director](#)
 - [Configure Unigy Zones](#)
 - [Configure certificate](#)
 - [Revise optional settings and save the configuration](#)
- [Configure the Media Recorder](#)
 - [Configure distributed Media Recorder and Recording Director](#)
- [IPC Unigy resilient recording configurations:](#)
 - [Configure 2N recording](#)
 - [Preparation](#)
 - [Configure the Recording Director:](#)
 - [Configure CTI failover \(N+1 Recording\)](#)
 - [Preparation](#)
 - [Configure the passive Recording Director:](#)

Active the Unified Call Recorder service on the Recording Servers

Step 1 - In the Verba Web Interface go to **System \ Servers**

Step 2 - Select the Recording Server from the list

Step 3 - Click on the **Service Activation** tab

Step 4 - Activate the **Verba Unified Call Recorder Service** by clicking on the



icon.

Step 5 - Repeat the steps on all Recording Servers (all servers with either a Media Recorder or Recording Director role or both) if there are multiple

Configure the Recording Director

Step 1 - In the Verba Web Interface go to **System \ Servers**

Step 2 - Select the server with the Recording Director role from the list

Step 3 - Click on the **Change Configuration Settings** tab and navigate to **Unified Call Recorder / Recording Providers / IPC Unigy**

Configure Unigy Zones


Step 4 - Add a new zone with the



icon under **Unigy Zones**. On the right panel, configure the zone configuration settings as described below:

IPC Zone

Zone VIP CTI URL	<input type="text" value="http://10.0.1.2/ctisvc/recording/CSTAService"/>
Local CTI port (leave empty for random port)	<input type="text" value="2320"/>
CCM SIP port (leave empty if default is used)	<input type="text" value="5060"/>
Secondary Recorder (2N)	<input type="checkbox"/>

Name	Description
Zone VIP CTI URL	<p>Enter the URL of the Unigy CTI service. It should be like http://zone_vip/ctisvc/recording/CSTAService where the host part must identify the Zone VIP.</p> <p>If secure communication is required the URL should be https://.... If HTTPS is configured recorder establishes recording channels via SIP over TLS as well.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"><p> If secure communication is configured, Verba should be configured to use a Unigy trusted certificate.</p></div>
Local CTI port	<p>This is a port on which Verba listens to CTI events from Unigy after subscription on these. If not configured, a random free port is selected in range 1024-65535. If for firewall reasons this should be a specific port then it can be configured. The port must be unique for each zone and free (ie other applications should not use it).</p>
CCM SIP port	<p>If for some reason Unigy does not use the standard/default 5060/5061 ports, then the SIP port number should be configured here.</p>
Secondary Recorder (2N)	<p>If 2N recording is required then one Recording Director should have the primary role, and the other Recording Director the secondary role. If it is enabled, the Recording Director will subscribe to "duplicate" mixes defined in the recording profile.</p>

Configure certificate

Step 5 - Configure the certificate settings if secure communication is used in zone configuration:

Name	Description
SSL/TLS Certificate	<p>Specify the certificate file/certificate thumbprint (a certificate stored in the Windows Certificate Store or PEM /PFX certificate file path). The certificate must be signed by Unigy.</p>
SSL/TLS Key	<p>If a file-based certificate (PEM) is used, the path of the private key file. If it is bundled with the certificate, then the same file should be set here.</p>
SSL/TLS Key Password	<p>Specify the password for the file that contains the certificate keys</p>

SSL/TLS Trust List	<p>Specify the list of certificates validating Unigy's certificate:</p> <ul style="list-style-type: none"> • empty: no validation on Verba side • thumbprint: either self-signed certificate with the thumbprint or CA-signed certificate where CA certificate matches the thumbprint is accepted • *: use windows top-level CA store • PEM file path: the file should contain the certificate chain for Unigy Enterprise
---------------------------	---

Revise optional settings and save the configuration

Step 6 - Review the following optional configuration settings:

Name	Description
CDR/Agent Event Subscription Keepalive (seconds)	The keepalive timer for the subscription. The lower value detects failure quicker but causes more load on Unigy.
Agent State Polling Period (seconds)	The timer for agent state polling, lower value detects failure quicker but causes more load on Unigy.
Unigy Controlled Recording	Recording decision from IPC should or not override Verba decision

Step 7 - Save the changes by clicking on the



icon.

Step 8 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

Configure the Media Recorder

Besides the general recording specific configuration, there are the following IPC Unigy specific configurations:

- **Unified Recorder / Media Recorder / Media Processing / IPC - Call Splitting (seconds)**: default value 3600 (1hr). Long calls (Speaker channel/Open lines) will be recorded as multiple records split every x seconds (1hr). This makes easier searching in the recorded content
- **Unified Recorder / Media Recorder / Media Processing / IPC - Voice Inactivity (seconds)**: default value 30. If turret stops sending media (even call is still ongoing) and timer elapses we stop the recording. As soon as media starts flowing again we create a new record for this segment. Detecting media activity helps to reduce required storage space (not recording long silence periods) and voice searchability. Voice detection relies on Turret's silence suppression/DTX feature

For more information on voice activity detection and call splitting, see [Configuring voice activity detection and call splitting for trader voice recording](#).

Configure distributed Media Recorder and Recording Director

If it is required, the Media Recorder and the Recording Director can be separated. The following guide contains our requirements and best practices on the subject: [Configuring recording high availability](#)

IPC Unigy resilient recording configurations:

Configure 2N recording

Preparation

The following method requires one Recording Server in each lane (or one Recording Director and a Media Recorder, in case of distributed components).

Configure the Recording Director:

Step 1 - In the Verba Web Interface go to **System \ Servers**

Step 2 - Select the server which has the Recording Director role

Step 3 - Click on the **Change Configuration Settings** tab and navigate to **Unified Call Recorder / Recording Providers / IPC Unigy**

Step 4 - Add a new zone with the



icon under **IPC Zones**. On the right panel, configure the zone configuration settings as described below:

IPC Zone

Zone VIP CTI URL	<input type="text" value="http://10.0.1.2/ctisvc/recording/CSTAService"/>
Local CTI port (leave empty for random port)	<input type="text" value="2320"/>
CCM SIP port (leave empty if default is used)	<input type="text" value="5060"/>
Secondary Recorder (2N)	<input type="checkbox"/>

Step 5 - Save the changes by clicking on the



icon.

Step 6 - Repeat the previous steps until Step 4 on the Secondary Recording Director, but under the **IPC Zones** check the Secondary Recorder (2N) option under the IPC Zones

IPC Zone

Zone VIP CTI URL	<input type="text" value="http://10.0.1.2/ctisvc/recording/CSTAService"/>
Local CTI port (leave empty for random port)	<input type="text" value="2320"/>
CCM SIP port (leave empty if default is used)	<input type="text" value="5060"/>
Secondary Recorder (2N)	<input checked="" type="checkbox"/>

Step 7 - Save the changes by clicking on the



icon.

Step 8 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

Configure CTI failover (N+1 Recording)

Preparation

For this setup two Recording Directors are required. One should be set as active CTI service, for this server, no additional configuration required, the other should be set as passive. A media stream can only be recorded by one server, the Recording Director decides the recording session based on agent login events \ polling.

⚠ If CTI failover redundancy is configured (standby Recording Director), there must be a very stable network connection between the two hosts. NIC teaming or crossover cable connection is required. If the network is lost between the two servers but both have an active connection to the IPC infrastructure, it could lead to unexpected situations and possible media loss, because both Recording Directors will actively try to control the same media stream.

Configure the passive Recording Director:

The following settings should be changed on passive Recording Director:

Step 1 - In the Verba Web Interface go to **System \ Servers**

Step 2 - Select the server which will act as the passive Recording Director

Step 3 - Click on the **Change Configuration Settings** tab and navigate to **Unified Call Recorder / Recording Providers / IPC Unigy**

Step 4 - Set the following configuration items:

- **Unified Recorder\Recording Providers\IPC Unigy\Passive CTI Service:** Yes
- **Unified Recorder\Recording Providers\IPC Unigy\Active CTI Service Address:** Monitoring address (FQDN, hostname, IP) of active Recording Director. If not the default API port (10031 UDP) is configured it should be specified too in server: port format

Step 5 - Save the changes by clicking on the



icon.

Step 6 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

IPC Unigy recorder resiliency

Media Recorder load-balancing and failover

Unified Recorder service has two logical roles which can be colocated on the same server or distributed across multiple servers.

These roles are in nutshell:

- Recording Director: integration point with telephony vendors, provides a unified layer/acts as a mediator for media establishment, CDR events to Media Recorder role
- Media Recorder: controlled by Recording Director it records media and stores CDR information in the database

If Recording Director and Media Recorders are separated on multiple servers and there are at least one Recording Director and two Media recorders, the Recording Director can:

- Distribute the media recording tasks between Media Recorders to provide load-balancing between them. Load-balancing takes into account recorder load feedbacks (CPU, number of concurrent recording, available disk space etc...). Due to the characteristics of Unigy's recording interface, load-balancing for Unigy unlike in case of other vendors does not happen at call level rather at turret level, i.e. since there are persistent recording channels established, the Media Recorder for a turret is selected at agent login time
- If a failed/offline recorder is detected then all the calls recorded on it can failover to other Media Recorders and recording continues from the failure point.

2N recording

In this setup two recorders receive the same CTI events and media streams, ie. each call is recorded twice, once by each of the two recorders.

One recorder must be marked as secondary due to:

- it should establish the duplicated mixes/media channels in the recording profile
- should mark the CDRs as a secondary record, so the UI/search can filter out the "duplications". There is an option to show secondary records too if something is missing

This setup can scale by separating Recording Director and Media Recorder role and adding the required number of Media Recorders. In each primary - secondary group there can be a single Recording Director and multiple Media Recorders. Secondary Media Recorders cannot be used by primary Recording director and vice versa

CTI/Recording Director failover

In this setup, there are two Recording Directors, one considered as active CTI service the other one as passive. To scale the deployment Media Recorders can be added.

The passive must be configured with a monitoring port pointing to the active. The passive service continuously monitors the availability of the active.

As soon as it fails, it takes over the CTI control until the active becomes available again.

This setup is only recommended if 2N recording is not desired but resiliency is a concern.

Configuring IP Trade recording

The Verba Unified recorder service allows you to record IP Trade calls using the RTP forking feature.

Step 1 - [Configuring IP Trade](#)

Step 2 - [Configuring Verba for IP Trade recording](#)

Step 3 - Add recorded users / traders to Verba

This can be done manually ([Extension list](#)) or using [Active Directory Synchronization](#). In case of IP Trade recording, instead of configuring the SIP addresses and directory numbers as recorded extensions, the user / trader IDs have to be configured. When adding (or synchronizing) the user IDs, the **Type** setting of the extensions has to be set to **User/Agent ID**. For TPO-based recording the name of the TPO has to be added as a recorded extension, and as the Description of the extension.

Step 4 - Test all recording scenarios

Configuring IP Trade

This section provides information on configuring the IP Trade trading solution for recording. For the latest configuration guides and options, please contact IP Trade directly.

For the supported turrets and versions, see [BT IP Trade](#)

For the detailed information regarding the configuration of the Verba IP Trade Recorder service, see [IP Trade Recorder settings](#).

- [TSS 9.3 and later](#)
 - [Recording server configuration](#)
 - [Turret-based recording configuration](#)
 - [Separated recorder mode](#)
 - [Mixed recorder mode](#)
 - [TPO-based recording configuration](#)
 - [Configuring Redundancy](#)
- [TSS 9.2 and earlier](#)
 - [System-wide configuration](#)
 - [Turret-based recording configuration](#)
 - [TPO-based recording configuration](#)
 - [Configuring Redundancy](#)
- [Playback on turret](#)
- [Parameter reference](#)

TSS 9.3 and later

Recording server configuration

- Step 1** Login to the web-based “TSS Console” administration interface.
- Step 2** Navigate to the **Device Management \Recording servers** menu.
- Step 3** Add a new recording server with **Add new**

The screenshot shows the configuration interface for a recording server. It has two tabs: 'General' and 'Links'. The 'General' tab is selected. The form contains the following fields:

- Title *: HU-BUDLAB-2N
- Recorder Brand: Verba (dropdown)
- Primary URI *: vrc://10.110.78.129:8000
- Secondary URI: vrc://10.110.78.128:8001
- Recorder Mixing Mode: Mixed (dropdown) with a warning icon and text: (⚠️ TPOs only support mixed recording mode and thus this value is ignored by TPOs.)

At the bottom, there are buttons for 'Update', 'Update and Go Back', 'Reset', 'Refresh', 'Cancel', and 'Delete' (which is highlighted with a red border).

Configure the recording server according to the following table:

Item	Example value	Description
Title	HU-BUDLAB-MR	Descriptive name of the recording server
Recorder Brand	Verba	Type of the recorder

Primary URI	vrc://10.110.77.129:8000	vrc://<IP address>:port number
Secondary URI	vrc://10.110.77.128:8000	vrc://<IP address>:port number
Recorder mixing model	Mixed	The recording mixing mode used

Turret-based recording configuration


- Step 1** Login to the web-based “TSS Console” administration interface.
- Step 2** Make sure **TPO-based recording** is not enabled.
- Step 3** Navigate to **Device Management** -> **Zones** -> System (or custom zone)
- Step 4** Go to the **General** tab then select the previously created recording server (*select disabled to turn off turret based recording*)
- Step 5** Click on the **Update** button to save the changes.
- Step 6** Select **Turret Boot Settings** tab, select the **Expert mode** Tab within, and select **Recorder** settings.
- Step 7** Set the **Recorder keep alive timeout** (*default recommended value is 1300*)
- Step 8** Set the following options to **True**:
 - Recorder keep alive
 - Send device type information
 - Recorder parse displayname in UTF8
 - Recorder wait DDI master callID

Separated recorder mode

Recording channels should not be set for separated mode, any defined channels should be removed

Mixed recorder mode

If mixed recording mode is used for turret based recording, it is necessary to set Recording channels.

- Step 1** Navigate to **Device Management** -> **Zones** -> System (or custom zone)
- Step 2** Go to the **Turret boot settings** tab then select the **Recorder** settings.
- Step 3** Go to the **Basic Mode** tab and define the Recording channel devices (Hints are provided by the right side in the  icon)
- Step 4** Select the **Expert mode** Tab, and set Send multi calls information to true.

TPO-based recording configuration

- Step 1** Login to the web-based “TSS Console” administration interface.
- Step 2** Make sure **Turret based recording** is not enabled.
- Step 3** Navigate to the **Device Management \ TPO Clusters** menu.
- Step 4** Go to the **General** tab then select the previously created recording server (*select disabled to turn off TPO based recording*)
- Step 5** Click on the **Update** button to save the changes.


Step 6 Select **Turret Boot Settings** tab, select the **Expert mode** Tab within, and select **Recorder** settings.

Step 7 Set the **Recorder keep alive timeout** (*default recommended value is 1300*)

Step 8 Set the following options to True:

- Recorder keep alive
- Send login in call information
- Send multi calls information
- Talkstate in call information
- Use TPO name/DNS name as Device Id and User Id for recording

Step 9 Click on the **Update** button to save the changes.

 The TPO should be added as a recorded extension in Verba, the Type of the extension has to be set to **User/Agent ID**, and the description should be TPO. This extension can be assigned to a technical user, or left unassigned.

Retention of TPO recordings

The media records from the TPO cannot be deleted as long as CDR records from users are referencing it. If [Data retention](#) is utilized, this means that the media records are implicitly under the longest retention. It is recommended to set this retention explicitly if **Automatically Delete Conversations after the Retention Period is Over** is used in the [Upload policy](#). In this case the best practice is to assign the TPO extensions to a technical user, and set the highest retention period for this technical user.

Configuring Redundancy

Step 1 In the Recording server configuration two recording servers should be provided

- For **2N** recording: [vrc://192.168.2.1:8000;vrc://192.168.2.2:8001](#)
- For **N+1** recording: [vrc://192.168.2.1:8000;vrc://192.168.2.2:8000](#)

Step 2 After **Step 4** in the TPO or Turret based recording configuration select **Boot Settings**

Step 3 Move to the **Expert mode** Tab, and select **Recorder** settings.

Step 4 Select the **Redundancy dual stream mode** setting. Set to true for **2N** or false for **N+1** recording mode.

Step 5 Click on the **Update** button to save the changes.

TSS 9.2 and earlier

System-wide configuration

Step 1 Login to the web-based “TSS Console” administration interface.

Step 2 Navigate to **Device Management -> Zones -> System (or custom zone) -> Turret Boot Settings** (Tab)

General TPO Boot Settings **Turret Boot Settings** Turrets Mobile Trader TPO TPO Cluster TPO DNS Users Shared Profiles Adv. Telephony

Turret Boot Settings + Pre-defined settings

Basic Mode Expert Mode Advanced Mode

	Name	Value	Description
PBX Features Recorder RTP	<input type="checkbox"/> Recording channel 10 devices	<input type="text"/>	?
	<input type="checkbox"/> Recording channel 11 devices	<input type="text"/>	?
	<input type="checkbox"/> Recording channel 12 devices	<input type="text"/>	?
	<input type="checkbox"/> Recording channel 13 devices	<input type="text"/>	?

Step 3 Go to **Recorder** (on Left Button/Tabs) and on the **Basic** (Tab) check **Recorder compatibility** to "iptrade".

Step 4 Move to the **Expert** (Tab) still under the Recorder settings and Enable **Keep-Alive** on all recorded turrets.

Step 5 Move to the **Advanced Mode** (Tab), and add the following key:

profile.setting.disablerecorder = false

`profile.setting.disablerecorder` false

Turret-based recording configuration

Step 1 Create a **Shared Profile** which will be attached to all of the recorded turrets (if there is an existing shared profile for recording it can be used for these settings but make sure it is assigned to all of the recorded turrets).

Device Management Account Management **Telephony** Security System Console

Users Shared Profiles

Server time: 12:33:08 Last refresh time: 12:32:22 Refresh Add new Bulk admin selected 1 / 1

Name *	Zone	Comment	Last modification date *
Mixed Mode	System		11/20/2018 11:28:45 AM

Step 2 In the **Shared Profile** (created above) apply the following settings:

Account Management: Shared Profile Edition (Mixed Mode)

Device Management Account Management **Telephony** Security System Console

[<< Back to Shared Profiles list](#)

General Lines Adv. Telephony **Settings** Screen Layout Call Notification Shortcuts Call History

Settings

Basic Mode Expert Mode Advanced Mode

	Name	Value	Description
PBX Features Recorder	<input type="checkbox"/> Recording channel 10 devices	<input type="text"/>	?
	<input type="checkbox"/> Recording channel 11 devices	<input type="text"/>	?

Step 3 Select the **Settings** (Tab) and then the **Recorder** (Button/Tab on left) and go to **Basic Mode** (Tab) and set the Recording server address. (<vrc://192.168.5.69:8000>)

Step 4 Set **Recording Mixing mode** to **separated**.

Step 5 Set at least 1 or both Handsets to record. (There is additional help provided on the right side in the



icon)

Step 6 Click on the **Update** button to save the changes.

<input checked="" type="checkbox"/> Recording channel 0 devices	<input type="text" value="HS1"/>
<input checked="" type="checkbox"/> Recording channel 1 devices	<input type="text" value="HS2"/>
<input checked="" type="checkbox"/> Recording channel 2 devices	<input type="text" value="applet.1"/>
<input checked="" type="checkbox"/> Recording channel 3 devices	<input type="text" value="applet.2"/>

TPO-based recording configuration

Step 1 Login to the web-based TSS administration interface.

Step 2 Navigate to the **Device Management \ TPOs** menu.


Step 3 Select the TPO from the list.

Step 4 Go to the **Boot Settings** tab (Basic Mode).

Step 5 Set the **Recorder compatibility** setting to **iptrade**.

Step 6 Provide the Verba Recording Server(s) in the **Recorder Server** setting in `vrc://server_name:port` format.

Step 7 Click on the **Update** button to save the changes.

 The TPO should be added as a recorded extension in Verba, the Type of the extension has to be set to **User/Agent ID**. This extension should not be assigned to a user.

Configuring Redundancy

Step 1 Login In **Step 7** of Turret-based recording or **Step 6** of TPO-based recording, two recording servers should be provided:

- For **2N** recording: `vrc://192.168.2.1:8000;vrc://192.168.2.2:8001`
- For **N+1** recording: `vrc://192.168.2.1:8000;vrc://192.168.2.2:8000`

Step 2 Move to the **Expert mode** (Tab) still under the Recorder settings and select the **Redundancy dual stream mode** setting. Set to true for **2N** or false for **N+1** recording mode.

Step 3 Click on the **Update** button to save the changes.

Playback on turret

 The Verba Recording System **does not require a separate IP Trade ReplayBox component** to provide playback-on-turret functionality. The Agent needs the [User permission](#) Play Conversation in Verba for the playback functionality.

❗ If the recording server is not co-located with the media repository, the playback will not work if the configured storage target is Media Repository Local Disk.

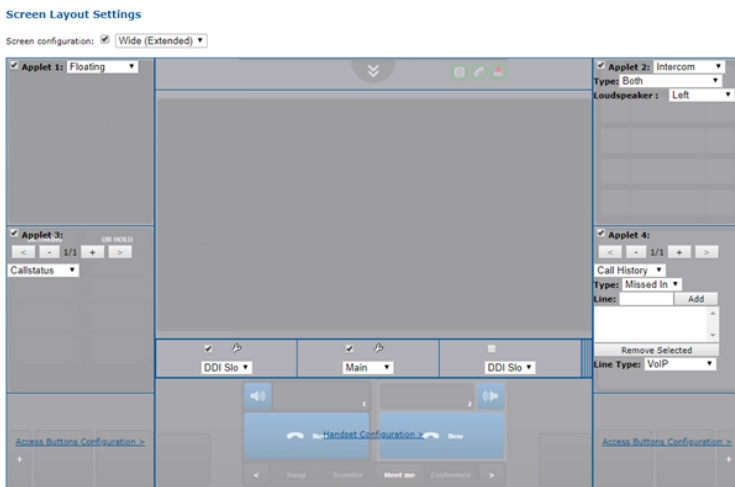
Step 1 Set **Authorize Replay** to **true**.

Authorize replay true false

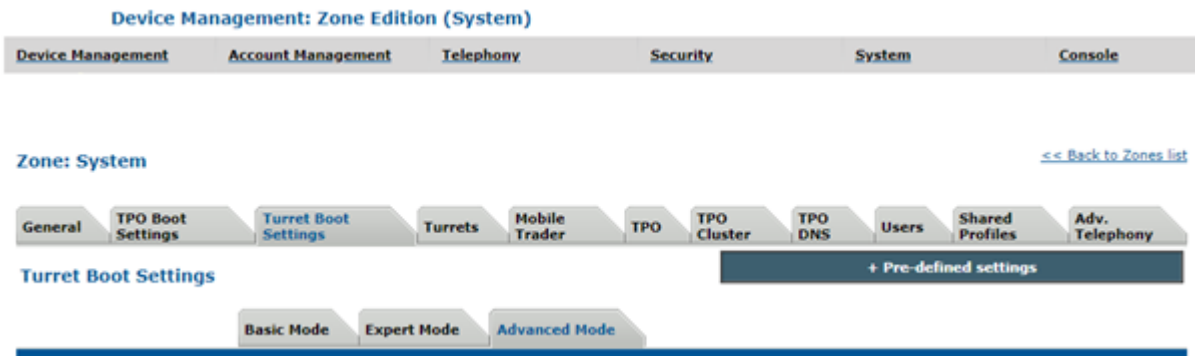
Step 2 Set the **ReplayBox URL** to <http://192.168.5.69:8000> (Verba recorder IP)

ReplayBox URL

Step 3 To see the Replay panel on the turrets, go to the shared profile's for all turrets and go to the **Screen Layout** tab and from there go to the **Access Button Configuration** and add the **Recorder** button to the menu.



Step 4 In **Device Management** -> **Zones** -> **System** (or custom zone), select the **Turret Boot Settings** (Tab) and then the **Advanced Mode** (Tab)



Step 5 Add the following key:

application.global.replay.mode = TCP

`application.global.replay.mode` TCP

Step 6 Make sure to reboot all recorded turrets after the configuration changes.

Recorder configuration

Audio	Name	Value	Description
Recorder Server	<input checked="" type="checkbox"/>	vrcc://10.12.1.104:11999	
Automatic actions	<input type="checkbox"/> Recording mixing mode	<input type="radio"/> separated <input type="radio"/> mixed	
Bluetooth	<input type="checkbox"/> Record group intercom through active recording	<input type="radio"/> false <input type="radio"/> true	
Call History	<input type="checkbox"/> Default recording channel	0	
CRM	<input type="checkbox"/> Recording channel 0 devices		
Devices	<input type="checkbox"/> Recording channel 1 devices		
DDI - Sharing	<input type="checkbox"/> Recording channel 2 devices		
Dial Plan	<input type="checkbox"/> Recording channel 3 devices		
Highlights	<input type="checkbox"/> Recording channel 4 devices		
Inter-turret messaging (highmax)	<input type="checkbox"/> Recording channel 5 devices		
Intercom	<input type="checkbox"/> Recording channel 6 devices		
Join - Barge	<input type="checkbox"/> Recording channel 7 devices		
Layout	<input type="checkbox"/> Recording channel 8 devices		
PBX Features	<input type="checkbox"/> Recording channel 9 devices		
PTN Synchronization	<input checked="" type="checkbox"/> Authorize replay	<input checked="" type="radio"/> true <input type="radio"/> false	
Recorder	<input checked="" type="checkbox"/> ReplayBox URL	http://10.12.1.104:11999/	
Search	<input type="checkbox"/> ReplayBox secondary URL		
Session	<input type="checkbox"/> ReplayBox userid		
Shortcut Notification	<input type="checkbox"/> ReplayBox user password		
Text messaging			
TPO	<input type="button" value="Update"/> <input type="button" value="Refresh"/>		

Keep alive configuration

Recorder	<input type="checkbox"/> Call retry timer	All	500,1000,2000,4000
Search	<input type="checkbox"/> Registration valid on call failure	All	30000
Session	<input type="checkbox"/> Maximum delay before registration check on call failure	All	10000
Shortcut Notification	<input type="checkbox"/> Disable recorder private button	All	<input type="checkbox"/> true <input type="checkbox"/> false
Text messaging	<input type="checkbox"/> Replay advanced call merge	All	<input type="checkbox"/> true <input type="checkbox"/> false
TPO	<input type="checkbox"/> Replay receive timeout	All	90000
User Settings	<input type="checkbox"/> Recording mode	All	dynamic static
Video	<input type="checkbox"/> Recorder mixing codec	All	0
	<input type="checkbox"/> Optional start/stop recording message	All	<input type="checkbox"/> true <input type="checkbox"/> false
	<input checked="" type="checkbox"/> Recorder keep alive	All	<input checked="" type="radio"/> true <input type="radio"/> false
	<input type="checkbox"/> Recorder keep alive	All	00-18-10-00-01-SE <input type="checkbox"/> true <input type="checkbox"/> false
Key: application.global.recorder.keepalive			
Description: The keep alive mode should be activated both on the Recorder Server side and on the Turret side. If keep alive mode is activated, the Recorder Server sends periodically a keep alive message. The connection will be considered as lost if no keep alive message is received by the turret during a defined time.			
	<input type="checkbox"/> Passive recorder IP address	All	
	<input type="checkbox"/> Passive recorder port for channel 0	All	
	<input type="checkbox"/> Passive recorder port for channel 1	All	
	<input type="checkbox"/> Passive recorder port for channel 2	All	
	<input type="checkbox"/> Passive recorder port for channel 3	All	
	<input type="checkbox"/> Passive recorder port for channel 4	All	

Parameter reference

! Please make sure you follow the **Location** field (FTP or Shared Profile) in this table. If not properly followed, **recording and/or playback-on-turret will not work.**

Configuration Name and Key	Location	Value	Description
----------------------------	----------	-------	-------------

Recorder compatibility application.recorder.compatibility	FTP	iptrade	Defines which type of recorder is in use. For Verba Recording System it has to be the default value: iptrade.
Recorder server profile.setting.activerecording	Shared Profile	vrc://192.168.2.1:8000	Recorder Server URI for active recording. Format: vrc://recorder_address:port For redundancy, add the second recorder after ";" Example: vrc://192.168.2.1:8000;vrc://192.168.2.2:8001 The port number is configured in the Verba Recording System, see IP Trade Recorder settings .
Recording mixing mode profile.setting.recording.mixingmode	Shared Profile	separated	Indicates the mixing mode: <ul style="list-style-type: none"> • separated: each call is recorded separately by recorder channel at the same time. We use one recorder channel per call. • mixed: calls can be recorded on the same recorder channel at the same time. One recorder channel can be used for several calls at the same time.
Default recording channel profile.setting.recording.default.channel	Shared Profile	0	All devices which are not configured to be recorded on a particular channel are recorded on the default channel set using this key No effect if mixing mode is not "mixed".
Recording channel 0..9 devices profile.setting.recording.channel.0..9.devices	Shared Profile		Devices recorded on channel 0 (mixing mode only). Multiple devices may be listed separated by ',' character. For advanced GUI editions, applet may be referenced in this key.
Authorize replay profile.setting.authorizereplay	Shared Profile	true	Defines if recorder replay is authorized on the turret.
ReplayBox URL profile.setting.replaybox.url	Shared Profile	http://192.168.2.1:8000	Defines the URL path to the ReplayBox module for recording replay features. Format: http://recorder_address:port The port number is configured in the Verba Recording System, see IP Trade Recorder settings . If you have multi-server deployment, where you have a separated Media Repository, you have to point the replay URL to a server where the Verba Unified Call Recorder Service is running.
Replay mode application.global.replay.mode	FTP	TCP	Defines the replay mode.
Disable recorder profile.setting.disablerecorder	Shared Profile	false	Specifies if the recorder button is disabled on the screen. If true, the user is not able to access the recorder panel.
Recorder icon blink count profile.setting.recorderblinkingcount	Shared Profile	10	Defines the number of times the recorder icon has to blink (red) when the recorder connection fails.

Configuring Verba for IP Trade recording

Step 1 - In the Verba Web Interface, go to **Administration / Verba Servers**. Select your Recording Server and click on the **Service Activation** tab.

Step 2 - Activate the **Verba Unified Call Recorder Service** by clicking on the



icon.

Step 3 - Click on the **Change Configuration Settings** tab. Expand the **Unified Call Recorder** section.

Step 4 - Under the **Recording Providers \ IP Trade** node, verify the settings. Update the **Listening Port** if required.

Step 5 - If TPO-based recording is utilized, under the **Recording Providers \ Integration** node, verify that the the **Force Recording Media on Director** is set to **Yes**.


Step 6 - Review the **Media Recorder** and **Media Processing** configuration. For more information on voice activity detection and call splitting, see [Configuring voice activity detection and call splitting for trader voice recording](#).

Step 7 - Save the changes by clicking on the



icon.

Step 8 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

 There are tasks to be executed regarding the configuration of this Verba Server. If you would like to execute these tasks now, please [click here](#) .

Step 9 - Click on the **Service Control** tab.

Step 10 - Start the **Verba Unified Call Recorder Service** by clicking on the



icon.

Configuring BT ITS recording

AVAILABLE IN VERSION 9.4 AND LATER

For more information on the integration with BT ITS, see [BT ITS](#)

The configuration consists of:

Step 1 - Review the [BT ITS recording network and server requirements](#) and [Understanding TTP numbering rules](#)

Step 2 - Configure the BT ITS switch for recording, contact your BT representative for more information

Step 3 - [Configuring BT ITS media recording](#)

Step 4 - [Configuring BT ITSLink CTI](#)

Step 5 - [Configuring BT ITS TMS and LDAP based provisioning](#)

Step 6 - [Configure recorded traders as users](#) and [their associated extensions](#). It is necessary to create all traders as users and to add trader IDs as extensions in order to apply recording rules (the system only records configured trader IDs) and to enable security for conversation browsing. At extension configuration select **User/Agent ID** for type. The LDAP/TMS file based configuration does not automatically create /update/delete users and extensions in the system. To restrict the visibility of recordings, [configure groups, and add users to groups](#). Based on a group you can control access to other user's calls. Users, groups, and extensions can be also provisioned via [Active Directory Synchronization](#).

Step 7 - [Configuring media stitching adjustment](#)

Step 8 - [Configure search layout to extend view with BT ITS specific metadata](#)

Step 9 - [Creating a BT ITS dashboard](#)

Step 10 - Verify functionality by making test calls and checking the results in search. It is possible to search based on user/trader id (even if the call is not assigned to a user) in the Conversation View. You can achieve specific call type filtering according to Source Platform. For example, select **BT ITS** to search for trading recordings.

BT ITS recording network and server requirements

BT ITS recording has very specific requirements for the network. Below you can find the key requirements. For more detailed information, contact your BT representative.

- **One-way network delay** between IP Voice Recorders and the IPSI should not exceed 400ms on a LAN or WAN. Delays of more than this will affect the ability to link CTI data with Vox segments.
- **Network jitter** on the same path should not exceed 20ms on LAN or WAN.
- **Separate Network connections** for N+1 deployments and use separate NICs for Management, IPSI LAN A and IPSI LAN B. NIC teaming is not supported and it is mandatory to use separate physical network connections for the VM hosts. In the case of 2N recording, use a separate NIC for the ITS voice traffic and another NIC for everything else.
- **Sufficient network bandwidth** must be provided for the number of TTPs and Management traffic. Since TTPs do not use a VAD codec, silence is always present and therefore a continuous 32 channel voice stream for each TTP. This will occupy around 2.6 Meg of bandwidth on an IP network. The TTP packets will be QOS marked as EF by default and will need to be treated as Class 1 voice by the network.
- **Minimal network hops:** the factory default IPSI heartbeat TTP Voice LAN settings are required to ensure reliable voice delivery and it is not recommended they be adjusted.
- **NetBIOS must be disabled** on all LANs that the recorder components are connected to, except the Management LAN. Specifically, this means the Voice LAN. The reason for this is that server names would be resolved on the Voice LAN and that would break the fault-tolerant model, i.e., when Management LAN cable is removed, the Unified Recorder or Director is still accessible via the Voice LAN. Access Control Lists (ACLs) might need to be put in place to prevent this. No Default Gateway must be configured for any recorder Voice LAN NICs.
- **Maximum 64 TTPs** can be allocated to a single recorder. The system is distributing the TTPs across the Media Recorders evenly by default. The system can be configured to assign specific TTPs to specific Media Recorders. In either case, a single Media Recorder will be only assigned to maximum 64 TTPs by the Recording Director.

BT ITS TTP numbering conventions

The recorder filters the recorded verticals based on the Voice Recorder ID (or Cluster ID) defined for the TTPs. Filtering applies for both to establish media streams and processing calls from CTI messages. In general, the Voice Recorder ID(s) of the TTPs configured on the BT ITS switch side and the list of recorded Voice Recorder IDs configured on the recorder side must be consistent.

2N deployments

2N recording is not natively supported by the BT ITS system, but with consistent TTP allocation and configuration, the same vertical can be assigned to multiple TTPs, so each TTP is sent to two separate recorders. The duplicated streams can be correlated by a mapping between the TTP IDs (addresses). 2N recording deployments have two lanes: a primary and a secondary, which define the recorder group (both Recording Director and Media Recorders) recording the primary copy or the secondary copy of the calls.

The mapping/correlation algorithm is as follows:

- Each primary lane TTP has an odd Voice Recorder ID (or Cluster ID)
- The secondary pair has the next even number as the Voice Recorder ID (or Cluster ID)
- This implies that a device assigned to a timeslot must have the same trunk and channel/slot ID on the primary/secondary TTP

For example, the left handset of a turret is assigned to the TTP channel 1.1.1 (Voice_Recorder_ID.Trunk_ID.Channel_ID) then the secondary 2N pair must be assigned to TTP 2.1.1

Campus deployments

In a BT ITS campus deployment, the recording must be done on recorders closest to the given DC, sharing recorders across multiple DCs is not supported. CTI / LDAP / TMS is not aware of turret location in a campus deployment as the BT ITS system is a single switch deployed across two locations. The Voice Recorder ID(s) of the TTPs are intended to use for distinguishing recorder pools deployed in the different data centers.

The mapping/correlation algorithm is as follows:

- DC A turrets must be linked to recorders in DC A, so their TTPs must have a DC A specific Voice Recorder ID and this ID should be configured on the recorder side as well to filter for these devices, respectively the same has to be done for the other DC as well
- if 2N is configured then the odd-even numbering rule must be taken into account when assigning Voice Recorder IDs

For example:

- N+1 recorder redundancy in 2 DCs: DC A has Voice Recorder ID 1, DC B has 2, this means that the TTP channels 1.x.x will be handled by DC A and 2.x.x will be handled by DC B
- 2N recorder redundancy in 2 DCs: DC A has Voice Recorder ID 1,2, DC B has 3,4, this means TTP channels 1.x.x and secondary 2N pairs 2.x.x will be handled by DC A, 3.x.x and secondary 2N pairs 4.x.x will be handled by DC B


Configuring BT ITS media recording

Media recording involves the BT Heartbeat and Directory service which acts as a proxy/mediator between the Media Recorder and the BT ITS IPSI system. Once the recorder service is started, it controls the state of the BT services as well, i.e. it starts/stops and monitors their state. When the BT service is up, it periodically checks the recorder service for TTPs in interest and establishes PWE3 streams to media ports provided by the recorder service. The configuration consists of configuring the BT services and Media Recorder (Unified Recorder service).

- [Prerequisites](#)
 - [The local_ipconfig.txt file](#)
 - [Example for unicast setup](#)
 - [Example for multicast setup](#)
 - [The global_ipconfig.txt file](#)
- [Configuring the Unified Recorder service](#)
 - [Mandatory configuration steps](#)
 - [Active the Unified Call Recorder service on the Recording Servers](#)
 - [Configure the Media Recorder servers](#)
 - [Configure the Recording Director servers](#)
 - [Configuration reference](#)

Prerequisites

- Create NICs as per failover/redundancy requirements and configure static IP routing
- Install BT Voice Recorder Heartbeat service (3.0.0 or newer)
- Create c:\ITS\TFTP_Root\local_ipconfig.txt

 The ITS Heartbeat Voice Recorder Service and the ITS Directory Service must set with "manual" startup mode (default after installation). Do not change it to automatic or disabled.

The local_ipconfig.txt file

The config file should enumerate the friendly name of NICs. It tells the BT services which NICs should be used for specific network communications

Example for unicast setup

```
[Adapters]
ITSdataLan=Management LAN
ITSVoiceLanA=VLAN A
ITSVoiceLanB=VLAN B
[Physical]
CardId=VoiceRecorder

[Unicast Directory Services]
VoiceRecorder=ds_proxy.1,ds_proxy.2
```

Example for multicast setup

```
[Adapters]
ITSdataLan=Management LAN
ITSVoiceLanA=VLAN A
ITSVoiceLanB=VLAN B
```

[Physical]
CardId=VoiceRecorder

The global_ipconfig.txt file

This file is provided by the ITSProfile server via TFTP share and is populated automatically by the recorder service at startup. Please make sure the following setting is present:

[VR]
SwapTTPonHealthy=false

Configuring the Unified Recorder service

BT ITS/IPSI	
Recording Server Role:	<input checked="" type="checkbox"/> Recording Director and Media Recorder
Voice Recorder IDs:	<input checked="" type="checkbox"/> 1 2
TTP Codec:	<input type="checkbox"/> G.711 A-Law
IPSI/Media 2N Recording Mode:	<input checked="" type="checkbox"/> Primary
Active TTP Manager:	<input checked="" type="checkbox"/> rs-standby.verbalabs.com
Management VLAN IP:	<input checked="" type="checkbox"/> 10.10.10.10
Voice VLAN1 IP:	<input checked="" type="checkbox"/> 10.10.11.10
Voice VLAN2 IP:	<input checked="" type="checkbox"/> 10.10.12.10
Number of Media Processing Threads:	<input type="checkbox"/> 64
BT Heartbeat Listening Port:	<input type="checkbox"/> 4010
TTP Timeout (seconds):	<input type="checkbox"/> 15
TTP Distribution Timer (seconds):	<input type="checkbox"/> 5
BT Heartbeat Service Timeout (seconds):	<input type="checkbox"/> 12
IPSI TFTP 1 URL:	<input checked="" type="checkbox"/> tftp://itsink1.verbalabs.com/global_ipconfig.txt

Mandatory configuration steps

Related configuration can be found under Unified Call Recorder\BT ITS\IPSI

Active the Unified Call Recorder service on the Recording Servers

Step 1 - In the Verba Web Interface go to **System \ Servers**

Step 2 - Select the Recording Server from the list

Step 3 - Click on the **Service Activation** tab

Step 4 - Activate the **Verba Unified Call Recorder Service** by clicking on the



icon.

Step 5 - Repeat the steps on all Recording Servers (all servers with either a Media Recorder or Recording Director role or both) if there are multiple.

Configure the Media Recorder servers

Step 1 - In the Verba Web Interface go to **System \ Servers**

Step 2 - Select the Recording Server from the list

Step 3 - Click on the **Change Configuration Settings** tab and navigate to **Unified Call Recorder / Recording Providers / BT ITS/IPSI**

Step 4 - Enable Media Recorder mode at **Recording Server Role**

Step 5 - Configure **TTP Codec** as per BT side codec being used (TTP Codec)

Step 6 - Configure the IPv4 address of the IPSI Management VLAN NIC at **Management VLAN IP***. If the setting is empty, it defaults to "Network \ System \ Server IPv4 Address".

Step 7 - Configure the IPv4 address of the IPSI Voice A VLAN NIC at **Voice VLAN1 IP***. If the setting is empty it defaults to "Network \ System \ Server IPv4 Address".

Step 8 - Configure the IPv4 address of the IPSI Voice B VLAN NIC at **Voice VLAN2 IP***. If the setting is empty it defaults to "Network \ System \ Server IPv4 Address".

Step 9 - Configure the TFTP address(es) of the ITS Profile server at **IPSI TFTP1/2 URL****, where the global_ipconfig.txt file is shared.

Step 10 - Review the **Media Recorder** and **Media Processing** configuration. For more information on voice activity detection and call splitting, see [Configuring voice activity detection and call splitting for trader voice recording](#).

Step 11 - Save the changes by clicking on the



icon.

