Verint Financial Compliance Capture (Verba)
1. Configure
   1.1 Configuring Verba for Cisco recording
      1.1.1 Configuring Verba for Cisco network-based recording
         1.1.1.1 Configuring Cisco UCM for network based recording
         1.1.1.2 Configuring Secure JTAPI
         1.1.1.3 Adding a new extension for recording in Cisco UCM
         1.1.1.4 Adding an extension with Extension Mobility in Cisco UCM
         1.1.1.5 Removing extensions from recording in Cisco UCM
         1.1.1.6 Defining a SIP Trunk Security Profile
         1.1.1.7 Configuring recording notifications in Cisco UCM
         1.1.1.8 Creating a recording profile in Cisco UCM
         1.1.1.9 Disable the unsupported ISAC codec
         1.1.1.10 Codec guidelines for Cisco network based recording
         1.1.1.11 Known Cisco bugs affecting recording reliability
         1.1.1.12 Configuring gateway preferred forking
         1.1.1.13 Configuring call routing in Cisco UCM for recording
         1.1.1.14 Create and configure a SIP Trunk
         1.1.2 Configuring the Cisco IP Phone Service
         1.1.2.1 Configure the IP Phone Service in UCM Express
      1.1.3 Configuring the Verba Cisco MediaSense connector
         1.1.3.1 Configuring Cisco MediaSense for Verba integration
      1.1.4 Cisco UCX Integration
      1.1.5 Configuring Cisco Unified IM and Presence 8.x, 9.x and Verba for Jabber IM recording
      1.1.6 Configuring Cisco Unified IM and Presence 10.x, 11.x, 12.x and Verba for Jabber IM recording
      1.1.7 Configuring Verba for Cisco proxy based recording
      1.1.7.1 Verba Media Collector and Proxy Service Reference
      1.1.8 Create and Associate Calling Search Spaces and Route Partitions
      1.1.9 Configuring Central Silent Monitoring and Whisper Coaching
      1.1.10 Configuring Cisco UC Gateway for recording
      1.1.11 Configuring Verba Cisco Recording Announcement for Inbound Call Recording
         1.1.11.1 Configuring Verba Cisco Recording Announcement for Inbound Calls (UCM based)
      1.1.12 Cisco UCCE Integration
      1.1.13 Configuring Verba Cisco Recording Announcement for Outbound PSTN Calls
      1.1.14 Genesys contact center integration in Cisco environment
      1.1.15 Genesys integration for Cisco network based recording
      1.1.16 Configuring Verba for Cisco Jabber File Transfer recording
      1.1.17 Configuring Cisco Expressway for recording through Mobile and Remote Access (MRA)
   1.2 Configuring Verba for Skype for Business and Lync recording
      1.2.1 Configuring Verba recording announcement service
      1.2.2 Configuring Remote Capture on Lync servers
      1.2.3 Configuring Lync conference call invitation
      1.2.4 Configuring Verba for Skype for Business / Lync IM recording
      1.2.5 Configuring Verba for Mediation - AVMCU based recording
      1.2.6 Recorder load balancing and failover design
      1.2.7 Port range and GoS settings for proxy based recording
      1.2.8 Configuring Lync call blocking on recording failure
      1.2.9 Configuring persistent chat room recording for SIB and Lync
      1.2.10 Configuring Lync - SIB Screen and Application Share recording
      1.2.11 Configuring Verba for RTP Proxy based recording
      1.2.12 Configuring Verba for Dual-Relaying
      1.2.13 Configuring Media Collector on Edge servers
      1.2.14 Configuring Lync - SIB P2P File Transfer Recording
      1.2.15 Installing and configuring the Verba SIB - Lync Announcement service
      1.2.15.1 Creating a Trusted Application Pool for the Verba Announcement Service
      1.2.16 Configuring SIB - Lync archive import
      1.2.17 SIB - Lync proxy load balancing and failover design
   1.3 Configuring Microsoft Teams Recording
      1.3.1 Adding Verba Tab to a Microsoft Teams Channel
      1.3.2 Administering Compliance Policy for Microsoft Teams Users
      1.3.3 Binding the SSL certificate to the Ports of the Verba Microsoft Teams Bot Server
      1.3.4 Configuring the Verba Microsoft Teams Bot and Unified Call Recorder Services
      1.3.5 Creating a Microsoft Teams Compliance Policy
      1.3.6 Enabling the Verba Web Application in 3rd Party Frame
      1.3.7 Registering the Microsoft Teams Bot in Azure
      1.3.8 Whitelisting the Microsoft Teams Bot App
   1.4 Configuring Microsoft Teams Chat Recording
      1.4.1 Configuring the Verba Unified IM Recorder Service for Microsoft Teams Chat Recording
      1.4.2 Configuring the Verba Unified IM Recorder Service on the Media Recorder Servers
      1.4.3 Configuring the Verba Unified IM Recorder Service on the Recording Director Servers
      1.4.4 Registering an App for Microsoft Teams Chat Recording in Azure
   1.5 Configuring IPC Unigy recording
      1.5.1 Configuring secure recorder communication for IPC Unigy
      1.5.2 Configuring turrets for recording
      1.5.3 Configuring Verba for IPC Unigy recording
      1.5.4 Unigy recorder resiliency
   1.6 Configuring IP Trade recording
      1.6.1 Configuring IP Trade
      1.6.2 Configuring Verba for IP Trade recording
   1.7 Configuring BT ITS recording
# Verint Verba Collaboration Compliance Platform

1.7.1 BT ITS recording network and server requirements .................................................. 238
1.7.2 BT ITS TTP numbering conventions ............................................................................ 239
1.7.3 Configuring BT ITS media recording ............................................................................. 240
1.7.4 Configuring BT ITSTLink CTI ....................................................................................... 241
1.7.5 Configuring BT ITS TMS and LDAP based provisioning ............................................. 247
1.7.6 BT ITS recorder resiliency ............................................................................................. 249
1.7.7 Configuring media stitching adjustment ....................................................................... 250
1.8 Configuring Speakerbus recording .................................................................................. 251
1.9 Configuring Avaya Central recording .............................................................................. 253
1.9.1 Configuring Avaya CM and AES for central recording .............................................. 254
1.9.1.1 Configure Avaya AES for recording ......................................................................... 255
1.9.1.2 Configure Avaya CM for recording ......................................................................... 256
1.9.1.3 Verify Avaya CM and AES recording configuration ............................................... 257
1.9.2 Configuring Verba for Avaya recording ...................................................................... 258
1.10 Configuring Genesys active recording .......................................................................... 263
1.10.1 Configuring Genesys .................................................................................................. 264
1.10.2 Configuring Verba for Genesys active recording ....................................................... 270
1.11 Configuring Verba for passive recording ..................................................................... 272
1.11.1 Configuring monitor port for passive recording .......................................................... 274
1.11.2 Overview of monitor ports for passive recording ....................................................... 277
1.11.3 Using Cisco switches to filter SPAN traffic .................................................................. 281
1.12 Configuring Verba for SIPREC recording .................................................................... 282
1.12.1 Configuring Acme Packet platform for SIPREC based call recording ....................... 283
1.12.2 Configuring Broadworks for SIPREC based call recording ...................................... 286
1.12.3 Configuring Cisco Unified Border Element (CUBE) based recording ...................... 289
1.12.4 Configuring Cisco VCS for Permanent Conference Recording ................................... 291
1.12.5 Configuring Polycom RMX for conference recording ............................................... 292
1.13 Central License Management ...................................................................................... 295
1.14 Cisco Video on Hold and Video in Queue ..................................................................... 297
1.14.1 Command line converter for VoH and ViQ ................................................................. 300
1.14.2 Configuring VoH and ViQ call rules ......................................................................... 301
1.14.3 SIP integration for VoH and ViQ ................................................................................. 304
1.15 Configuring media file upload ...................................................................................... 306
1.16 Configuring DTMF control and recording .................................................................... 308
1.17 Configuring Phone-based Silent Monitoring .................................................................. 309
1.18 Configuring SMS Recording .......................................................................................... 312
1.19 Configuring Synway Analog Tap Card recording ........................................................... 314
1.20 Configuring the Verba Desktop Agent ........................................................................... 318
1.20.1 Deploying Multiple Verba Desktop Agents ................................................................. 322
1.21 Configuring the Verba Dial-in Recorder Service ............................................................ 324
1.21.1 Configuring Cisco UCM for dial-in recording ............................................................ 325
1.21.2 Configuring Microsoft Lync for dial-in recording ...................................................... 330
1.22 Configuring Verba for On-demand recording ............................................................... 336
1.23 Database configuration .................................................................................................. 337
1.23.1 Configuring database connection .............................................................................. 338
1.23.2 Configuring encryption for database connections ..................................................... 340
1.23.3 Configuring SQL Server Failover Partner for mirroring .......................................... 342
1.23.4 Configuring SQL Server database encryption ........................................................... 343
1.24 Advanced Call Recording Rules .................................................................................... 344
1.25 Configuring recording high availability ....................................................................... 347
1.26 How to pull the server specific settings after the initial installation ............................... 352
1.27 Installing an SSL certificate for HTTPS access ............................................................... 353
1.28 Configuring TLS 1.2 ...................................................................................................... 355
1.29 Configuring the Monthly License Summary Email ........................................................ 358
1.30 Configuration reference ................................................................................................. 359
1.30.1 Network settings ........................................................................................................ 360
1.30.2 Directory settings ...................................................................................................... 361
1.30.3 Cisco Central Silent Monitoring Configuration settings ......................................... 362
1.30.4 Cisco JTAPI Configuration settings ......................................................................... 363
1.30.5 Unified Call Recorder service configuration reference for Cisco network based recording .......................... 365
1.30.6 Web application settings ........................................................................................... 369
1.30.7 CDR and Archived Content Importer settings .......................................................... 374
1.31 Verba Dial-out Recording ............................................................................................... 376
1.32 Integrated Windows Authentication ............................................................................... 380
1.32.1 Integrated Windows Authentication browser requirements .................................... 382
1.32.2 Integrated Windows Authentication server requirements ..................................... 383
1.33 Configuring IP-based Radio Recording ......................................................................... 384
1.34 Verifying System Readiness .......................................................................................... 386
1.35 Installing and configuring an external Recording Server ............................................... 390
1.36 Conversation direction detection using internal domain and number patterns ................ 393
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:
Verint Verba Collaboration Compliance Platform