Step 12 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

Step 13 - Click on the **Service Control** tab.

Step 14 - Start the **Verba Unified Call Recorder Service** by clicking on the



icon.

Step 15 - Repeat the steps on all Media Recorder servers.

* Addresses must be consistent with the NIC names provided in local_ipconfig.txt.

** At least one TFTP URL is required. The config file is retrieved at service startup. If it cannot be retrieved then the previous local copy is used and alert is raised.

Configure the Recording Director servers

Step 1 - In the Verba Web Interface go to **System \ Servers**

Step 2 - Select the Recording Server from the list

Step 3 - Click on the **Change Configuration Settings** tab and navigate to **Unified Call Recorder / Recording Providers / BT ITS/IPSI**

Step 4 - Enable Recording Director or Recording Director & Media Recorder mode under **Recording Server Role**. In case both Recording Director and Media Recorder roles are required, configuring the Media Recorder component as well.

Step 5 - Configure the list of the **Voice Recorder IDs** (previously configured on the BT side) the service should handle. It must contain both primary and secondary IDs in case of 2N recording.

Step 6 - Set 2N mode depending on the deployment architecture at **IPSI / Media Recording 2N Mode**.

Step 7 - In case it is a Standby Recording Director, define the API address of the Active Recording Director at **Active TTP Manager**.

If TTP Manager redundancy is configured (standby Recording Director), there must be a very stable network connection between the two hosts. NIC teaming or crossover cable connection is required. If the network is lost between the two servers but both

have an active connection to the BT infrastructure and to the Media Recorder servers, it could lead to unexpected situations and possible media loss, because both Recording Directors will actively try to control TTPs.

Step 8 - Save the changes by clicking on the



icon.

Step 9 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

Step 10 - Click on the **Service Control** tab.

Step 11 - Start the **Verba Unified Call Recorder Service** by clicking on the



icon.

Step 12 - Repeat the steps on all Recording Director servers.

Configuration reference

Name	Description
Recording Server Role	<p>Defines the role of the server:</p> <ul style="list-style-type: none"> Recording Director: deals only with TTP management only, it distributes and moves TTPs across media recorders Media Recorder: deals only with media recording. It receives TTPs to be handled from the Recording Director, establishes PWE3 streams via BT Heartbeat and Directory services and creates media records on the channels we are interested in Recording Director + Media Recorder: includes both functionality <p>For Recording Director functionality either TMS or LDAP based BT ITS platform provisioning and Voice Recorder IDs must be configured</p>
Voice Recorder IDs	<p>New line separated list of the Voice Recorder IDs configured in the BT ITS switch. The Recording Director will allocate only the TTPs to the Media Recorder(s) which are assigned to the configured Voice Recorder IDs in the BT ITS configuration.</p>
TTP Codec	<p>Voice codec which is being used to compress voice streams, it can be G.711 A-Law or U-Law</p>
IPSI / Media 2N Recording Mode	<p>Defines if this Recording Director should deal with primary or secondary TTPs for 2N recording, or no 2N recording is configured. The following valid values apply:</p> <ul style="list-style-type: none"> Disabled Primary Secondary
Active TTP Manager	<p>Defines the IP address / hostname (and port number) of the active Recording Director in case it is a Standby Recording Director. The standby Recording Director monitors the state of the active Recording Director and once there is no connectivity, it takes control over for TTP management across the Media Recorders.</p> <p>In case the default API port (10031) is configured on the active Recording Director, only the IP address /hostname has to be defined.</p> <p>In case the API port is not the default 10031 on the active Recording Director, define the port number as well: ip_address_or_hostname:port</p>

Management VLAN IP	IPv4 address of the NIC connecting IPSI management LAN. If it is not defined, it defaults to Server Local IPv4 address configuration.
Voice VLAN1 IP	IPv4 address of the NIC connecting IPSI VLAN A. If it is not defined, it defaults to Server Local IPv4 address configuration.
Voice VLAN2 IP	IPv4 address of the NIC connecting IPSI VLAN B. If it is not defined, it defaults to Server Local IPv4 address configuration.
Number of Media Processing Threads	Number of media processing threads to be used by the Media Recorder component
BT Heartbeat Listening Port	UDP port on which the Media Recorder listens to BT Heartbeat Service requests
TTP Timeout (seconds)	Defines media timeout in seconds on a TTP. After the timeout value, it is considered unhealthy and, if possible, the Recording Director moves the TTP to another Media Recorder.
TTP Distribution Timer (seconds)	Defines how often the Recording Director checks the state of the TTPs on the Media Recorders and changes TTP allocation when needed. The value should be set to TTP Timeout / 2 or less.
BT Heartbeat Service Timeout (seconds)	The timeout value in seconds for the BT Heartbeat service. The Media Recorder controls when the BT Heartbeat and Directory services should start and stop and also monitors their state. If the BT service is not responding within the configured timeout value, the BT services will be restarted to recover from error states.
IPSI TFTP 1 URL	TFTP address on the IT Profile server where the global_ipconfig.txt is downloaded from. ftp://itslnkserver/global_ipconfig.txt
IPSI TFTP 2 URL	TFTP address on the IT Profile server where the global_ipconfig.txt is downloaded from. ftp://itslnkserver/global_ipconfig.txt

Configuring BT ITSLink CTI

The CTI connection is established between the BT ITS ITSLink server and the Recording Director servers. The CTI feed from BT ITS switch provides call meta information and events for the recording service.

Configuring the Unified Recorder service


Step 1 - In the Verba Web Interface go to **System \ Servers**

Step 2 - Select the Recording Director from the list

Step 3 - Click on the **Change Configuration Settings** tab and navigate to **Unified Call Recorder / Recording Providers / BT ITS/IPSI**

Step 4 - Configure the settings based on the description below:

ITS Links:	<input checked="" type="checkbox"/>	<input type="text" value="itslink.verbalabs.com 3001 0"/>
ITS Link Timeout (seconds):	<input type="checkbox"/>	<input type="text" value="70"/>
Use ITS Timestamps in CDR:	<input type="checkbox"/>	<input type="text" value="No"/>

Name	Description
ITS Links	List of BT ITSLink servers connected to the Recording Director. Click on the  icon to add a new server using the form on the right. <ul style="list-style-type: none">• ITSLink Server: FQDN or IP address of the BT ITSLink server• Port: port on which the BT ITSLink server listens (defaults to 3001)• Secondary: defines if the CTI/CDR record is primary or secondary when multiple Recording Directors are deployed.
ITS Link Timeout (seconds)	Defines the ITSLink timeout value in seconds. There is a keepalive mechanism between the Recording Director and the ITSLink service. This setting must be consistent with BT side setting and should be +5-10 sec bigger to have a safe room for clock drifts, network/processing delays.
Use ITS Timestamps in CDR	Defines if the local clock or the ITS provided timestamps should be used for CTI event timestamps.

Step 5 - Save the changes by clicking on the



icon.

Step 6 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

Step 7 - Repeat the steps on all Recording Director servers.

Configuring BT ITS TMS and LDAP based provisioning

The following information is continuously synchronized from ITSProfile server(s) by the Recording Director(s):

- Lines: line number, name, type
- DDIs: number, name
- Users: trader id, user name
- Verticals: console/turret number, type, name, TTP id, device (speaker, handset) assigned,

The system uses the information above to extend the metadata recorded for the recorded calls on the turrets. Provisioning is supported by the following sources:

- TMS share
- LDAP

TMS share

The data is published in CSV like files on a CIFS/SMB share on the ITS Profile server(s).

Step 1 - In the Verba Web Interface go to **System \ Servers**

Step 2 - Select the Recording Director from the list

Step 3 - Click on the **Change Configuration Settings** tab and navigate to **Unified Call Recorder / Recording Providers / BT ITS/IPSI**

Step 4 - Configure the settings based on the description below:

Trader Provisioning Source:	<input type="checkbox"/>	TMS Share
LDAP/TMS Polling Timer (seconds):	<input type="checkbox"/>	300
TMS Files SMB Folder Path:	<input checked="" type="checkbox"/>	\\itslink.verbalabs.com\DataFiles
TMS Files SMB User:	<input checked="" type="checkbox"/>	verbalabs\verbaservice
TMS Files SMB Password:	<input type="checkbox"/>

Name	Description
Trader Provisioning Source	Defines the source of information for provisioning BT ITS configuration. The following valid values apply: <ul style="list-style-type: none">• TMS Share• LDAP
LDAP/TMS Polling Timer	Defines how often the TMS files are read and the data is synchronized
TMS Files SMB Folder Path	The path of the DataFiles folder on the ITS Profile server
TMS Files SMB User	The username configured for SMB authentication
TMS Files SMB Password	The password configured for SMB authentication

Step 5 - Save the changes by clicking on the



icon.

Step 6 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

Step 7 - Repeat the steps on all Recording Director servers.

LDAP

The data is published via LDAP which provides better security than the TMS share option (LDAP is not available in all BT ITS deployments).

Step 1 - In the Verba Web Interface go to **System \ Servers**

Step 2 - Select the Recording Director from the list

Step 3 - Click on the **Change Configuration Settings** tab and navigate to **Unified Call Recorder / Recording Providers / BT ITS/IPSI**

Step 4 - Configure the settings based on the description below:

LDAP Server:	<input checked="" type="checkbox"/> itslink.verbalabs.com
LDAP User:	<input checked="" type="checkbox"/> Browser
LDAP Password:	<input checked="" type="checkbox"/>
LDAP Base DN:	<input type="checkbox"/> ou=ITSAdmin;o=BT

Name	Description
Trader Provisioning Source	Defines the source of information for provisioning BT ITS configuration. The following valid values apply: <ul style="list-style-type: none">• TMS Share• LDAP
LDAP/TMS Polling Timer	Defines how often the LDAP directory is read and the data is synchronized
LDAP Server	Hostname or IP address of the BT ITS LDAP server
LDAP User	Username for the LDAP server user
LDAP Password	Password for the LDAP server user
LDAP Base DN	Base DN for the data in the LDAP directory

Step 5 - Save the changes by clicking on the



icon.

Step 6 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

Step 7 - Repeat the steps on all Recording Director servers.

BT ITS recorder resiliency

Media recording redundancy

Voice LAN redundancy

There can be two independent Voice LANs configured for media delivery. If VLAN A fails, the media streams can automatically fail over to VLAN B within <~5 seconds and recording continues with a small gap in the media record. Please note, IPSI management LAN is still a single point of failure.

Media Recorder load-balancing and failover (N+1)

The Recording Servers have two roles which can be co-located on the same server or distributed across multiple servers:

- Recording Director: integration point with telephony vendors, provides a unified layer/acts as a mediator for media establishment, CDR events to Media Recorder role
- Media Recorder: controlled by Recording Director, it records media and stores CDR information in the database


If the Recording Director and the Media Recorders are separated on multiple servers and there are at least one Recording Director and two Media Recorders, the Recording Director can:

- Distribute the media recording tasks between Media Recorders to provide load-balancing between them. Load-balancing takes into account the recorder utilization report (CPU, number of concurrent recording, available disk space etc...) sent by the Media Recorders on a periodic fashion. Due to the characteristics of BT IPSI recording interface, load-balancing for BT IPSI, unlike in case of other vendors, does not work on a per call basis. Load balancing is implemented on a per TTP (Trunk Termination Point) basis. Since there are persistent recording channels established via the TTPs, the Media Recorder for a TTP is selected at service startup time.
- If a failed/offline Media Recorder is detected then all the TTPs recorded on the server can failover to other Media Recorders and recording continues from the point of failure.

Detecting Media Recorder failure and moving TTPs to other recorders might take 10-15 seconds.

TTP manager redundancy

The Recording Director is responsible of distributing and moving TTPs over in case of Media Recorder failure and establishing new TTPs and media records in case of new verticals are provisioned for recording. In order to provide redundancy for the TTP management functionality in the Recording Director, an active - standby Recording Director can be deployed. It means that only the active Recording Director is able to manage TTP allocation across the Media Recorders, while the standby Recording Director only monitors the TTP distribution. When the active Recording Directors fails, the standby takes over and takes over TTP management. Until there is no need to change the current distribution (there is no Media Recorder failure, no new verticals provisioned with new TTP channels), the same distribution persists as before the failover.

 If TTP Manager redundancy is configured (standby Recording Director), there must be a very stable network connection between the two hosts. NIC teaming or crossover cable connection is required. If the network is lost between the two servers but both have an active connection to the BT infrastructure and to the Media Recorder servers, it could lead to unexpected situations and possible media loss, because both Recording Directors will actively try to control TTPs.

2N recording

The system can be deployed in a 2N recording configuration, where:

- 2 separate Recording Server groups are deployed, implementing 2 separate recorder groups/lanes (primary and secondary)
- all TTPs are duplicated and recorded twice by assigning the TTPs to 2 separate Media Recorders in the different recorder groups
- the TTP allocation for 2N recording requires special care, see [BT ITS TTP numbering conventions](#) for more information
- 2 Recording Directors are configured to manage the primary and secondary TTP allocation in each of the recorder groups
- the 2 Recording Directors are separately connected to the BT CTILink server, handling the CTI messages

CTI redundancy

CTI resiliency can only be supported by deploying 2 Recording Directors in a 2N configuration (even if media recording might be N+1 or 2N, related CTI will always be 2N). For one recorder group, maximum 2 Recording Directors, acting as CTI listeners, can be configured. Each Recording Director creates the copy of the same CDR record, one marking it primary and the other marking it secondary. A deduplication data management policy can be configured to correlate and keep only one of the related records.

Configuring media stitching adjustment

In trader voice recording, the media records are separately created from the CTI events in many cases. This is usually due to the nature of the integration, but it also ensures that all media streams are captured, irrespectively if CTI information is available or not. In case the time synchronization of the servers is not accurate, it could lead to issues when the system is trying to find the related media-only records for the CDR entry. Especially when there are very short calls, a slight drift in the servers' time could cause playback issues, when the users will not be able to play back the related media. It is critically important to configure highly accurate time synchronization for the servers. However, the system also provides a feature, called media adjustment to cope with this problem.

Configuring default media adjustment for all calls

The system allows configuring a default media adjustment which is then applied automatically for all calls during playback, download, and export. Follow the steps below to configure the default adjustment:

Step 1 - In the Verba Web Interface go to **System \ Servers**

Step 2 - Select the server from the list where you have the Media Repository role installed

Step 3 - Click on the **Change Configuration Settings** tab and navigate to **Storage Management \ General**

Step 4 - Change the **Media Stitch Begin Adjustment (msec)** and **Media Stitch End Adjustment (msec)** values according to your preference. With a negative value, you can set the starting/ending of the stitching earlier/later in time, with positive you can offset the start/end to a later/earlier time than the CDR start.

Step 5 - Save the changes by clicking on the



icon.

Step 6 - Repeat the steps on all servers with a Media Repository role. Make sure you configure exactly the same values on all servers, otherwise it will lead to unexpected behavior.

Step 7 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

Configuring media adjustment for playback

The system allows configuring media adjustment for a single call during playback.

After the playback started, users can adjust the media by clicking on the



icon in the player, the adjustment controls will be shown.

The screenshot displays a 'Conversation View' interface. At the top, there is a search bar and a title 'Conversation View'. Below this is a timeline from 00:00 to 00:36. A blue audio waveform is visible. A 'Paused' indicator is on the left. A context menu is open, showing options like 'Hide Markers', 'Playback Speed', and 'Skip silence longer than 10 seconds'. A green box highlights the 'Adjust Media (max. 10 second(s))' section, which includes 'Start' (2), 'End' (3), and a 'Reload Media' button. Below the audio player are 'Markers' (1.-, 2.-, 3.-) and a 'Conversation Details' panel showing a date range (Apr 10, 2019 7:36:48 PM - Apr 10, 2019 7:37:24 PM), a duration (00:00:36.000), a user ID (6003), and a device name (658 (USB Audio 658 LG)).

Users can define additional seconds at the beginning and end of the call to extend the time range which is used to find and load related media. Once you configured the adjustment, press the **Reload Media** button. The system will override the default setting configured above.

Configuring Speakerbus recording

Verba Unified Call Recorder service provides a handler to Speakerbus iCDS (Internetworking Call Data Service) call event streams and to record media.

Verba can act either as a client connecting to configured iCDS services or act as a server accepting a connection from any iCDS service.

Verba side settings


The screenshot shows the configuration interface for Speakerbus recording. It includes a tree view on the left with the following structure:

- Unified Call Recorder
 - Media Recorder
 - Recording Providers
 - General
 - Remote Media Recorders
 - SIP / SIPREC
 - IPC Unigy
 - IP Trade
 - BT ITS / IPSI
 - Speakerbus

The Speakerbus configuration section contains the following settings:

ICDS Addresses (Client Mode, 2N Primary):	<input type="checkbox"/>	
ICDS port (Server Mode, 2N Primary):	<input type="checkbox"/>	7788
ICDS Addresses (Client Mode, 2N Secondary):	<input type="checkbox"/>	
ICDS port (Server Mode, 2N Secondary):	<input type="checkbox"/>	7789
Station Timeout (seconds):	<input type="checkbox"/>	180
Use Optimized Data Storage Model:	<input type="checkbox"/>	Yes

- ICDS Addresses: list of ip:port of iCDS servers Verba should connect. Please note this is required only if Verba cannot be configured as iCDS connection server for some firewall considerations.
- ICDS port: Verba listens by default on TCP 7788 to iCDS connections. The preferred and default operation mode is acting as server
- Station Timeout: drop registered turret contexts if neither keepalive nor any call event is received anymore
- The optimized data model is the [Data models](#) which is important if silence suppression is utilized.
- Review the **Media Recorder** and **Media Processing** configuration. For more information on voice activity detection and call splitting, see [Configuring voice activity detection and call splitting for trader voice recording](#).

 If redundant recording is not used, you only need the primary port/addresses configured.

Media termination

Speakerbus turrets fork RTP to preconfigured recorder ports. One turret is able to stream max 7 different media streams according to 7 media source mixing layout configured via iCMS (iManager Centralised Management Server). Intercom devices support one media stream

only. Verba receives media on the same 7 configured ports from multiple devices and demultiplexes them based on media source address and turret address/expansion board address seen in call events. The port configuration is learnt from call events and ports are allocated on-demand.

Please be aware of that media ports should be selected from a range which can be dedicated to Verba service and are not subject of use from other applications. Verba active recorders (for Cisco/SIPREC/IP Trade....) might use media port range 16384-65535) which should not overlap this range if recorder server is integrated with these systems as well. The recommended range is: 3000-3007.

Recording redundancy

Speakerbus provides redundancy in 2N fashion (duplicated call events and media streams). This requires two Verba Unified Call Recorder instance one marked as primary other one as backup/secondary.

User provisioning

The Speakerbus user-id should be added to Verba as a recorded extension. This can be done manually ([Extension list](#)) or using [Active Directory Synchronization](#). When adding (or synchronizing) the user IDs, the **Type** setting of the extensions has to be set to **User/Agent ID**.

Configuration Checklist

- Activate and start Verba Unified Call Recorder service
- Configure iCDS to connect Verba recorder(s) on port 7788
- Configure turret profiles in iCMS according to desired media mixing layouts, media codecs and configure related primary (and in case of 2N topology: secondary) Verba RTP ports
- Provision Speakerbus userids for recording

Configuring Avaya Central recording

The Verba Unified Recorder service allows you to record Avaya Communication Manager (Avaya Aura) calls using the RTP forking feature through DMCC. In order to setup extensions/directory numbers for recording, the Avaya Communication Manager has to be configured properly and the extension has to be added in the Verba system.

Step 1 - [Configure the Avaya environment for recording.](#)

Step 2 - [Configure Verba for Avaya recording.](#)

Step 4 - [Configure recorded extensions in Verba.](#)

Step 5 - Test the recording.

Configuring Avaya CM and AES for central recording

In order to take advantage of the recording support in Avaya CM and AES servers and use the Verba Recording System's Central Avaya Recording method, configuration on the Avaya side is necessary.

Initial configuration


The initial Avaya configuration for central recording includes the following steps:

Step 1 - [Configure Avaya CM for recording](#)

Step 2 - [Configure Avaya AES for recording](#)

Step 3 - [Verify Avaya CM and AES recording configuration](#)

After these steps you can start adding extensions.

 When you use Avaya-based central recording, the Verba system can record only those extensions that are properly configured on the Avaya side. It is not enough to add extensions in the Verba Recording System.

Configure Avaya AES for recording

The Avaya Application Enablement Services (AES) server enables Computer Telephony Interface (CTI) applications to control and monitor telephony resources on Avaya Communication Manager. The Avaya Application Enablement Services (AES) server receives requests from CTI applications, and forwards them to Avaya Communication Manager. Conversely, the Avaya Application Enablement Services (AES) server receives responses and events from Avaya Communication Manager and forwards them to the appropriate CTI applications.

This section assumes that installation and basic administration of the Avaya Application Enablement Services server has been performed. The steps in this section describe the configuration of a Switch Connection, a CTI user, a CMAPI port, and creating a CTI link for TSAPI.

Configuring switch connection

Follow the steps below to configure Avaya CM and AES connection.

Step 1 Launch a web browser, enter `https://IP_address_of_AES_server:8443/MVAP` in the address field, and log in with the appropriate credentials for accessing the AES CTI OAM pages.

Step 2 Select the **CTI OAM Administration** link from the left pane of the screen.

Step 3 Click on **Administration / Switch Connections** in the left pane to invoke the **Switch Connections** page. A Switch Connection defines a connection between the Avaya AES and Avaya Communication Manager. Enter a descriptive name for the switch connection and click on **Add Connection**.

Step 4 The next window that appears prompts for the Switch Connection password. Enter the same password that was administered in Avaya Communication Manager. Default values may be used in the remaining fields. Click on **Apply**.

Step 5 After returning to the Switch Connections page, select the radio button corresponding to the switch connection added previously, and click on **Edit CLAN IPs**.

Step 6 Enter the CLAN-AES IP address which was configured for AES connectivity and click on **Add Name or IP**. Repeat this step as necessary to add other C-LAN boards enabled with Application Enablement Services.

Configuring the CTI user

The steps in this section describe the configuration of a CTI user.

Step 1 Launch a web browser, enter `https://IP_address_of_AES_server:8443/MVAP` in the URL, and log in with the appropriate credentials to access the relevant administration pages.

Step 2 The Welcome to OAM page is displayed next. Select **User Management** from the left pane.

Step 3 From the Welcome to User Management page, navigate to the **User Management / Add User** page to add a CTI user.

Step 4 On the Add User page, provide the following information: User Id, Common Name, Surname, User Password, Confirm Password. The above information (User ID and User Password) must match with the information configured in Verba. Select **Yes** using the drop down menu on the CT User field. This enables the user as a CTI user. Click the **Apply** button at the bottom of the screen to complete the process. Default values may be used in the remaining fields.

Step 5 Once the user is created, select **OAM Home** in upper right and navigate to the **CTI OAM Administration / Security Database / CTI Users / List All Users** page. Select the User ID created previously, and click the **Edit** button to set the permission of the user.

Step 6 Provide the user with unrestricted access privileges by clicking the **Enable** button on the Unrestricted Access field. Click the **Apply Changes** button.

Step 7 Navigate to the **CTI OAM Home -> Administration -> Ports** page to set the DMCC server port. The following screen displays the default port values. Set the Unencrypted Port field to **Enabled**. Click the **Apply Changes** button at the bottom of the screen to complete the process. Default values may be used in the remaining fields.

Configuring the TSAPI CTI link

Step 1 Navigate to the **OAM Home -> CTI OAM Admin / Administration / CTI Link Admin / TSAPI Links** page to set the **TSAPI CTI Link**. Click on **Add Link**.

Step 2 Select a Switch Connection using the drop down menu configured in Avaya Communication Manager. Select the **Switch CTI Link Number** using the drop down menu. Switch CTI Link Number should match with the number configured in the cti-link form in Avaya Communication Manager. Click the **Apply Changes** button. Default values may be used in the remaining fields.

Configure Avaya CM for recording

This section provides the procedures for configuring an ip-codec-set and ip-network region, a switch connection and Computer Telephony Integration (CTI) links, recorded/monitored stations on Avaya Communication Manager. All the configuration changes in Avaya Communication Manager are performed through the System Access Terminal (SAT) interface.

Codec configuration

Enter the **change ip-codec-set t** command, where **t** is a number between 1 and 7, inclusive. Select **t** as the appropriate codec set for the ip-network-region used by the recorded stations.

Configuring IP network regions

In most cases a C-LAN board dedicated for H.323 endpoint registration is assigned to IP network region 1. One consequence of assigning the aforementioned IP telephones, IP Softphones, and MedPro boards to a common IP network region is that the RTP traffic between them is governed by the same codec set. The second C-LAN board (CLAN-AES), which is dedicated for the AES server is assigned to network region 2.

Configuring switch connection and CTI links between Avaya CM and Avaya AES

The Avaya AES server forwards CTI requests, responses, and events between Verba and Avaya Communication Manager. The AES server communicates with Avaya Communication Manager over a switch connection link. Within the switch connection link, CTI links may be configured to provide CTI services to CTI applications such as Verba. The following steps demonstrate the configuration of the Avaya Communication Manager side of the switch connection and CTI links. See the topics below for the details of configuring the AES side of the switch connection and CTI links.

Step 1 Enter the add **cti-link m** command, where **m** is a number between 1 and 64, inclusive. Enter a valid extension under the provisioned dial plan in Avaya Communication Manager, set the **Type** field to **ADJ-IP**, and assign a descriptive **Name** to the CTI link.

Step 2 Enter the **change node-names ip** command. In most cases the CLAN IP address is utilized for registering H.323 endpoint (Avaya IP Telephones and IP Softphones, and AES Device, Media and Call Control API stations) and the CLAN-AES IP address is used for connectivity to Avaya AES.

Step 3 Enter the **change ip-services** command. On **Page 1**, configure the Service Type field to **AESVCS** and the Enabled field to **y**. The Local Node field should be pointed to the **CLAN-AES** board that was configured previously in the IP NODE NAMES form in this section.

Step 4 On **Page 4**, enter the hostname of the AES server for the AE Services Server field. The server name may be obtained by logging in to the AES server using ssh, and running the command **uname a**. Enter an alphanumeric password for the **Password** field. Set the **Enabled** field to **y**. The same password will be configured on the AES server.

Configuring recorded (monitored) stations

Step 1 Enter the **add station s** command, where **s** is an extension valid in the provisioned dial plan.

Step 2 On **Page 1** of the STATION form, set the **Type** field to an IP telephone set type, enter a descriptive **Name**, specify the **Security Code** (this code will be configured in the Verba Recording System as well for each recorded station), and make sure that the **IP Softphone** field is set to **y**.

Allowing H.323 endpoints for IP Interfaces

Step 1 Enter the **change ip-interface** command and set **Allow H.323 Endpoints?** to **y** for the CLAN that is set up in the **Avaya Connection Settings** in the Verba Recording System configuration options.

Verify Avaya CM and AES recording configuration

This section provides the tests that can be performed to verify proper configuration of Avaya Communication Manager and Avaya AES.

Verify Avaya Communication Manager

Step 1 Verify the status of the administered AES link by using the **status aesvcs link** command.

Step 2 Verify the Service State field of the administered TSAPI CTI link is in established state, by using the **status aesvcs cti-link** command.

Verify Avaya Application Enablement Services

Step 1 From the CTI OAM Admin web pages, verify the status of the TSAPI and DMCC Services are ONLINE, by selecting **Status and Control / Services Summary** from the left pane.

Configuring Verba for Avaya recording

The Verba Avaya Recorder is separated into two different services: The Verba Avaya DMCC/JTAPI Service and the - Media Recorder portion of the - Verba Unified Call Recorder Service. These services can run on the same machine or different servers.

The DMCC/JTAPI service is essentially the interface towards the AES and CM servers, and the Unified Call Recorder is recording the media stream itself.

Configuring the Verba Unified Call Recorder service

Step 1 - In the Verba web interface go to **System / Servers**, select the Recording Server and click on the **Service Activation** tab.

Step 2 - Activate the **Verba Unified Call Recorder Service** by clicking on the



icon.

Step 3 - Click on the **Change Configuration Settings** tab.

Step 4 - Expand the **Unified Call Recorder** section.


Step 5 - Under **Media Recorder / Incoming Connection**, configure the authentication credentials for the connections with the Avaya DMCC service. Define the **User** and **Password** values. These credentials will be used later when configuring the connections in the Avaya DMCC service.

Step 6 - Save the changes by clicking on the



icon.

Step 7 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

 There are tasks to be executed regarding the configuration of this Verba Server.
If you would like to execute these tasks now, please [click here](#) .

Step 9 - Go to the Service Control tab, and start the Verba Unified Call Recorder service by clicking on the



icon.

Configuring the Verba Avaya DMCC service

Step 1 - In the Verba web interface go to **System / Servers**, select the Recording Server and click on the **Service Activation** tab.

Step 2 - Activate the **Verba Avaya DMCC/JTAPI Service** by clicking on the



icon.

Step 3 - Click on the **Change Configuration Settings** tab.

Step 4 - Expand the **Avaya Recorder** node.


Step 5 - Configure the settings under the **Avaya DMCC** node:

Setting Name	Description
AES IP Address	The IP Address of the AES server. One Recording Server can only connect to one AES server
AES Port Number	Communication port of the AES server
AES User Name	The user in AES that has the rights for DMCC to execute the necessary commands
AES User Password	The password of the AES User
AES Secure Connection	Set to Yes if you want the channel between the AES and the Verba server to be secure. In this case, you need to set the Trust Store location and password as a minimum
AES JKS Trust Store File	Location of the Trust Store. This needs to contain the public certificate of the AES
AES JKS Trust Store File Password	The password of the Trust Store
AES JKS Key Store File	Location of the Key Store. An additional security layer can be set in the AES. In that case, it will be expecting an additional key, that needs to be added to the Key Store
AES JKS Key Store File Password	The password of the Key Store
Communication Manager IP Address	The IP address of your Avaya Communication Manager. If there are ESS servers, then list them separated by commas (,) after the primary CM. Only one of the two entries need to be set (either the IP or the hostname)
Communication Manager Name	The name of your Avaya Communication Manager. If there are ESS servers, then list them separated by commas (,) after the primary CM. Only one of the two entries need to be set (either the IP or the hostname)
AES API Version	Define the version of the AES
Preferred Codec	The comma (,) separated list of supported codecs
Dependency Mode for Multiple Registration	DEPENDENT or INDEPENDENT
Registration Retry Interval (seconds)	Upon failed registration, the component will wait for this amount of time before trying again
Default Device Password	The default password for extensions
Internal Domain, Number Pattern	A regex pattern that should match the internal directory numbers
Secondary Recording Server	Sets whether the Recording Server should be considered as secondary or not
Ignore Recording Rule Entries Without Device Password	On the extension configuration page, the password for the extension can be set. If this option is set to yes, then the extensions, where the passwords are not set will not be recorded
Advanced Recording Rules Enabled	Enables XML-based advanced recording rules
Enable Beep Tones	Enables recording beep tones
Worker Thread Count	Amount of worker threads

Work Folder	The system will place temporary files into this folder
--------------------	--

Avaya Recorder

Avaya DMCC

AES IP Address:	<input checked="" type="checkbox"/>	192.168.1.18
AES Port Number:	<input type="checkbox"/>	4721
AES User Name:	<input checked="" type="checkbox"/>	verba_user
AES User Password:	<input checked="" type="checkbox"/>	*****
AES Secure Connection:	<input type="checkbox"/>	No
AES JKS Trust Store File:	<input type="checkbox"/>	
AES JKS Trust Store File Password:	<input type="checkbox"/>	*****
AES JKS Key Store File:	<input type="checkbox"/>	
AES JKS Key Store File Password:	<input type="checkbox"/>	*****
Communication Manager IP Address:	<input checked="" type="checkbox"/>	192.168.1.19
Communication Manager Name:	<input checked="" type="checkbox"/>	CM65
AES API Version:	<input type="checkbox"/>	5.2
Preferred Codec:	<input checked="" type="checkbox"/>	g711U
Incoming Media Encryption:	<input type="checkbox"/>	No Encryption
Dependency Mode for Multiple Registration:	<input type="checkbox"/>	INDEPENDENT
Controllable by Other Sessions:	<input type="checkbox"/>	Yes
Device Instance:	<input type="checkbox"/>	0
Registration Retry Interval (seconds):	<input type="checkbox"/>	60
Default Device Password:	<input checked="" type="checkbox"/>	*****
Internal Domain, Numbers Pattern:	<input type="checkbox"/>	
Secondary Recording Server:	<input type="checkbox"/>	Recorder Decides
Ignore Recording Rule Entries Without Device Password:	<input type="checkbox"/>	No
Advanced Recording Rules Enabled:	<input type="checkbox"/>	No
Enable Beep Tones:	<input type="checkbox"/>	No
Worker Thread Count:	<input type="checkbox"/>	100
Work Folder:	<input type="checkbox"/>	C:\Program Files\Verba\work\avayaactiverec 

Step 6 - Configure the settings under the **Avaya JTAPI** node:

Setting Name	Description
Avaya Tlink Name	Tlink name to the Communication Manager. This is displayed on the interface of the AES
JTAPI User Name	The name of the AES user that has the necessary rights to communicate through JTAPI (This can be the same user as is used for DMCC in the previous section)
JTAPI User Password	The password of the AES user

JTAPI JKS Trust Store File	Location of the Trust Store. This is needed if the AVAYATlink is configured for secure communication. This needs to contain the public certificate of the AES.
JTAPI JKS Trust Store File Password	The password of the Trust Store
Disable Agent ID Handling	The use of agent IDs can be disabled
Hunt Group for Monitored Agent(s)	special/"dummy" group that includes all agents. This is needed for JTAPI to gather additional information on the users
Agent Status Check Interval (seconds)	The system queries the agents for their status with a time interval that is set here

- Avaya Recorder
 - Avaya DMCC
 - Avaya JTAPI

Avaya Tlink Name:	<input checked="" type="checkbox"/>	AVAYA#CM65#CSTA#AES65
JTAPI User Name:	<input checked="" type="checkbox"/>	verba_api_user
JTAPI User Password:	<input checked="" type="checkbox"/>	*****
JTAPI JKS Trust Store File:	<input type="checkbox"/>	
JTAPI JKS Trust Store File Password:	<input type="checkbox"/>	
Disable Agent ID Handling:	<input type="checkbox"/>	No ▼
Hunt Group for Monitored Agent(s):	<input checked="" type="checkbox"/>	45678
Agent Status Check Interval (seconds):	<input type="checkbox"/>	3600

Step 7 - Under the **Media Recorders** node click on the



icon at the **Media Recorder Servers** setting.

Step 8 - In the right panel select the Recording Server at the **Host** setting. Provide the username and password configured in the **Verba Unified Call Recorder Service** above for the connections. Set the **Port** to **10500**.

Remote Media Recording Servers

Protocol	vrp
User	verba
Password	*****
Host	TESTRS1.VERBATEST.LOCAL ▼
Port	

Step 9 - Click on the **Save** button at the bottom.

- ▲ Avaya Recorder
 - ▶ Avaya DMCC
 - ▶ Avaya JTAPI
 - ▲ Media Recorders


Media Recorder Servers:	<input checked="" type="checkbox"/>	<input type="text" value="vrp://verba:1vcYm2yq7Fr5WuO3yi9oQQ==@TESTRS1.VERBATEST.LO"/>		
		<input data-bbox="758 392 790 436" type="button" value="+"/>		
Minimum Number of Active Media Recorder Servers:	<input type="checkbox"/>	<input type="text" value="1"/>		
Number of Connection Retry Attempts:	<input type="checkbox"/>	<input type="text" value="2"/>		
Sleep Time Between Retries (seconds):	<input type="checkbox"/>	<input type="text" value="5"/>		
Connection Keepalive Interval (seconds):	<input type="checkbox"/>	<input type="text" value="5"/>		
Connection Timeout (seconds):	<input type="checkbox"/>	<input type="text" value="5"/>		

Step 10 - Save the changes by clicking on the



icon.

Step 11 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

 There are tasks to be executed regarding the configuration of this Verba Server.
If you would like to execute these tasks now, please [click here](#) .

Step 12 - Go to the Service Control tab, and start the Verba Avaya DMCC/JTAPI service by clicking on the



icon.

Configuring Genesys active recording

AVAILABLE IN VERSION 9.6.10 AND LATER

For more information on the integration with Genesys, see [Genesys](#)

The configuration consists of:

Step 1 - [Configuring Genesys](#)

Step 2 - [Configuring Verba for Genesys active recording](#)

Step 3 - Add recorded users to Verba

This can be done manually ([Extension list](#)) or using [Active Directory Synchronization](#). In the case of Genesys active recording:

- the directory number of the agent has to be added as recorded extensions,
- if the directory number is shared across multiple agents (free seating), the "Shared Line" text has to be added to the description of the recorded extension,
- and in addition, the agent IDs have to be added as well (when adding (or synchronizing) the agent IDs, the **Type** of the extensions has to be set to **User/Agent ID**).

Step 4 - Test all recording scenarios

Configuring Genesys

Configuring Genesys voice platform for active recording

The full configuration guide is accessible in the online Genesys Documentation: [Genesys Active Recording System Setup](#)

The below guide is emphasizing the necessary configuration steps for Verba.

SIP Server configuration

Step 1 - Configure the application level SIP Server - The application used as the TServer for the SIP Softphones

Section Name	Parameter	Required Value	Description
TServer	msml-support	true	Set to true to enable support of the call recording solution.
TServer	resource-management-by-rm	true	Set to true to enable support of the call recording solution. Resource monitoring and notification will be done by the Resource Manager. SIP Server will contact Media Server through Resource Manager.
TServer	record-consult-calls	true	Specifies whether to record consult calls: <ul style="list-style-type: none">• true—record consult calls• false—do not record consult calls
TServer	msml-record-support	true	Set to true to enable SIP Server to engage GVP as a Media Server through the msml protocol for call recording.

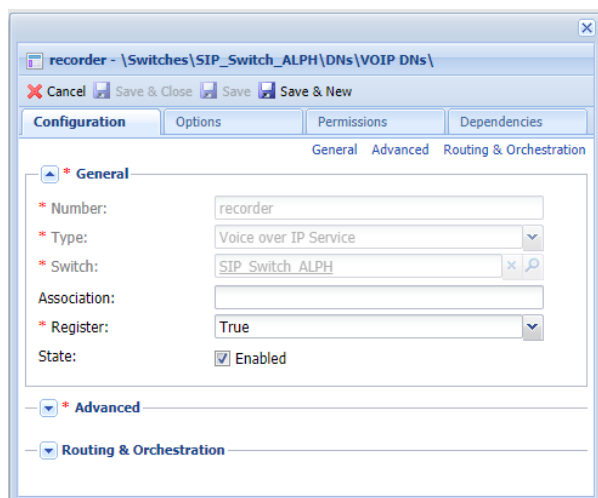
Step 2 - Configure a DN for VoIP service

Create a new MSML DN Object

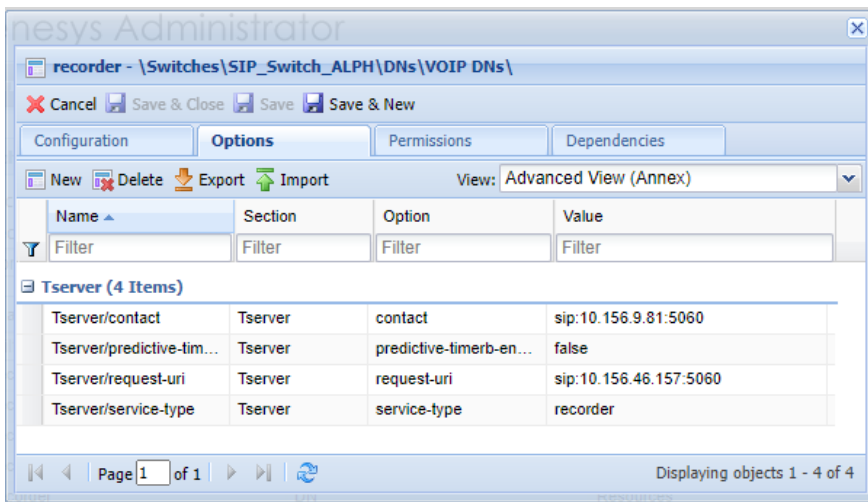
Step 3 - Create a new MSML DN object and configure the following:

Number: Name of the Recording Server

Type: Voice over IP Service



Step 4 - Configure the following values on the 'Options' tab



Section Name	Parameter	Required Value	Description
TServer	contact	sip:<resource-manager-ip>:<resource-manager-sip-port> OR sip:<tserver-ip>:<tserver-sip-port>	Set this to the Resource Manager IP address and port. Specifies the contact URI that SIP Server uses for communication with the treatment server.
TServer	predictive-timerb-enabled	false	
TServer	request-uri	sip:<recording-server-ip>:<recording-server-sip-port>	Recording servers URI, where the SIP Server sends the invite.
TServer	service-type	recorder	

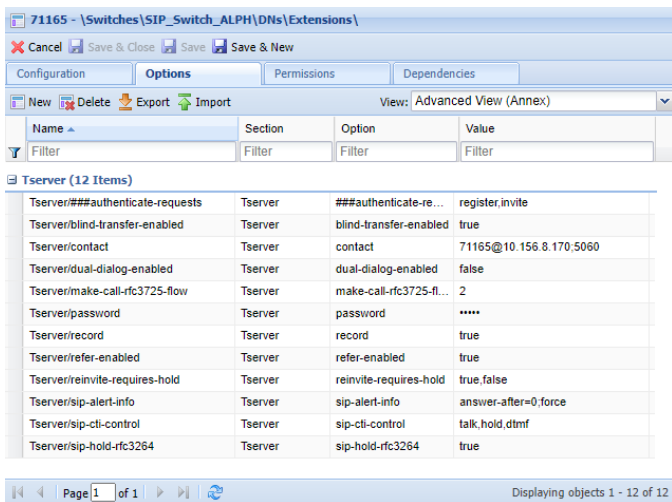
Enable full-time recording

Step 5 - Enable full-time recording

To start recording based on static DN-level settings, **set the record parameter to true** in any of the following:

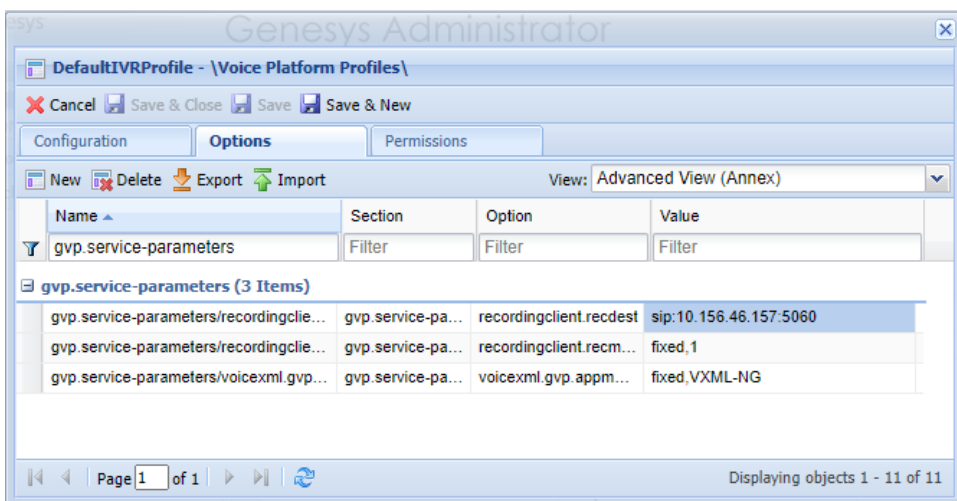
- Extension or ACD Position DN for agent-side recording
- Agent Login for agent-side recording
- Trunk DN for customer-side recording
- Trunk Group DN to record GVP interaction
- Voice Treatment Port DN to record GVP interaction

An extension configured for recording:



Create an IVR Profile

Step 6 - Create an IVR profile or modify an existing



Section Name	Parameter	Required Value	Description
gvp.service-parameters	recordingclient.recdest	fixed,sip:<recording-server-ip>:<recording-server-sip-port>	Recording servers URI, where the SIP Server sends the invite.
gvp.service-parameters	recordingclient.recmmediactl	fixed,1	This value represents the number of invites

Create Recording Server Application

Step 7 - Create a Recording Server application and provision a Resource Group

Step 8 - Using Genesys Administrator, import VP_CallRecordingServer_81x.apd template file, and the corresponding VP_CallRecordingServer_81x.xml metadata file. These files are located on the Media Server installation CD, in the Resource Manager installation package.

Step 9 - Create one or more new Application object(s) using the template imported in step a.

Step 10 - Add or modify the following options in the gvp.rm section

VP_CallRecordingServer_851 - \GVP_ALPH_Recorder_LRG\ALPH_Recorder\

Cancel Save & Close Save Save & New Reload Start Stop Graceful Stop

Configuration Options Permissions Dependencies Alarms Logs

New Delete Export Import View: Advanced View (Options)

Name	Section	Option	Value
Filter	Filter	Filter	Filter

gvp.rm (3 Items)

gvp.rm/aor	gvp.rm	aor	sip:10.156.46.157:5060
gvp.rm/port-capacity	gvp.rm	port-capacity	20
gvp.rm/redundancy-type	gvp.rm	redundancy-...	

provision (1 Item)

provision/recording-server	provision	recording-se...	1
----------------------------	-----------	-----------------	---

Page 1 of 1 Displaying objects 1 - 4 of 4

Section Name	Parameter	Required Value	Description
gvp.rm	aor	sip:<recorder-server-ip host>:<recorder-server-sip-port>	Host and port are the FQDN or IP-address and listening SIP port of the recording server.
gvp.rm	port-capacity	5000	This parameter specifies the maximum port capacity of the resource. The number of active SIP sessions to the resource will not be allowed to exceed this capacity.
gvp.rm	redundancy-type	active	This parameter specifies the redundancy type of the resource. If all of the active redundancy type resources are up, then only the resources with the active redundancy-type will be used. If any one of them is down, then passive redundancy type resources will also be used.
provision	recording-server	1	This parameter indicates to the Resource Manager that this is a recording server resource. Unless this parameter is set to 1, this application will not be used by the RM as the recording server resource.

Step 11

- Using Genesys Administrator, create a new Resource Group for Recording Servers.

Genesys Genesys Adminis New Window Log out

MONITORING PROVISIONING OPERATIONS

PROVISIONING > Voice Platform > Resource Groups

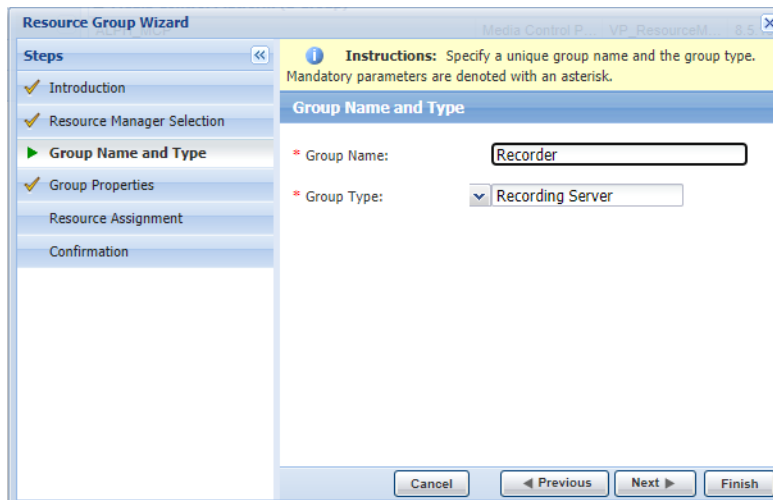
Navigation Search Environment Switching Routing/eServices Desktop Accounts Voice Platform DID Groups IVR Profiles Resource Groups Outbound Contact

New Edit Delete

Resource Group Name	Group Type	RM Name	RM Version
Gateway (1 Group)			
ALPH_Gateway	Gateway	VP_ResourceM...	8.5.130.58
Media Control Platform (1 Group)			
ALPH_MCP	Media Control P...	VP_ResourceM...	8.5.130.58
Recording Server (1 Group)			
ALPH_Recorder	Recording Server	VP_ResourceM...	8.5.130.58

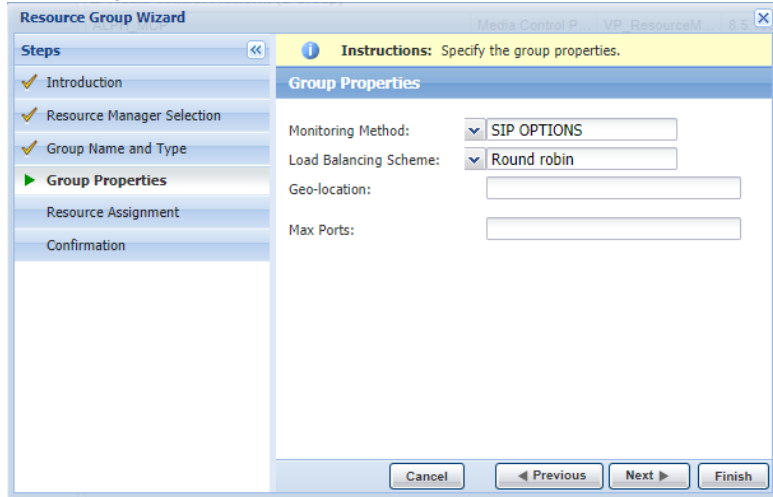
Page 1 of 1 Page Size 20 Displaying 1 - 3 of 3

- Add a resource manager.
- When prompted in the Wizard, set the Group Type to Recording Server.

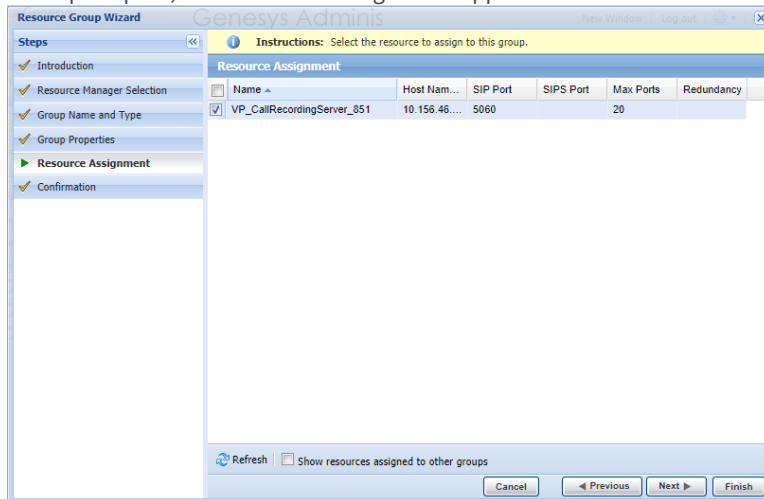


- When prompted, select valid values for the following options:

Monitoring Method - Set to SIP OPTIONS

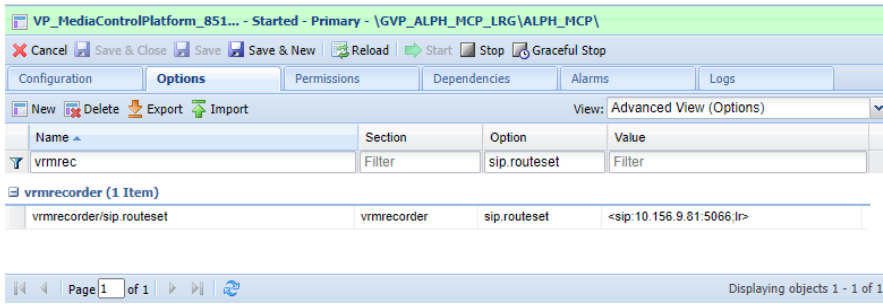


- When prompted, select the Recording Server Application



Configuring the MCP Application

Step 12 - Configure the MCP application and corresponding Resource Group



Section Name	Parameter	Required Value	Description
vmrecorder	sip.routeset	sip:<[rm-ip or FQDN]:[rm-port];lr>	Host and port of Resource Manager

Configuring Verba for Genesys active recording

Please follow the step in this article: [Configuring Verba for Genesys active recording](#)

Configuring Verba for Genesys active recording

In order to complete the steps below, you must have a System Administrator role in Verba.

The configuration consists of the following steps:

- [Configuring the Unified Call Recorder service](#)
- [Configuring the Genesys CTI service](#)
 - [Activating the services](#)
 - [Configuring and starting the service](#)
- [Adding custom metadata fields](#)

Configuring the Unified Call Recorder service

The Unified Call Recorder service does not require any additional configuration. By default, it listens and accepts SIP INVITEs from the Genesys Voice Platform.

Follow the steps below to activate and start the service on the Recording Server(s):

Step 1 - In the Verba Web Interface go to **System / Servers**

Step 2 - Select the Recording Server from the list

Step 3 - Click on the **Service Activation** tab

Step 4 - Activate the **Verba Unified Call Recorder Service** by clicking on the



icon.

Step 5 - Click on the **Service Control** tab.

Step 6 - Start the **Verba Unified Call Recorder Service** by clicking on the



icon.

Step 7 - Repeat the steps on all Recording Servers if there are multiple.

Configuring the Genesys CTI service

Activating the services

Step 1 - Log in to the Verba web interface and go to **System \ Servers** menu.

Step 2 - Select your Recording Server from the list, then click on the **Service Activation** tab.

Step 3 - Activate the **Verba Genesys CTI Service** by clicking on the



icon.

Configuring and starting the service

Step 4 - Click on the **Change Configuration Settings** tab and expand the **Genesys CTI Service / General** section.

Step 5 - Fill out the configuration fields according to the table below.


Parameter name	Description
Genesys T-Server IP(s)	After clicking on the gear icon at the end of the line, the following fields can be configured: <ul style="list-style-type: none">• User• Password• IP Address(es) and ports the port should be separated by a (pipe) character, the default port is 9020
Internal Domain, Number Pattern	See Conversation direction detection using internal domain and number patterns
Target Genesys Field for Verba Call ID	Verba will attach the Verba Call ID to this Genesys User Data Field.
Secondary Recording Service	Defines if the Recording Server is a secondary server when duplicate / 2N recording is configured

Step 6 - Save the changes by clicking on the



icon.

Step 7 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

 There are tasks to be executed regarding the configuration of this Verba Server.
If you would like to execute these tasks now, please [click here](#) .

Step 8 - Click on the **Service Control** tab.

Step 9 - Start the **Verba Genesys CTI Service** by clicking on the



icon.

Adding custom metadata fields

The collected data is configurable in the Metadata Template, thus if you change the Property Id of the fields or add new fields to the template, the system will start collecting that data as well. In order to read the data of custom attached user fields from Genesys, in the Genesys Metadata Template use the "UserData." prefix in the **Property Id**. For example: UserData.MyField

After a Genesys Metadata Template changed, the affected Verba Genesys CTI Service(s) have to be restarted on the Recording Server(s).

Configuring Verba for passive recording

Step 1 - Prerequisites

Step 1 - Configure your network mirror ports

Plan where you want to tap your network. For a good recording both signaling and RTP traffic related to the recorded phones /trunks must be seen on the monitoring port.
You can read more about this here:

- [Overview of monitor ports for passive recording](#)
- [Configuring monitor port for passive recording](#)
- [Using Cisco switches to filter SPAN traffic](#)

Step 2 - Active the Passive Recorder Service

Step 1 - Login to the web interface with System administrator rights.

Step 2 - Navigate to the **System / Servers** menu item and select the corresponding server from the list.

Step 3 - Click on the **Service Activation** tab.

Step 4 - Activate the following services using the 'Activate this service' button:

Verba Passive Recorder Service



(Activate this service)

Step 3 - Configure the Passive Recorder

Go to the **Change Configuration Settings** tab in the Verba Server management screen (see in steps above).

Step 1 - Set **gateway addresses** to determine call direction info (outgoing/incoming/internal) (Common Configuration/Recording Settings)

Step 2 - Select **interface** connected to monitoring port (Passive Recorder Configuration/Basic Settings/Recording interface)

Step 3 - Select **video call recording mode** (Passive Recorder Configuration/Advanced Settings/Record video call as audio)

Step 4 - If you are interested in **incomplete calls** (calls canceled, called busy...), enable logging of them (Passive Recorder Configuration/Advanced Settings/Record incomplete calls)

Step 5 - If you are interested in **DTMF recording** [configure it](#)

Step 6 - After making your changes clicking on the **Save** button in top right corner of the configuration tree

Step 7 - Follow the instruction in the yellow stripe above the configuration tree to **apply changes** to Verba services.

Step 8 - Start the **Verba Passive Recorder Service** in the Service Control tab

If the services start properly, you can start making **test calls** from your configured endpoints and verify them by [searching for phone calls](#).

Configuration parameter reference

Basic settings

- **Recording interface:** NIC on which the recorder is listening to network traffic
- **Audio format:** storage format for audio only calls
- **Bidirectional/Stereo recording:** if storage format allows then caller is recorded on left called on right channel in stereo media file
- **Automatic Gain Control:** enables AGC on voice streams
- **Conference Resources IP addresses:** IP addresses of conference resources, used for recognizing conference calls
- **Experimental H.323 support:** enables recording of H.323 calls. Module is still under development
- **SIP support enabled:** enables recording of SIP calls
- **Call timeout:** stucked in calls after RTP timeout are cleared after this interval

Advanced settings

- **Capture buffer size:** packet capture buffer size in megabytes
- **Database cache folder:** database cache file folder
- **RTP address translation enabled:** recording calls at SBC/RTP proxy usually needs to translate local/private addresses reported by phones behind NAT to the addresses seen in the IP header rewritten by NAT (public address). You can enable a special mechanism that tries to fix RTP address issues here.
- **PCM mixer buffer length:** length of mixing buffer in milliseconds. Greater value provides better quality but higher memory load and bursty CPU usage.
- **RTP stream reorder buffer length:** length of RTP reorder buffer can be controled here. Greater value provides better reordering but increases memory usage
- **Record video call as audio call:** if enabled only audio part of video calls are recorded, else video calls are recorded in Verba Media Format
- **Media format fallback:** in case of not supported codecs, too many streams, not supported streams, transcoding quality issue, the recorder can intelligently change storage format to different kind of codecs which might preserve the recording in more optimal quality.
- **Filter duplicated recordings by caller-called:** only one call with the same participants will be recorded. This can avoid call duplication in case of SBC/RTP proxy recording related to inbound and outbound legs.
- **Skip calls without media:** Do not insert CDR at calls where no RTP has been received/processed
- **SIP URI modification:** control how to transform SIP uri
- **Record incomplete calls:** if enabled CDR related to not established calls due to call cancellation, busy/not available response will be recorded with appropriate end cause info

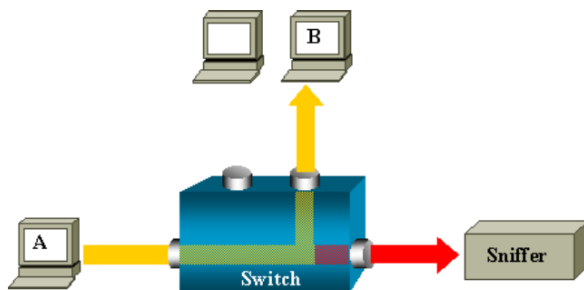
Configuring monitor port for passive recording

For network monitoring based call recording the recorder needs a mirror copy of the network traffic that includes the VoIP calls.

- [Monitor port on a switch](#)
 - [More information on the Cisco site](#)
 - [Configuration example](#)
- [Monitor port on an IP phone \(Verba Desktop configuration\)](#)
- [\(Deprecated\) Monitoring through a hub](#)

Monitor port on a switch

In order to aggregate VoIP call traffic into one port, a monitor has to be configured on the switch facility. The Switch Port Analyzer (SPAN) feature was introduced on switches because of a fundamental difference they have with hubs. After a switch boots up, it will start to build up a Layer 2 forwarding table based upon the source MAC address of the different packets received. Once this forwarding table has been built, the switch forwards traffic destined for a MAC address directly to the corresponding sport.



In this above diagram, Verba is attached to a port that is configured to receive a copy of every single packet that is sent by host A. This port is called a SPAN port.

More information on the Cisco site

You can find more information about configuring and using monitor ports in Cisco switching environment, please read the following documentation's:

Port Monitoring

http://www.cisco.com/en/US/tech/tk389/tk816/tsd_technology_support_protocol_home.html

Configuring SPAN on Catalyst 5000

<http://www.cisco.com/en/US/docs/switches/lan/catalyst5000/catos/5.x/configuration/guide/span.html>

Configuring SPAN and RSPAN on Catalyst 4000 Running Hybrid Mode

<http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.2/18ew/configuration/guide/span.html>

Configuring SPAN and RSPAN on Catalyst 3550

http://www.cisco.com/en/US/docs/switches/lan/catalyst3550/software/release/12.1_19_ea1/configuration/guide/swspan.html

Configuring SPAN and RSPAN on Catalyst 2950

http://www.cisco.com/en/US/docs/switches/lan/catalyst2950/software/release/12.1_22ea/SCG/swspan.html

Configuring SPAN on Catalyst 2900XL/3500XL

http://www.cisco.com/en/US/products/hw/switches/ps708/products_tech_note09186a008015c612.shtml#topic1

Configuration example

In the following example we provide a short description about setting up a monitor port on a Cisco Catalyst 3524-XL-PWR switch.

You can use SPAN to monitor traffic on a given port by forwarding incoming and outgoing traffic on the port to another port in the same VLAN. A SPAN port cannot monitor ports in a different VLAN, and a SPAN port must be a static-access port. You can define any number of ports as SPAN ports, and any combination of ports can be monitored:

Step 1 - Connect your computer to the switch (through the LAN or the console port).

Step 2 - *configure terminal*

Enter global configuration mode.

Step 3 - *interface FastEthernet 0/24*

Enter interface configuration mode, and enter the port that acts as the monitor port.

Step 4 - *port monitor FastEthernet 0/1*

Enable port monitoring on the desired port.

Step 5 - Repeat Step 4. until you configured all VoIP ports.

Step 6 - *end*

Return to privileged EXEC mode.

Step 7 - *show running-config*

Verify your entries.

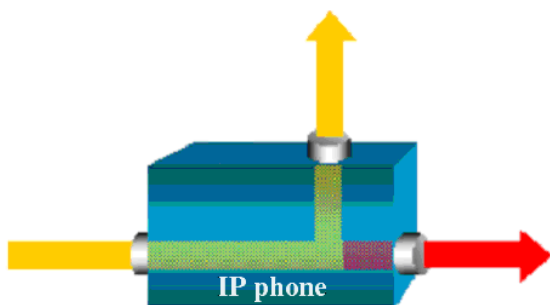
Step 8 - *copy running-config startup-config*

Copy running configuration to startup configuration.

For more information, please ask your switch manufacturer or your system integrator/distributor.

Monitor port on an IP phone (Verba Desktop configuration)

In order to aggregate VoIP call traffic into one port in a Verba Desktop environment, we can configure the PC to monitor voice traffic through the 10/100 Ethernet port of the IP phone which is connected to the desktop computer.



In the above diagram, Verba is attached to the 10/100 Ethernet port of the IP phone. All voice traffic is monitored directly on the IP phone PC port.

Below Unified Communications Manager 3.3(3) versions, voice traffic is automatically forwarded to the PC port. From 3.3(3) version onward you can forbid voice traffic monitoring on the PC port. You are able to configure this option for every phone through the Unified Communications Manager administration interface:

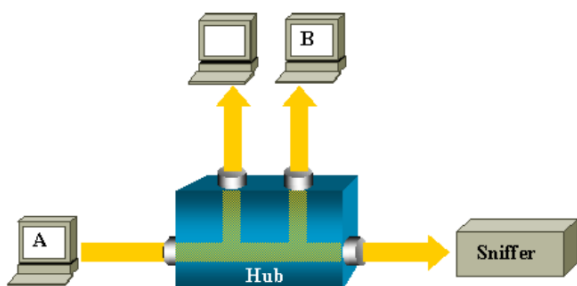
PC Voice VLAN Access,

Which indicates whether the phone will allow a device attached to the PC port to access the Voice VLAN. Disabling Voice VLAN Access will prevent the attached PC from sending and receiving data on the Voice VLAN. It will also prevent the PC from receiving data sent and received by the phone. You Must set this setting to be able to use Verba Desktop Edition for call recording.

(Deprecated) Monitoring through a hub

⚠ This option is **deprecated and not recommended in production environments**. It is documented here to just cover all available technologies.

When IP phones connected through a hub, there is no special configuration task in order to aggregate call traffic, because when a hub receives a packet on one port, it will send out a copy of that packet on all ports except on the one where it was received. So you can simply connect Verba server to a hub port, and all VoIP traffic will appear on Verba recording interface.



For example, if you want to capture Ethernet traffic sent by host A to host B and both are connected to a hub, just attach Verba to this hub as all other ports see the traffic between host A and B.

Overview of monitor ports for passive recording

This topic describes the recommendations for configuring monitor ports.

! The most important issue that system engineers have to keep in mind when planning Verba system is the following (regarding to monitor ports):
One of the **signaling endpoints** and one of the **RTP media stream endpoints** of a call must to be monitored on the same Recording Server in order to record a conversation.

Internal calls - Verba can record a call between two IP phones if signaling messages are monitored for at least one of the stations and the RTP media streams are monitored at least for at least one endpoint.

Incoming and outgoing calls - Verba can record an incoming or outgoing call if signaling messages for an IP phone are monitored and the RTP media streams are monitored for at least one endpoint. Verba is also record the IP trunk traffic directly, if the signaling is set to SIP.

Conference calls - Verba can record a conference call if all signaling messages for the participants are monitored and the RTP media streams are monitored for every endpoint, that participates in the conference.

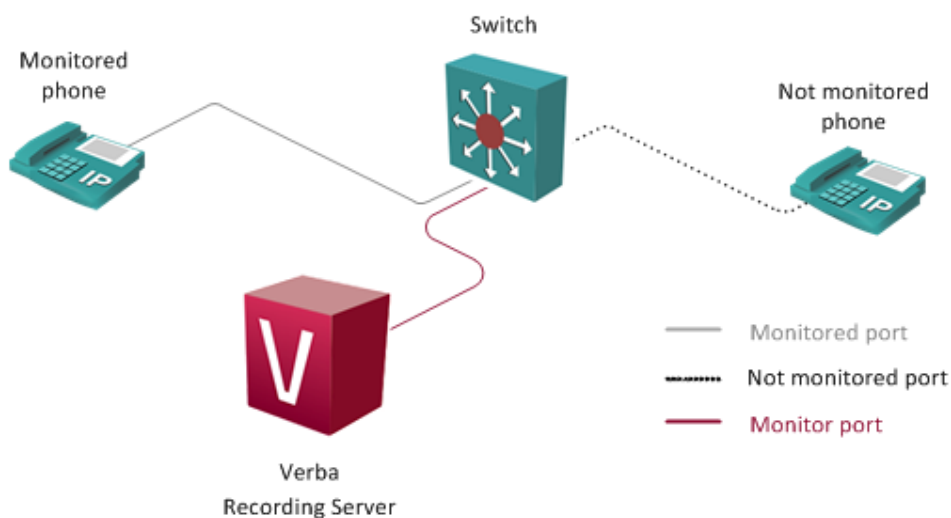
The following scenarios are supported in the Verba system:

- Internal call between monitored phones
- Incoming and outgoing call between a monitored phone and a gateway
- Internal call between a monitored and a not monitored phone
- Incoming and outgoing call between a monitored gateway and a not monitored phone
- Conference call among monitored phones

The above listed scenarios can be combined depending on your switching infrastructure. e.g. in some cases monitoring the PBX port cannot be done or the network topology does not allow monitoring all of the phones.

Internal call between monitored phones

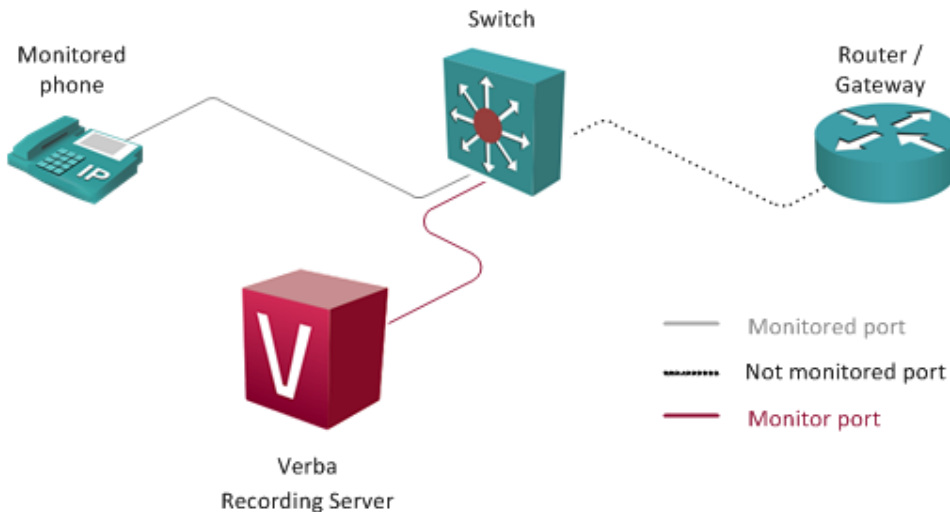
Scenario description: Internal call between two IP phones (SCCP, SIP) when both phones are monitored on the same port.



Using this scenario, only those IP phones which have to be recorded are monitored. Incoming and outgoing calls (calls which go through a gateway) are also recorded.

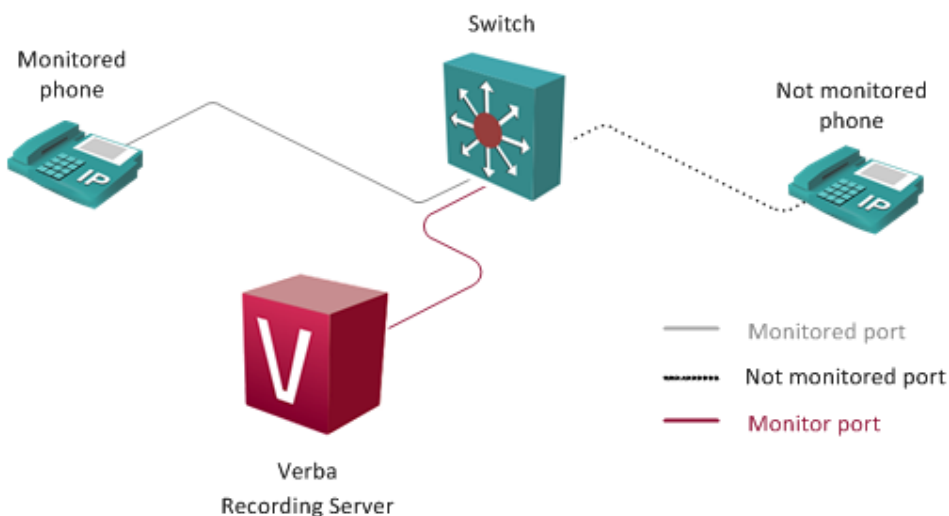
Incoming and outgoing call between a monitored phone and a gateway

Scenario description: Incoming and outgoing call between an IP phone (SCCP, SIP) and a gateway (H.323, MGCP or SIP) when the IP phone is monitored.



Internal call between a monitored and not monitored phone

Scenario description: Internal call between two IP phones (SCCP, SIP) when one of the phones and the PBX are monitored on the same port.

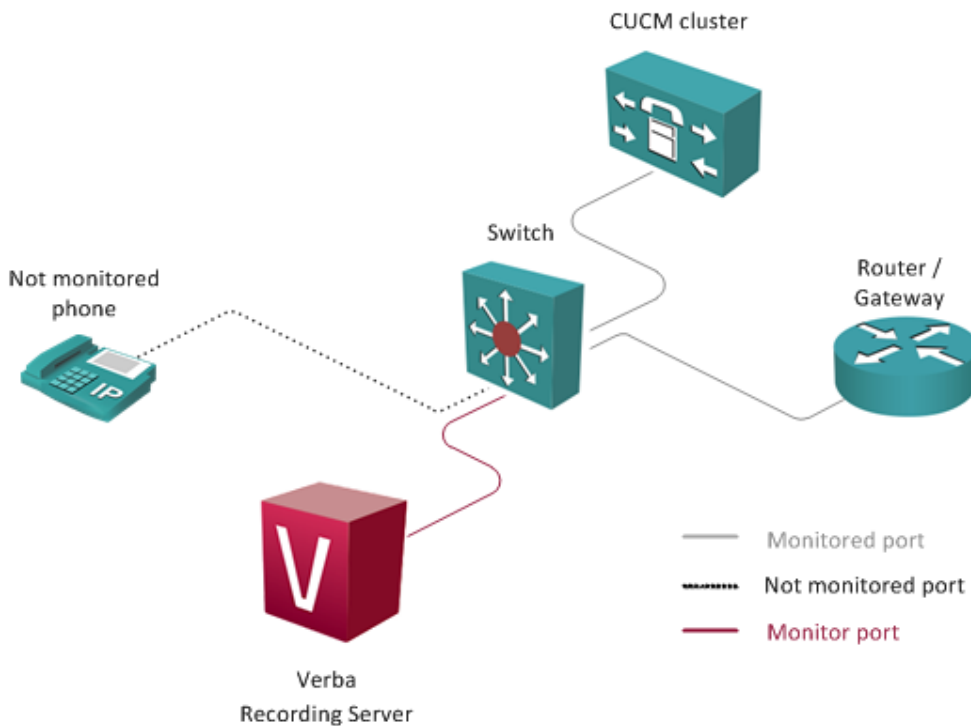


With this scenario, you can record calls between a monitored and a not monitored IP phone, because monitoring one of the call endpoints will provide RTP media streams, and monitoring one of the IP phones will provide signaling messages for both endpoints.

Incoming and outgoing calls between a monitored IP phone and a not monitored gateway are also recorded.

Incoming and outgoing call between a monitored gateway and a not monitored phone

Scenario description: Incoming and outgoing call between an IP phone (SCCP, SIP) and a gateway (H.323, MGCP or SIP) when the gateway and the PBX are monitored on the same port.

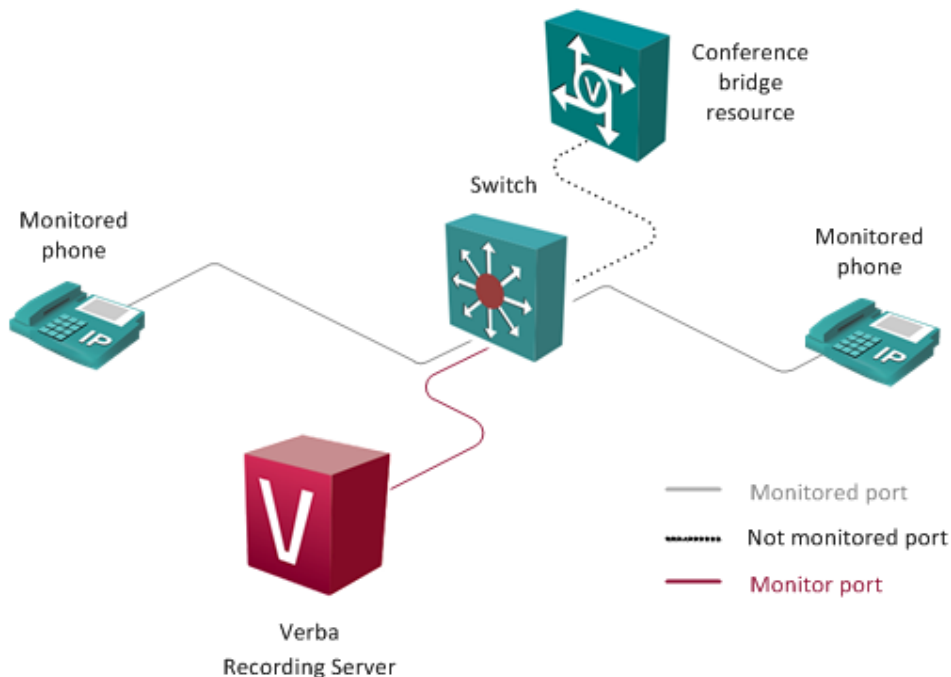


With this scenario, you can record calls between a not monitored IP phone and monitored gateway, because monitoring one of the call endpoints will provide RTP media streams, and monitoring the PBX will provide signaling messages for the IP phone.

Internal calls between not monitored IP phones are not recorded.

Conference call among monitored phones

Scenario description: Conference call among IP phones (SCCP, SIP), when all the phones are monitored on the same port.



With this scenario, you can record conference calls among monitored IP phones, because monitoring the call endpoints will provide RTP media streams and signaling messages for the IP phones. In a PBX environment, conference calls flow in a star topology, where the center of the star mixes the audio channels (a mixer can be the PBX or another media resource e.g. a gateway, if transcoding is necessary).

If one of the IP phones is not monitored, the audio stream of the conference for that device will not be recorded.

If a conference participant is connected through a gateway (whether it is monitored or not), the conference will be not recorded for that device.

Using Cisco switches to filter SPAN traffic

Overview

Using passive recording scenarios (when traffic is delivered to the Verba recording servers through monitoring or SPAN ports) large amounts of traffic could overload the recording servers. In a typical IP telephony environment, this problem can be handled easily by monitoring only the voice VLANs, which should only contain voice traffic.

This technique, however, can not be used in all situations. If a dedicated voice VLAN is not available in the network architecture, or if the voice and video traffic is mixed with other kinds of traffic (e.g. when using **softphones installed on desktop PCs**), the best solution is to filter the SPAN traffic. SPAN traffic filtering is available only on selected Cisco switches.

Cisco's Flow-based SPAN allows filtering

Here is the Cisco definition of the feature that allows SPAN traffic filtering:

Flow-Based Switch Port Analyzer (FSPAN) - SPAN provides a mechanism to capture data appearing on specified ports or VLANs, mirroring it on destination ports. It is very useful for security monitoring and traffic management. *However, sometimes the amount of traffic captured with SPAN can be too large and difficult to analyze.* Flow based SPAN provides a mechanism to capture only required (interesting) data between endhosts, by using specified filters. The filters are defined in terms of access-lists that limit IPv4, IPv6 or IPv4 + IPv6, or non IP traffic (MAC) between specified source and destination addresses.

You can use the **Cisco Feature Navigator** to find which products support it (e.g. type "Flow-based" to find it).

<http://tools.cisco.com/ITDIT/CFN/jsp/by-feature.jsp>

E.g. the **Cisco 3560-X and Cisco 3750-X** Series switches all support FSPAN.

Sample configuration for Cisco or SIP passive recording

If your RTP port range is 16384-32767 (standard on Cisco gateways) you could use the followings to filter out the majority of none-voice traffic.

```
extended IP access list verbafilter
 10 permit udp any any range 16384 32767
 20 permit udp any range 16384 32767 any
 30 permit ip any <ip-pbx>

 40 permit ip <ip-pbx> any
```

Where the <ip-pbx> part shall be replaced with the IP address of your IP PBX, e.g. Cisco UCM. In your SPAN traffic you should mostly see SIP, Cisco SCCP and RTP packets.

Sample configuration for Microsoft Lync passive recording

In [Microsoft Lync passive recording](#), signalling is coming to the recorders directly from the Lync Front End servers, therefore you will only need to allow RTP traffic in your filter. You can configure Lync to use a narrow UDP range for RTP traffic, e.g. 18000-18040. This will effectively filter-out most non-RTP traffic from the monitor port.



```
extended IP access list verbafilter
 10 permit udp any any range 18000 18040
 20 permit udp any range 18000 18040 any
```

After this, you should mostly see UDP packets (which are encrypted RTP packets) in your SPAN traffic.

Configuring Verba for SIPREC recording

Verba Unified Recorder has SIPREC implementation and is responsible for recording calls via this new interface/standard. It detects proprietary vendor-specific extensions in the SIPREC CDR xmls automatically, no vendor-specific configuration is needed at Verba side.

Activate recording

Step 1 - Provision recording in PBX. Read more:

- [Configuring Broadworks platform for SIPREC based call recording](#)
- [Configuring ACME Packet platform for SIPREC based call recording](#)
- [Configuring Cisco Unified Border Element \(CUBE\) based recording](#)
- [Configuring Polycom RMX for conference recording](#)
- [Configuring Cisco VCS for Permanent Conference Recording](#)

Step 2 - In the Verba Web Interface, go to **Administration > Verba Servers > Select your Recording Server > Click on the Service Activation** tab.

Step 3 - Activate the **Verba Unified Call Recorder Service** by clicking on the



icon.

Step 4 - Click on the **Change Configuration Settings** tab. Expand the **Unified Call Recorder** section.


Step 5 - Under **Recording Providers \ SIP \ SIPREC** set the **SIP Port** setting according to the port configured at the PBX side.

Step 6 - Save the changes by clicking on the



icon.

Step 7 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

 There are tasks to be executed regarding the configuration of this Verba Server.
If you would like to execute these tasks now, please [click here](#) .

Step 8 - Click on the **Service Control** tab.

Step 9 - Start the **Verba Unified Call Recorder Service** by clicking on the



icon.

Configure extensions

After finalizing the configuration of the recording services, make sure you have added the extensions you want to record to the Verba extension list. This can be done manually ([Extension list](#)) or using [Active Directory Synchronization](#).

Configuring recorder numbers/lines (Huawei only)

In the case of the Huawei platform, the **recording access codes (phone number(s) to which recorder call is routed)** have to be configured at the Verba side.

Under **Recording Providers \ Huawei \ Recorder Extensions/Lines** add number(s) to which recorder calls are routed from Huawei PBX.

For Huawei side configuration please refer to <http://support.huawei.com/enterprise/en/doc/DOC1000073852?section=10082> Telephone recording section

Configuring advanced network-based recording

With the advanced network-based recording configuration load-balancing and mid-call failover can be achieved. For the configuration steps see [Configuring advanced network-based recording](#).

Configuring Acme Packet platform for SIPREC based call recording

In order to use the Acme Packet SIPREC recording interface configuration of the SBC is required.

You can use this SIPREC integration to record:

- audio sessions and
- video sessions.

Requirements

SIPREC requires the purchase of a **Session Recording license**. Contact your Acme Packet Representative for more information

SIPREC is currently supported on the following platforms running Acme Packet Release: **E-C(xz)6.4.0F1**:

- Net-Net 3820
- Net-Net 4500
- Net-Net Enterprise Session Director-Server Edition (ESD-SE)
- Net-Net Enterprise Session Director-Virtual Machine Edition (ESD-VME)

SBC Provisioning Steps

Step 1 - Provision session recorder server(s)

In this step recorder server(s) are assigned to SBC.
The most important parameters:

- **realm**: the realm to which the recorder belongs. Acme Packet recommends to use separate/dedicated realm for recorder servers. If you create dedicated realm, make sure related sip-interface and steering-pool configuration has been also done.
- **destination**: IP address of the recorder server
- **port**: listening port of recorder server (default SIP port of Verba Dial-in Recorder is 5065)
- **transport-method**: SIP transport, we support all possible values except SCTP, but prefer StaticTCP

Example configuration script

```
# configure terminal
(configure)# session-router
(session-router)# session-recording-server
(session-recording-server)# name VERBA0
(session-recording-server)# select VERBA0
(session-recording-server)# realm REALM_TO_RECORD
(session-recording-server)# destination recorder_ip
(session-recording-server)# port 5065
(session-recording-server)# transport-method StaticTCP
(session-recording-server)# done
```

Step 2 - Create recorder server group (for load-balancing & failover support)

In this optional step recorder servers are assigned to a recorder group. Load-balancing and failover support can be configured at group level

The most important parameters:

- **strategy:** load-balancing/call distribution method to use
- **simultaneous-recording-servers:** number of recorder servers simultaneously recording a call. You can configure redundant recording with this feature
- **session-recording-servers:** enumeration of recording server names belonging to the group (configured in Step 1.). You can add servers by 'session-recording-servers +SERVER_NAME' or remove by 'session-recording-servers -SERVER_NAME' command

Call distribution strategies:

- **Round-robin (default)** - The SBC remembers the last Session Recording Server (SRS) that was used. Each new recording session selects the next SRS in the session recording group. When simultaneous-recording-servers is greater than 1, the next n recording servers are selected from the session recording group.
- **Hunt** - The SBC successively attempts to contact SRSs in the session recording group until a successful recording dialog is established with the SRS, starting from the first SRS in the session recording group. The SBC attempts to contact each SRS in the session reporting group once. When contact is exhausted, the recording device is considered failed. A SIP failure (response greater than 399, timeout or TCP setup failure) causes the SBC to attempt the next possible SRS. When simultaneous-recording-servers is greater than 1, the SBC attempts to establish n recording devices in a hunting fashion.
- **Least busy** - For some 3rd party recording devices, the number of concurrent recording servers proves to be the most taxing for system resources. The SBC tracks the number of recording servers active to a given SRS at any given time. It uses this information to determine which SRS would be the best candidate for the next RS. The SRS with the fewest number of active recording servers receives the next RS. If two or more SRSs in a session recording group currently have the same number of active recording servers, the SRS configured first in the session recording group takes precedence.
- **Lowest sustained rate (fewest-setups-per-minute)** - For some 3rd party recording servers, processing large amounts of sessions in a short amount of time proves to be the most taxing on their system's resources. The SBC tracks the number of recording server setups over a sliding window of five minutes. The SRS within the session recording group with the fewest setups per the window of time is selected as the next candidate for receiving the recorded session. If two or more SRSs in a session recording group currently have the same value for setups in the given window of time, then the SRS configured first in the session recording group takes precedence.