- 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 Verba 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.

Step 8 - Click Save.

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.

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.
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 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.
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.

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

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

Step 4 - Make sure that both Cisco CTL Provider and Cisco Certificate Authority Proxy Function are 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.

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.

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.
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

![Download](Download.png)

**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.

![Cisco Unified Communications Manager](CiscoUnifiedCommunicationsManager.png)

**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.
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.

**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**

<table>
<thead>
<tr>
<th>Display (Internal Caller ID)</th>
<th>John Harrison</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASCII Display (Internal Caller ID)</td>
<td>John Harrison</td>
</tr>
<tr>
<td>Line Text Label</td>
<td></td>
</tr>
<tr>
<td>ASCII Line Text Label</td>
<td></td>
</tr>
<tr>
<td>External Phone Number Mask</td>
<td></td>
</tr>
<tr>
<td>Visual Message Waiting Indicator Policy*</td>
<td>Use System Policy</td>
</tr>
<tr>
<td>Audible Message Waiting Indicator Policy*</td>
<td>Default</td>
</tr>
<tr>
<td>Ring Setting (Phone Idle)*</td>
<td>Ring</td>
</tr>
<tr>
<td>Ring Setting (Phone Active)</td>
<td>Use System Default</td>
</tr>
<tr>
<td>Call Pickup Group Audio Alert Setting (Phone Idle)</td>
<td>Use System Default</td>
</tr>
<tr>
<td>Call Pickup Group Audio Alert Setting (Phone Active)</td>
<td>Use System Default</td>
</tr>
<tr>
<td>Recording Option*</td>
<td>Automatic Call Recording Enabled</td>
</tr>
<tr>
<td>Recording Profile</td>
<td>Recorder profile</td>
</tr>
<tr>
<td>Monitoring Calling Search Space</td>
<td>&lt; None &gt;</td>
</tr>
</tbody>
</table>

**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.
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.
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.

You need to reset every phone you configure for recording.