Example configuration script:

```
# configure terminal
(configure)# session-router
(session-router)# session-recording-group
(session-recording-server)# name VERBA
(session-recording-server)# select VERBA
(session-recording-group)# strategy LeastBusy
(session-recording-group)# simultaneous-recording-servers 1
(session-recording-group)# session-recording-servers +VERBA0
(session-recording-group)# session-recording-servers +VERBA1
(session-recording-group)# session-recording-servers +VERBA2
(session-recording-server)# done
```

Step 3 - Assign recorder server (group) to recorded entity

After recorder server or group has been defined it should be assigned to recorded entity, Session recorder servers can be assigned either to sip-agent, realm, or sip interface. Recording mode is selective, according to Acme's design the responsibility to select to be recorded calls is at SRS side. This means that SBC invites the recorder into all calls processed by recorded entity

(sip-agent, realm, sip-interface) and recorder explicitly refuses not to be recorded sessions based on caller/callee id or other properties of the call, and establishes session only for to be recorded calls.

The most important parameters:

- **session-recording-server:** assigns the already configured (Step 1.) recorder server or server group (Step 2.) to the entity. To assign recorder server group the name of group must be prefixed with 'SRG:' as it is done in the example below.
- **session-recording-required:** if set to enabled the SBC does not establish the recorded call if recorder is not available to record the session

Example configuration script (assigns VERBA recording server group to 'PBXS' sip-interface)

```
# configure terminal
(configure)# session-router
(session-router)# sip-interface
(sip-interface)# select PBXS
(sip-interface)# session-recording-server SRG:VERBA
(sip-interface)# session-recording-required disabled
(sip-interface)# done
```

Step 3 - Verify, save and activate configuration

After configuration has been done, you should verify, save and activate it on the SBC:

```
# verify-config
# save-config
# activate-config
```


Configuring Broadworks for SIPREC based call recording

In order to use the Broadsoft SIPREC interface configuration of PBX is required.

Application Server Provisioning Steps

Step 1 - Activate the service feature as follows:

```
AS_CLI/System/ActivatableFeature> activate 46941
```

Feature details:

- Activatable Feature ID: 46941.
- Activatable Feature Name: Call Recording.
- Dependencies: FR 140637 "Enable CDR schema version R17 SP4 for Activatable Features".

Step 2 - Add call recording platform:

```
AS_CLI/Service/CallRecording/add [name] [netAddress] [port] [transportType] [mediaStream] description [description label]
```

name	The name of the recording platform. (1-80 characters)
netAddress	This is the FQDN, host, or IP address of the recording platform.
port	This is the address port of the recording platform. (Integer 1 to 65535).
transportType	This is the SIP interface type ("UDP", "TCP", "Unspecified").
mediaStream	This is the type of media stream defined either as "dual" or "single" stream.
description value	This is the description of this recording platform.


Example:

```
AS_CLI/Service/CallRecording> add platformA RD_FQDN 5065 TCP dual description RecordingDeviceFQDN
```

...Done

Step 3 - Set the Default Call Recording Platform

```
AS_CLI/Service/CallRecording/set [name] systemDefault true
```

-  • **Check firewall rules and allow connection between recorders and Broadsoft platform.** You can check/control SIP and RTP listening address range in recorder configuration.
- **Ensure Verba Dial-in Recorder server is listening on the provisioned address.** We recommend using static IP and referencing the recorder by IP instead of NETBIOS/DNS name.

BroadWorks Call Recording Service Administration Configuration

The following menus have been modified to add links to the new *BroadWorks Recording Services* page:

ServiceProvider/Enterprise → *Resources* → *Services*

Group → Resources → Services

User → Call Control

The following pages have been added to support the new BroadWorks Call Recording service:

Service Provider/Enterprise → Utilities → Feature Access Codes

Group → Utilities → Feature Access Codes

User → Call Control → BroadWorks Call Recording (administrator view)

User → Call Control → BroadWorks Call Recording (user view)

Step 1 - Under **Service Provider/Enterprise/Resources/Services** enable Call Recording and set appropriate limitation. This will authorize call recording service for provider/enterprise

Step 2 - Under **Service Provider/Enterprise/Utilities/Feature Access Codes** set appropriate FAC for on demand call keep/record command

Step 3 - Under **Group/Resources/Services** enable Call Recording and set appropriate limitation for the intended group. This will authorize call recording service at group level if service is authorized for the provider/enterprise to which it belongs

Step 4 - Under **Group/Utilities/Feature Access Codes** set appropriate FAC for on demand call keep/record command. You can configure this at group level as well.

Step 5 - Under **Group/Resources/Call Recording Platform** select the previously provisioned call recording platform

Step 6 - Under **User/Profile/Assign Services** add Call Recording service to the user

Step 7 - Under **User/Call Control/Call Recording** select the desired call recording mode

Configuring Cisco Unified Border Element (CUBE) based recording

Overview

CUBE supports SIP/SIPREC based recording for voice and video calls passing the CUBE. CUBE supports standard SIPREC based integration and SIP based with customer CUBE specific headers. Both integrations are supported by the Verba platform.

You can learn more from official Cisco documents about CUBE based recording:

- SIP based recording: <https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/configuration/cube-book/voi-ntwk-based.html>
- SIPREC based recording: <https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/configuration/cube-book/voi-sip-recording.html>
- Additional information for video recording: <https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/configuration/cube-book/voi-ntwk-based-rec-video-calls.html>

Prerequisites for CUBE recording

Please visit the related Cisco documentation, linked above for up to date information on supported Cisco routers and IOS versions.

Restrictions for CUBE recording

- SIP-SIP call flows are only supported, For TDM, H.323 please check our [WSAPI based recording](#) solution. TDM and H.323 recording can be also achieved with a trick: TDM calls should be forced to pass through CUBE
- Any media service parameter change via Re-INVITE or UPDATE from recording server is not supported. For example, hold-resume or any codec changes
- IPv6-to-IPv6 call recording
- IPv6-to-IPv4 call recording if the recording server is configured on the IPv6 call leg
- Calls that do not use Session Initiation Protocol (SIP). Must be a SIP-to-SIP call flow
- Flow-around calls
- Session Description Protocol (SDP) pass-through calls
- Real-time Transport Protocol (RTP) loopback calls
- High-density transcoder calls
- Secure Real-time Transport Protocol (SRTP) passthrough calls
- SRTP-RTP calls with forking for SRTP leg (forking is supported for the RTP leg)
- Multicast music on hold (MOH)
- Mid-call renegotiation and supplementary services like Hold/Resume, control pause, and so on are not supported on the recorder call leg
- Recording is not supported if CUBE is running a TCL IVR application with the exception of survivability.tcl, which is supported with SIPREC based recording
- Media mixing on forked streams is not supported
- Digital Signal Processing (DSP) resources are not supported on forked legs
- If the main call has multiple video streams (m-lines), the video streams other than the first video m-line are not forked
- Application media streams of the primary call are not forked to the recording server
- Forking is not supported if the anchor leg or recording server is on IPv6
- Server Groups in outbound dial-peers towards recorders is not supported.

Configuration

The recording method and configuration steps are very similar to [UCM phone forking based recording](#) solution. Recorder servers are invited into the to be recorded calls via SIP, RTP forking is done by the recorded endpoint. Configuration steps are also similar, UCM phone forking based recording analogous steps are highlighted to make it easier to understand the concept for users who has been using phone-based recording as well.

- Create dial-peer(s) pointing to recorder server(s) (similar to UCM recorder trunk configuration)
- Create a media profile dedicated to the recording, enumerate dial-peers pointing to the recorder servers. This is a logical link between recorders - to be recorded calls (similar to UCM central recording recorder profile configuration)
- If you want to record video calls then create a video profile, specify the reference frame requesting method
- Assign the media profile and optional video profile to a media class
- Assign the media class to the to be recorded incoming dial-peer(s) (similar to UCM central recording extension-specific recording options)

High Availability

You can configure failover and load-balancing for recorder servers:

- Failover: media-recording command should enumerate the destination number of recorders. If the active recorder becomes unavailable the CUBE will assign the next recorded call to the next available recorder in the list.
- Load-balancing: Load-balancing of recorder servers can also be achieved. In this case, the recorder dial-peers should be configured for the same destination number and with the same priority. In this case, CUBE will randomly distribute the calls between recorders with the same destination number
- Failover + Load-balancing: You can also combine the two methods and so have an active and backup recorder pools

Configuring CUBE for SIP based recording

The following steps with example values will enable voice and video recording of all 4-digit called numbers on recorder 192.168.1.200. Commands should be issued in terminal configuration mode.

Step 1 - Allow voice connections to recorder servers. Add all of your recorder servers IP or IP subnets so the CUBE will trust and allow communication over SIP with them.

```
voice service voip
ip address trusted list
ipv4 192.168.1.0 255.255.255.0
```

Step 2 - Create a codec class enumerating supported codecs and codec preferences by the recorder. You can skip this step and assign a specific codec to the recorder dial-peer but with codec class enumerating multiple codecs you can save transcoding resources since we support most of the codecs natively.

```
voice class codec 1
codec preference 1 g722-64
codec preference 2 g711alaw
codec preference 3 g711ulaw
codec preference 4 g729r8
codec preference 5 g729br8
video codec h264
```

Step 3 - Create a dial-peer pointing to the recorder

```
dial-peer voice 9999 voip
description Verba CUBE Forking Recorder 0
destination-pattern 9999
session protocol sipv2
session target ipv4:192.168.1.206:5060 (specify the address on which Verba Unified Call Recorder is listening)
session transport tcp
voice-class codec 1 (specify the codec list supported by the recorder natively)
dtmf-relay rtp-nte (RFC 4733/2833 based DTMF is supported by the recorder)
```

Step 4 - Create a recorder profile

```
media profile recorder 100
media-recording 9999 (here you can enumerate the destination number of recorder servers)
```

Step 5 - Create video profile (optional, only if you want to record video calls)

```
media profile video 101
monitor-ref-frames
ref-frame-req sip-info
```

Since video compression algorithms are recursive and contain referencing to previous frames (inter-frame, motion-compensated prediction) it is crucial to start the recording at a key/reference frame. CUBE is able to request keyframe automatically after the recorder establish a connection with the call session from participating endpoints

To control keyframe request two generally used method is available and configurable:

- SIP INFO request with Fast Picture Update encoder request: can be set by ref-frame-req sip-info command
- RTCP FIR: can be set by ref-frame-req rtcp retransmit-count 4 command

Step 6 - Create media class and assign media and video profile

```
media class 100
recorder profile 100
video profile 101 (optional, only if video calls are to be recorded)
```

Step 7 - Assign recorder media class to the to be recorded incoming dial-peers. It is important to assign it to incoming and not to outgoing peer.

```
dial-peer voice 9999 voip
description Inbound dial-peer for recorded calls
session protocol sipv2
incoming called-number ....
voice-class codec 1
media-class 100
```

Configuring Cisco VCS for Permanent Conference Recording

Overview

Using the Cisco Video Communications Server (VCS), you can configure permanent conferences, which will automatically add a Verba Recording Server into the conference.

This lets you record video conferences with minimal change in user behavior.

Step 1 - Configuring the Verba Recording System

Please follow the configuration steps in [Configuring Verba for SIPREC recording](#).

Step 2 - Configuring VCS

Follow these guidelines when creating a Permanent Conference:

Step 1 - Configure the Verba Recording Server as an **Endpoint**

Step 2 - Make sure on the Endpoint you configure **Automatic Disconnect**

Step 3 - Pick a user and create a **Permanent Conference** for that user as "chair" (each regulated user could have their own Permanent Conference number created)

Step 4 - Configure the Verba Recording Server alias as **pre-configured participant** in the Permanent Conference

i About **Automatic Disconnection** in the Endpoint configuration: when a participant disconnects from a conference and only endpoints set to Automatic disconnection are left, all those participants are disconnected. If this is enabled the Verba Recording Server will be automatically terminated when no more participants are on the call.

End User experience

In order to do recorded conversations the users should follow this procedure:

Step 1 - The chair should call a Permanent Conference

Step 2 - Other participants should join the same conference

Step 3 - Execute the meeting then terminate normally

Behind the scenes:

- After **Step 2**, the MCU will automatically call the Verba Recording Server into the call.
- After **Step 3** (when the last person leaves the call), the connection to the Verba Recording Server is terminated

Configuring Polycom RMX for conference recording

Overview

Verba Dial-in Recorder service is able to record video conference calls automatically via recorder link interface. For this to work, the Verba recorder must be provisioned via RMX configuration.

- [Overview](#)
- [Supported call scenarios](#)
- [Verba configuration steps](#)
- [Configuration steps](#)
- [Recording link encryption](#)

Supported call scenarios

This solution supports the following scenarios:

- **all Polycom "conference room" calls on RMX bridge**
- the recorded "conferences rooms" can be joined with **H.323 and SIP both unencrypted and encrypted modes**
- peer-to-peer calls are not forced to go through the RMX bridge, therefore **peer-to-peer calls are not recorded** in this scenario

Verba configuration steps

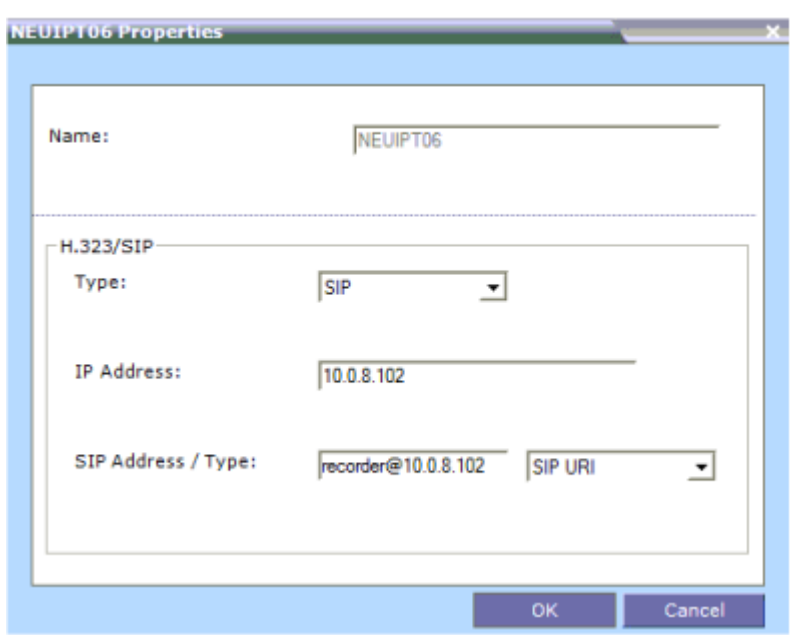
Please follow the configuration steps in [Configuring Verba for SIPREC recording](#).

Configuration steps

Step 1 - Create Recorder link

To define a Recording Link: in the RMX Management pane, click Recording Links, in the Recording Links list, click the New Recording Link button.

1. Select **SIP as the controlling protocol**
2. Enter the IP address of the recorder
3. Enter a SIP URI pointing to the recorder

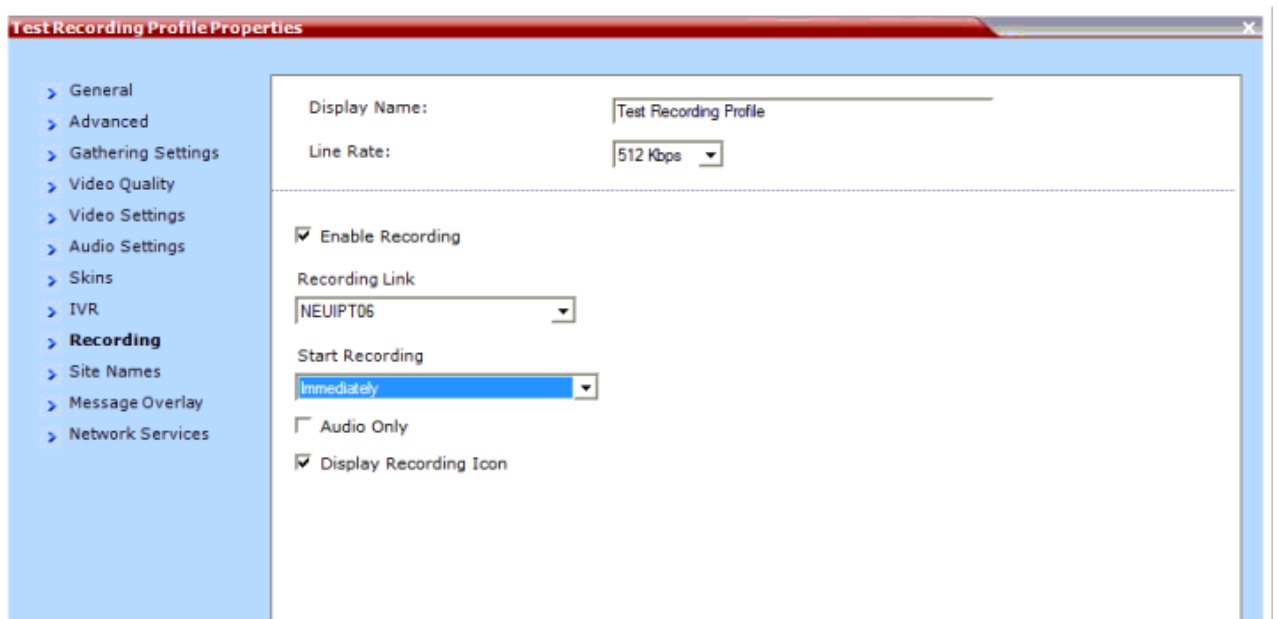


Step 2 - Create/modify existing conference profile

To be able to record a conference, the recording options must be enabled in the

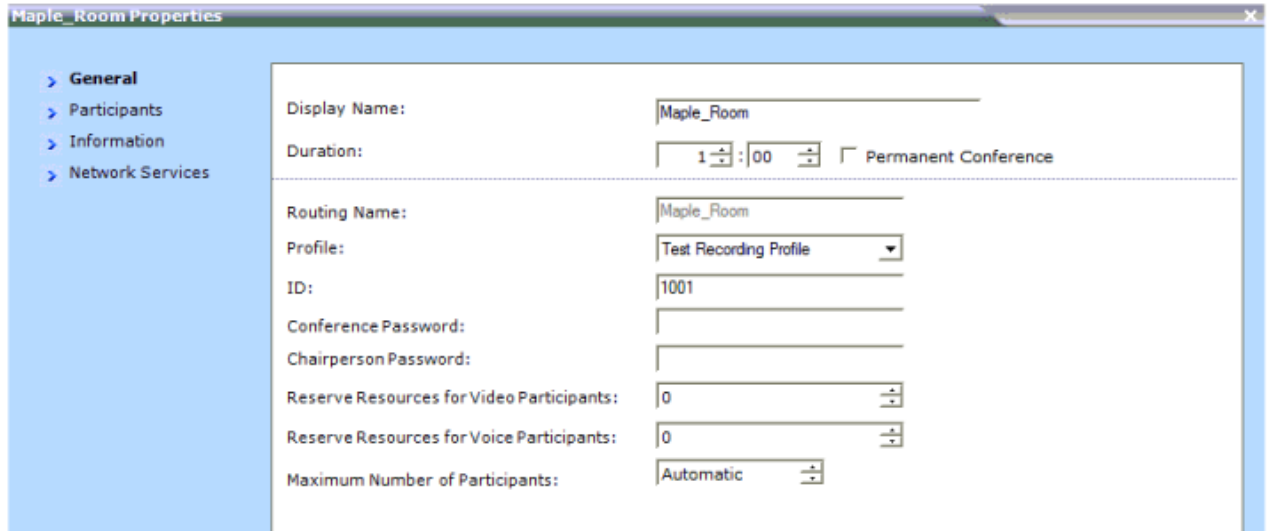
Conference Profile assigned to it. You can add recording to existing Profiles by modifying them. In the RMX Management pane, click the Conference Profiles button. Create a new profile by clicking the New Profile button or modify an existing profile by double-clicking.

1. In Advanced menu set **Encryption to Encrypt when possible**
2. In Advanced menu set **Auto terminate when the last participant remains** (recorder is threatened as normal participants from this point of view)
3. In IVR menu on-demand recording DTMF codes can be changed
4. In Recording select the recorder link, check enable recording and select recording start mode (immediately or upon request). You can also limit the recording line's bitrate



Step 3 - Assign profile for conferences

Assign the recording enabled profile to the conference rooms that need to be recorded.



Recording link encryption

According to Polycom documentation the recording link can be encrypted when recording an encrypted conference, this requires H.323 recorder signaling. Since Verba supports only SIP, the recording link cannot be encrypted, but still, it is possible to record an encrypted conference. To achieve this system flag **ALLOW_NON_ENCRYPT_RECORDING_LINK_IN_ENCRYPT_CONF** must be set to **YES**. Recording Link Encryption Flag Setting Recording Links are treated as regular participants, however, if the **ALLOW_NON_ENCRYPT_RECORDING_LINK_IN_ENCRYPT_CONF** System Flag is set to YES a non-encrypted Recording Link is to be allowed to connect to an encrypted conference.

Conference Profile Setting	Recording Link Connection Status according to flag: ALLOW_NON_ENCRYPT_RECORDING_LINK_IN_ENCRYPT_CONF	
	YES	NO
Encrypt All	Connected encrypted if possible, otherwise connected non-encrypted.	Connected only if encrypted, otherwise disconnected.
No Encryption	Connected non-encrypted.	Connected non-encrypted.
Encrypt when possible	Connected encrypted if possible, otherwise connected non-encrypted.	Connected encrypted if possible, otherwise connected non-encrypted.

For more information, you can read the Polycom® RealPresence® Collaboration Server (RMX) 1500/2000/4000 Administrator's Guide: Recording Conferences chapter.

Central License Management

Overview

- Deployments with multiple Verba instances can centralize license management, instead of deploying a separate (or the same) license for each instance.
- One Media Repository can be designated as a Remote License Server (RLS) for other Media Repositories belonging to other Verba instances
- If multiple Media Repositories are installed within a deployment, then the Verba Cluster ID should be set to avoid counting the usage multiple times
- Media Repositories are fetching license information periodically and send usage data to the RLS
- RLS computes the total usage and does license checks
- RLS sends a compliance answer (OK / not OK)
- If RLS says not OK, the license error on the MRs that use an RLS just shows the URL of the RLS
- If a Media Repository sends its usage to the RLS which is installed in the same deployment, then the RLS recognizes the conflict based on the Verba Cluster ID setting and ignores this data
- Authentication is done using API keys

Configure a Remote License Server

The Remote License Server configuration is done on the client servers.

Step 1 - Log in to the web interface with the Administrator user and navigate to **System > License**

Step 2 - Click on the **Set Remote License Server** link at the top right corner

License Information

[Upload Local License File](#)
[Set Remote License Server](#)



License Data

Product Verba Recording System - Not For Resale Kit
License Identifier 001b000000hoVWw
Issue Date 2014-12-17 01:00:00
Support Expiration 2020-12-17 01:00:00
Customer Verint Verba Customer

License Items

Name	Code	Quantity	Valid From	Expiration	Value
Verba Enterprise Server License	VR3-SR-ENT-L	4		Never	
Verba Recording Server License	VR3-SR-RS-L	10		Never	

Step 3 - Set configuration (an API Key and API User has to be set in advance on the RLS)

Set Remote License Server

[Back to License Information](#)



Server HTTPS API URL *

API Key *

API User *

API Password *

Save

If the configuration is correct and the RLS was accessible, then the RLS information will be shown on the License screen.

License Information Upload Local License File
Change Remote License Server

⚠ Remote License Server: https://fenyvesi:447/verba/api ?

License Data

Product	Verba Recording System - Not For Resale Kit
License Identifier	001b000000hoVWw
Issue Date	2014-12-17 01:00:00
Support Expiration	2020-12-17 01:00:00
Customer	Verint Verba Customer

Change / Unbind a Remote License Server

- If the RLS needs to be changed, then just set up a new one exactly the same way as the first one was set up
- If no RLS is needed anymore, then the RLS can be unbound by uploading a license file on the License Information screen
- Both the former and the new RLS will be informed about the change

Remote License Server Side

The Remote License Server automatically gets the RLS role as the first client connects to it.

The License Information screen displays the accumulated numbers by default, but the independent usage can also be viewed by selecting a server from the client's list box:

License Information Upload Local License File

⚠ This is a Remote License Server for 2 Client(s).

Show Usage: -- Cumulate -- ?

License Data: -- Cumulate --
[Local] (2018-02-09)
Verint Verba London (2018-02-03)
Verint Verba Singapore (2018-02-03)

Product	Verba Recording System - Not For Resale Kit
License Identifier	001b000000hoVWw
Issue Date	2014-12-17 01:00:00
Support Expiration	2020-12-17 01:00:00
Customer	Verint Verba Customer

License Items

Name	Code	Quantity	Valid From	Expiration	Value
Verba Enterprise Server License	VR3-SR-ENT-L	4		Never	
Verba Recording Server License	VR3-SR-RS-L	10		Never	

The list box shows the clients' hostname (or the Verba Cluster ID in case of multiple MRs), and the last date the client sent its license usage.

Technical Information

- The settings are stored in JSON format on the hard drive in Verba\settings\license-rls.json
- Modifications to the settings file become effective immediately
- Local and remote license usages are stored in the SQL database within the RLS cluster
- The RLS does the daily license check one hour later than the other daily jobs to ensure that the clients have already sent the usage

- If a client sends the usage after the RLS already did the license check, then the RLS will perform the license check again

Cisco Video on Hold and Video in Queue

VoH/ViQ overview

A built-in capability of the Verint Verba platform, the Verba Cisco Announcement service can act as a Video On Hold server and provides Video on Hold (VoH) and Video in Queue (ViQ) in Cisco environments. This is a replacement option for the corresponding feature in the discontinued Cisco Mediasense product line.

Both for VoH and ViQ Verba does the following:


- Verba service listens on SIP, it is connected to CUCM via a SIP trunk
- Video call is routed to Verba then the service looks up media resource - directory number (DN) association and determines video clip to be played back
- After call is established and media negotiated the service starts streaming the video clip to the user endpoint

VoH and ViQ can be used both standalone or as part of a Verint Verba ethical wall or recording deployment.

Load-balancing and failover are available using CUCM route group/list configuration. It does not provide mid-call, only next-call failover.

The following tools are provided for configuration:

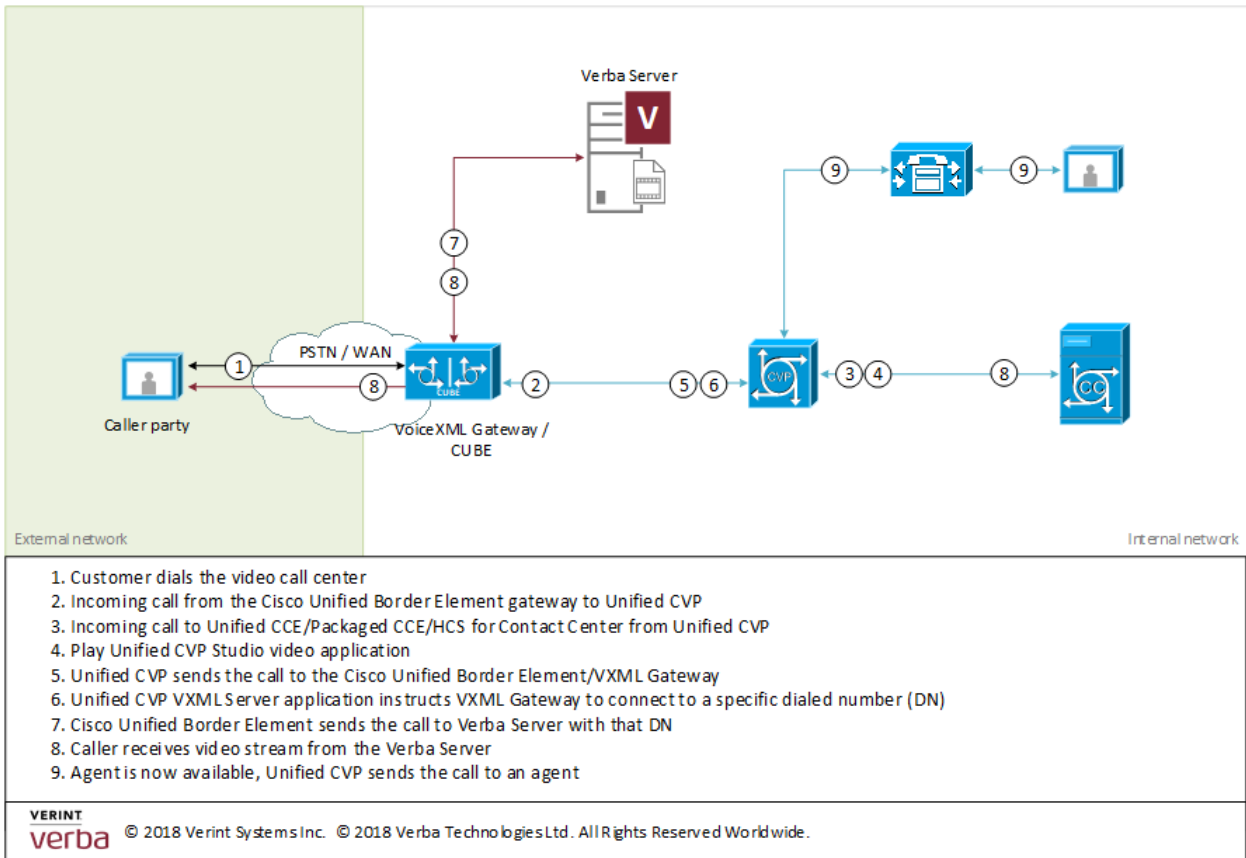
- A desktop application is provided to MP4 files to streaming-optimized format.
- Central video file and inbound DN management via the web interface

 VoH/ViQ requires a separate feature license. Please contact sales for more information.

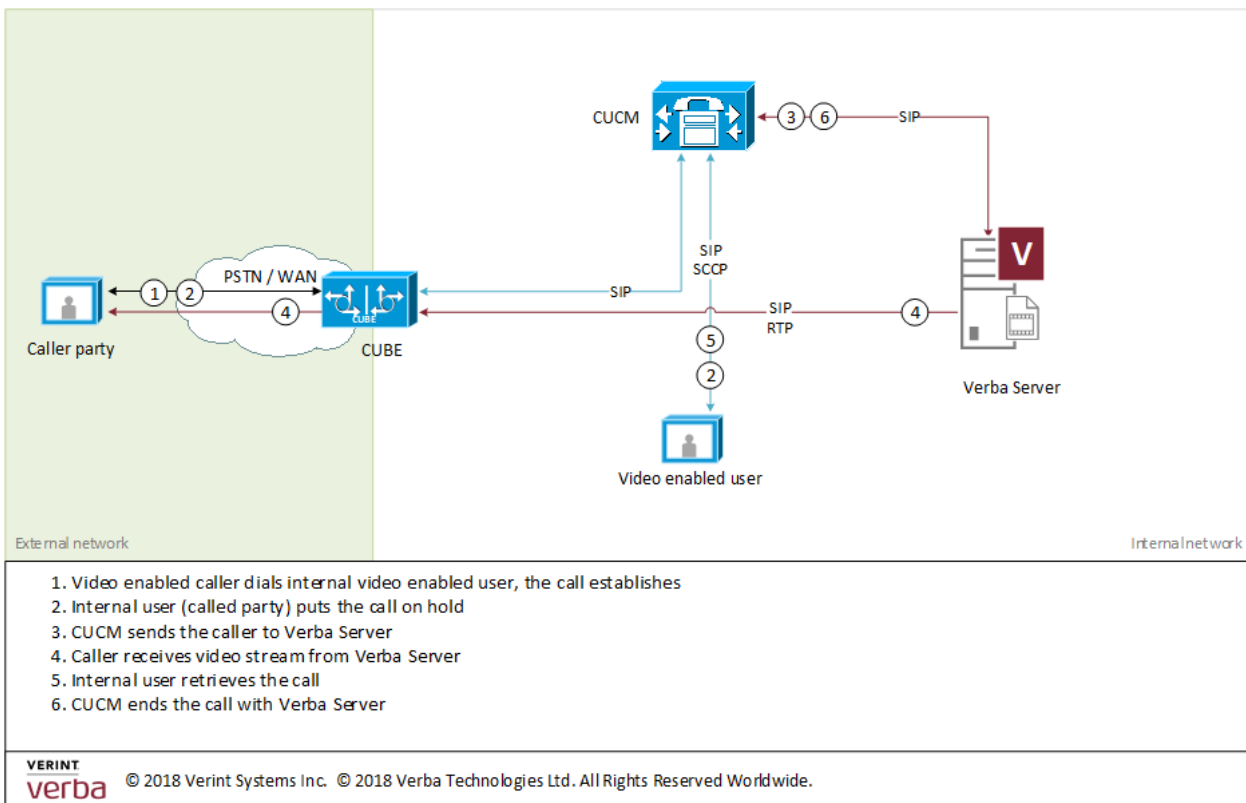
Understanding VoH/ViQ call flows

The following diagrams explain the related call flows.

Cisco ViQ Call Flow



Cisco VoH Call Flow



Configuring VoH/ViQ

Setting up this feature consist of the following steps:

1. [Create a SIP trunk between Cisco platform and Verba](#)
2. [Convert MP4 video clips to streaming optimized Verba format with the provided utility](#)
3. [Upload media files and distribute between Verba nodes](#)
4. [Create "Incoming call rules" for VoH/ViQ which defines the directory number - video clip matching](#)

Use the following Cisco documentation to configure VoH/ViQ on the Cisco side:

- VoH: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/12_0_1/systemConfig/cucm_b_system-configuration-guide-1201/cucm_b_system-configuration-guide-1201_chapter_0111110.html#CUCM_TK_CB007239_00
- ViQ: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/remote_expert_mobile/remote_expert_mobile_1061/configuration/guide/RCCT_BK_C58889DD_00_cisco-remobile-solution-configuration/RCCT_BK_C58889DD_00_cisco-remote-expert-mobile-standard_chapter_0100.pdf

Command line converter for VoH and ViQ

For streaming media is not generated real-time as it would heavily reduce the number of concurrent sessions the service would be able to serve, rather the to be streamed content is pre-generated and stored in Verba proprietary media format.

The `vmfconverter.exe` command line tool shipped with Verba is the conversion tool to generate the streaming optimized media files from any standard MP4 video clips.

It generates the following streams from which the most desired one is selected by the streaming service at call setup based on capabilities of remote video endpoints/phones and available bandwidth advertised:


Video:

- H.264 1080p - 4 mbps
- H.264 720p - 2.5 mbps
- H.264 720p - 1.5 mbps
- H.264 288p - 512 kbps
- H.264 288p - 256 kbps

Audio

- Opus 48 KHz stereo
- G.722.1 32 KHz
- G.722
- G.711 u/a
- G.729

Video streams will be generated only for those resolutions from the above list which are less or equal of the input video stream's resolution, ie. if a 720p MP4 file is converted then 1080p video stream will not be generated.

 Processing video files is highly CPU and disk intensive task, running it on any production Verba node might overload the server and interfere with other Verba services. It is recommended to run the tool either on Media Repository or non-Verba PC.

The tool can be started on any Windows 7/Windows 2008R2 or newer machine by copying `verba_install\bin\vmfconverter.exe` and `libsiren.dll`

The tool has the following cmd syntax:

```
vmfconverter.exe input.mp4 output.vmf (where input/output is either a full or relative path of th
```

During processing the tool provides progress information and estimated time to finish processing.


```
c:\Program Files\Verba\bin>vmfconverter.exe "f:\example.mp4" "f:\example.vmf"
Converting f:\example.mp4->f:\example.vmf
MP4_PLAYER: creating MP4 player for file: f:\example.mp4
Current position: 5 s, total length: 61 s, 8% ready, ETA: 223 s
Current position: 10 s, total length: 61 s, 16% ready, ETA: 216 s
Current position: 15 s, total length: 61 s, 24% ready, ETA: 202 s
Current position: 20 s, total length: 61 s, 32% ready, ETA: 182 s
Current position: 25 s, total length: 61 s, 40% ready, ETA: 162 s
Current position: 30 s, total length: 61 s, 49% ready, ETA: 142 s
Current position: 35 s, total length: 61 s, 57% ready, ETA: 119 s
Current position: 40 s, total length: 61 s, 65% ready, ETA: 97 s
Current position: 45 s, total length: 61 s, 73% ready, ETA: 73 s
Current position: 50 s, total length: 61 s, 81% ready, ETA: 51 s
Current position: 55 s, total length: 61 s, 90% ready, ETA: 27 s
Current position: 60 s, total length: 61 s, 98% ready, ETA: 4 s
Current position: 61 s, total length: 61 s, 100% ready, ETA: 0 s
Conversion finished
```

- ⓘ Please note due to many resolutions and bitrates of video streams the processing of media is quite slow. It is ~1/4-1/10 of real-time, which means processing 60-second video might take 600 seconds or more depending on hardware, number of available CPU cores

Configuring VoH and ViQ call rules

Configuration checklist

Step 1 - Enable VoH/ViQ feature on the UI. This can be set by Web Application\Miscellaneous\VoH/ViQ enabled option. Changing this will prompt a web application restart


Step 2 - Generate streaming files (.vmf) from MP4 clips (more info [here](#))


Step 3 - Upload and distribute files across Verba nodes including Cisco Announcement service

It can be done under System\Voh/ViQ\Media Files menu:

Find and List Media File

[Add New Media File](#)

 Your email monitoring settings have changed. Email verification is required. [Send me a verification email.](#)

 VoH/ViQ configuration should be applied on recording servers.
If you would like to apply the configuration now, please [click here](#).

File Name begins with

File Name	Description	Size	Duration	Originally Uploaded To
Video-In-Queue-Clip1.vmf	Video-In-Queue Clip 1	31 MB	00:34	PETER-PC.doddiscombsleigh.wastedtechnologies.co.uk
Video-In-Queue-Clip2.vmf	Video In Queue Clip 2	31 MB	00:34	PETER-PC.doddiscombsleigh.wastedtechnologies.co.uk
Video-On-Hold-Clip1.vmf	Video On Hold Clip 1	31 MB	00:34	PETER-PC.doddiscombsleigh.wastedtechnologies.co.uk
Video-On-Hold-Clip2.vmf	Video On Hold Clip 2	31 MB	00:34	PETER-PC.doddiscombsleigh.wastedtechnologies.co.uk

4 items found, displaying all items.

Export options: [Excel](#) | [RTF](#) | [PDF](#)

Media File Configuration

[Add New Media File](#)
[Back to Previous Page](#)

File Name Video-In-Queue-Clip1.vmf

Description

Video-In-Queue Clip 1

Size 31 MB

Duration 00:34

Originally Uploaded To PETER-PC.doddiscombsleigh.wastedtechnologies.co.uk

Replace File No file chosen

Creation Date: Jan 19, 2018 11:56:40 AM
Created By: Verba Administrator (Administrator)
Last Modification Date:
Last Modified By:
[View Change History](#)


* Indicates required item.


Step 4 - Create call rule to map video clip to directory number

It can be done under System\Voh/ViQ\Incoming Call Rules menu:

Find and List Incoming Call Rule

[Add New Incoming Call Rule](#)

 Your email monitoring settings have changed. Email verification is required. [Send me a verification email.](#)

 VoH/ViQ configuration should be applied on recording servers. If you would like to apply the configuration now, please [click here.](#)

Address begins with

Address	Media File	Action
3000	Video-In-Queue-Clip1.vmf	Once
3001	Video-In-Queue-Clip2.vmf	Continuously
3003	Video-On-Hold-Clip1.vmf	Continuously
3004	Video-On-Hold-Clip2.vmf	Continuously

4 items found, displaying all items.

Export options: [Excel](#) | [RTF](#) | [PDF](#)

Incoming Call Rule Configuration

[Add New Incoming Call Rule](#)
[Back to Previous Page](#)

Address *

Action *

Media File *

* Indicates required item.

The call rule defines:

- Address (incoming number): should be the same as VOH server's "Default Video Content Identifier", this is based on which Verba can associate video clip to VOH server
- Action: Once - if video clip ends Verba terminates the call, continuous - repeat video clip playback till caller terminates
- Media file: select video clip to be associated to the address from the uploaded clips

Step 5 - Apply configuration changes by clicking on the appearing banner (see the above screenshot). Depending on changes it will:

- Download media files on Verba servers running Announcement service
- Refresh services' configuration with changes in clip - incoming number association

SIP integration for VoH and ViQ

Configuration checklist for UCM

Step 1 - [Create SIP trunk](#)

Step 2 - Create Video On Hold Server (Media Resources\Video On Hold Server)

Video On Hold Server

Save Delete

Video on Hold Server

Name*

Description

Default Video Content Identifier*

SIP Trunk*

- Default Video Content Identifier should be a number which on Verba side is assigned to a video clip. See this configuration later.
- SIP Trunk is either a trunk list or trunk selected from the available trunks, pointing to Verba Cisco Announcement service

Step 3 - Assign Video On Hold to a Media Resource Group / Media Resource Group List

Media Resource Group Status

Media Resource Group: MRG_VOH (used by 255 devices)

Media Resource Group Information

Name*

Description

Devices for this Group

Available Media Resources**

- ANN_2
- ANN_3
- IVR_2
- IVR_3
- MOH_2

Selected Media Resources*

- CFB_2 (CFB)
- CFB_3 (CFB)
- MTP_2 (MTP)
- MTP_3 (MTP)
- VOH Test (VOH)

Use Multi-cast for MOH Audio (If at least one multi-cast MOH resource is available)

Step 4 - Assign the Media Resource Group List containing MRG/VOH to the desired devices either via Device Pool\Media Resource Group List or Device\Media Resource Group List

Please note if hold is initiated on voice only call then still the Verba service will provide MOH for these devices streaming the voice /audio part of the clips

Step 5 - For testing purpose, a route pattern might be set for the same number as provisioned in VOH server config. Calling this number the routing to trunk and streaming can be tested from the video endpoints

Step 6 - Check CAC and Codec Region settings to ensure video bitrate is configured properly between Verba trunk region and other regions

Configuration checklist for Verba

Step 1 - Activate Verba Cisco Announcement service. For full configuration reference click [here](#)

Step 2 - Create SIP port to terminate trunk from CUCM

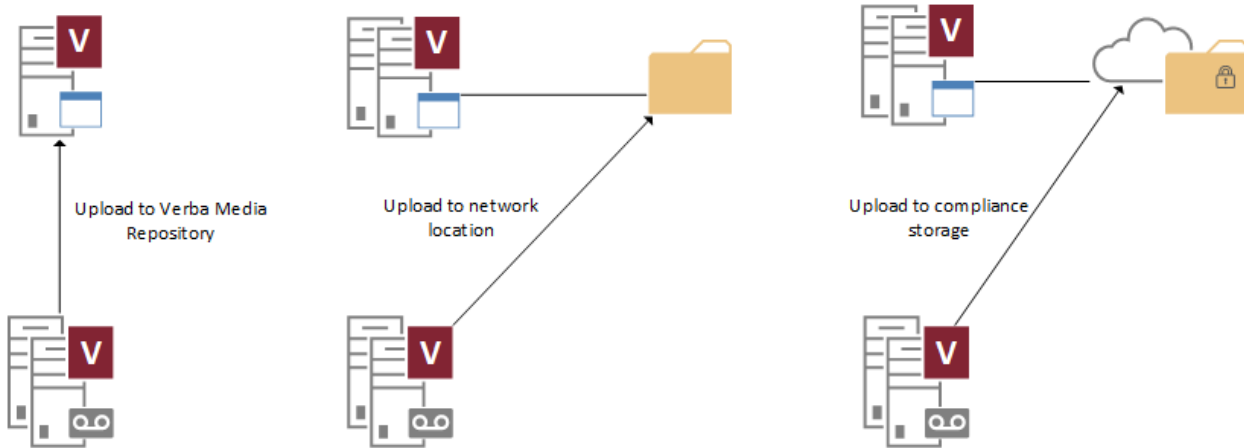
The screenshot displays the configuration interface for Verba. On the left, the 'Server Configuration' section is expanded to show 'Cisco Recording Announcement' settings. These include: CURRI Listening Port (checkbox, 10205), CURRI TLS Certificate (checkbox, empty), CURRI TLS Key (checkbox, empty), CURRI TLS Key Password (checkbox, empty), RTP Port Range Start (checkbox, 16384), RTP Port Range End (checkbox, 65535), and SIP Ports (checkbox, empty with a '+' icon). On the right, the 'Secure SIP Ports' section is visible, containing: Port (5061), SSL/TLS Certificate (c:\verba_cucm.crt), SSL/TLS Key (c:\verba_cucm.key), SSL/TLS Key Password (masked with dots), and SSL/TLS Trust List (empty).

- With SIP Ports + icon add a new port
- Fill SIP port (port on which service listens). On CUCM as trunk destination this address should be configured, see Step 1 CUCM side configuration
- If secure trunk is configured set the SSL/TLS certificate to use with this port.
 - The certificate can be either a local PEM/PFX file (in this case file path and key password should be filled) or certificate stored in Windows Certificate Store Local Computer\Personal folder (in this case the certificate's thumbprint should be provided and key should be exportable and available)
 - If mutual authentication is desired set Trust list based on which Verba can validate incoming SIP connections. The setting can be:
 - empty: no validation on Verba side
 - thumbprint: either self-signed certificate with the thumbprint or CA-signed certificate where CA certificate matches the thumbprint is accepted
 - *: use windows top-level CA store
 - PEM file path: the file should contain certificate chain for CUCM

Step 3 - Start the service and reset the trunk on CUCM side

Configuring media file upload

The recorded media has to be uploaded from the Recorder Servers to a central location. This central location can be a Verba Media Repository Server, a Combo Server, a network location or other compliance storages supported by Verba. Based on the settings non-policy based and policy based upload can be configured. When multiple Media Repositories used then it's recommended to use network location or policy based upload.



Non-policy based upload

Non-policy based upload is the default setting of the Verba Recorder Servers. In order to configure a Media Repository or a network location for a target, do the following steps:

Step 1 - Open the Verba Web interface, go to **System > Servers**, and select your Recording server (or Desktop Recorder).

Step 2 - Click on the **Change Configuration Settings** tab and in the configuration tree go to **Storage Management > Upload** node.

Step 3 - If you want to use a **Media Repository local disk** to store the media files then set the **Upload Target** setting to **Media Repository Local Disk** (default). If you want to use a network location then set it to **Network Storage**.

Step 4/a - If you previously chose **Media Repository Local Disk** then provide the Media Repository server hostname or IP address at the **Storage Management > Storage Targets > Media Repository Local Disk > Media Repository IP Address or Hostname** setting.

Step 4/b - If you previously chose **Network Storage** then provide the UNC path to the network location at the **Storage Management > Storage Targets > Network Storage > UNC Path** setting.

! In case of Desktop Agents, the files have to be uploaded to the default media folder of the Media Repository (or Single) Server. (MR configuration \ Directories \ Media Folder)

i Using Network Locations

When network location is used then it's important to note some requirements:


- The service user of the Verba Storage Management services on all Verba servers needs full control privilege with special permissions to the location
- The service user of the Verba Web Application and the Verba Media Utility services on the Verba Media Repository server (s) needs full control privilege with special permissions to the location

- The network location has to be configured as **Media Folder** at the Verba Media Repository. This setting can be located in the server configuration under the **Directories**.

Step 5 - Save the configuration then **repeat** these steps for each Recording Server in your system. Finally, execute the changes.

Policy-based upload

In order to configure the policy based upload please see [Upload policy](#).

 Policy-based upload is not supported by the Verba Desktop Agent.

Configuring DTMF control and recording

Passive and SIPREC based recording services support the following DTMF specific features for RFC 2833 DTMF:

- On demand call keeping by feature access code
- Marker addition by feature access code
- Recording of DTMF sequences as Verba call markers

Active feature and specify FACs

Server Configuration	
▲ Common Configuration	
▶ System Settings	
▶ Recording Settings	
▶ Database Connection Configuration	
▶ Directories	
▲ DTMF Configuration	
▲ Control via DTMF	
Feature enabled:	<input checked="" type="checkbox"/> Yes
Add marker point sequence:	<input type="checkbox"/> *2
Begin a marker sequence:	<input type="checkbox"/> *3
End a marker sequence:	<input type="checkbox"/> *4
Keep ondemand call sequence:	<input type="checkbox"/> *1
▲ Recording	
Record DTMF:	<input checked="" type="checkbox"/> Yes
DTMF grouping timeout (sec):	<input type="checkbox"/> 2

Step 1 - Navigate to the **Administration / Verba Servers** menu item and select the corresponding server from the list.

Step 2 - Go to the **Change Configuration Settings** tab in the Verba Server management screen.

Step 3 - Enable feature, and set feature access codes:

- **Add marker point:** adds a zero length marker
- **Begin a marker:** starts a new marker, implicitly closes previous open.
- **End a marker:** ends an open marker, so call segments can be marked
- **Keep ondemand call:** records on demand call
- **DTMF grouping timeout:** timeout till recorder is looking for DTMF chars to put in the same marker

Configuring Phone-based Silent Monitoring

Verba provides an option for configuring phone-based silent monitoring for Skype for Business / Lync or for Cisco. In case of Cisco, it's done without the use of the JTAPI connection or the Built-in Bridge. This feature can use in cases like:

- When the web-based silent monitoring is not available
- When the phone device doesn't have Built-in Bridge (Cisco passive recording)
- There is no JTAPI connection (Cisco)

Prerequisites

Before the Verba side configuration, a trunk has to be configured at the PBX side. For the configuration steps, see: [Configuring Cisco UCM for dial-in recording](#), [Configuring Microsoft Lync for dial-in recording](#)

Configuration Verba for Phone-based Silent Monitoring

Step 1 - In the Verba Web Interface go to **System > Servers** menu.

Step 2 - Select your **Recording (or Single) Server** where the recorder service runs. In case of Skype for Business / Lync, this is the Verba Passive Recorder service. In case of Cisco, this is the Verba Unified Call Recorder or the Verba Passive Recorder service. Click on the **Service Activation** tab.

Step 3 - Activate the **Verba Dial-in Recorder Service** by clicking on the



icon.

Step 4 - Click on the **Change Configuration Settings** tab.

Step 5 - Expand the **Dial-in Recorder** node.

Step 6 - Under the **SIP** node, set the **SIP User** setting. Provide a SIP user in the following format: "sip:num/user@pbx_domain/ip". If required, provide the **SIP User Password**.

▾ Dial-in Recorder

▶ Lines

▾ SIP

Call timeout in sec:	<input type="checkbox"/>	30
RTCP support:	<input type="checkbox"/>	No ▼
SIP r-port support:	<input type="checkbox"/>	No ▼
Force duplex streams:	<input type="checkbox"/>	Yes ▼
SIP User:	<input checked="" type="checkbox"/>	sip:5000@testsfpool.local
SIP User Password:	<input type="checkbox"/>	
Recorder Display Name:	<input type="checkbox"/>	Verba Recorder
Register as client:	<input type="checkbox"/>	No ▼
RTP port range begin:	<input type="checkbox"/>	16384
RTP port range end:	<input type="checkbox"/>	65535
SIP Signaling Transport:	<input type="checkbox"/>	TCP ▼
Local SIP port:	<input type="checkbox"/>	5065
Service URI:	<input type="checkbox"/>	
SIP TLS Certificate:	<input type="checkbox"/>	
SIP TLS Key:	<input type="checkbox"/>	
SIP TLS Key Password:	<input type="checkbox"/>	
SIP TLS Trust List:	<input type="checkbox"/>	

▶ Recording

▶ Recording Control


▶ Advanced

Step 7 - Save the changes by clicking on the



icon.

Step 8 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

 There are tasks to be executed regarding the configuration of this Verba Server.
If you would like to execute these tasks now, please [click here](#) .

Step 9 - Click on the **Service Control** tab.

Step 10 - Start the **Verba Dial-in Recorder Service** by clicking on the



icon.

Enabling the Phone-based Silent Monitoring

Step 1 - In the Verba Web Interface go to **System > Servers > Select your Media Repository (or Single) Server > Click on the Change Configuration Settings** tab.

Step 2 - Expand the **Web Application > Miscellaneous** node.

Step 3 - Set the **Silent Monitoring of Recorded Calls** setting either to **Make Phone Call or Allow Both**.

Step 4 - Save the changes by clicking on the



icon.

Step 5 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.



There are tasks to be executed regarding the configuration of this Verba Server.
If you would like to execute these tasks now, please [click here](#) .

Configuring SMS Recording

Configuring the Verba SMS Recorder service

Step 1 - In the Verba Web Interface go to **System > Servers > Select your Recording (or Single) Server > Click on the Service Activation** tab.

Step 2 - Activate the **Verba SMS Recorder Service** by clicking on the



icon.

Step 3 - Click on the **Change Configuration Settings** tab.

Step 4 - Expand the **SMS Recorder** node.

Step 5 - Set the **Internal Domain, Numbers Pattern** setting. This has to be a regex which matches to all internal numbers.

Step 6 - At the **SMPP Connections** setting, click on the



icon to add a new connection.

Step 7 - In the left panel, provide the **SMS-C Host** and the **SMS-C Port** settings.

Step 8 - Provide the credentials in the **System ID** and **Password** settings.

Step 9 - Select the **SMPP version**.

Smpp connection	
ESME outbind port (leave empty if outbind is not supported)	<input type="text"/>
TLS Certificate	<input type="text"/>
TLS Key file	<input type="text"/>
TLS Key file password	<input type="text"/>
TLS trust list	<input type="text"/>
SMS-C host	<input type="text" value="sms.contoso.com"/>
SMS-C port	<input type="text" value="2775"/>
System ID	<input type="text" value="johndoe"/>
System Type	<input type="text"/>
Password	<input type="password" value="*****"/>
SMPP version	<input type="text" value="3.4"/>

Step 10 - Click on the **Save** button.



Secure Connection

If secure connection is required, the following settings have to be set:

TLS Certificate: The thumbprint of the Verba server certificate being used for the connection.

TLS Trust List: The thumbprint of the remote server certificate, or the thumbprint of the CA certificate which issued the remote server certificate. Alternatively, "*" can be used. In this case, every certificate going to be trusted, whose CA certificate can be found in under the Trusted Root Certificate Authorities folder. If left empty, every certificate going to be trusted.

Alternatively, .crt/.cer and .key files can be used. In this case, UNC paths can be provided in the STLS Certificate and the TLS Key file settings, and the TLS Key file password has to be provided.

SMS Recorder


Write XML Metadata:	<input type="checkbox"/>	No
Internal Domain, Numbers Pattern:	<input checked="" type="checkbox"/>	+441234567\d{3}
SMPP Connections:	<input checked="" type="checkbox"/>	Ogrvt40fRps= sms.contoso.com 2775 johndoe 1vcYm2yq7Fr5WuO3yi9oQQ== 3.4
<input type="button" value="+"/>		

Step 11 - Save the changes by clicking on the



icon.

Step 12 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

 **There are tasks to be executed regarding the configuration of this Verba Server.**
If you would like to execute these tasks now, please [click here](#) .

Step 13 - Click on the **Service Control** tab.

Step 14 - Start the **Verba SMS Recorder Service** by clicking on the



icon.

Configure extensions

After finalizing the configuration of the recording services, make sure you have added the extensions you want to record to the Verba extension list. This can be done manually ([Extension list](#)) or using [Active Directory Synchronization](#).

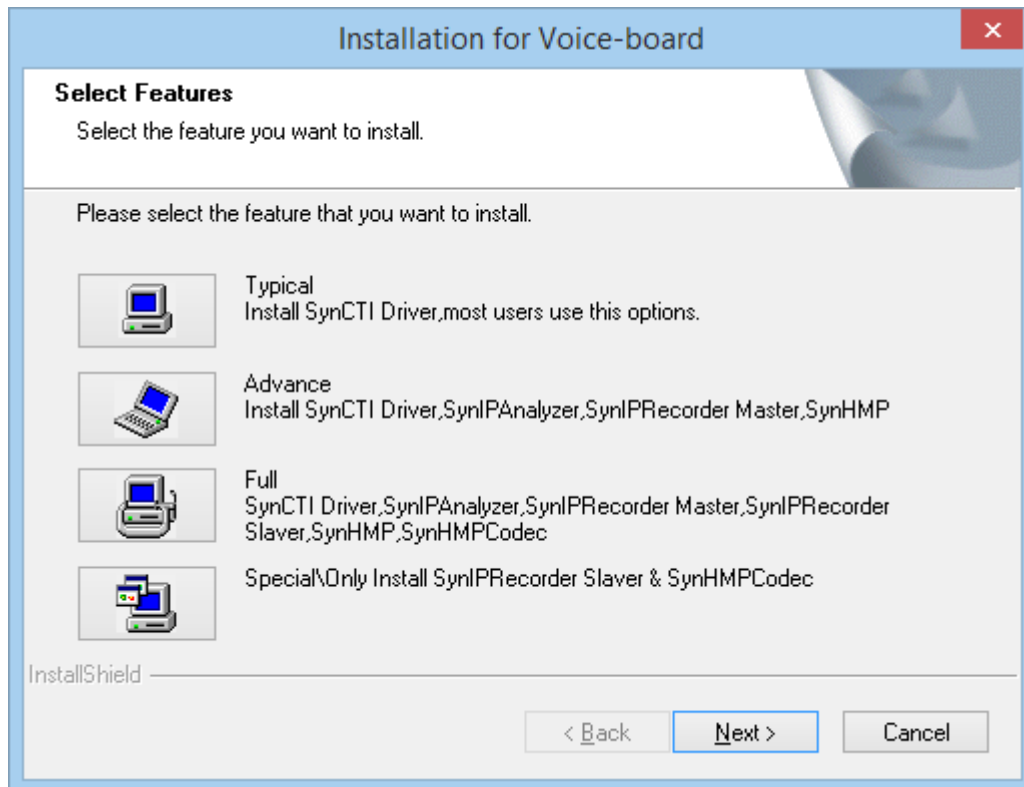
Configuring Synway Analog Tap Card recording

Installing the Analog Tap Passive Board

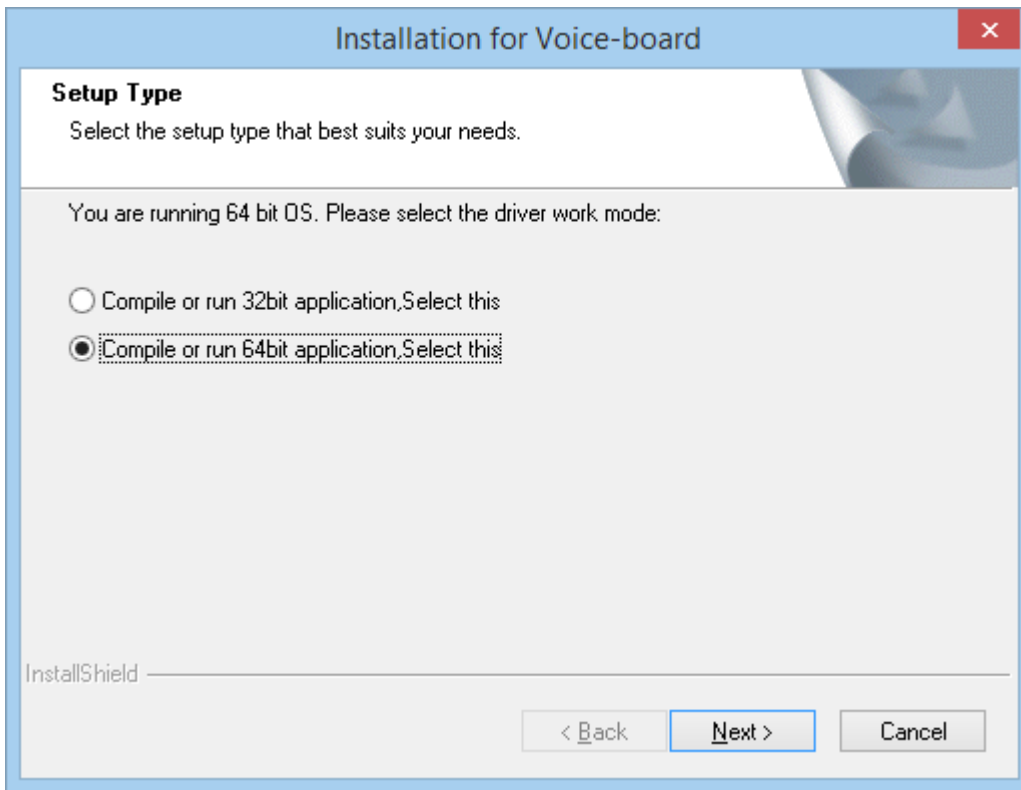
After you plugged in the ATP board to the computer, you have to install the corresponding driver.

Synway driver download link: [http://www.synway.net/Download/Driver/Windows/shcti5430/SYNWAY_PCI\(USB\)_5430_EN.exe](http://www.synway.net/Download/Driver/Windows/shcti5430/SYNWAY_PCI(USB)_5430_EN.exe)

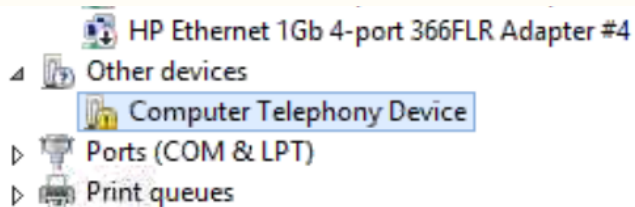
Step 1 - After starting the installer, select **Typical**



Step 2 - Please make sure that you install the 64 bit version of the driver for v9.x or later, and the 32 bit driver for Verba 8.x or earlier



⚠ Alternative Synway Driver
If after installing the previous driver you get an unknown "Computer Telephony Device", please uninstall the previous driver then download and install [this driver](#).



Your card now should be recognized properly.

For more information, see the Synway board installation manual: http://www.synway.net/Download/Manual/HardwareManual/Rec_ATP006.pdf

Configuring Verba for Synway ATP recording

If you installed the ATP card, you have to configure the **Verba Analogue and Radio Recorder Service (Verba General Media Recorder Service)** in the older versions of Verba.:

Step 1 - Create a new recordingchannels.xml file in the C:\Program Files (x86)\Verba\setting folder. You can download the sample from [here](#).

Step 2 - To configure a channel for recording, add the following lines:

```
<Channel type="analog" id="" eid="">
  <Device id="" name="" tapPort="" continuousRecord=""/>
</Channel>
```

Step 3 - Fill in the properties of the channels and save the file.

Attribute	Description
Channel	
type	analog/voip: for Synway ATP recording use the "analog" value.
id	It can be a random string, you have to change it every configuration change in the channel.
eid	4char: Optional. For multi-tenant system this attribute shows the tenant id of the channel.
Device	
id	The phone number of the agent.
name	The name of the agent.
tapPort	The tap port number where the line is plugged in.
continuousRecord	true/false: For continuous recording set it to "true". For onhook-offhook based recording set it to "false". NOTE: It only works with normal analog PSTN lines.

Example:

```
<?xml version="1.0" encoding="utf-8"?>
<Channels>
  <Channel type="analog" id="analog_000" eid="">
    <Device id="+12013550400" name="Jack Hoffman" tapPort="0" continuousRecord="false"
  </Channel>
  <Channel type="analog" id="analog_001" eid="">
    <Device id="+12017254926" name="Will Smith" tapPort="1" continuousRecord="false"/
  </Channel>
</Channels>
```

Step 4 - Log in to Verba and go to the **System \ Servers**, select your server, click on the **Service Activation** Tab, and activate the **Verba Analogue and Radio Recorder Service** by clicking on the



icon.

Step 5 - After activating the service click on the **Change Configuration Settings** Tab and scroll to the service's node and enter the path of the ShConfig.ini file:

- ▲ Analogue and Radio Recorder
 - ▶ Recording
 - ▶ VoIP channels
 - ▲ Analog channels

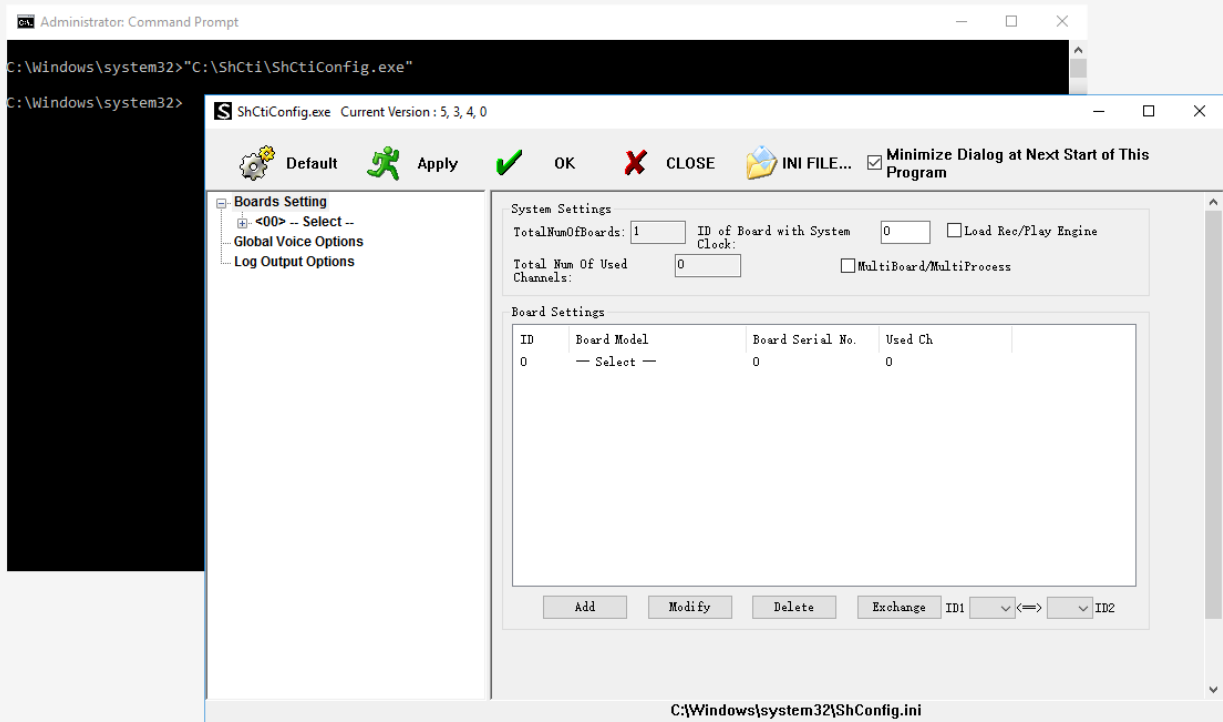
Synway device config: C:\ShCtl\ShConfig.ini
 - ▶ Advanced

✔ ShConfig.ini

The default path is: C:\ShCti\ShConfig.ini

To make sure that the ShConfig.ini contains the correct driver information please run the C:\ShCti\Test.exe

If you encounter issues with the Test.exe application, please run the C:\ShCti\ShCtiConfig.exe as administrator and click on the Default then on the Apply buttons: (It's possible that you have to do this multiple times to force the changes to be written to the file)




Step 6 - Save the changes by clicking on the



icon.

Step 7 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

 There are tasks to be executed regarding the configuration of this Verba Server.
If you would like to execute these tasks now, please [click here](#) .

Spet 8 - Click on the **Service Control** tab, and start the **Verba Analogue and Radio Recorder Service** by clicking on the



icon.

Configuring the Desktop Agent

- [Overview](#)
- [Prerequisites](#)
- [Configure the Desktop Recorder Configuration Profile](#)
- [Configuring new Desktop Agent installations](#)
- [Deploying multiple Verba Desktop Agents](#)
- [Starting the Verba Screen Capture Multiplexer Service](#)
- [Configure extensions](#)

Overview

The Desktop Agent enables several advanced features:

- Agent View: a supervisor feature to monitor agent screen activity in real time using the web interface
- Recording pop-up: the agents can control various aspects of the recording using the popup toolbar
- Screen recording: while recording the agent phone call, the Desktop Agent can capture the screen of the agent desktop computer
- Auto-pause for PCI DSS: the Agent Desktop application can detect if the agent navigates to configured web sites or starts using a specific application, and automatically pause the recording to avoid capturing sensitive data

Prerequisites

The Agent Desktop application can only be installed in Windows desktop operating systems.

Most of the Verba Desktop Agent functionalities relies on the Voice recording. For the Voice recording configuration see **Step 3** at this article: [Configure](#)

The Agent View feature requires the **hostname of the desktop PCs** to be **resolvable** from the Media Repository server.

The **Windows user name of the users have to match to the Verba user ID**. The user's extensions have to be associated to the Verba user.

For the installation steps of the Verba Desktop Agent see: [Installing the Verba Desktop Agent](#)

If the desktop screen recording is required then the **Media Foundation (Windows Server 2012 or newer) / Desktop Experience (Windows Server 2008 R2)** feature have to enabled on the Media Repository server where the Desktop Agent uploads the recordings to.

The auto-pause feature only supports:

- Chrome,
- FireFox,
- Internet Explorer,
- Edge (from v9.7.2),
- and Opera (from v9.7.2) browsers.

Configure the Desktop Recorder Configuration Profile

Since in most cases, multiple Desktop Agents are installed, and all of them needs the same configuration, the Desktop Agent should be configured at **profile level**.

Step 1 - In the Verba web interface go to **System \ Configuration Profiles** then select the **Default Desktop Recorder Configuration Profile**.

Step 2 - Click on the **Change Configuration Settings** tab. Expand the **Desktop Agent** section.

Step 3 - Under the **Basics** section provide the Recording Server hostnames with the correct port (**HOSTNAME:PORT**) at the **Recording Service(s)** setting. If there are multiple Recording Servers then they can be separated by comma.

The ports for the different recording services are:

Verba Passive Recorder Service (SfB/Lync, Passive): 10000

Verba Unified Recorder Service (Cisco, IPTrade, Speakerbus, Avaya, SIP): 10031

Verba Cisco Central Recorder Service (Cisco legacy): 10003

Step 4 - Under the **Verba Connection** section provide the Verba Web Interface URL at the **MR HTTP API Server URL** setting.

The screenshot shows the configuration interface for the Desktop Agent, divided into two sections: Basics and Verba connection.

Basics section:

- Enable Call Muting: Yes
- Enable Call Popups: Yes
- Enable Silent Monitoring: No
- Blank Screen During Pause: Yes
- Recording Service(s): testrs1:10000,testrs2:10000
- Disable Tray Icon: (dropdown menu)

Verba connection section:

- Connect to MR via HTTP: Yes
- MR HTTP API Server URL: http://testmr1/verba/
- API User: verbadesktopapi
- API Password: (masked with dots)

Step 5 (Optional, only for Screen Recording) - Under the **Storage Management** section. For more information see [Configure media file upload](#)

Step 6 (Optional, only for Agent View) - Under the **Basics** section set the **Enable Silent Monitoring** setting to **Yes**.

Step 7 (Optional, only for PCI DSS) - Under the **Auto-Pause** section web URLs and Windows controls can be configured.

Auto-Pause can be configured based on web URLs and Windows controls. When web URLs configured, the Desktop Agent going to stop the recording when the URL opened in a web browser. When a Windows control configured, the Desktop Agent going to stop the recording when the focus is on the specified control.

For the web **URL based** auto-pausing specify the URLs at the **Auto-Pause Recording on URL** setting. This option only works when the browsers emit specific Windows events which are recognized by the application.

The application currently supports:

- Chrome,
- FireFox,

- Internet Explorer,
- Edge (from v9.7.2),
- and Opera (from v9.7.2) browsers.

It works with **partial match** using regular expressions. This is much more flexible than simple matching, but care must be taken not to type something that is not meant. For example "facebook.com" as a regular expression will match on anything that has in it the word "facebook" followed by **any** character and the word "com", as the "." has a special meaning. "facebook.com", "facebookocom", "facebookxcom" would all match on the expression. In this example the correct way would be to escape the "." character with a backslash signifying that the "." no longer means "any character", but a simple ".". In conclusion the correct input to mute on "facebook.com" would be "facebook\\.com". To make sure the expression used is correct use this online tool for testing called [RegExr](#).

For the **Windows control based** auto-pausing specify controls at the **Controls to be Discarded in Focus** setting. The format is: process_name|parent_class|parent_id|parent_caption|control_class|control_id|control_caption|mute_voice. The process_name and mute_voice (0/1) parameters are mandatory. For example NOTEPAD.EXE|||||Notepad|1 for not recording when the notepad is started. Properties can be checked by Spy++ or WinSpy++ tools.

Desktop Agent

- Basics
- Verba Connection
- Dictation
- Auto-Pause

Auto-Pause Recording on URL:	facebook\\.com
Controls to be Discarded in Focus:	NOTEPAD.EXE Notepad 1
Allow User Resume During Auto-Pause:	Yes

Step 9 - If there are already installed Desktop Agents, then a notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.**Step 8** - Save the changes by clickin on the



icon.

! There are tasks to be executed regarding the configuration of this Verba Server. If you would like to execute these tasks now, please [click here](#) .

Configuring new Desktop Agent installations

The configuration is have to be sent down to the new Desktop Agent installations. The following steps describes how to apply the configuration on the new agents:

Step 1 - In the Verba Web Interface go to **Administration > Verba Servers** menu.


Step 2A (if the Desktop Agent doesn't have database access) - If the Desktop Agents don't have databse access, then they have to be added to the server list manually.

Click on the **Add New Verba Server** link. Provide the hosname at the **Hostname** setting, set the **Role** to **Desktop Recorder**, set the **Configuration Profile** then click **Save**.

Step 2B (if the Desktop Agent have database access) - Select the PC from the list.


Step 3 - Go to the **Change Configuration Settings** tab.


Step 4 - Select **Use configuration only from the central database**, then click **Start**.

 Configuration differences were found between the central database and the server's local configuration. Please decide how to resolve these differences.

- Use central database configuration in case of profile values, otherwise use the server's local configuration (recommended)
- Use configuration only from central database
- Use configuration only from server's local registry

Step 5 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

 Changes can be execute at once at the end. In that case don't forget to click on **'Check All'**.

 There are tasks to be executed regarding the configuration of this Verba Server. If you would like to execute these tasks now, please [click here](#) .

Deploying multiple Verba Desktop Agents

It is also possible to deploy multiple Verba Desktop Agents using pre-created configuration. For the details, see: [Deploying Multiple Verba Desktop Agents](#)

Starting the Verba Screen Capture Multiplexer Service

If the desktop screen recording is required then the recorded video files have to be multiplexed with the recorded audio files. This is done by the Verba Screen Capture Multiplexer Service on the Media Repository (or Single) Server. The **Media Foundation (Windows Server 2012 or newer) / Desktop Experience (Windows Server 2008 R2)** feature have to enabled on the server.

Step 1 - In the Verba web interface go to **Administration > Verba Servers > Select your Media Repository (or Single) Server > Click on the Service Activation** tab.

Step 2 - Activate the **Verba Screen Capture Multiplexer Service** by clicking on the



icon.

Step 3 - Click on the **Service Control tab** tab.

Step 4 - Start the **Verba Screen Capture Multiplexer Service** by clicking on the



icon.

Configure extensions

After finalizing the configuration of the recording services, make sure you have added the extensions you want to record to the Verba extension list. This can be done manually ([Extension list](#)) or using [Active Directory Synchronization](#).

Deploying Multiple Verba Desktop Agents

It is possible to deploy multiple Verba Desktop Agents with Group Policy using pre-created registry and certificate files.

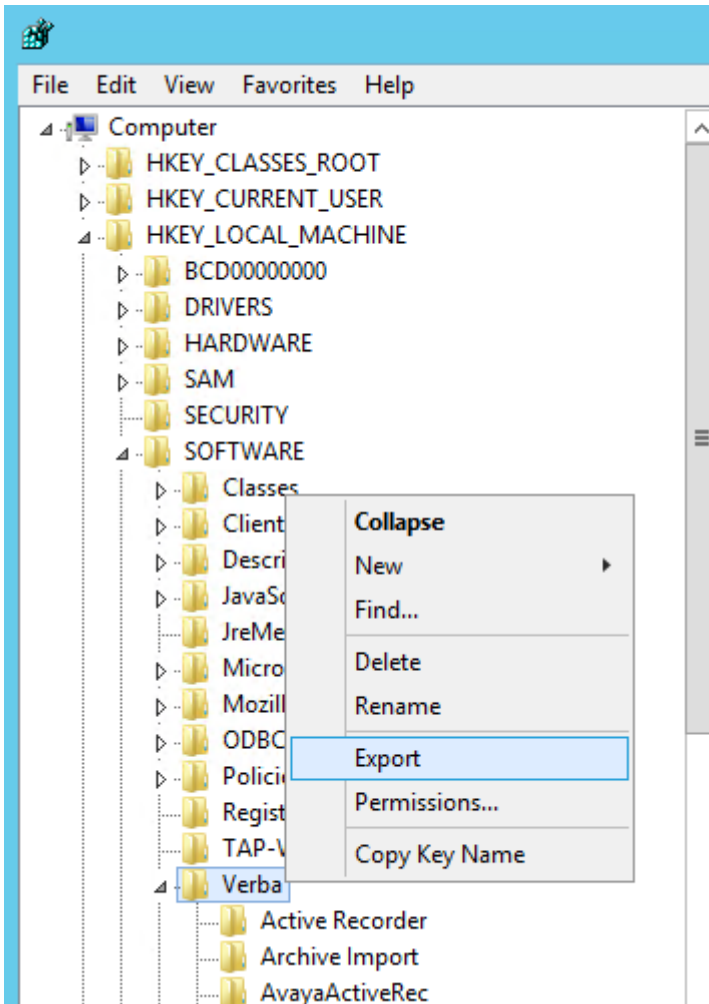
Stage 1:

Install and configure a Verba Desktop Agent the regular way, using the [Configuring the Desktop Agent](#) article.

Stage 2:

Step 1 - Log into the desktop where the Desktop Agent is installed.

Step 2 - Open the Start menu, type "regedit" and press Enter. The Registry Editor opens. Go to the **HKEY_LOCAL_MACHINE\SOFTWARE\Verba** node. Right-click on the Verba key, then select **Export**.



Step 3 - Save the registry to a file.

Stage 3:

Step 1 - Log into the Verba Web Interface and go to the **System | Request Server Certificate** menu.

Step 2 - Provide a **Subject** and a **Password** for the certificate.

Organization	<input type="text"/>
Organizational Unit	<input type="text"/>
Country/Region	<input type="text"/>
State/Province	<input type="text"/>
City/Locality	<input type="text"/>
Subject*	<input type="text" value="desktopagent"/>
Subject Alternative Name	<input type="text"/>
Password	<input type="password" value="*****"/>
Validity (Days)*	<input type="text" value="18250"/>

[Generate](#)

Step 3 - Click on the **Generate** button.

Step 4 - In the upper right corner click on the **Download CA Certificate** link.

Stege 4:

Step 1 - Create a new network share which is accessible to everyone, and put all files there (.cer, .pfx, .reg), and the VerbaDesktop.msi installer.

Step 2 - Create a .bat file using the template below:

```
certutil -addstore -enterprise Root \\share\Verba-CA.cer
certutil -f -p your_password_here -importpfx \\share\verba_desktopagent.pfx
msiexec /i \\share\VerbaDesktop.msi /L*V /quiet
reg import \\share\desktop.reg
sc restart verbaagent
sc restart verbasysmon
sc restart verbastorage
sc restart VerbaScreenController
```

Step 3 - Change the filenames and the certificate password.

Step 4 - Create a new Group Policy for running the .bat file on startup, based on the following guide:

[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc770556\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc770556(v=ws.11))

Alternatively, the .bat file can be executed manually.

Configuring the Verba Dial-in Recorder Service

Prerequisites - PBX side configuration

Step 1 - Plan directory numbers used for different available features:

- **Unattended recorder line:** Call is recorded silently, without any notification. The directory number has to be added to the Verba extension list and the PIN-based authentication has to be turned off.
- **Voice recorder line:** After directory number and/or PIN code based authentication via voice prompts call is recorded with beep notification.
- **Voice player line:** After directory number or PIN code based authentication user can playback his/her calls.
- **Voice portal line:** After directory number or PIN code based authentication user can record the current call or playback his/her calls, or playback calls by directory number if access is granted Controlling is done via DTMF - instant voice response.
- **Video portal line:** After directory number or PIN code based authentication user can record current video call or playback his/her calls (audio, video), or playback calls (audio, video) by directory number if access is granted. Controlling is done via DTMF - instant video response.
- **Open recording lines enabled:** Incoming calls to the Verba Dial-in Recorder, regardless the actual called number, will be recorded with beep notification. The caller number has to be added to the Verba extension list.

Step 2 - Create trunk pointing to the address where recorder is planned to listen

Step 3 - Create route patterns for dedicated directory numbers

See PBX specific configuration checklists here: [Configuring Cisco UCM for dial-in recording](#), [Configuring Microsoft Lync for dial-in recording](#), [Configuring Polycom RMX for conference recording](#)

Configuring the Verba Dial-in Recorder Service

Step 1 - In the Verba Web Interface go to **System > Servers > Select your Recording (or Single) Server > Click on the Service Activation** tab.

Step 2 - Activate the **Verba Dial-in Recorder Service** by clicking on the



icon.

Step 3 - Click on the **Change Configuration Settings** tab.

Step 4 - Expand the **Dial-in Recorder** node.

Step 5 - Under the Lines node, set the **Enable open recording lines** setting to **Yes** if required. Provide the line numbers at the following settings, based on your requirements:

- **Voice playback lines**
- **Voice recorder lines**
- **Unattended recorder lines**
- **Video portal lines**
- **Voice portal lines**


Step 6 - Set the **Internal Domain, Numbers Pattern** setting. This has to be a regex which matches to all internal numbers.

Step 7 - Save the changes by clicking on the



icon.

Step 8 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

 There are tasks to be executed regarding the configuration of this Verba Server.
If you would like to execute these tasks now, please [click here](#) .

Step 9 - Click on the **Service Control** tab.

Step 10 - Start the **Verba Dial-in Recorder Service** by clicking on the



icon.

Assign users to recorder lines

First of all, all users have to be added to the Verba [user list](#), and their line numbers and SIP URIs has to be added to the Verba [extension list](#) for enabling for them using the recorder lines. All users have to have a user role which contains the **Dial-in interface** right under the **Application Access** section. This can be done also by [Active Directory Synchronization](#).

Once the users and their extensions are present in Verba, the PIN code related settings can be set. If the PIN-based authentication is required, then a PIN code has to be set for every user. To do that, go to the **Users \ Users** menu, select the user from the list, then set the **Recorder Line PIN** setting. If the PIN-based authentication is not required, then go to the **Users \ Extension** menu, select the extension from the list, and turn on the **Do not request PIN on Recorder Line** setting under the **Dial-in Recorder Specific Settings** section.

Configuration reference

Recording line settings

- **Default voice prompt language:** voice prompt language for unauthenticated or users where language is not specified
- **Enable open recording lines:** if enabled all calls going to unspecified directory number will be recorded without any authentication
- **Voice and video prompt's directory:** directory for IVR prompts. For customization see xxxxxx
- **User response timeout:** call will be timed out and terminated if there is no user response for requested action until this time
- **Different feature lines:** one or multiply numbers where given feature will invoked.