Step 7 - Remove the device from the JTAPl application user. Go to User Management / Application User and remove the device from the Controlled Devices list.

Step 8 - Click on the Save button.
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.

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 Recording)** group.
- **Step 5** - Click on the **Save** button.

<table>
<thead>
<tr>
<th>Clusterwide Parameters (Feature - Call Recording)</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Play Recording Notification Tone To Observed Target</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>Play Recording Notification Tone To Observed Connected Parties</td>
<td>False</td>
<td>False</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Put your section name here</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Recording Calling Search Space</td>
</tr>
<tr>
<td>Recording Destination Address</td>
</tr>
</tbody>
</table>

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 no 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

<table>
<thead>
<tr>
<th>Codec</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>G.711 A-law Codec Enabled</td>
<td>Enabled for All Devices Except Recording-Enabled Devices</td>
</tr>
<tr>
<td>G.711 u-law Codec Enabled</td>
<td>Enabled for All Devices Except Recording-Enabled Devices</td>
</tr>
<tr>
<td>G.722 Codec Enabled</td>
<td>Enabled for All Devices Except Recording-Enabled Devices</td>
</tr>
<tr>
<td>iLBC Codec Enabled</td>
<td>Enabled for All Devices Except Recording-Enabled Devices</td>
</tr>
<tr>
<td>iSAC Codec Enabled</td>
<td>Enabled for All Devices Except Recording-Enabled Devices</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recorder and recorded phone are on different sites, WAN link bandwidth limitation requires low bitrate voice codec</td>
<td>In this case it is recommended to put the recorder into different UCM region, and set inter-region codec according to available bandwidth.</td>
<td>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.</td>
</tr>
<tr>
<td>Recorder and recorded phones are in different UCM regions</td>
<td>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.</td>
<td>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).</td>
</tr>
<tr>
<td>Codec change in consultative transfer or joining a conference</td>
<td>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. Verb 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.</td>
<td>Consultative transfer, Agent A calls recorded Agent B to transfer Customer C calling from PSTN. A-&gt;B internal call leg use G.722 codec, after transfer C-&gt;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.</td>
</tr>
</tbody>
</table>

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
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

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

### Cisco CallManager

**Intermittent secure recording**


**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**


**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**


**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**


**Symptom:** Unable to record voice for some SIP calls. The issue will be encountered only during redirects over a SIP Trunk 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)**


**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


**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**


**Symptom:** Agents will get a one way audio after resume calls on hold/transfer. This defect happen when RTL is act as call recording 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**


**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


**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:

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))

```
Device# configure terminal
Device(config)# uc wsapi
Device(config-uc-wsapi)# provider xmf
Device(config-uc-wsapi)# no shutdown
Device(config-uc-wsapi)# remote-url 1 http://192.168.111.111:8090/ucm_xmf
Device(config-uc-wsapi)# end
Device# show wsapi registration all
```