SIP settings

- **Call timeout in sec:** SIP session timer, if call keepalive fails call is terminated and considered timed out
- **RTCP support:** support for Real-Time Control Protocol, based on this network/bandwidth adaptation for encoders/decoders is possible
- **SIP r-port:** support for SIP symmetric response routing (RFC 3581)
- **Force duplex streams:** the recorder can act as receive only endpoint according to SIP/SDP negotiation, however some devices do not honor this, and terminates the call because of media timeout. If duplex media is forced recorder acts as send-receive endpoint, and generates media. If it is not forced most of the MCUs hide the recorder in the conference, so from video conference recording point of view we would recommend disable it.
- **SIP user, password, uri for registration, register as client:** if trunk based integration with PBX is not preferred, the recorder can register as user agent, however in this case it can serve only one directory number. SIP address is registration uri config, user name is the user used for digest authentication
- **Recorder display name:** SIP display name of the recorder
- **RTP port range begin - end:** RTP port range used by the recorder
- **SIP signaling transport:** preferred transport for recorder initiated SIP sessions
- **Local SIP port:** SIP port on which the recorder is listening. Be sure that configured IP address and local SIP port match the trunk destination address in the PBX

Recording settings

- **Automatic Gain Control:** enables AGC on voice streams
- **Verba API port:** API port for internal service management
- **Voice call recording format:** storage format for audio only calls
- **Database cache directory:** database cache file path
- **Endpoint emulation:** endpoint profile, the followings are supported currently:
 - **Basic Audio:** audio only endpoint with G.722.1, G.722, G.729, G.711 and GSM support
 - **Basic Video:** audio and video endpoint with G.722.1, G.722, G.729, G.711 and GSM, H.264 (SQCIF - 1080p) support
 - **SIPREC single stream:** SRS: SIPREC based endpoint, calls with SIPREC content will be always recorded, it overrides line settings. Single stream media is forced
 - **SIPREC dual stream:** SRS: SIPREC based endpoint, calls with SIPREC content will be always recorded, it overrides line settings. Dual stream media is preferred, but SRC might negotiate in single stream
 - **Different Cisco Telepresence endpoints:** TIPv7.1 based interoperability with Cisco Telepresence. **It is still under development, only for experimental use.**
- **Recorder API port:** controlling port, which makes possible starting outgoing calls from the recorder to playback, and/or record the call
- **Video call recording format:** storage format for video calls
- **Write XML metadata:** write CDR XML with the calls

Advanced settings

- **Strip domain part of SIP phone number:** keep only the user part of SIP uri
- **RTP stream reorder buffer length:** audio reorder buffer size
- **Media format fallback enabled:** in case of not supported codecs, too many streams, not supported streams, transcoding quality issue, the recorder can intelligently change storage format to different kind of codecs which might preserve the recording in more optimal quality.
- **Always negotiate single codec:** in case of SDP offer the recorder will select one codec in each media stream's codec list in the answer. We support handling of list of codecs, and dynamic codec changes, so only in case of interoperability issue should this be enabled.

Service Reference

Configuration Parameter Name	Description
Local SIP Port Number	Port number used for SIP signaling communication. This port number has to match the configuration in other systems connecting to the service.
Silent Monitoring Enabled	Enable silent monitoring capabilities for the service. By enabling this option, any ongoing call recorded by any recording service supporting silent monitoring, can be monitored through the phone playback access numbers. This option does not enable/disable the silent monitoring feature on the web application for calls recorded by this service.
Called Party Name	Display name of the service, which will be displayed as called party name on the caller phone device.
Default Menu Language	Default language setting for the voice menu.
SIP Transport Protocol	SIP signaling transport protocol configured in the SIP proxy. Values can be TCP or UDP. TCP is recommended.
Audio Format	The recorder application will use the selected file format and codec option to create the audio files.
PIN Entry Retries	Number of allowed PIN code entry attempts. After exceeding this number, the system plays an error prompt and disconnects the caller.

Public Recorder Access Number	<p>Entry point (directory number) used to access the recording functionality. Using this access number, the system does not authenticate the caller and allows to access the recording service from any phone number. After connecting the caller, the system plays in a prompt to notify the parties in the call about the call recording, and automatically starts the recording.</p> <p>If you do not want to allow unauthenticated access to the recording service, do not configure this access number, leave it empty.</p>
Authenticated Recorder Access Number	<p>Entry point (directory number) used to access the recording functionality. The system authenticates and identifies the caller based on the calling party phone number and optionally the user also has to enter a PIN code. If the calling party phone number cannot be found, the user has to enter the PIN code. After authentication, the system plays in a prompt to notify the parties in the call about the call recording, and automatically starts the recording.</p>
Authenticated Recorder Access Number without Prompt	<p>Entry point (directory number) used to access the recording functionality. The system authenticates and identifies the caller based on the calling party phone number and optionally the user also has to enter a PIN code. If the calling party phone number cannot be found, the user has to enter the PIN code. After authentication, the system DOES NOT play in any prompt, it automatically starts the recording.</p>
Authenticated and Unauthorized Playback Access Number	<p>Entry point (directory number) used to access the playback functionality. The system authenticates and identifies the caller based on the calling party phone number and optionally the user also has to enter a PIN code. If the calling party phone number cannot be found, the user has to enter the PIN code. After authentication, the system asks for a phone number, which is used to query the database and offer calls for playback or silent monitoring. Silent monitoring is only available for the ongoing calls.</p> <p>It is important to understand, that using this access number, the system does not check any authorization to access certain calls or group membership right or information while offering calls for playback or silent monitoring. The system simply offers all calls. If you do not want to offer unauthorized access to the calls, do not configure this access number, leave it empty.</p> <p>The playback functionality is available for all voice calls recorded by any recording service. It is not limited to the calls recorded by the Dial-in recording service.</p>
Authenticated and Authorized Playback Access Number	<p>Entry point (directory number) used to access the playback functionality. The system authenticates and identifies the caller based on the calling party phone number and optionally the user also has to enter a PIN code. If the calling party phone number cannot be found, the user has to enter the PIN code. After authentication, the system asks for a phone number, which is used to query the database and offer calls for playback or silent monitoring. Silent monitoring is only available for the ongoing calls.</p> <p>The system automatically checks the user authorization to access the calls and only offers those calls for playback or silent monitoring, which are available for the user based on her/his settings.</p> <p>The playback functionality is available for all voice calls recorded by any recording service. It is not limited to the calls recorded by the Dial-in recording service.</p>

Advanced settings

The following table provides detailed instructions on each configuration setting:

Configuration Parameter Name	Description
Process Unicode Names	If enabled, the system treats the calling party names as unicode characters.
Store Call Time in UTC/GMT	Enables the use of UTC time when writing to the database or XML CDRs. The Verba Web Application treats every date and time value as UTC, so if this setting is turned off, it may result to displaying inaccurate date and time values.
Strip Domain	If enabled, the system automatically strips the domain information from the SIP addresses and leaves the phone

from SIP Phone Numbers	number information only.
Menu Timeout (seconds)	The system wait that long in seconds for a DTMF input from the user. If the timeout expires and the user did not enter any code, the system automatically disconnects the call after a warning prompt.
Call Timeout (seconds)	Defines the call timeout value in seconds, which is used to terminate the call if the reinvoke was not successful.
Database Cache Folder	The path to the database cache file without filename. Network drives are not supported, because of reliability and performance issues, so please do not use mapped network drives or UNC network drives, use only local folders. Use the browse button to select the proper folder.
Automatic Gain Control Enabled	If this setting is enabled, the application automatically controls the gain in the audio file to provide more convenient user experience while listening back recordings.
IVR Prompt Path	The path to the folder containing the prompt files used by the IVR. Network drives are not supported, because of reliability and performance issues, so please do not use mapped network drives or UNC network drives, use only local folders. Use the browse button to select the proper folder.

Configuring Cisco UCM for dial-in recording

In order to use the Dial-In capabilities of the Verba Recording System configuration of the Cisco Unified Communication Manager is required.


Initial configuration

The initial Cisco UCM configuration for dial-in recording includes the following steps:

Step 1 - [Create and configure the SIP trunk](#) that points to the recorder(s). **Note! Use 5065 as SIP port with this recorder service instead of 5060.**

Step 2 - [Configure routing](#) that let's Cisco UCM to direct calls to the recorder (includes configurations for multiple recorders).

After these steps you can start enabling dial-in recording on your Verba extensions.

 If you are using both central and dial-in recording with Cisco UCM, make sure that you use to two **different extensions** in your route patterns.

Adding and removing extensions

Extensions can be added to the recording system by enabling Dial-In recording in the [Verba extension management](#).

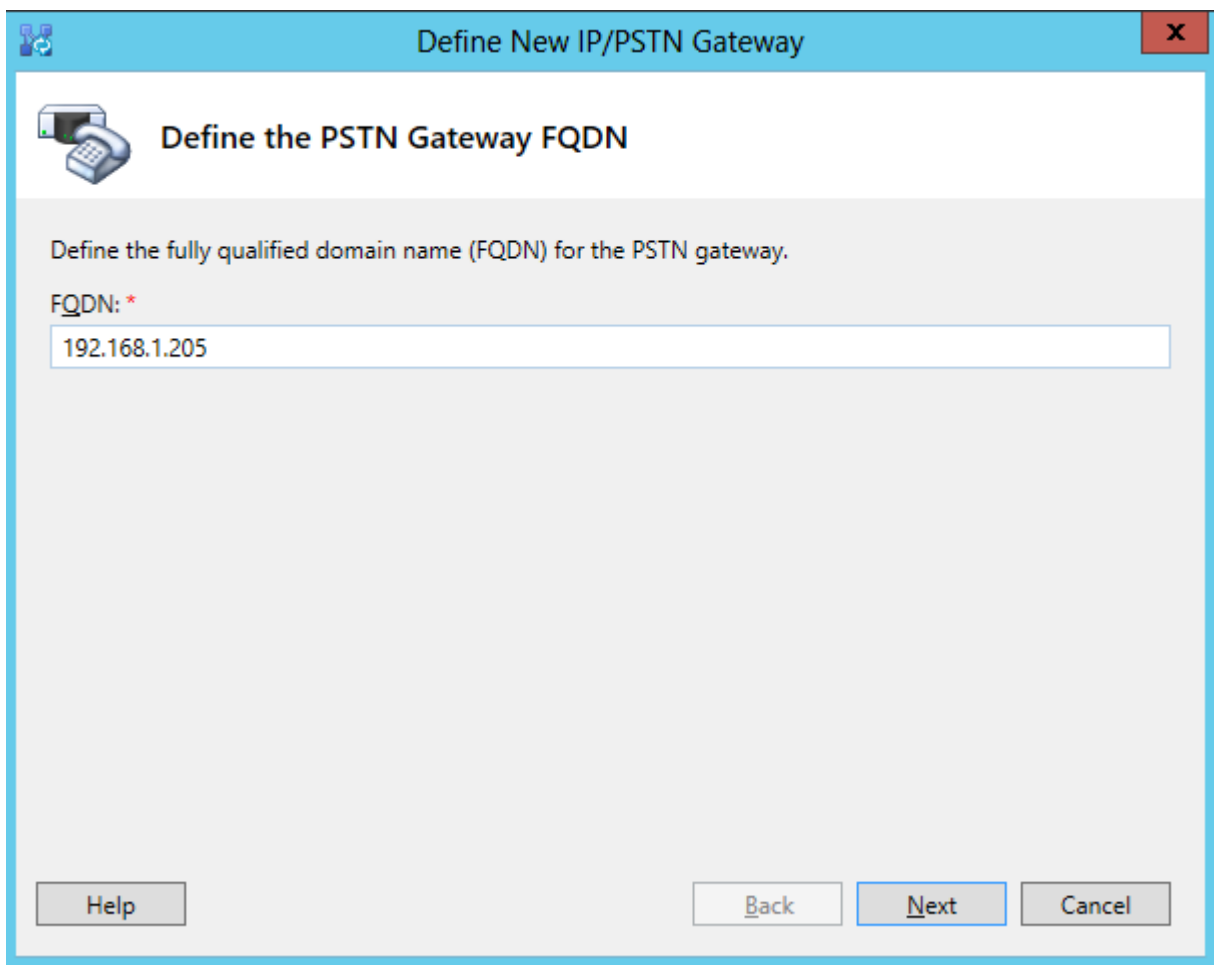
Configuring Microsoft Lync for dial-in recording

In order to use the Dial-In capabilities of the Verba Recording System configuration of the Microsoft Lync pool is required. The recorder is connected to Lync through mediation server as a SIP gateway.

Basic configuration


The basic Lync configuration for dial-in recording includes the following steps:

Step 1 - Create a PSTN gateway trunk in Lync Topology Builder. Its destination address must match the SIP listening address of Dial-in Recorder. Assign it to the mediation pool. Publish the new topology. **Note! Use 5065 as SIP port with this recorder service instead of 5060. TLS is currently not supported, TCP is the preferred transport.**



The screenshot shows a dialog box titled "Define New IP/PSTN Gateway" with a close button (X) in the top right corner. The main heading is "Define the PSTN Gateway FQDN" next to a telephone icon. Below the heading, the instruction reads: "Define the fully qualified domain name (FQDN) for the PSTN gateway." There is a label "FQDN: *" followed by a text input field containing the IP address "192.168.1.205". At the bottom of the dialog, there are four buttons: "Help", "Back", "Next", and "Cancel".

Define New IP/PSTN Gateway

 Define the root trunk

Trunk name: *
192.168.1.205

Listening port for IP/PSTN gateway: *
5065

SIP Transport Protocol:
TCP

Associated Mediation Server:
MEDIATION.verbalabs.com VERBALABS

Associated Mediation Server port: *
5068

Help Back Finish Cancel

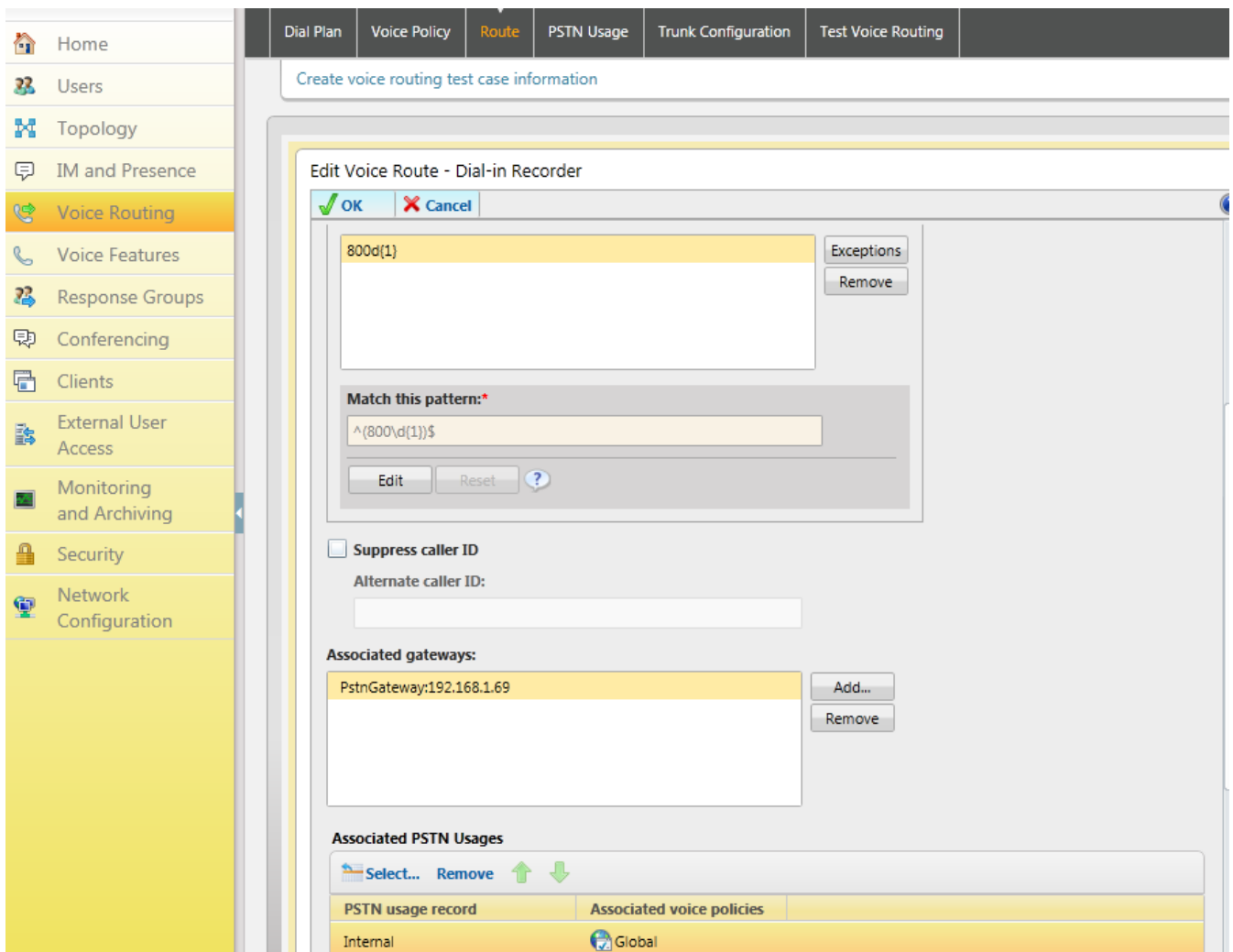
Step 2 - Enter Lync Configuration Center

Step 3 - Create new Normalization Rule in **Global dial** plan under Voice Routing/Dial Plan page. This example creates pattern for 8000-8009 range, with internal numbers attribute..

The screenshot displays the 'Edit Normalization Rule' configuration page in CUCM. The left sidebar shows the navigation menu with 'Voice Routing' selected. The top navigation bar includes 'Dial Plan', 'Voice Policy', 'Route', 'PSTN Usage', 'Trunk Configuration', and 'Test Voice Routing'. The main content area is titled 'Edit Dial Plan > Edit Normalization Rule - Verba Dial-in Recorder'. It features a 'Name' field with the value 'Verba Dial-in Recorder' and an empty 'Description' field. Below this is a 'Build a Normalization Rule' section with instructions: 'Fill in the fields that you want to use, or create the rule manually by clicking Edit.' The fields in this section are: 'Starting digits' (800), 'Length' (Exactly, 4), 'Digits to remove' (0), 'Digits to add' (empty), 'Pattern to match' (^{800\d{1}}\$), and 'Translation rule' (\$1). At the bottom of the form are 'Edit', 'Reset', and a help icon. A checkbox for 'Internal extension' is checked.

Step 4 - Create trunk settings: under Trunk Configuration add new settings based on pool, select the new gateway (recorder trunk). Set media encryption policy to not supported. Prefer media bypass and centralized media processing.

Step 5 - Create route: define the route pattern, and assign the recorder trunk/gateway and internal PSTN usage, and global voice policy. Internal PSTN usage is assigned to Global Voice Policy by default, you can also create special voice policies to limit the access of users to recorder route.



You can test your routing settings on Test voice routing page. After these steps you can start enabling dial-in recording on your Verba extensions.

ⓘ If you are ready with configuration Mediation Server service in Lync must be restarted to apply the changes

Adding and removing extensions

Extensions can be added to the recording system by enabling Dial-In recording in the [Verba extension management](#).

Configuring Verba for On-demand recording

Overview

On-demand recording allows users to decide if a call recording should be kept or discarded. If you configure on-demand recording for an extension, all calls will be recorded automatically from the beginning. However they are first placed into a special place called the On-demand Calls Buffer. The user can mark the call for recording during or after the call. After marking a call, the call is removed from the buffer and can be found among the other normally recorded calls. Calls that are not marked for recording will be deleted after a configurable amount of time. Since this feature is based on database and file transactions, it's entirely platform independent and therefore works with any phone system and call recording technology.

Enabling On-demand recording for extensions

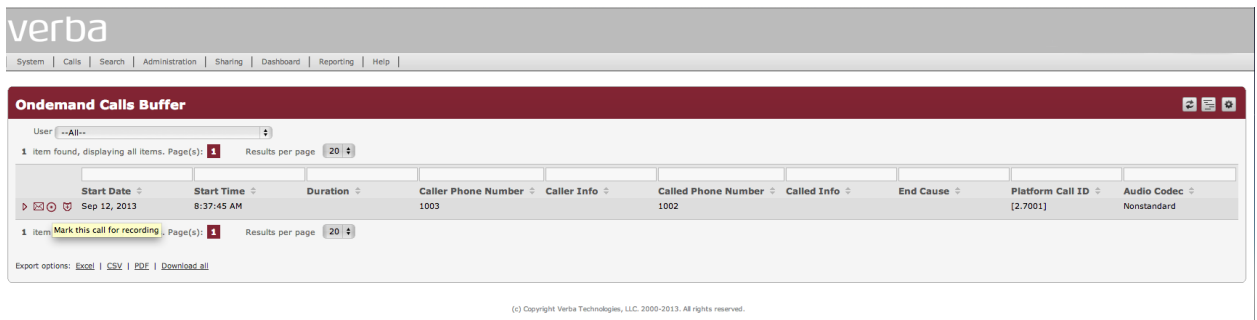
You can configure Verba for on-demand call recording by following the steps below:

- Step 1:** Configure the required extensions in your phone system and Verba for automatic always-on recording. ([Configure Recording](#)).
- Step 2:** In the Verba web application go to Administration > Extensions.
- Step 3:** Choose an extension for which you want to enable on-demand recording or if you haven't added it to Verba yet, add it by clicking 'Add New Extension'.
- Step 4:** On the extension configuration page, set 'Recording Mode' to 'On-demand', then click Save.
- Step 5:** Apply the changes to extension configuration across all Verba servers

Working with on-demand recording

User assigned to an on-demand extension can keep calls using the following options:

- Verba web interface: select Calls > On-demand calls buffer and click on the Record icon to mark the desired call for recording.



- Cisco Phone Service: users with Cisco phones can mark a call for recording through the Verba phone service using the Record soft key. To configure the Cisco phone service, please refer to the corresponding article: [Configuring the Cisco Phone service](#).
- DTMF control from the phone. To configure DTM control, please refer to the following article: [Configuring DTMF Control](#).

Changing the on-demand buffer size

Unmarked calls will be deleted by the storage system after a set amount of time. To configure this time window, follow the steps below.

- Step 1:** In the Verba web application go to Administration > Verba Servers and select your Media Repository.

Step 2: Select the 'Change configuration settings' tab, then click Storage Management > On-demand Recording.

Step 3: Set the 'On-demand Recording Buffer Length (hours)' property to the desired value.

Step 4: Save your settings.

Database configuration

- [Configuring database connection](#)
- [Configuring encryption for database connections](#)
- [Configuring SQL Server Failover Partner for mirroring](#)
- [Configuring SQL Server database encryption](#)

Configuring database connection

Database connection can be configured in Verba on profile or on per server level.

- In order to configure the database connection settings on the **profile level**, go to the **Administration / Configuration Profiles** menu and select the profile. The configuration can be found at the **Change Configuration Settings** tab.
- In order to configure the database connection settings on the server **level**, go to the **Administration / Verba Servers** menu then select the server that needs to be configured. The configuration can be found at the **Change Configuration Settings** tab.

The database connection settings can be found under the **Database Connection** node.

Database Connection

Database Hostname:	<input type="checkbox"/>	(local)
Database Name:	<input type="checkbox"/>	verba_demo
Database Windows Authentication:	<input type="checkbox"/>	▼
Database Login:	<input type="checkbox"/>	sa
Database Password:	<input type="checkbox"/>	*****
Database Failover Partner:	<input type="checkbox"/>	
Database Multi-Subnet Failover:	<input type="checkbox"/>	▼
Database Driver:	<input type="checkbox"/>	SQL Server ▼
Enable SSL Encryption:	<input type="checkbox"/>	▼
Java Trust Store Path:	<input type="checkbox"/>	
Java Trust Store Password:	<input type="checkbox"/>	

Settings Name	Description
Database Hostname	The hostname or IP address where the database server hosted. If the database is a named instance then provide the instance also. In case of Always-on database, the connector name. If custom port used then use the hostname:port format or turn on the SQL Server Browser service at the database side. Examples: <ul style="list-style-type: none">• <i>(local)</i> - (SQL Server running co-hosted on the Verba server using the default 1433 port)• <i>verba-db-server.acme.com</i> - (SQL Server using the default 1433 port)• <i>verba-db-server.acme.com:15001</i> - (SQL Server using the 15001 port)• <i>verba-db-server.acme.com\InstanceName</i> - (SQL Server named instance using the default 1433 port)
Database Name	The name of the Verba database.
Database Windows Authentication	Set to Yes if Windows authentication used.
Database Login	The SQL username or the Windows username with the domain for the database access. In case of Windows authentication, a Windows service user has to be used for the Verba services.
Database Password	The password for the SQL/Windows user.

Database Failover Partner	The hostname or IP address where the failover partner database server hosted. If the database is a named instance then provide the instance also. If custom port used then turn on the SQL Server Browser service at the database side. Please note that if mirroring is configured then the ODBC 13.1 have to be used as Database Driver.
Database Multi-Subnet Failover	Set to Yes if Always-on database used with Multi-Subnet Failover configuration. Please note that in this case the ODBC 13.1 have to be used as Database Driver.
Database Driver	<p>The driver used for database connection. This driver configuration is only used by specific services in the system, other services use different SQL Server drivers bundled with the product (JDBC driver) or provided by other prerequisites (.NET framework). The following options available:</p> <ul style="list-style-type: none"> • SQL Server (default driver) • Microsoft ODBC Driver 13.1, certain advanced features requires this driver instead of the default: <ul style="list-style-type: none"> • Mirroring • Always-on with multi-subnet failover • SSL based connection encryption and when TLS 1.0 is disabled on the OS level <p>Microsoft ODBC Driver 13.1 download</p>
Enable SSL Encryption	Set to Yes if you want to set up SSL encryption. For more information see: Configuring SSL encryption for database connections
Java Trust Store Path	Java Trust Store path used for SSL encryption. For more information see: Configuring SSL encryption for database connections
Java Trust Store Password	The password for the Java Trust Store. For more information see: Configuring SSL encryption for database connections

Check the firewall configuration on the SQL Server to ensure connectivity with the Verba servers, see <https://docs.microsoft.com/en-us/sql/sql-server/install/configure-the-windows-firewall-to-allow-sql-server-access?view=sql-server-2016>

Configuring encryption for database connections

Available in version 8.2 and later

Encryption enables transmitting encrypted data across the network between an instance of SQL Server and the Verba applications. SSL/TLS is a protocol for establishing a secure communication channel to prevent the interception of critical or sensitive information across the network and other Internet communications. SSL/TLS allows the client and the server to authenticate the identity of each other. After the participants are authenticated, SSL/TLS provides encrypted connections between them for secure message transmission.

Enabling encryption increases the security of data transmitted across networks between instances of SQL Server and applications. However, enabling encryption results in slower performance.

Encryption needs to be configured in both SQL Server and Verba, although you can turn on the encryption support on the SQL Server side without configuring the Verba servers. In this case, the connection will be encrypted but not validated. You can also use this approach with earlier Verba releases, where encryption-related settings are not available for the Verba applications.

- [Enabling encryption for the SQL Server](#)
- [Enabling encryption for Verba services](#)
 - [Export the certificate](#)
 - [Import the certificate on the Verba servers](#)
 - [Import the certificate into a Java Trust Store on the Verba servers](#)
 - [Configure Verba database connection parameters](#)
- [Checking encryption](#)

Enabling encryption for the SQL Server

Microsoft provides detailed guidance on configuring encryption for an SQL Server: <https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/enable-encrypted-connections-to-the-database-engine>

Make sure you follow the guideline properly. We strongly recommend consulting your database administrator before proceeding with the configuration.

Enabling encryption for Verba services

Follow the steps below to enable SSL encryption for the SQL Server connections in Verba:

Export the certificate

For Verba to request the encryption, Verba servers must trust the SQL Server certificate and the certificate must already exist on the SQL Server. For more information, see <http://support.microsoft.com/kb/316898>

To export the SQL Server certificate's, follow these steps:

Step 1 - Click **Start** and then **Run**, and type MMC. (MMC is an acronym for the Microsoft Management Console)

Step 2 - In MMC, open the **Certificates**.

Step 3 - Expand **Personal** and then **Certificates**.

Step 4 - Right-click the server certificate, and then select **All Tasks\Export**.

Step 5 - Click **Next** to move past the welcome dialog box of the **Certificate Export Wizard**.

Step 6 - Confirm that "No, do not export the private key" is selected, and then click **Next**.

Step 7 - Make sure that either DER encoded binary X.509 (.CER) or Base-64 encoded X.509 (.CER) is selected, and then click **Next**.

Step 8 - Enter an export file name.

Step 9 - Click **Next**, and then click **Finish** to export the certificate.

Import the certificate on the Verba servers

Follow these steps to import the SQL Server certificate on all Verba servers:

Step 10 - Navigate to the Verba server by using the MMC snap-in, and then browse to the **Trusted Root Certification Authorities** folder.

Step 11 - Right-click the **Trusted Root Certification Authorities** folder, point to **All Tasks**, and then click **Import**.

Step 12 - Browse, and then select the certificate (.cer file) that you generated in Step 1 - 9. Select the defaults to complete the remaining part of the wizard.

Step 13 - Repeat Step 10 through Step 12 on all Verba servers.

Import the certificate into a Java Trust Store on the Verba servers

Follow these steps to import the SQL Server certificate to a Java trust store on all Verba servers:

Step 14 - Use the Java "keytool" utility that is installed with the JRE (Java Runtime Environment). The following command prompt demonstrates how to use the "keytool" utility to import the certificate from a file:

```
keytool -import -v -trustcacerts -alias myServer -file caCert.cer -keystore truststor
```

Where *myServer* is the FQDN of the SQL Server, *caCert.cer* is the SQL Server certificate file exported, and *truststore.ks* is the name of the Java trust store you will use in Verba configuration.

Make a note of the password entered when executing the command.

Step 15 - Repeat Step 14 on all Verba servers. Make sure you use the same parameters (trust store name and path, password) on all servers to enable simple configuration using configuration profiles.

Configure Verba database connection parameters

Follow these steps to configure encryption for the Verba services:

Step 16 - In the Verba web interface click on **Administration > Verba Servers** and select your server, or select the appropriate Configuration Profile at **Administration -> Configuration Profiles**.

Step 17 - Click on the **Change Configuration Settings** tab.

Step 18 - Expand **Database Connection** and **SSL Encryption for Connections**.

Step 19 - Enable the **SSL Encryption** option.

Step 20 - Enter the full path of the Java trust store, created on the server at Step 14 above, into **Java Trust Store Path**.

Step 21 - Enter the password, used at Step 14 above, into **Java Trust Store Password**.

Step 22 - Click the **Save** icon to save your settings

Step 23 - The system will notify you that the changes need to be applied to the server by restarting the involved services. Execute the required tasks.

Step 24 - Repeat Step 16 through 23 for each Verba server.

Checking encryption

The best way to check if encryption is enabled is to use Wireshark or other network capturing tool and validate that SQL connections are encrypted and cannot be read.

Configuring SQL Server Failover Partner for mirroring

Verba supports SQL Server mirroring configurations. The mirror database can be added to the so-called "Connection String". This string is used by the SQL Server client libraries, and if it contains the Failover Partner information, then after the original principal server goes down, the library will automatically reconnect to the new principal server.

Using this method, the mirror databases are configured in advance, so no additional configuration is required when the database roles are switched, and no service restart is needed.

After a role switch, each Verba component's each database connection will be invalid, and the next database query will fail. Again, that will not cause any loss in regards to the recorded data, because when a SQL query fails, the recorder services put the data to their cache, and will try to synchronize later. The web interface periodically tests the database connections, and if a connection is invalid, it tries to reconnect to the database. As a result, the interface will be usable in a few seconds after the roles switched.

Follow the steps below to configure this option:

Step 1 - Install the **Microsoft ODBC Driver** compatible with your SQL Server on the Verba servers. For more information see [Prerequisites](#).

Step 2 - On the Verba web interface, click on **Administration / Verba Servers** and select your server, or select the appropriate Configuration Profile at **Administration / Configuration Profiles**.

Step 3 - Click on the **Change Configuration Settings** tab.

Step 4 - Expand **Database Connection** and enter the IP address or hostname of the mirror database into **Database Failover Partner**.

Step 5 - Change the **Database Driver** to **ODBC Driver 17 for SQL Server** (the version might be different in your install).

Step 6 - Save the changes by clicking on the



icon.

Step 7 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

Step 8 - Repeat the steps on each Verba server and/or configuration profile.

Configuring SQL Server database encryption

The Verba system supports database encryption features provided by Microsoft SQL Server. More information on encryption technology: <https://msdn.microsoft.com/en-us/library/bb510663.aspx>

Transparent data encryption (TDE) performs real-time I/O encryption and decryption of the data and log files. The encryption uses a database encryption key (DEK), which is stored in the database boot record for availability during recovery. The DEK is a symmetric key secured by using a certificate stored in the master database of the server or an asymmetric key protected by an EKM module. TDE protects data "at rest", meaning the data and log files. It provides the ability to comply with many laws, regulations, and guidelines established in various industries. For more information on TDE, refer to <http://msdn.microsoft.com/en-us/library/bb934049.aspx>.

Important considerations:

- Microsoft offers TDE as part of its Microsoft SQL Server 2008, 2008 R2, 2012, 2014, 2016, 2017. TDE is only supported on the Evaluation, Developer, Enterprise and Datacenter editions of Microsoft SQL Server.
- Only the complete Verba databases can be encrypted, there is no option to encrypt a single database table.
- Some performance overhead is involved in using TDE. The encryption and decryption process does require additional CPU cycles. The overhead for using TDE ranges from about 3 percent to 30 percent, depending on the type of workload. SQL Server instances with low I/O and low CPU usage will have the least performance impact. Servers with high CPU usage will have the most performance impact.

Configuring database encryption

The **verba** database has to be updated/alterd in order to use the encryption feature. The following T-SQL script shows the required steps to enable database encryption. You need to adjust it according to your needs.

```
USE master;
GO
CREATE MASTER KEY ENCRYPTION BY PASSWORD = '<UseStrongPasswordHere>';
GO
CREATE CERTIFICATE MyServerCert WITH SUBJECT = 'My DEK Certificate';
GO
USE verba;
GO
CREATE DATABASE ENCRYPTION KEY
WITH ALGORITHM = AES_128
ENCRYPTION BY SERVER CERTIFICATE MyServerCert;
GO
ALTER DATABASE verba
SET ENCRYPTION ON;
GO
```

There is no configuration required on the Verba side.

Creating a backup of the certificate and the private key

When enabling TDE, you should immediately back up the certificate and the private key associated with the certificate. If the certificate ever becomes unavailable or if you must restore or attach the database on another server, you must have backups of both the certificate and the private key or you will not be able to open the database. The encrypting certificate should be retained even if TDE is no longer enabled on the database. Even though the database is not encrypted, parts of the transaction log may still remain protected, and the certificate may be needed for some operations until the full backup of the database is performed. A certificate that has exceeded its expiration date can still be used to encrypt and decrypt data with TDE.

For more information on the T-SQL commands, please check <https://msdn.microsoft.com/en-us/library/ms178578.aspx>.

Microsoft offers TDE as part of its [Microsoft SQL Server](#) 2008, 2008 R2, 2012, 2014, 2016, 2017 and 2019.^[1] TDE was only supported on the Evaluation, Developer, Enterprise and Datacenter editions of Microsoft SQL Server, until it was also made available in the Standard edition for 2019

Advanced Call Recording Rules

Overview

In certain situations selective recording rules defined through the Verba web interface might not be powerful enough to define the filter rules you are planning to implement. For these cases you can use an **alternative method, that provides more powerful recording conditions**.

Supported integrations

The XML based recording rule configuration is supported with [Cisco Network Based](#) and [Avaya](#) recording. Extensions need to be configured with Full [Recording mode](#).


The solution is based on an XML file that defines these advanced recording rules:

```
<VERBA_APP_PATH>\settings\rules.xml
```

The rules.xml file contains an **ordered list of rules**, where each rule has:

- **conditions** - a list of conditions, where all should succeed for the rule to match
- **action** - an action that should be taken when a rule matches

See the rules.xml example below for syntax and usage details.

 The default action for calls not matching any rule is not recording!

Configuring advanced call recording rules

If you want to use the advanced call recording rules, you need to take the following steps:

Step 1 - In case of Cisco recording, configure the line on recorded phones with **Recording Option** = 'Application Invoked'. See [Adding a new extension for recording in Cisco UCM](#).

Step 2 - Create the **rules.xml file** and copy it to the <VERBA_APP_PATH>\settings\ folder

Step 3a - In case of Cisco recording - set **Cisco JTAPI Configuration / Advanced Settings / Advanced Recording Rules Enabled** to 'Yes'.

Step 3b - In case of Avaya recording - set **Avaya Recorder / Avaya DMCC / Advanced Recording Rules Enabled** to 'Yes'.

Step 4 - Start (or restart) the **Verba Cisco JTAPI Service\Verba Avaya DMCC/JTAPI Service**

Repeat step 2 and 3 on all Verba recording servers that run the central recording service.

Changing the rules XML file

When you make changes to the rules.xml file, you have to restart the **Verba Cisco JTAPI Service\Verba Avaya DMCC/JTAPI Service**. Make a backup copy of your old xml file to be able to restore operations in case of an XML syntax problem.

Example rules.xml file

The following example shows the available rules, conditions and actions in a rules.xml file. You can [download this example rules.xml file here](#).

rules.xml

```
<?xml version = '1.0' encoding = 'UTF-8'?>

<!-- This Rules XML file defines advanced
      call recording rules used by the Verba Recording System.
      ROOT tag of the file is 'rules' -->
<rules>

  <!-- Every rule is defined as a 'rule' tag,
        rules are processed from top to bottom,
        if a rule condition matches the rest is ignored. -->
  <rule>

    <!-- 'rule' tags can have two children:
          non-mandatory 'conditions' tag
          mandatory 'action' tag -->
    <conditions>

      <!-- 'conditions' tag have children called 'condition' tags with attributes:
            'type' - AnyConfigured | CallerParty | CalledParty (mandatory)
            'patternType' - regex | dos | simple (optional, default is regex)
            If multiple condition are listed, AND operator is applied between them.
            If any of the 'condition' tests fail, the next 'rule' will be evaluated,
            without processing the 'action'.

            See 'condition' examples below: -->

      <condition type="CallerParty" patternType="regex">^\d{4}$</condition>
      <!-- caller party is 4 characters long, contains numbers only -->

      <condition type="CalledParty" patternType="regex">^\d{5}$</condition>
      <!-- called party is 5 characters long, contains numbers only -->

      <condition type="CallerParty" patternType="dos">????</condition>
      <!-- caller party is 4 characters long DOS style -->

      <condition type="CalledParty" patternType="dos">?????</condition>
      <!-- called party is 5 characters long DOS style -->

      <condition type="CallerParty" patternType="simple">1234</condition>
      <!-- caller party is 1234 -->

      <condition type="CalledParty" patternType="simple">12345</condition>
      <!-- called party is 12345 -->

      <condition type="CallerParty" patternType="dos">123?</condition>
      <!-- caller party is 4 characters long and starts with 123 -->

      <condition type="CalledParty" patternType="dos">123?5</condition>
      <!-- called party is 12345 -->

    </conditions>

    <!-- The 'action' tags specifies the action to be taken when all 'condition' tags match.
          Action values can be: record | dont_record -->
    <action>record</action>

  </rule>
```

```
<!-- The following rule matches for all calls where at least one of
the parties are configured for recording in the extension list of the system. -->
<rule>
  <conditions>
    <condition type="AnyConfigured" />
  </conditions>
  <action>record</action>
</rule>

<!-- The following 'rule' tag shows that the 'conditions' tag is not mandatory.
This will match every call which did not match any of the above 'rule'. -->
<rule>
  <action>dont_record</action>
</rule>

</rules>
```

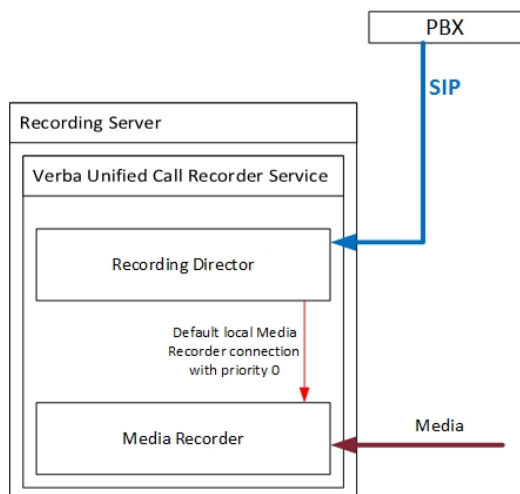

Configuring recording high availability

The Verba Unified Call Recorder is capable of priority-based load balancing and mid-call failover. This configuration is available for Cisco and other phone systems with SIP-based recording.

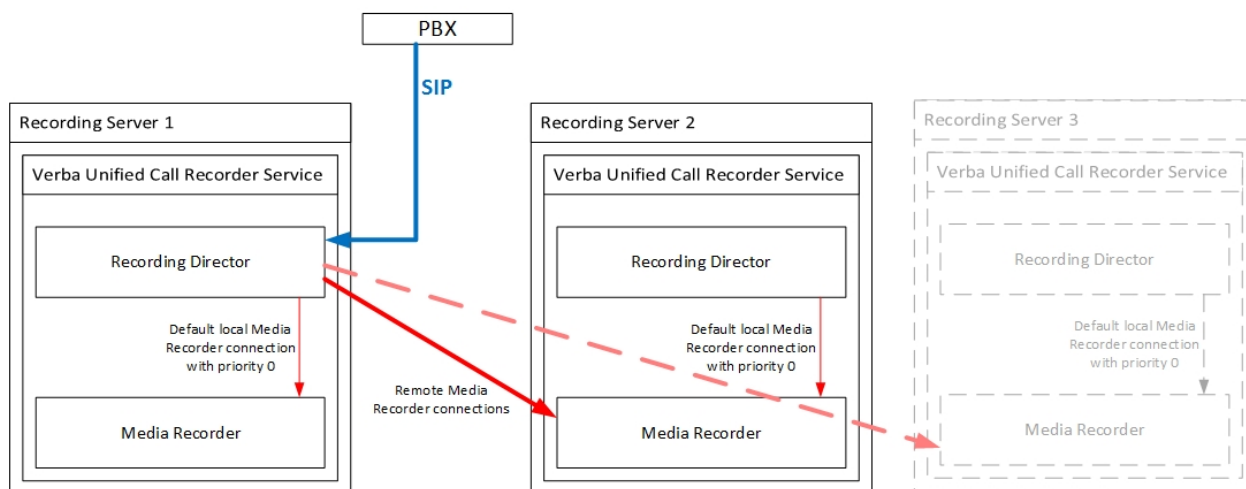
⚠ The load balancing and mid-call failover capabilities are highly dependent on the phone system!

Overview

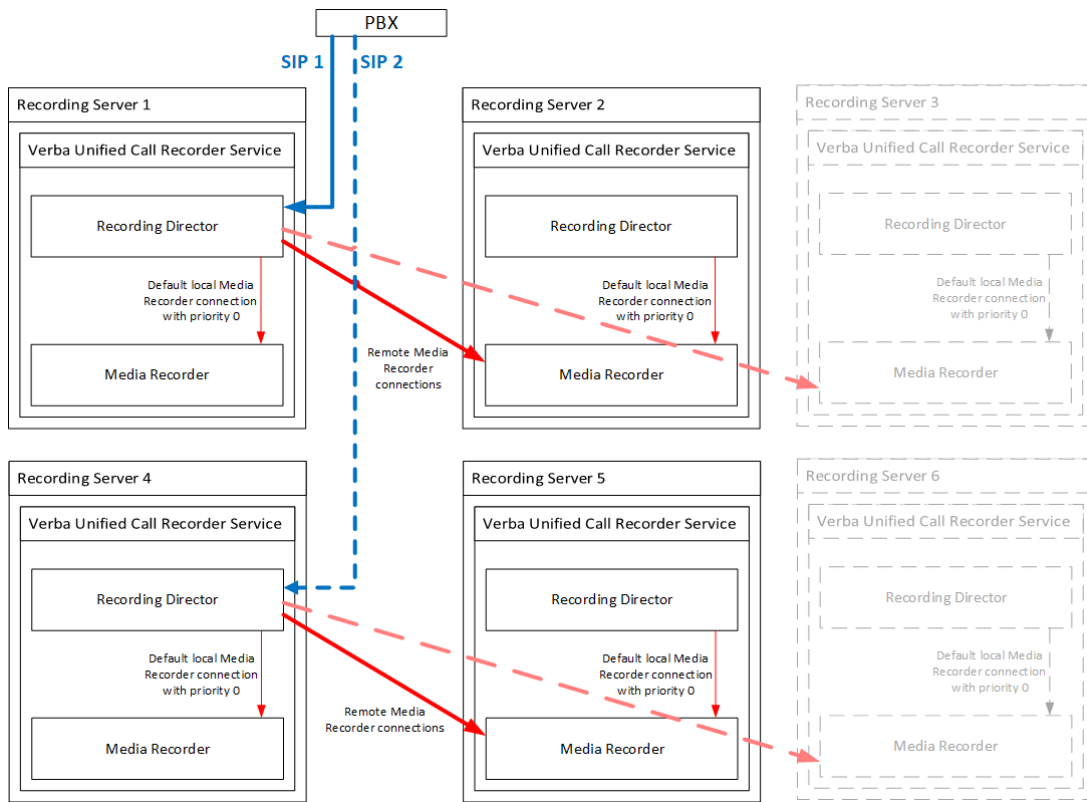
The Verba Unified Call Recorder contains a Recording Director and a Media Recorder module. The Recording Director module handles the incoming SIP connection(s) and decides which Media Recorder should receive which call's media stream. The Media Recorder does the recording and the media processing of the incoming media streams. By default, the Recording Director module is always connected to the local Media Recorder module within the same service, with priority 0.



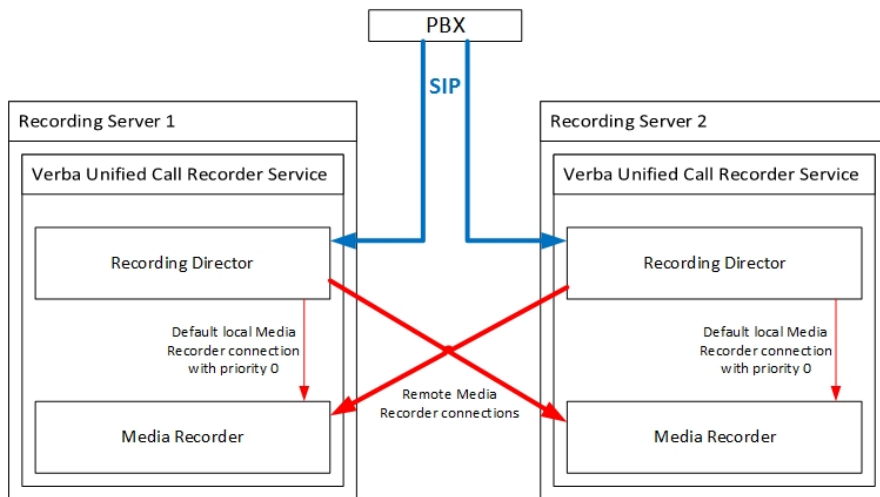
On the other hand, the Recording Director can be connected to other Media Recorder modules, hosted by other Verba Unified Call Recorder services on other servers. The Recording Director module can do mid-call failover between the connected Media Recorders.



Multiple Recording Director connections can be set up using multiple SIP trunk / CTI connections. Each Recording Director can have his own Media Recorder, or they can have common Media Recorders also. If a Recording Director doesn't have an available Media Recorder, it responds with SIP 503 to the incoming SIP sessions, so it initiates a SIP trunk failover where it is possible.



The services also can be cross-connected.



The priorities of the Media Recorder connections are adjustable. The Media Director always using the Media Recorder with the highest priority. If the Media Recorders have the same priority, then there will be load-balancing between them. If a Media Recorder in use goes down, then the Recording Director can reassign the call to another Media Recorder, providing mid-call failover.

The JTAPI service connections (if used) have to be configured on the servers used as Media Recorders.

Configuring Media Recorder connections

Preparations

On all Recording (or Single) Servers the **Verba Unified Call Recording service** has to be activated. The ones that receiving the SIP connections going to function as Recording Directors.

! If the [Data models](#) is used and the recorder server clocks are not synchronized, the Media and CDR records will be recorded with different timestamps, and the playback will not work as expected.

Configuring remote Media Recorders

! The local Media Recorder should not be added as a remote Media Recorder. If it is added and communication is not done via memory as desired, it can lead to unexpected issues, especially with VOX triggered CDR keeping

Step 1 - In the Verba web interface go to **System / Servers**, select the Recording Server which functions as a Recording Director, and click on the **Change Configuration Settings** tab.

Step 2 - Under the **Unified Call Recorder / Recording Providers / Remote Media Recorders** node, click on the



icon at the **Remote Media Recording Servers** setting.

Step 3 - In the right panel select the remote Media Recorder server at the **Host** setting. Provide the username and password configured in the **Verba Unified Call Recorder Service** on the Recording Server acting as a Media Recorder (**Unified Call Recorder / Media Recorder / Incoming Connection, User and Password**). Set the **Port** to **10500** and set the **Priority**.

Remote Media Recording Servers

Protocol	<input type="text" value="vrp"/>
User	<input type="text" value="verba"/>
Password	<input type="password" value="*****"/>
Host	<input type="text" value="DEVFE1SFB"/>
Port	<input type="text" value="10500"/>
Priority	<input type="text" value="1"/>


Step 4 - Click on the **Save** button at the bottom. If there are multiple remote Media Recorders, then repeat steps 2-4.

Step 5 - Save the changes by clicking on the



icon.

Step 6 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

 There are tasks to be executed regarding the configuration of this Verba Server.
If you would like to execute these tasks now, please [click here](#) .

Step 7 - Start the Verba Unified Call Recorder service on all servers.

Configuring the local Media Recorder

The Recording Director module is always connecting to the local Media Recorder module within the same service, with priority 0.

The Media Recorder module can be turned off by setting the **Media Recorder Enabled** setting to **No** under the **Unified Call Recorder \ Media Recorder \ Basics** node.

Override media recorder selection

AVAILABLE IN 9.5 AND ABOVE

The load balancing and mid-call failover are enabled for turret integrations by default, in some recording scenarios, it is recommended to disable it.

To disable the remote recording for an integration:

Step 1 - In the Verba Web Interface go to **Administration > Verba Servers > Select your Recording (or Single) Server which functions as Recording Director > Click on the Change Configuration Settings** tab.

Step 2 - Under the **Unified Call Recorder \ Recording Providers \ Integration** node and change the **Force Recording Media on Director** to **Yes**.

Step 3 - Save the changes by clicking on the



icon.

Step 4 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

 In case of active/active (2N) recording cross-connecting the services is not recommended, the best practice is to keep the servers independent of each other.

PBX specific high availability options

Although Verba supports both Recording Director and Media Recorder failover, the actual possibilities are highly dependent on the phone system.

Cisco


With the Cisco Unified Call Manager, both the Recording Director (SIP connection) failover and the Media Recorder mid-call failover is possible. The number of the SIP connections is unlimited, and the SIP sessions are independent of the media sessions, therefore the failover of the components can be done independently.

Avaya

Avaya does not support active/passive (N+1) DMCC connection failover, instead, it does active/active (2N) recording. The recording will be started at each connected Avaya Recorder service. The DMCC connections are independent of the media sessions, therefore in case of a DMCC connection problem, the recording won't be interrupted at the corresponding Media Recorders.

BT IPTrade

BT IPTrade supports both active/passive (N+1) and active/active (2N) recording. The media sessions are tied to the SIP connections but can be handled separately. Media Recorder load balancing is possible, but in case of a SIP connectivity problem, IPTrade closes all corresponding ongoing media sessions. Mid-call failover is not possible on the Media Recorder level. Instead, in case of Media Recorder fault, the Recording Director closes the SIP connection, and IPTrade reestablishes all ongoing media sessions with another Media Director (and Media Recorders).

 If TPO recording is utilized, the re-establishment of sessions may cause IP Trade TPO to get stuck and needs a restart to recover. It is highly recommended to use the Force Recording Media on Director described in the Override media recorder selection.

Speakerbus

Speakerbus supports 2N recording only. The media sessions and the SIP connections are tied together and cannot be handled separately. Therefore load-balancing is not possible.

IPC Unigy

IPC Unigy supports 2N recording only. The SIP sessions are independent of the media sessions, so load balancing and mid-call failover are also possible between the Media Recorders.

Broadsoft

Broadsoft supports only one SIP connection, so Recording Director failover is not possible. The SIP session is independent of the media sessions, so load balancing and mid-call failover are also possible between the Media Recorders.

How to pull the server specific settings after the initial installation

During the installation of the first Media Repository (or Combo) server the default configuration profiles are created in the database. These profiles contain the default setting values for all Verba server roles but don't contain the server-specific values.

When installing an additional Verba server or component, the default setting values belonging to the server role is stored in the server registry, plus the server-specific values provided during the installation. These server-specific values have to be copied to the central database, so the configuration in the registry and the database become synced.


Step 1 - Log in to the Verba Web Interface.

Step 2 - Navigate to the **System > Servers** menu.

Step 3 - Select the first server from the list.

Step 4 - Go to the **Change Configuration Settings** tab.

Step 5 - A notification will be shown that there are differences between the server registry and the central database. Choose **Use configuration only from the server's local registry**.

 Configuration differences were found between the central database and the server's local configuration. Please decide how to resolve these differences.

Use configuration only from server's local registry (recommended after initial installation)

Use configuration only from central database (recommended after upgrade/reinstall)

[Show the differences](#)

Start

Cancel

Step 6 - Click **Start**.


Step 7 - Repeat the steps on all Verba servers and components.

Installing an SSL certificate for HTTPS access

Overview

The Verba Recording System comes with a **preconfigured HTTPS port** for web access and **HTTP access can be turned off**.

In order to avoid HTTPS related security warnings when your end-users access the Verba web application you need to **install an SSL certificate**.

 [Generating or purchasing the SSL certificate](#) for your solution is a customer responsibility. Verba can only assist with installation of the certificate.

Steps

Here are the steps to import your SSL certificate (the steps below assume that you have installed the product in the default folder):

 Having .pfx or .p12 file instead of .crt and .key files? Scroll down for the conversion guide.

Step 1 - Copy the new .key and .crt files to the Verba Media Repository server.

Step 2 - Create a backup of C:\Program Files\Verba\tomcat\conf\server.xml

Step 3 - Open the server.xml file with an editor

The SSL configuration is around the 100th line and looks something like this:

server.xml till 9.6.16

```
<Connector
  SSLEnabled="true"
  port="443"
  protocol="org.apache.coyote.http11.Http11AprProtocol"
  clientAuth="false"
  scheme="https"
  secure="true"
  SSLCertificateFile="c:\Verba.crt"
  SSLCertificateKeyFile="c:\Verba.key"
  SSLPassword="verba123456"
  SSLCipherSuite="RC4-MD5:RC4-SHA:AES128-SHA:DHE-DSS-AES128-SHA:DES-CBC3-SHA:DHE-DSS-DES-CBC3-SHA"
  SSLProtocol="SSLv3+TLSv1"
  URIEncoding="UTF-8"
  maxHttpHeaderSize="16384"
 />
```

server.xml in 9.6.17 and later

```
<Connector
  SSLEnabled="true"
  port="443"
  protocol="com.verba.util.tomcat.VerbaHttp11AprProtocol"
  clientAuth="false"
  scheme="https"
  secure="true"
  SSLCertificateFile="c:\Verba.crt"
```

```
SSLCertificateKeyFile="c:\Verba.key"  
SSLPassword="Verba123456"  
SSLCipherSuite="RC4-MD5:RC4-SHA:AES128-SHA:DHE-DSS-AES128-SHA:DES-CBC3-SHA:DHE-DSS-DES-CBC3-SHA"  
SSLProtocol="SSLv3+TLSv1"  
URIEncoding="UTF-8"  
maxHttpHeaderSize="16384"  
</>
```

Change the **SSLCertificateFile**="c:\Verba.crt" to the new .crt file

Change the **SSLCertificateKeyFile**="c:\Verba.key" to the new .key file

Change **SSLPassword**="Verba123456" to the private key's [encrypted password](#).

Optionally add an **SSLCertificateChainFile** setting, and specify the intermediate certificate file.

Step 4 - Restart Verba Web Application Service

Creating .key and .crt files from .p12 or .pfx file

Step 1 - Download the OpenSSL from here: <https://indy.fulgan.com/SSL/openssl-1.0.2g-i386-win32.zip>

Step 2 - Extract the downloaded .zip file and start the openssl.exe

Step 3 - Execute the following commands:

For .p12 files

```
pkcs12 -in yourP12File.p12 -nocerts -out privateKey.pem  
pkcs12 -in yourP12File.p12 -clcerts -nokeys -out publicCert.pem
```

For .pfx files

```
pkcs12 -in yourPfxFile.pfx -nocerts -out privateKey.pem  
pkcs12 -in yourPfxFile.pfx -out publicCert.pem  
x509 -inform pem -in publicCert.pem -pubkey -out publicCert.pem -outform pem
```

When it asks for a password enter the password of the certificate

Step 4 - Change the created privateKey.pem to .key and publicCert.pem to .crt

Encrypt the private key's password

AVAILABLE IN 9.6.17 AND LATER

In the webserver's configuration file the private key's password is stored in an encrypted form. During the software installation, the installer handles the password encryption. However, if the private key's password is changed without upgrading the system, the following process can be used to encrypt the password.

Step 1 - Open a command prompt in the Verba Media Repository server and execute the following command

```
> "C:\Program Files\Verba\bin\pwenc.exe" -t=tomcatssl PRIVATE_KEY_PASSWORD
```

Step 2 - Copy the output result and insert it in the server.xml file as *SSLPassword* attribute value like above

Configuring TLS 1.2

AVAILABLE IN 9.4 AND ABOVE

By default, all Verba services prefer TLS 1.2. For security or compliance reasons, administrators can choose to lock down the TLS version of the Verba system to 1.2, and therefore disable TLS 1.0 and TLS 1.1. This document provides an overview of how to enable TLS 1.2 and disable TLS 1.0 and 1.1 for the Verba product.

Component	How to Configure TLS 1.2
Internal communication between Verba servers and components	<p>Step 1 - Ensure that TLS 1.2 is not disabled on the Verba servers</p> <p>Step 2 - Open the Web Application and navigate to System\Servers and select the server</p> <p>Step 3 - Select the Change Configuration Settings tab, Server Certificate - Advanced TLS Settings node</p> <p>Step 4 - Set Enable TLSv1 and Enable TLSv1.1 to No, and Enable TLSv1.2 to Yes</p> <p>Step 5 - Save the changes and click on the click here link to apply the changes</p>
Additional configuration for the following services: Verba Avaya DMCC/JTAPI Service Verba Cisco Central Silent Monitoring Service Verba Cisco Compliance Service Verba Cisco JTAPI Service	<p>Step 1 - Go to the Java home directory</p> <p>Step 2 - Open the conf/security/java.security or lib/security/java.security (JDK 8 and earlier) file using notepad with</p> <p>Step 3 - Change the <code>jdk.tls.disabledAlgorithms</code> property by appending <code>", TLSv1, TLSv1.1"</code> As an example: <code>jdk.tls.disabledAlgorithms=SSLv3, RC4, DES, MD5withRSA, DH keySize < 1024, \</code> <code>EC keySize < 224, 3DES_EDE_CBC, anon, NULL, TLSv1, TLSv1.1</code></p> <p>Step 4 - Save the changes</p> <p>Step 5 - Restart the impacted Verba Service</p>
HTTPS connection with the Web Application	<p>Follow the instructions on all Media Repository Servers:</p> <p>Step 1 - Go to C:\Program Files\Verba\tomcat\conf</p> <p>Step 2 - Create a backup of the server.xml file</p> <p>Step 3 - Open the server.xml file using notepad with elevated permissions</p> <p>Step 4 - Change the value of the <code>SSLProtocol</code> from "TLSv1+TLSv1.1+TLSv1.2" to "TLSv1.2"</p> <p>Step 5 - Save the changes</p> <p>Step 6 - Restart the Verba Web Application Service</p>
Encrypted SQL Server communication	<p>Follow the information in the following article: https://support.microsoft.com/en-gb/help/3135244/tls-1-2-support-for-</p> <p>To enable encrypted communication with the SQL Server in Verba, follow Configuring encryption for database connecti</p>

Communication between the installer and the Web Application during certificate generation	The installer uses TLS 1.2 by default when requesting certificates from the Verba CA.
Verba Microsoft Teams Bot Service's HTTPS listeners	<p>The TLS 1.0 and TLS 1.1 protocols need to be disabled OS level on the servers hosting the bot service. To disable the TLS Windows follow the instructions:</p> <p>Step 1 - Add the following registries on all bot servers:</p> <pre>[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS_1_0\AcceptedTypes "DisabledByDefault"=dword:00000001 "Enabled"=dword:00000000 [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS_1_1\AcceptedTypes "DisabledByDefault"=dword:00000001 "Enabled"=dword:00000000 [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS_1_2\AcceptedTypes "DisabledByDefault"=dword:00000001 "Enabled"=dword:00000000 [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS_1_0\Server "DisabledByDefault"=dword:00000001 "Enabled"=dword:00000000</pre> <p>The following .reg file contains the above registries and it can be simply run on the servers:</p> <div data-bbox="304 1077 810 1581" style="border: 1px solid black; padding: 20px; text-align: center; width: fit-content; margin: 10px auto;"><p>DisableTLS10-11.reg</p></div> <p>Step 2 - Restart the Verba Microsoft Teams Bot Service</p>

Configuration reference

Accessing the configuration settings

The configuration of the Verba components can be reached by following the steps below:

Step 1 - Point your browser to http://server_ip_address_or_hostname and login to the system by an account with **System administrator** user right.

Step 2 - Navigate to the **System \ Servers** menu item and select the server from the list.


Step 3 - Click on the **Change Configuration Settings** tab.

 Settings of a feature are shown on the Change Configuration Setting tab **only if the corresponding service is activated** on the **Service Control and Activation** tab.

In order to save the changes click on the



icon. A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

 There are tasks to be executed regarding the configuration of this Verba Server.
If you would like to execute these tasks now, please [click here](#) .

Configuration settings

- [Network settings](#)
- [Database Connection settings](#)
- [Directory settings](#)
- [Server Certificate settings](#)
- [Cisco Central Silent Monitoring Configuration settings](#)
- [Cisco JTAPI Configuration settings](#)
- [Verba Unified Call Recorder settings](#)
- [Web application settings](#)
- [CDR and Archived Content Importer settings](#)

Network settings

System

The following table provides detailed instructions on each configuration setting:

Configuration Parameter Name	Description
Server IP Address	IPv4 address of the server. This setting is used to define the proper network interface to use by various Verba Recording System components on the network. This IP address should be accessible by other components of the system in the network. If this setting is not configured, certain services may not start at all.
Server S-NAT /Public IPv4 Address	The IPv4 address of the server is visible from outside the network. This is required in several cases when the recorder has to advertise its external IP address also, so the remote party can connect.
Server IPv6 Address	IPv6 address of the server. If empty, then the IPv4 address will be used. This setting is used to define the proper network interface to use by various Verba Recording System components on the network. This IP address should be accessible by other components of the system in the network. If this setting is not configured, certain services may not start at all.
Server S-NAT /Public IPv6 Address	The IPv6 address of the server is visible from outside the network. If empty, then the corresponding IPv4 setting will be used. This is required in several cases when the recorder has to advertise its external IP address also, so the remote party can connect.
Multi-Tenant Mode	If set to Yes, then the server will be in Multi-Tenant mode. For more information see: Multitenancy
Manage Verba Servers Via HTTP	Node Manager connection can be encapsulated into HTTPS

Recording

The following table provides detailed instructions on each configuration setting:

Configuration Parameter Name	Description
Telephony Gateway IP Addresses	IP addresses of telephony gateways. The recorder services can determine the call directions based on this setting, if the recording service-specific Internal Domain, Number Pattern setting is not set.

Directory settings

The following table provides detailed instructions on each configuration setting:

Configuration Parameter Name	Description
Media Folder	Folder where media files of recorded calls will be saved. Network drives are not supported, because of reliability and performance issues, so please do not use mapped network drives or UNC network drives, use only local folders. Use the browse button to select the proper folder.
Log Folder	The log folder for Verba Recording System applications. Network drives are not supported, because of reliability and performance issues, so please do not use mapped network drives or UNC network drives, use only local folders. Use the browse button to select the proper folder.
Application Folder	The home folder for Verba Recording System applications. DO NOT CHANGE it, unless you explicitly told to do so. Use the browse button to select the proper folder.
Temporary Folder	The temporary folder for Verba Recording System applications. Network drives are not supported, because of reliability and performance issues, so please do not use mapped network drives or UNC network drives, use only local folders. Use the browse button to select the proper folder.

Cisco Central Silent Monitoring Configuration settings

Features

The following table provides detailed instructions on each configuration setting:

Configuration Parameter Name	Description
Silent Monitoring Enabled	Sets whether the silent monitoring is enabled or not.
Whisper Coaching Enabled	Sets whether the whisper coaching is enabled or not.

Settings

The following table provides detailed instructions on each configuration setting:

Configuration Parameter Name	Description
Cisco UCM IP Address(es)	Comma(,) separated list of Cisco Unified Communications Manager servers IP addresses. The application will connect to these servers' JTAPI service provider to establish the CTI connection.
JTAPI User Name	Login name of the user configured in Cisco Unified Communications Manager allows monitoring the recorded phones via JTAPI.
JTAPI User Password	Password of the user configured in Cisco Unified Communications Manager, which monitoring the recorded phones via JTAPI.
Play Tone Setting	Indicates whether the tone needs to be played to the target, to the caller, or both during the silent monitoring session.
Work Folder	Folder where the application stores temporary files. Network drives are not supported, because of reliability and performance issues, so please do not use mapped network drives or UNC network drives, use only local folders. Use the browse button to select the correct folder.
API Port	Sets the incoming API port of the Verba Cisco Central Silent Monitoring service.

Cisco JTAPI Configuration settings

Basics

The following table provides detailed instructions on each configuration setting:

Configuration Parameter Name	Description
Cisco UCM Cluster(s)	
Cisco UCM IP Address(es)	Comma (,) separated list of the IP Addresses of the CUCM servers. All CUCM addresses need to be configured where theCTIManager service is enabled. The system will always use the first address, and fail over to the next one in the list if the primaryCTIManager is down. Only a single CUCM cluster can be configured.
JTAPI User Name	The name of the user configured in the CUCM as an Application user.
JTAPI User Password	The password of the user configured in the CUCM as an Application user.

Cisco UCCX Integration

The following table provides detailed instructions on each configuration setting:

Configuration Parameter Name	Description
Cisco UCCX IP Address(es)	List of IP addresses of Cisco UCCX servers. Master and Slave UCCX servers should be listed in the same row separated by commas (,). Independent UCCX servers should be separated by new lines. For more information, see Cisco UCCX Integration .

Cisco UCCE Integration

The following table provides detailed instructions on each configuration setting:

Configuration Parameter Name	Description
Cisco UCCE PG CTI Server IP(s) and port(s)	
CTI Server Protocol Version	
Peripheral ID	

Genesys Integration

The following table provides detailed instructions on each configuration setting:

Configuration Parameter Name	Description
------------------------------	-------------

Genesys T-Server IP(s)	
Target Genesys Field for Verba Call ID	Verba will attach the Verba Call ID to this Genesys User Data Field.

Advanced

The following table provides detailed instructions on each configuration setting:

Configuration Parameter Name	Description
Service Port	Port number for the service.
Work Folder	Work folder path.
Advanced Recording Rules Enabled	When enabled, the service uses a special XML file for recording rules. For more information, see Advanced Call Recording Rules .


Unified Call Recorder service configuration reference for Cisco network based recording

Configuration Parameter Name	Description
Secondary Recording Service	If set to Yes, the service will be marked as secondary. In this case, the conversations recorded by the service will be hidden by default in the Search menu.

Media Recorder



The following table provides detailed instructions on each configuration setting:

Configuration Parameter Name	Description
Unified Call Recorder \ Media Recorder \ Incoming Connection	
User	The username for authenticating the connection between the local Media Recorder and the Recording Directors.
Password	The user password for authenticating the connection between the local Media Recorder and the Recording Directors.
Priority	Defines the priority of the local Media Recorder to provide weighted load balancing among the configured recorders.
Port	The port number used for the Recording Director connections.
Unified Call Recorder \ Media Recorder \ Basic	
Media Recorder Enabled	Enables the Media Recorder component in the service. If the server is deployed as a Recording Director, this component needs to be disabled.
Automatic Gain Control Enabled	The application automatically controls the gain in the audio file to provide more convenient user experience while listening back recordings
Audio Format	The recorder application will use the selected file format and codec option to store the audio/voice conversations.
Video Format	The recorder application will use the selected file format and codec option to store the video conversations.
Bidirectional /Stereo Recording	Enables creation of dual channel audio files (one channel for calling party, one channel for called party). Certain file format and codec options do not support stereo recording.
Call Timeout (seconds)	Defines the call timeout value in seconds, which is used to terminate the call recording automatically if the last RTP packet is received before this value.
Media Port Range Begin	Defines the beginning of the media port range used by the application to receive RTP streams from the UC platform.
Media Port Range End	Defines the end of the media port range used by the application to receive RTP streams from the UC platform.
Voice Activity Statistics	Enabled silence and talk-over detection.
Unified Call Recorder \ Media Recorder \ Advanced	

Database Cache Folder	The path to the database cache folder without the name of the file. Use the  icon to select the folder.
Skip Calls Without Media	When enabled, the system will not create a database record for calls without any media.
Media Format Fallback Enabled	When enabled, the system is able to fall back to raw stream recording if certain codecs are detected to avoid drastic decrease in quality.
PCM Mixer Buffer Length (milliseconds)	Length of the mixer buffer in milliseconds.
RTP Stream Reorder Buffer Length (packets)	Size of the RTP packet capture/receiver buffer in packets used for RTP packet reordering.
Write XML Metadata	Enables XML-based CDR/metadata file generation, written next to the media files. These files can be used later if the database crashes and cannot be recovered. These files are also used for various integration options.
SSL/TLS Certificate	Path to the SSL/TLS certificate file used for the encryption of the communication between the Media Recorder and the Recording Director components. When the server roles are co-located, both components use the same configuration setting.
SSL/TLS Key	Path to the SSL/TLS key file.
SSL/TLS Key Password	Password for the SSL/TLS key.
Unified Call Recorder \ Media Recorder \ JTAPI Integration	
Cisco JTAPI Integration Enabled	Enables the integration with the Cisco JTAPI Service component.
Cisco JTAPI Services	The IP address or hostname of the Recording Director servers where the Cisco JTAPI Service is enabled. Multiple addresses can be configured.
Unified Call Recorder \ Media Recorder \ Overload Thresholds	
Concurrent Calls	Limitation on the maximum number of calls recorded by the server. When the threshold is reached, the system will notify the Recording Director component to stop assigning calls to the server.
CPU (%)	Limitation on the maximum CPU load (%) on the server. When the threshold is reached, the system will notify the Recording Director component to stop assigning calls to the server.
Network (%)	Limitation on the maximum network load (%) on the server. When the threshold is reached, the system will notify the Recording Director component to stop assigning calls to the server.
Disk Space (%)	Limitation on the minimum free disk space (%) on the server. When the threshold is reached, the system will notify the Recording Director component to stop assigning calls to the server.
Disk Space (mbyte)	Limitation on the minimum free disk space in megabytes on the server. When the threshold is reached, the system will notify the Recording Director component to stop assigning calls to the server.

Recording Providers

The following table provides detailed instructions on each configuration setting:

Configuration Parameter Name	Description
Unified Call Recorder \ Recording Providers \ General	
Internal Domain, Numbers Pattern	Regular expression to describe the internal numbers/domains in the organization. The system uses the setting to identify the direction of the recorded conversation (internal, outgoing, incoming, external).
SIP URI Modification	<p>The following valid value apply:</p> <ul style="list-style-type: none"> • Do not modify SIP addresses - The system will not modify the SIP URIs and will insert the URIs as they appear in the SIP signaling messages to the database. • Remove domain part - The system will remove the domain part from all SIP URIs. E.g. john.doe@contoso.com -> john.doe • Remove domain part for numbers only - The system will remove the domain part for SIP URIs containing a phone number only. Other SIP URIs will not be updated. E.g. +1234778899@contoso.com -> +1234778899
Use Recording Rules	When enabled, the system will only record configured extensions.
Unified Call Recorder \ Recording Providers \ Remote Media Recorders	
Remote Media Recording Servers	<p>List of remote Media Recorders connected to the Recording Director. Click on the  icon to add a new server using the form on the right.</p> <ul style="list-style-type: none"> • Protocol - The protocol used between the Media Recorder and the Recording Director. • User - The user name configured for the connection. It has to match the value configured under Unified Call Recorder \ Media Recorder \ Incoming Connection \ User on the Media Recorder. • Password - The user password configured for the connection. It has to match the value configured under Unified Call Recorder \ Media Recorder \ Incoming Connection \ Password on the Media Recorder. • Host - Hostname of the Media Recorder selected from the list of available Recording Servers. • Port - Port number used for the communication on the Media Recorder. • Priority - Defines the priority of the Media Recorder to provide weighted load balancing among the configured recorders.
Connection Keepalive Interval (seconds)	Keep alive interval in milliseconds between the Media Recorder and the Recording Director.
Unified Call Recorder \ Recording Providers \ SIP/SIPREC	
SIP Port	The port number used for SIP communication. It has to match the value configured at the UC platform.
Secure SIP Ports	<p>Secure SIP ports with custom SSL/TLS certificate options. Click on the  icon to add new secure SIP ports using the form on the right.</p>
Cisco Partition Based Multitenant Processing	When enabled, the system will use the partition information received from the Cisco JTAPI service to identify the tenant. It only works when the JTAPI integration is enabled.
Prefer Session Local Refreshing	SIP keepalive preferred role.
Session Expires Timer (seconds)	SIP session keep alive timer.
SIP Trunk Status Monitoring	When enabled, the system sends alerts if there is no SIP OPTIONS ping request on the SIP trunk.

Web application settings

- [Network](#)
- [Password policy](#)
- [User lockout policy](#)
- [Integrated Windows Authentication \(IWA\)](#)
- [Reporting](#)
- [Active Directory Synchronization](#)
- [Media Utility](#)
- [Recording Announcement](#)
- [HTTP Business API](#)
- [Conference Invitation](#)
- [Provisioning API](#)
- [Secondary Recording Servers](#)
- [Playback](#)
- [Phone Number Masking](#)
- [Miscellaneous](#)
- [Wave formatter settings](#)
- [Recording notification settings](#)

Network

The following table provides detailed instructions on each configuration setting:

Configuration Parameter Name	Description
Verba Web Application HTTP Port	HTTP port of the Verba Web Application server. Changing this parameter does not change the HTTP port on Verba Web Application, but it is used by various Verba Recording System functions. This value shall match the HTTP port set in Verba Web Application server.xml configuration file, which is located under C:/Program Files/Verba/tomcat /conf folder. After changing this file you have to restart the service.

Password policy

Various settings for rules applied to Database Credentials passwords.

The following table provides detailed instructions on each configuration setting:

Configuration Parameter Name	Description
Minimum Password Length	Defines the minimum length of the password fields in the system. The setting applies for all users configured on the web interface.
Passwords Expire after (days)	Defines the number of days, after which the passwords expire in the system. This setting only applies for users where this feature is enabled. 0 means that the password never expires.
Passwords Must Include Capital Letter	Password phrases must include at least one capital letter or not. The setting applies for all users configured on the web interface.

Passwords Must Include Numeric Character	Password phrases must include at least one numeric character or not. The setting applies for all users configured on the web interface.
Passwords Must Include Special Character	Password phrases must include at least one special character or not. The setting applies for all users configured on the web interface.
Password History Count	Defines how many passwords will be stored for each user. Password history prevents users from changing their passwords to ones that they have used in the past. If the value equals to 0, it means that password history is disabled. The setting applies for all users configured on the web interface.

User lockout policy

When enabled the user lockout settings automatically locks users out after a certain number of incorrect Database Credentials login attempts.

The following table provides detailed instructions on each configuration setting:

Configuration Parameter Name	Description
User Lockout Attempts Threshold	The lockout threshold can be set to any value from 0 to 999 (attempts). If the lockout threshold is set to zero, users will not be locked out due to invalid logon attempts. Any other value sets a specific lockout threshold. The setting applies for all users configured on the web interface.
User Lockout Threshold Reset After (minutes)	This value represents how long a user will be locked out after unsuccessfully logging into the system. By default, the lockout threshold is maintained for 30 minutes, but any value can be set from 1 to 99,999 minutes. The setting applies for all users configured on the web interface.

Integrated Windows Authentication (IWA)

The Verba Recording System supports Windows Domain authentication and provides seamless authentication for the web application.

The system also supports custom SSO authentication with 3rd party solutions. For more information, see [Single Sign-On overview](#).

The following table provides detailed instructions on each configuration setting:

Configuration Parameter Name	Description
Strip Domain Information from Login ID	If enabled, the system will not use the Windows domain information during the single sign-on process. Practically it means, that the users - configured in the Verba system - do not contain the domain information in the login ID.
Domain User Account Format	If the Windows domain information is used during the single sign-on process (the Strip Domain Information from Login ID setting is disabled), then the users - configured in the Verba system - have to contain the domain information. This setting allows users to select the way the domain information is stored in the login ID in the Verba system.

Allow Single Sign-On for System Administrators	Enables or disables the single sign-on feature for system administrators. If disabled, the users with system administrator privileges are not allowed to authenticate using the single sign-on functionality.
---	---

Reporting

Configuration settings for the Verba Reporting module.

The following table provides detailed instructions on each configuration setting:

Configuration Parameter Name	Description
Allowed Reporting Interval Start Time	Start time value for allowed reporting time period in hour: minute format.
Allowed Reporting Interval End Time	End time value for allowed reporting time period in hour: minute format.
Scheduled Reports Folder	Directory where the report scheduler service saves reports to.
Enable External Reporting Database	Enable or disable external reporting database. If enabled the system will connect to an external Verba reporting database according to the settings below. If disabled the system will use the default database connection parameters for reporting.
External Reporting Database Name	Name of the database.
External Reporting Database Hostname or IP Address	Hostname or IP address of the external Verba Recording System reporting database.
External Reporting Database User Name	Database user name for reporting database login.
External Reporting Database Password	Database user password for reporting database login.

Active Directory Synchronization

Media Utility

Recording Announcement

HTTP Business API

Conference Invitation

Provisioning API

Secondary Recording Servers

Playback

Phone Number Masking

Miscellaneous

Miscellaneous settings for the Verba Web Application.

The following table provides detailed instructions on each configuration setting:

Configuration Parameter Name	Description
HTTP Access Enabled	HTTP access enabled or disabled in Verba Web Application is enabled. This setting does not have any effect on services (e.g. Verba XML Services), which are available only through HTTP.
Font Setting	The name of the font used on the entire web interface. The following valid values apply: Arial, Arial Narrow, Tahoma, Verdana, etc.
Event Log Purging Threshold (days)	If this value is set to greater than 0, then a process deletes all event log entries older than the defined value on each day. If the value is set to zero, the deletion will be disabled.
Default List Page Size	The number of listed records on one page.
Maximum Active Sessions	Defines the maximum number of simultaneous user sessions for the Verba Web Application. If a new user tries to log in after the value is reached, the user will be rejected. Verba XML service sessions are not counted.
Maximum Query Rows	Sets the maximum number of rows to retrieve in the result set of the call lists (results of the search screen).
Support Site URL	URL of the support site, which is available as a link in the menu of the web interface.
Click2Dial Enabled	Enable or disable Click2Dial feature.
Cisco Unified Communications Manager IP Address or Hostname	IP address or Hostname of the Cisco Unified Communications Manager. This parameter is used in the Click2dial feature.
Video Transcoding Enabled	If this setting is turned on, users are able to initiate video transcoding jobs in the Verba Player. This video transcoding function enables to convert VF (Verba Media Format) files to standard Windows Media Video (WMV) files.
Hide Menu Item(s)	Comma(,) separated list of menu items, which has to be disabled on the web interface.
Record URL Clipboard Copy in Search List Enabled	If this setting is turned on, call lists will include an icon, which allows to copy the URL pointing to the given call to the client computer's clipboard.
Display Alert after Clipboard Copy Disabled	If this setting is turned on, the system will NOT display an alert message if an UTL pointing to a call is copied to the client computer's clipboard.

Publishing Enabled	If this setting is enabled, the users are able to publish and share recordings and other users can access these records through the Verba Publishing Server. The default URL of this server: http://x.x.x.x/verba/pub
Exported Call File Name Format	<p>Defines the filename convention used when the user downloads multiple calls from the user interface. The following variable fields are available:</p> <p>[year] [month] [day] [hour] [minute] [second] [caller] [called]</p> <p>You can also define meta data fields to be added to the file name: [meta_field] where the 'field' part should be the Field Identifier variable configured as a Metadata Template Field.</p> <p>You can use any type of other characters to separate the fields. If this parameter is empty, the default setting is applied: [caller]--[called]_[year]-[month]-[day]_[hour]_[minute]</p>
Enable direct download folder field on export page	Enables the direct download option from the conversation export view.
Conversation export direct download target folder	When the direct download option is used with conversation export, the conversations are first downloaded to the local drive of the Media Repository by default, and then the user can download from there. Using this configuration setting, this can be changed and another temporary location can be selected.
Send License Email Notifications	<p>Determines when license alerts are sent to the administrators. Available Options:</p> <ul style="list-style-type: none"> • Only On Violation • When Approaching the Limit

Wave formatter settings

Configuration settings for the Verba Wave Formatter service.

The following table provides detailed instructions on each configuration setting:

Configuration Parameter Name	Description
Hostname or IP Address of Waveform Service	Hostname or IP address of the Wave Formatter service. It is installed on the Verba Media Repository server by default.
HTTP Port	HTTP port number for accessing the Wave Formatter service.
Sampling Rate	Defines the number of samples used to draw the amplitude of the audio signal. The value is multiplied by the total number of samples in the audio files.
Call Segment Export Codec	Call segments exported are saved using the configured codec.

Recording notification settings

If this feature is enabled then Verba Web Application Server pushes an XML message to the given Cisco phone right after the recording has been started. If the Verba Recording Server cannot reach the Verba Media Repository then this service is not available. All of those IP phones, which receive recording notification messages, must be associated with a Cisco Unified Communications Manager user.

The following table provides detailed instructions on each configuration setting:

Configuration Parameter Name	Description
Recording Notification Display Enabled	Enables or disables the sending of recording notification messages to XML capable IP phones. If this setting is enabled then Verba Web Application Server pushes an XML message to the given phone right after the recording has been started. If the Verba Recording Server cannot reach the Verba Media Repository then this service is not available.
Cisco Unified Communications Manager Push XML User ID	The login name of that Cisco Unified Communications Manager user, which is used to send recording notification messages to XML capable IP phones. All of those IP phones, which will receive these notification messages have to be associated with this user. Alternatively you can enable the Enable CTI Super Provider option for this user (if this option is enabled you do not have to associate the phones to this user).
Cisco Unified Communications Manager Push XML User Password	The password of that Cisco Unified Communications Manager user, which is used to send recording notification messages to XML capable IP phones.
Recording Notification Language	This parameter defines the language used for the recording notification messages. This setting is a global value, the language setting of a given user, does not effect this parameter. Select the desired language from the drop-down list.
Recording Notification Display Timeout	The notification message sent after the recording has been started can be displayed for a given amount of time. This parameter in milliseconds controls this automatic feature. If the value of this parameter less than 0, the notification message is displayed until the user navigates away manually. So, if you would like to disable the automatic deletion of the notification message, enter -1.