Provider XCC

```
Provider XMF
```

```
registration index: 1
id: 32ECSA98-XMF: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.

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.
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.

Step 5 - Select the previously created route group at the Route Group setting, then click Save.
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.
<table>
<thead>
<tr>
<th><strong>Pattern Definition</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Route Pattern</strong></td>
<td>9999</td>
</tr>
<tr>
<td><strong>Route Partition</strong></td>
<td>&lt; None &gt;</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Numbering Plan</strong></td>
<td>-- Not Selected --</td>
</tr>
<tr>
<td><strong>Route Filter</strong></td>
<td>&lt; None &gt;</td>
</tr>
<tr>
<td><strong>MLPP Precedence</strong></td>
<td>Default</td>
</tr>
<tr>
<td><strong>Resource Priority</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Namespace Network Domain</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Gateway/Route List</strong></td>
<td>Recorder Route List</td>
</tr>
<tr>
<td><strong>Route Option</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Route this pattern</td>
</tr>
<tr>
<td></td>
<td>Block this pattern</td>
</tr>
<tr>
<td><strong>Call Classification</strong></td>
<td>OffNet</td>
</tr>
<tr>
<td><strong>Allow Device Override</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Provide Outside Dial Tone</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Allow Overlap Sending</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Urgent Priority</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Require Forced Authorization Code</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Authorization Level</strong></td>
<td>0</td>
</tr>
<tr>
<td><strong>Require Client Matter Code</strong></td>
<td></td>
</tr>
</tbody>
</table>
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.

**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:
**Decive 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 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**

**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.

**Step 8** - Click on the **Save** button.

After saving the changes, **reset** the trunk to apply the configuration on the trunk!
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

The following sections describes how to configure the Verba Phone Service based on authentication type.

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.

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

<table>
<thead>
<tr>
<th>Service URL</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>http://verba_MR_address/verba/phoneservice.do?byDeviceOrIp=1&amp;name=#DEVICENAME#</td>
<td>Enters to the Verba Phone Service App.</td>
</tr>
<tr>
<td>http://verba_MR_address/verba/phoneservice.do?byDeviceOrIp=1&amp;name=#DEVICENAME#&amp;manual=1</td>
<td>Enters to the recording control menu, where the user can start / stop the recording.</td>
</tr>
<tr>
<td>http://verba_MR_address/verba/phoneservicesm.do?byDeviceOrIp=1&amp;name=#DEVICENAME#</td>
<td>Enters to the silent monitoring menu.</td>
</tr>
<tr>
<td>http://verba_MR_address/verba/ps_RecordByDeviceId.do?type=manualRecord&amp;name=#DEVICENAME#</td>
<td>Quick action for starting the recording.</td>
</tr>
<tr>
<td>http://verba_MR_address/verba/ps_RecordByDeviceId.do?type=manualRecord&amp;name=#DEVICENAME#&amp;unmark=1</td>
<td>Quick action for stopping the recording.</td>
</tr>
<tr>
<td>http://verba_MR_address/verba/ps_ProtectByDeviceId do?name=#DEVICENAME#</td>
<td>Quick action for marking the recording for keeping.</td>
</tr>
<tr>
<td>http://verba_MR_address/verba/ps_ProtectByDeviceId do?name=#DEVICENAME#&amp;unmark=1</td>
<td>Quick action for removing the protected mark.</td>
</tr>
<tr>
<td>http://verba_MR_address/verba/ps_DeleteByDeviceId.do?name=#DEVICENAME#</td>
<td>Quick action for stopping the recording, and delete it.</td>
</tr>
<tr>
<td>http://verba_MR_address/verba/ps_Mute.do?byDeviceOrIp=1&amp;name=#DEVICENAME#</td>
<td>Quick action for muting the recording.</td>
</tr>
<tr>
<td>http://verba_MR_address/verba/ps_Unmute.do?byDeviceOrIp=1&amp;name=#DEVICENAME#</td>
<td>Quick action for unmuting the recording.</td>
</tr>
<tr>
<td>http://verba_MR_address/verba/phoneservice.do?byDeviceOrIp=1&amp;name=#DEVICENAME#&amp;onLogin=Private</td>
<td>Quick action for marking the call as private.</td>