CDR and Archived Content Importer settings



General

The following table provides detailed instructions on each configuration setting:

Configuration Parameter Name	Description
Wait Time Between Query Cycles [sec]	If the schedule is set to No Schedule at any of the settings, this setting defines the time interval between the runs.
Internal Domain, Numbers Pattern	Covers all the numbers/number ranges with a regular expression. For example: 842 844 846
Create IM Transcript Files	Yes/No

CDR Import

The following table provides detailed instructions on each configuration setting:

Configuration Parameter Name	Description
Cisco CDR Column Filters	Sets which CDR records should be excluded from the CDR Import. Column names and values can be provided in "column_name:value" format, on at each line. The value is a regex.
Cisco External Device /IP Criteria	Devices to be excluded from the Cisco CDR Reconciliation can be provided in this setting with a regex, so they won't be recognized as a recorded party, even if their extension is added as recorded in the Verba extension list.
SfB UserAgent Filters	Skype for Business User Agent Filters
Import Schedule	Sets the schedule of the CDR Import. The configuration can be changed by clicking on the  icon, then following the wizard in the right panel.
Wait Time for Recorder's CDR [sec]	The CDR Reconciliation won't check the calls which are not older than the time specified in this setting.
Recheck Schedule	Sets the schedule of the CDR Import Recheck. The configuration can be changed by clicking on the  icon, then following the wizard in the right panel.
Number of Days to Recheck Imported Records	Set the number of days to recheck in case of CDR Import Recheck.

Microsoft Teams IM

The following table provides detailed instructions on each configuration setting:

Configuration Parameter Name	Description
------------------------------	-------------

API Version	For example: v1.0
Graph Api Url	For example: graph.microsoft.com

Cloud9 Recording System API

The following table provides detailed instructions on each configuration setting:

Configuration Parameter Name	Description
Audio Transcoder Profile	Audio Transcoder Profile, such as 16 bit PCM in wav, Speex (CELP) in Ogg with silence suppression, Opus in Ogg, etc.

Cloud9 Call Data API

The following table provides detailed instructions on each configuration setting:

Configuration Parameter Name	Description
Maximum Query Page Size	Default: 500
Query Interval [seconds]	Default: 60
Work Folder	Location of temporary data. If not set, the default is: {Verba path} \work\cdrimport\cloud9calldata
Cloud9 Call Data API URL	Default: https://calldataapi.xhoot.com:443
Cloud9 Call Data API Metadata Endpoint	Default: /v1/calls/metadata
Cloud9 Call Data API Recordings Endpoint	Default: /v1/calls/recordings
Delete Metadata from Local Cache After [hours]	Default: 72 (3 days)
Delete Media from Local Cache After [hours]	Default: 72 (3 days)
Initial Query Look Back [days]	Default: 14 (2 weeks)
Minimum Available DiskSpace [MB]	Default: 500. Alert is raised if disc space is less than this setting.
Enable User Filtering	Default: No
Metadata and Media Query Intervals (minutes)	Default: 240 (4 hours)

Query Start Time Compensation for Verba /C9 Time Drift (seconds)	Default: 90
Enable Media Filtering Workaround	Use end time as Call Detail Record create time. Default: Yes

Microsoft Azure Storage

The following table provides detailed instructions on each configuration setting:

Configuration Parameter Name	Description
Connection timeout (ms)	Default: 300000 (5 minutes)
TLS Key password	
TLS Key file	
TLS Certificate	
TLS CA Certificate	
Forward Proxy Address	
Forward Proxy Port	
Forward Proxy Username	
Forward Proxy Password	

Zoom Phones

The following table provides detailed instructions on each configuration setting:

Configuration Parameter Name	Description
API Lookback safety margin for imports in minutes	Extend the query interval backward in time this much before the last seen import. Phones APIs can not be queried by archiving time, and calls might not end in the order they are archived. This parameter makes sure no calls are missed because of that. Set to the expected maximum time it takes for Zoom to archive a call. Smaller values increase the risk a call might be missed, larger values slightly increase API load.
Worker Thread Count	The maximum number of (per policy) threads to parallelly download media. If set higher than the thread count of the underlying server's CPU, will limit to thread count. Low values like 1 will make download slightly less efficient. High values (4+) will not increase download speed as its fundamentally limited by bandwidth, not threads. Recommended values: 2 - 8
Give Up Timeout In Minutes	Minutes of time after which the service will abandon a failed import's daily re-try attempt. 1440 minutes = 1 day. Set to less than minimum of Zoom side archiving retention or meetings and phones calls, but more than 2 days. Recommended values 5,760 (4 days) - 14,400 (10 days)
Working Directory	Working Directory

Zoom Api Remaining Rate-Limit Threshold For Alerting	Number or remaining Zoom API calls in the daily limited APIs before a warning alert is sent. Recommended to set to a value that will warn you in time to take actions, 10%-30% of your total daily limit (please note this config should NOT be set to percent, but absolute value). If daily API limit is reached, import will continue from next day and no data will be lost. If daily limit is reached every day, data loss eventually will.
Reconciliation delay behind Import in minutes	Time in minutes that needs to pass between an interaction's end and its import's current progress for reconciliation to consider it. In other words: Reconciliation ignores everything that ended after import's current progress minus this value in minutes. It prevents reconciliation from producing false positives by processing events before they get archived by Zoom. Should be set to the lowest value possible that is strictly bigger than the time it takes for Zoom to archive an interaction. Too low value causes false positive alerts, too high value causes slow reaction of reconciliation for true positive cases. Recommended values: 15 - 90

Zoom Meetings

The following table provides detailed instructions on each configuration setting:

Configuration Parameter Name	Description
Maximum Number Of Entries To Import	Maximum number of meetings archiving / meeting logs to paginate in a single import interval. It does not affect the number of imports in an import cycle (single run of the policy), it only limits memory use. Low values will make API use inefficient, very high values will cause high memory use and potentially timeouts. Recommended values are 300 - 3000.
Worker Thread Count	The maximum number of (per policy) threads to parallelly download media. If set higher than the thread count of the underlying server's CPU, will limit to thread count. Low values like 1 will make download slightly less efficient. High values (4+) will not increase download speed as its fundamentally limited by bandwidth, not threads. Recommended values: 2 - 8
Give Up Timeout In Minutes	Minutes of time after which the service will abandon a failed import's daily re-try attempt. 1440 minutes = 1 day. Set to less than minimum of Zoom side archiving retention or meetings and phones calls, but more than 2 days. Recommended values 5,760 (4 days) - 14,400 (10 days)
Working Directory	Working Directory
Zoom Api Remaining Rate-Limit Threshold For Alerting	Number or remaining Zoom API calls in the daily limited APIs before a warning alert is sent. Recommended to set to a value that will warn you in time to take actions, 10%-30% of your total daily limit (please note this config should NOT be set to percent, but absolute value). If daily API limit is reached, import will continue from next day and no data will be lost. If daily limit is reached every day, data loss eventually will.
Reconciliation delay behind Import in minutes	Time in minutes, that needs to pass between an interaction's end and its import's current progress for reconciliation to consider it. In other words: Reconciliation ignores everything that ended after import's current progress, minus this value in minutes. It prevents reconciliation from producing false positives by processing events before they get archived by Zoom. Should be set to the lowest value possible that is strictly bigger than the time it takes for Zoom to archive an interaction. Too low value causes false positive alerts, too high value causes slow reaction of reconciliation for true positive cases. Recommended values: 15 - 90
Participant Cache TTL (minutes)	Participant Cache TTL (minutes)

Verint Ingestion

The following table provides detailed instructions on each configuration setting:

Configuration Parameter Name	Description
Remove Trailing Mac Address from extensions	Default: No
Delete Metadata from Local Cache After [minutes]	Default: 1440 (one day)
Sleep Time Between Metadata Cleanups for Local Cache [minutes]	Default: 60 (one hour)

Cisco Webex Teams

The following table provides detailed instructions on each configuration setting:

Configuration Parameter Name	Description
Maximum number of events per cycle	Limits how many Cisco Webex Teams events can the service process per import cycle. These events can be message events or leave/join events. Minimum value for this setting is 100, maximum is 1000.
User Cache TTL (hours)	Default: 24
Room Cache TTL (hours)	Default: 24
Participant Cache TTL (hours)	Default: 6

Generic Import

The following table provides detailed instructions on each configuration setting:

Configuration Parameter Name	Description
Maximum metadata file size [MB]	Sets the maximum valid metadata size. Default: 100
Use given URL only to find media files	This setting has an effect when a media URL provided in the input file is not pointing directly to the location of the media file. If No is set (default), then further searches are performed in the subdirectories for the media file. To speed up the processing of csv files that have incorrect media URLs or does not have any media file given, set this to Yes. In this case, the service does not perform additional searches for the missing media files.

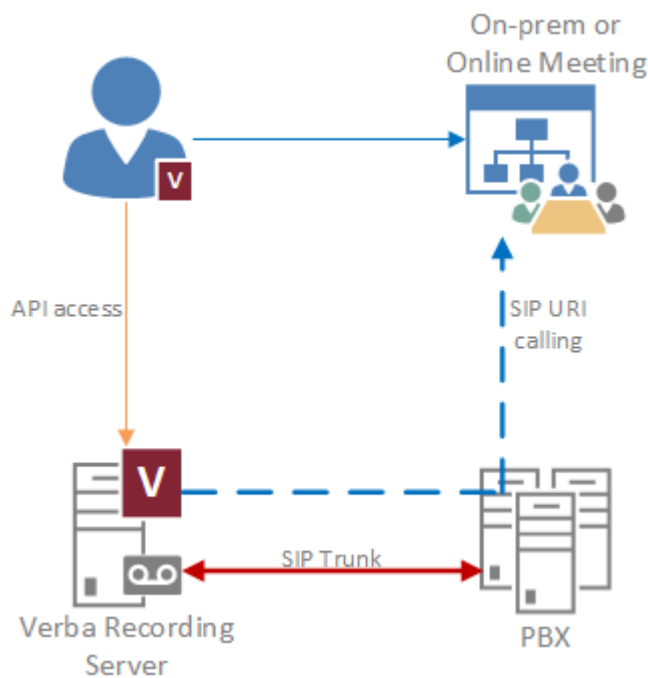
Verba Dial-out Recording

Besides handling incoming calls and providing an IVR for feature access, the Verba Dial-in Recorder service is also capable of actively initiating calls, so it can act as a dial-out recorder for meeting recording.

Once the Verba Dial-in Recorder service is connected to the PBX system with a SIP Trunk, or logged in as a 3rd party endpoint, it can be commanded by its API to initiate outgoing calls.

With the dial-out recorder solution, any kinds of meetings (Cisco CMS, Webex, etc.) can be dialed, if the meeting has a callable line number or SIP URI.

The Verba dial-out recorder solution cannot provide DTMF PIN codes for authentication while joining into the meetings.



Prerequisites

A SIP Trunk has to be set up between the Verba Recording Server and the PBX. For more information, see:

Cisco: [Create and configure a SIP Trunk](#)

Skype for Business / Lync: [Configuring Microsoft Lync for dial-in recording](#)

Configuring Verba for Dial-out Recording

Stage 1 - Turn off the Advanced API Security

Step 1 - In the Verba Web Interface go to **System > Servers > Select your Media Repository (or Single) Server > Click on the Change Configuration Settings** tab.

Step 2 - Expand the **Server Certificate** node.

Step 3 - Set the **Enable Advanced API Security** setting to **No**.

Step 4 - Save the changes by clicking on the



icon.

Step 5 - Repeat **Step 1 - 4** on all the Verba server nodes.

Step 6 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

There are tasks to be executed regarding the configuration of this Verba Server. If you would like to execute these tasks now, please [click here](#) .

Step 7 - The **Verba Node Manager Agent** service has to be restarted manually on all the servers using remote desktop.

Stage 2 - Configure the Verba Dial-in Recorder service

Step 1 - In the Verba Web Interface go to **System > Servers > Select your Recording (or Single) Server > Click on the Service Activation** tab.

Step 2 - Activate the **Verba Dial-in Recorder Service** by clicking on the



icon.

Step 3 - Click on the **Change Configuration Settings** tab.

Step 4 - Expand the **Dial-in Recorder \ Recording** node.

Step 5 - Set the **Endpoint emulation** setting to **General Video Endpoint**.

Step 6 - Save the changes by clicking on the



icon.

Step 7 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

There are tasks to be executed regarding the configuration of this Verba Server. If you would like to execute these tasks now, please [click here](#) .

Step 8 - Click on the **Service Control** tab.

Step 9 - Start the **Verba Dial-in Recorder Service** by clicking on the



icon.

Acting as an endpoint instead of using SIP Trunk

Instead of using a SIP Trunk, the Recording Server also can be used as a 3rd party endpoint. After the Recording Server was added as a 3rd party phone device on the PBX side, the following settings are required:

- Registries:
 - HKLM\SOFTWARE
 - HKLM\SOFTWARE
- Service Configuration:
 - Dial-in Recorder \ SIP \ SIP User: The login address of the user created for the recorder.
 - Dial-in Recorder \ SIP \ SIP User Password: The
 - Dial-in Recorder \ SIP \ Register as client: Yes.

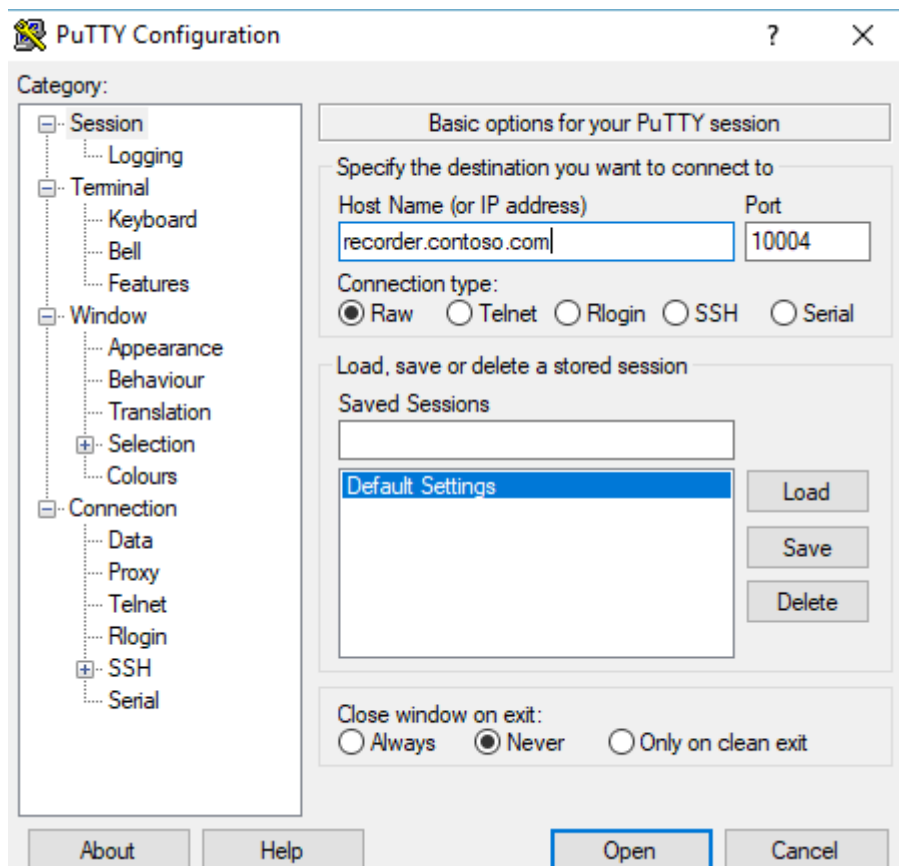
Using the Verba Dial-out Recording

The Verba Dial-in Recorder service can be controlled through its API. For the API access, any kind of client could work. In our example, we are using PUTTY.

Step 1 - Start the PUTTY application.

Step 2 - Provide the **hostname or the IP address** of the Recording Server, and the **port 10004**.

Step 3 - Set the **Connection type** to **Raw**, and set the **Close window on exit** setting to **Never**.



Step 4 - Click **Open**.

Step 5 - The recorder can be commanded by the following API call for initiating an outgoing call:

```
<?xml version="1.0" encoding="UTF-8"?>
<VerbaApi>
  <Request type="StartDialOutRecording" id="0" persistent="0">
    <CallId>random_guid</CallId>
    <From>sip:recorder_number@cucm_ip</From>
    <To>sip:meeting_sip_address</To>
  </Request>
</VerbaApi>
```

Step 6 - The recorder can be commanded by the following API call for hanging up the outgoing call:

```
<?xml version="1.0" encoding="UTF-8"?>
<VerbaApi>
  <Request type="StopDialOutRecording" id="0" persistent="0">
    <CallId>sip_call_id</CallId>
  </Request>
</VerbaApi>
```

Configuring IP-based Radio Recording

Verba can record several radio dispatch centers or radio gateways which are capable of sending a copy of the radio channels in RTP format to the Verba Recording Server over IP. The recording was tested with the following solutions:

- Bosch Telex IP-223
- [Motorola / TwistedPair WAVE](#)
- Avtec Scout

Configuring Verba for IP-based Radio Recording

Once the RTP ports are configured on the radio dispatch / gateway side, the **Verba Analogue and Radio Recorder Service (Verba General Media Recorder Service)** in the older versions of Verba) has to be configured:

Step 1 - Create a new recordingchannels.xml file in the C:\Program Files\Verba\setting folder. You can download the sample from [here](#).

Step 2 - To configure the channels for recording, add the lines to the recordingchannels.xml file according to the configuration on the radio dispatch / gateway side.

Attribute	Description
Channel	
type	The type of the channel. The options are "telex_roip" or "voip".
id	Unique ID for the channel. Can be anything.
eid	The Verba tenant environment ID for the channel. Required only in the case of multi-tenant Verba deployment.
Caller / Called	
id	The ID of the caller / called. This field will populate the "From" or "To" (phone number) fields of the record.
name	The name of the caller / called. This field will populate the "From Info" or "To Info" fields of the record.
multicast	The multicast IP address of the recorder. Required only in the case of multicast listening.
port	The incoming port for the channel. In the case of single-channel RTP recording, the caller and called ports are the same.
codec	The codec of the incoming RTP stream. The options are "G726_32", "VOX" or "DVI4". Required only in the case of Bosch Telex recording.

Step 3 - Fill in the properties of the channels and save the file.

Step 4 - Log in to Verba and go to the **System \ Servers**, select your server, click on the **Service Activation** Tab, and activate the **Verba Analogue and Radio Recorder Service** by clicking on the



icon.

Step 5 - After activating the service click on the **Change Configuration Settings** Tab and scroll to the service's node and configure the incoming port range according to the configuration in the recordingchannels.xml file:

▲ Analogue and Radio Recorder

▶ Recording

▲ VoIP channels

RTP port range begin:

20001

RTP port range end:

20010

▶ Analog channels

▶ Advanced

Step 6 - Save the changes by clicking on the



icon.

Step 7 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.



There are tasks to be executed regarding the configuration of this Verba Server.
If you would like to execute these tasks now, please [click here](#) .

Spet 8 - Click on the **Service Control** tab, and start the **Verba Analogue and Radio Recorder Service** by clicking on the



icon.

Verifying System Readiness

Once Verba is completely configured, the last step before going into production is testing the readiness of the system. This involves the testing of several components. Only those components have to be tested which are being used.

Verifying Server Connectivity and Service Statuses

Using the central management interface, the Verba Web Application, all Verba components, and their configuration should be accessible. The easiest way to verify the connectivity and the status of the Verba services, is via dashboards:




Step 1 - Log in to the Verba Web Interface, and go to the **Reports \ Dashboard \ Create Dashboard** menu.

Step 2 - Select **System Dashboard**.

Step 3 - Click on the **Create** button.

Step 4 - Check the server list in the **Server Status** widget.

Server Status

Server	Role Name	Description
 TESTFE1SFB.VERBATEST.LOCAL	Lync Filter	
 TESTFE2SFB.VERBATEST.LOCAL	Lync Filter	
 TESTMR4.VERBATEST.LOCAL	Media Repository	

Step 5 - In the case of an Error, check the connectivity to that server.


Step 6 - In the case of a Warning, hover the cursor on that server in the list, and a popup will show the stopped services on the server.

Verifying Unexecuted Tasks

There should be no unexecuted configuration tasks, otherwise, the system will use outdated configuration information. The tasks can be verified by the following steps:

Step 1 - Log in to the Verba Web Interface, and go to the **System \ Servers** menu.

Step 2 - On the top, there should be no yellow notification banner like this:

 There are tasks to be executed regarding the configuration of this Verba Server.
If you would like to execute these tasks now, please [click here](#) .

Step 3 - If there is a yellow notification banner, then click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

Step 4 - Go to the **Users \ Users** menu.

Step 5 - Look for the same yellow notification banner, and execute the changes if needed.

Verifying System Monitoring and Alerting

For the complete monitoring guide, see: [System Monitoring](#)

The alerting settings can be found in every server configuration under the **System Monitoring** and **Database Monitoring** node. The settings should be reviewed before going into production.

Verifying the Disk Space Monitoring

Step 1 - Log in to the Verba Web Interface, and go to the **System \ Servers** menu.

Step 2 - Select a server from the list.

Step 3 - Go to the **Change Configuration Settings** tab.

Step 4 - Review the settings under the **Directories** node. If there is any setting that points to a drive other than the C:\ drive, then that drive should be set up for disk space monitoring in the following steps.

Step 5 - Expand the **System Monitoring** node.

Step 6 - If there was any setting at Step 4 that pointed to a drive other than the C:\ drive, then those should be configured under the **Low Disk Space Monitoring - 2nd Disk Volume** or **Low Disk Space Monitoring - 3rd Disk Volume** settings.

Step 7 - Expand the **Low Disk Space Monitoring - #nd Disk Volume** setting.


Step 8 - Provide the letter of the drive to be monitored at the **Volume Path** setting (eg.: "D:\", "E:\")

Step 9 - Repeat steps 5-8 for every drive found configured at step 4.

Step 10 - Save the changes by clicking on the **Save** button on the top.

Step 11 - Repeat steps 2-10 for every Verba server node.

Step 12 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

 There are tasks to be executed regarding the configuration of this Verba Server.
If you would like to execute these tasks now, please [click here](#) .

Verifying the Alerting

Verify the alerting settings based on the monitoring method that is used:

- [Configuring email alerts](#)

- [Configuring SNMP Alert Traps](#)
- [SCOM Management Pack](#)

The alerting can be tested with the following steps:

Step 1 - Log in to one of the Verba servers via remote desktop.

Step 2 - Open the **Services** console.

Step 3 - Stop one of the Verba services (other than the Verba System Monitor Service).

Step 4 - Within a minute, the Verba System Monitor Service will notice that the service is stopped. It will send out a **Service DOWN** alert, and try to start the service. After the successful start, it will send out a **Service UP** alert.

Step 5 - Verify if the alerts arrived.

Verifying Active Directory Integration

Active Directory integration is a crucial part of the Verba deployment. A misconfigured AD integration can result in recording loss. The integration can be verified by the following steps:

Step 1 - Log in to the Verba Web Interface and go to the **Users \ Active Directory Synchronization** menu.

Step 2 - Select a synchronization profile from the list.

LDAP:

Step 3 - Verify the AD connection related settings under the **Active Directory Information** section.

Step 4 - Verify the filters at the **LDAP User Search Base** and the **AD Search Filter** settings.

Step 5 - Click on the **Test Connection** button at the bottom. It should retrieve the users from the AD successfully.

Azure AD:

Step 3 - Verify the AD connection related settings under the **Azure AD Information** section.

Step 4 - Verify the filter at the **User Search Filter** setting.

Step 6 - Repeat the steps for all synchronization profiles.

Verifying the integration with the UC environment

Verifying the Ethical Wall Functionality

If configured, the Ethical Wall features should be tested before going into production. The testing should involve the following Ethical Wall features:

- Presence blocking
- Session blocking
- Disclaimers
- Content filtering
- Notifications

For the complete guide, see: [Ethical Wall Guide](#)

Verifying the Recording Functionality

The verification of the recording functionality should involve several test cases in order to ensure the complete recording coverage before going into production. The following things should be tested:

- All recorded modalities
- All call scenarios
- All 3rd party devices
- Any special recording features configured (Announcement, Call Blocking)
- Failover scenarios
- Contact Center integration (if configured)
- Desktop Agent features (if configured)

In the case of import type of integrations, only the recorded modalities and the failover scenarios have to be tested.

Verifying the Data Management Policies and the Playback

Once the recording functionality is tested, the call retrieval can be checked in the **Conversations \ Search** menu. If the playback works, that means that the Upload policy(es) is also working correctly.

Verifying Storage Target Connectivity

Storage targets can be tested by moving / exporting a test call to them. This test can be done by the following steps:

Step 1 - Make a test call.

Step 2 - Log in to the Verba Web Interface and go to the **Conversations \ Search** menu.

Step 3 - Select the test call, and open the call details.

Step 4 - Take a note of the **Conversation Identifier** property.

Step 5 - Go to the **Data \ Data Management Policies** menu.

Step 6 - Click on the **Add New Data Management Policy** link in the upper right corner.

Step 7 - Provide a **Name**.

Step 8 - Select **Move Media or Export** at the **Action** setting based on the capabilities of the storage target to be tested.

Step 9 - Select the storage target to be tested at the **Destination Storage Target** setting.

Step 10 (Optional) - Set the scheduling setting under the **Scheduling** section.

Step 11 - Under the **Data Management Filtering Criteria** section, add a new **Conversation Detail Fields** filter by clicking on the



icon.

Step 12 - At the field select **Media File Name**, at the operator select **Starts with**, and in the value provide the conversation identifier.

Step 13 - Click **Save**.

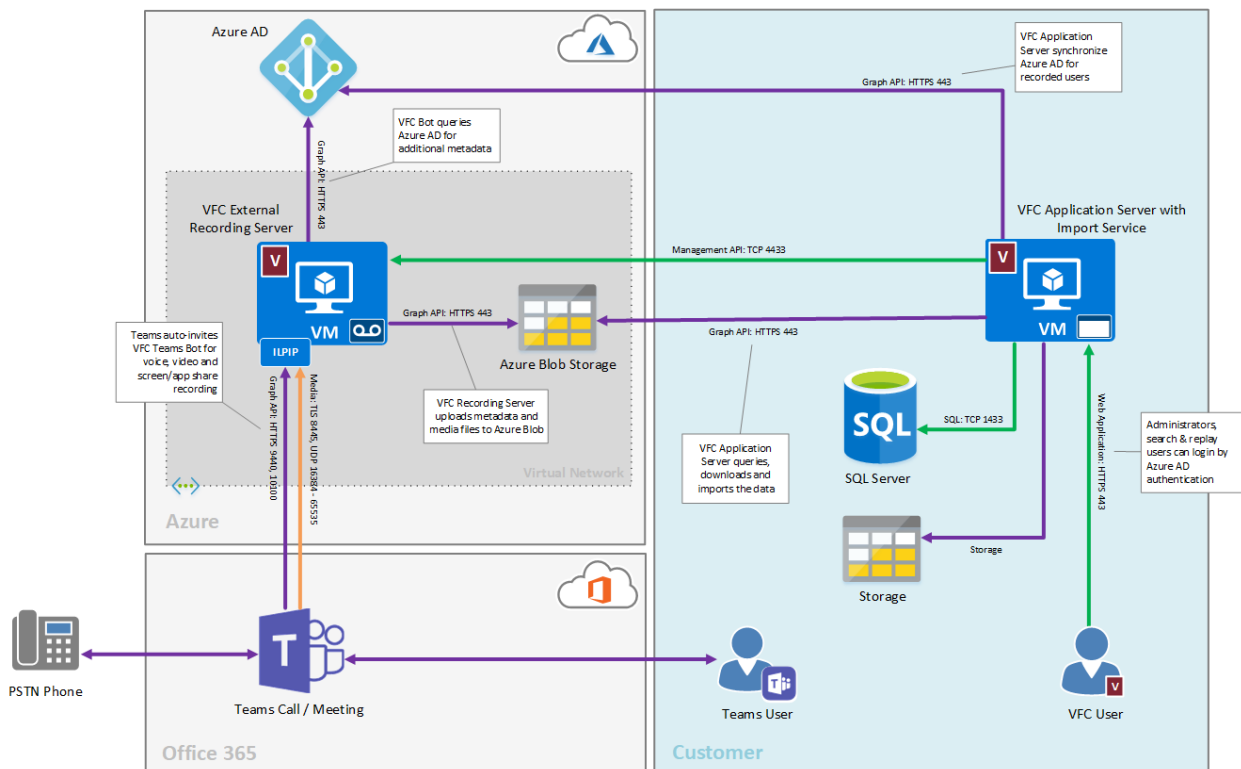
Once the new Data Management Policy moved / exported the test call to the new location (based on the scheduling setting), the location of the files should be verified. If the storage target supports playback, then the playback also should be verified. Repeat the steps for all configured storage targets.

Installing and configuring an external Recording Server

- [Overview](#)
- [Installing an external Recording Server](#)
- [Configuring an external Recording Server](#)
 - [Firewall configuration](#)
 - [Server configuration](#)
 - [Registering the server in the database](#)
 - [Enabling the external server mode](#)
 - [Configuring the integration specific settings](#)
 - [Configuring the Storage Management Service](#)
 - [Configuring the System Monitoring Service](#)
- [Configuring the Import Service](#)

Overview

External Recording Servers can be deployed in environments where the connection between the Recording Servers and the rest of the recorder infrastructure (database server, storage, application servers, etc.) is limited by strict security and firewall rules. A typical use case (shown in the diagram below) is when a hybrid architecture is deployed with components on-premise and in the cloud. In that case, customers want to restrict the communication to be initiated from the on-premise components only and the components in the cloud cannot open a communication channel at all. This requires changing the communication between the cloud and the on-premise components from a push to a pull approach. Normally, the services on the Recording Server connect directly to the database server and the storage infrastructure to insert and upload the data (pushing the data) directly from the Recording Server. The external Recording Server configuration allows uploading both the metadata and media to temporary storage (e.g. Azure Blob Storage) and using the on-premise components to download and add the data (pulling the data) to the on-premise recorder infrastructure.



A system will work in the following way when external Recording Servers are deployed:

- The recorder services (Unified Recorder Service, Passive Recorder Server, etc.) do not attempt to write the metadata to the database during recording. The services create the metadata XML files on the disk as in the normal mode.

- The Storage Management Service uses the local configuration to upload the data (media + metadata files) to a preconfigured storage target (any SMB storage medium or Azure File/Blob storage accessible from the cloud)
- On the on-premise Application Servers (Media Repositories), the Import Service downloads (media + metadata files) and import the data from the cloud storage target.
- On the on-premise Application Servers (Media Repositories), the Storage Management Service uploads the media files to the final storage target, just like the Storage Management Service does on an on-premise Recording Server.

Using external Recording Servers have the following limitations:

- Since the database records are only inserted after the recording is finished and the data is downloaded and imported, features related to ongoing calls are not available:
 - No ongoing recordings
 - No on-demand recording
 - No controlled recording
 - No silent monitoring
- Data management policies cannot be applied to the external Recording Server, the Storage Management Service can only support uploading all data to the pre-configured storage target.
- Encryption and signing can be optionally configured.
- Upload related features, such as retention period configuration, and voice quality checks are not supported on the external Recording Server. However, these features can be enabled once the data is imported.
- Alerts cannot be directly inserted into the database (via the database API on the Application Servers/Media Repositories), instead, the alerts can be uploaded to the cloud storage target and imported by the Import Service in the same way as recordings. Alternatively, other alert targets can be used such as SMTP, SNMP.
- Shared server configurations are not supported

Installing an external Recording Server

Follow the installation instructions for a standard Recording Server, explained at [Installing a Verba Recording Server](#), and review the differences listed below:

- When prompted for the **SQL Server Connection**, uncheck the **Enable SQL Server connection** setting which will disable the SQL Server connection on the server.
- When prompted for the **Server Certificate**, you cannot generate a certificate using the Application Server/Media Repository because usually there is no connection with the Web Application. Instead, the server certificate has to be generated in advance and uploaded to the server manually before the installation runs.
- When prompted for the node registration, check the **Skip API user check** option to skip the server registration into the database.

Configuring an external Recording Server

Firewall configuration

Follow the instructions of the firewall configuration guides applicable for the required integration(s). For instance, for Microsoft Teams recording, see [Firewall configuration for Microsoft Teams recording deployments](#).

Review the port requirements as follows:

- External Recording Serves do not connect to the SQL Server
- External Recording Servers do not connect to the on-premise storage infrastructure, only to the temporary cloud storage (e.g. Azure Blob Storage)
- External Recording Servers do not use the database API on the Application Servers/Media Repositories
- The Management API (Node Manager) port (TCP 4433) must be open on the external Recording Servers so it can be managed through the Web Application (server and service configuration, extension/recording rule configuration)
- All integration-related ports must be allowed

Server configuration

Registering the server in the database

After completing the installation, the new external Recording Server has to be added to the database so it can be managed from the Web Application (normally this step is automatic during the installation):

Step 1 - Open the Verba Web interface, go to **Configuration / Servers**, then click on the **Add New Verba Server** link on the top right

Step 2 - Enter the required information, make sure the hostname contains the FQDN of the external Recording Server which is accessible from the Application Servers / Media Repositories

Step 3 - Press **Save** to add the server.

Enabling the external server mode

After completing the server registration, the external server mode has to be enabled:

Step 1 - Open the Verba Web interface, go to **Configuration / Servers**, then select the new external server from the list

Step 2 - Click on the **Change Configuration Settings** tab and navigate to **System / External Recording Server** and set it to **Yes**

Step 3 - Save the changes by clicking on the



icon.

Step 4 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

Configuring the integration specific settings

Follow the instructions of the integration guides to enable and configure the required integrations on the server.

Configuring the Storage Management Service

Since the data management policies cannot be used on external Recording Servers, a service level upload has to be configured to allow moving the data to the temporary storage target.

Step 1 - Open the Verba Web interface, go to **Configuration / Servers**, then select the new external server from the list.

Step 2 - Click on the **Change Configuration Settings** tab and navigate to **Storage Management / Upload**.

Step 3 - Verify that the **Policy Based Uploading Enabled** setting is set to **No**.

Step 4 - Select the type of storage target which will be used for the upload under **Non-Policy Based Upload Target**. Note: not all types of storage targets are supported for non policy based upload.

Step 5 - Optionally, configure encryption and/or signing for the files under **Non-Policy Based Upload File Encryption Certificate** and **Non-Policy Based Upload File Digital Signature Certificate**. You need to configure the thumbprint of the certificates which are already configured in the system. The certificates must be uploaded to the Windows Certificate Store of the external servers. The import process will recognize the thumbprint information and store it in the database records accordingly. For more information, see [Encryption and integrity protection](#).

Step 6 - Under **Storage Targets** configure the upload target you want to use for the upload. This is the storage target that will be used to import the data. Make sure you have the right storage target type selected in Step 4.

Step 7 - Save the changes by clicking on the



icon.

Step 8 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

Configuring the System Monitoring Service

When the external mode is enabled, the System Monitor service does not insert the alerts into the database. Alternatively, the alerts can be uploaded and imported the same way as recordings:

Step 1 - Open the Verba Web interface, go to **Configuration / Servers**, then select the new external server from the list.

Step 2 - Click on the **Change Configuration Settings** tab and navigate to **System Monitoring / API Connection**.

Step 3 - Set the **Upload Alerts** setting is to **Yes**.

Step 4 - Save the changes by clicking on the



icon.

Step 5 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

Configuring the Import Service

In order to download and insert the data into the recorder infrastructure, an import source has to be created pointing to the temporary storage target which is used in the upload configuration on the external Recording Server.

Follow the instructions for creating a Verba import source that is able to import the uploaded data. For more information, see [Verba Conversation Import](#).

Conversation direction detection using internal domain and number patterns

Overview

This feature allows proper call direction detection for recordings. It is essential when call direction is used in recording rules. By using a simple pattern (regular expression), the system is able to distinguish internal and external participants and set the call direction properly.

The following call directions are available:

Call Direction	Description
Internal	Both participants are a match for the defined pattern
External	Neither of the participants is a match for the defined pattern
Incoming	Only the called party is a match for the defined pattern
Outgoing	Only the caller party is a match for the defined pattern

Internal Domain, Numbers Pattern Configuration

The configuration is available for multiple services. Refer to the corresponding configuration guide for more information.

All settings should contain the same pattern. Otherwise, it can lead to missing recorded conversations when "Recorded Directions" condition is set as something different than "all".

Example Patterns

For regular expression language please refer to [https://msdn.microsoft.com/en-us/library/az24scfc\(v=vs.110\).aspx](https://msdn.microsoft.com/en-us/library/az24scfc(v=vs.110).aspx).

To check and validate your regular expressions, you can use: <http://www.regexr.com/>.

Example domains, numbers:

- 1{DID}@128.144.122.12
- 12143221234@128.144.122.12
- some_extension_name@128.144.122.12:5080
- other_extension_name@voip.example.com
- extension_name@123456_subaccount
- {DID}@123456_subaccount

Example Description	Example Pattern
Match your domain	.*@yourdomain\.com
Match SIP URI that starts with "verba" plus one or more characters and ends with "@yourdomain.com"	verba(\w+)@yourdomain\.com

Match extension name that starts with "ext" plus one or more characters and ends with "@128.144.122.12:5080"	ext(\w+)@128\.144\.122\.12:5080
Match one digit numbers	[0-9]
Match four digit numbers	[0-9]{4}
Match numbers that start with 1213 and has one or more numbers at the end	1213[0-9]+
Match numbers that start with +1213 and has one or more numbers at the end	\+1213[0-9]+
Match numbers that start with 1213 and has 3 additional numbers at the end	1213[0-9]{3}
Match optional + sign at the beginning of a number	\+*1213
Multiple conditions, match numbers that start with +12 or +13 plus one or more numbers at the end	\+(12 13)[0-9]+
Multiple conditions, SIP URI / numbers	.*@yourdomain\.com 1213[0-9]+
Multiple conditions, multiple numbers	1213 1214 1215

Configuring voice activity detection and call splitting for trader voice recording

Trader voice recording has unique characteristics which require additional configuration when deploying a real time trader voice recording integration. These features allow a more efficient way of recording trader voice calls and potentially save on the cost of the infrastructure required for the deployment.

Voice Activity Detection (VAD) is an important feature of trader voice recording. VAD allows the recorder to detect voice activity and only record when a configured volume threshold (in decibels) is reached in the recorded audio. VAD is enabled by default for all trader voice recording integrations. It is not recommended to disable this feature, because certain call types, such as open lines, are continuously recorded while there is no continuous voice activity and the system would generate a lot of data (silence) unnecessarily.

Call Splitting is another important feature of trader voice recording. Certain call types, such as open lines, are very long calls that usually start automatically when the trader logs into the turret and only end when the trader logs out (there are use cases where the traders don't log in and out at all, and these calls are on for days). In order to allow a convenient search, playback, and export user experience for these calls, the system can automatically split the calls using a timer which will produce shorter calls (e.g. an hour-long call instead of a days-long call). The call segments will have identical metadata, except the start and end date and time values. The system provides 2 types of timers:

- **Absolute:** the absolute timer defines the time elapsed from the hour. For example, configuring a 15 minutes timer when the call has started at 03:18 will result in records that have a starting time at 03:30, 03:45, 04:00, 04:15, etc.
- **Relative:** the relative timer is from the start of the call. For example, configuring a 15 minutes timer when the call has started at 03:18 will result in records that have a starting time at 03:33, 03:48, 04:03, 04:18, etc.

2N recording considerations

If the trader voice recording is configured with active-active (2N) high availability, and [Deduplicate Recordings policy](#) is required, absolute splitting is recommended. The relative splitting is based on the recording start, and it may create recording pairs that are not possible to match.

VAD and call splitting also allow a useful feature called **Do Not Keep Openline CDRs Without VOX Activity** which means that the system will not create CDR-Only records for open lines when there was no media activity at all for a call segment. A call segment means a call that was split using the call splitting timer. Without this feature, the system creates CDR-Only records for open lines based on the call splitting timer configuration regardless if there was call activity or not. This can lead to creating a very large number of CDR-Only records in the system (because the open lines can be on for a very long time, see above) unnecessarily.

General settings

The following settings are applied to all integrations. You can find these settings under **Unified Call Recorder / Media Recorder / Media Processing / Voice Activity Detection (VAD)**.

Configuration Setting	Description	Default Value
Minimum Voice Length (milliseconds)	The minimum length for a media record to be recorded by the service.	80
Maximum Silence Length (milliseconds)	Length of silence in media records before closing the record with voice inactivity.	5000
Volume Threshold (dB)	Sets the volume difference at which recording starts.	40

CDR Trigger Adjustment (milliseconds)	Defines the window of CDR matching used in Do Not Keep Openline CDRs Without VOX Activity.	1500
---------------------------------------	--	------

Integration specific settings

The following settings can be configured separately for each trader voice recording integration. You can find these settings under **Unified Call Recorder / Media Recorder / Media Processing / <INTEGRATION>**.

Configuration Setting	Description	Default Value
Voice Activity Detection (VAD) Enabled	When enabled, the system will close the media records if silence is detected.	Yes
Media Inactivity Timeout for VAD (seconds)	Length of the timeout after the last RTP packet before closing a media record with voice inactivity.	30
Call Splitting Timer Type	Select the call splitting type. The following valid values apply: <ul style="list-style-type: none"> Absolute Relative <p>The absolute timer defines the time elapsed from the hour, the relative timer is from the start of the call.</p>	Absolute
Absolute Call Splitting Timer (minutes)	The time period for closing the CDR-Only + Media-Only records and creating new ones. Closed records become available for playback. VAD closed media records are available for playback from the Conversations \ Ongoing menu.	15
Do Not Split Records Shorter Than (seconds)	Minimum call length for call splitting. Must be less than the call splitting times configured at Unified Call Recorder \ Media Recorder \ Media Processing \ <INTEGRATION> \	300
Relative Call Splitting Timer (seconds)	The time period for closing the CDR-Only + Media-Only records and creating new ones. Closed records become available for playback. VAD closed media records are available for playback from the Conversations \ Ongoing menu.	900
Automatic Gain Control (AGC) Enabled	When enabled, the system will equalize the average volume.	No
Do Not Keep Openline CDRs Without VOX Activity	Discard the created CDR-Only record if there was no media activity. <ul style="list-style-type: none"> No - The recorder will not discard CDR-Only records Yes - The recorder will always discard the CDR-Only record if there is no corresponding media Only at call segmentation - The recorder will only discard the CDR-Only record if the recording is split. If the record ends for other reasons (such as the agent logging off) the CDR-Only record will be kept even with no media. 	Only at call segmentation