</tr>
<tr>
<td>http://verba_MR_address/verba/phoneservice.do?byDeviceOrIp=1&amp;name=#DEVICENAME#&amp;onLogin=Private&amp;unmark=1</td>
<td>Quick action for removing the private mark.</td>
</tr>
<tr>
<td>http://verba_MR_address/verba/phoneservice.do?byDeviceOrIp=1&amp;name=#DEVICENAME#&amp;onLogin=Important</td>
<td>Quick action for marking the call as important.</td>
</tr>
<tr>
<td>http://verba_MR_address/verba/phoneservice.do?byDeviceOrIp=1&amp;name=#DEVICENAME#&amp;onLogin=Important&amp;unmark=1</td>
<td>Quick action for removing the important mark.</td>
</tr>
<tr>
<td>http://verba_MR_address/verba/phoneservice.do?byDeviceOrIp=1&amp;name=#DEVICENAME#&amp;onLogin=AddTag</td>
<td>Quick action for adding a comment.</td>
</tr>
<tr>
<td>http://verba_MR_address/verba/phoneservice.do?byDeviceOrIp=1&amp;name=#DEVICENAME#&amp;onLogin=Marker</td>
<td>Quick action for adding a marker.</td>
</tr>
<tr>
<td>http://verba_MR_address/verba/phoneservice.do?byDeviceOrIp=1&amp;name=#DEVICENAME#&amp;onLogin=EmailMe</td>
<td>Quick action for emailing a link to the user.</td>
</tr>
<tr>
<td>http://verba_MR_address/verba/phoneservice.do?byDeviceOrIp=1&amp;name=#DEVICENAME#&amp;onLogin=EmailBoss</td>
<td>Quick action for emailing a link to the group supervisor.</td>
</tr>
</tbody>
</table>

### Service URLs for IP address based authentication - Click to expand
### Service URLs

<table>
<thead>
<tr>
<th>Service URL</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>http://verba_MR_address/verba/phoneservice.do?byDeviceOrIp=1&amp;name=#DEVICENAME#</code></td>
<td>Enters to the Verba Phone Service App.</td>
</tr>
<tr>
<td><code>http://verba_MR_address/verba/phoneservice.do?byDeviceOrIp=1&amp;name=#DEVICENAME#&amp;manual=1</code></td>
<td>Enters to the recording control menu, where the user can start / stop the recording.</td>
</tr>
<tr>
<td><code>http://verba_MR_address/verba/phoneservicesm.do?byDeviceOrIp=1&amp;name=#DEVICENAME#</code></td>
<td>Enters to the silent monitoring menu.</td>
</tr>
<tr>
<td><code>http://verba_MR_address/verba/ps_RecordByIp.do?type=manualRecord</code></td>
<td>Quick action for starting the recording.</td>
</tr>
<tr>
<td><code>http://verba_MR_address/verba/ps_RecordByIp.do?type=manualRecord&amp;unmark=1</code></td>
<td>Quick action for stopping the recording.</td>
</tr>
<tr>
<td><code>http://verba_MR_address/verba/ps_MuteByIp.do</code></td>
<td>Quick action for muting the recording.</td>
</tr>
<tr>
<td><code>http://verba_MR_address/verba/ps_UnmuteByIp.do</code></td>
<td>Quick action for unmuting the recording.</td>
</tr>
<tr>
<td><code>http://verba_MR_address/verba/phoneservice.do?byDeviceOrIp=1&amp;name=#DEVICENAME#&amp;onLogin=Private</code></td>
<td>Quick action for marking the call as private.</td>
</tr>
<tr>
<td><code>http://verba_MR_address/verba/phoneservice.do?byDeviceOrIp=1&amp;name=#DEVICENAME#&amp;onLogin=Important</code></td>
<td>Quick action for marking the call as important.</td>
</tr>
<tr>
<td><code>http://verba_MR_address/verba/phoneservice.do?byDeviceOrIp=1&amp;name=#DEVICENAME#&amp;onLogin=AddTag</code></td>
<td>Quick action for adding a comment.</td>
</tr>
<tr>
<td><code>http://verba_MR_address/verba/phoneservice.do?byDeviceOrIp=1&amp;name=#DEVICENAME#&amp;onLogin=Marker</code></td>
<td>Quick action for adding a marker.</td>
</tr>
<tr>
<td><code>http://verba_MR_address/verba/phoneservice.do?byDeviceOrIp=1&amp;name=#DEVICENAME#&amp;onLogin=EmailMe</code></td>
<td>Quick action for emailing a link to the user.</td>
</tr>
<tr>
<td><code>http://verba_MR_address/verba/phoneservice.do?byDeviceOrIp=1&amp;name=#DEVICENAME#&amp;onLogin=EmailBoss</code></td>
<td>Quick action for emailing a link to the group supervisor.</td>
</tr>
</tbody>
</table>

### Service URLs for manual authentication - Click to expand

<table>
<thead>
<tr>
<th>Service URL</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>http://verba_MR_address/verba/phoneserviceauth.do</code></td>
<td>Brings up the login page, and after successful login enters to the Verba Phone Service App.</td>
</tr>
<tr>
<td><code>http://verba_MR_address/verba/phoneservicesmauth.do</code></td>
<td>Brings up the login page, and after successful login enters to the silent monitoring menu.</td>
</tr>
</tbody>
</table>

**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.
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

<table>
<thead>
<tr>
<th>Service URL for user ID based authentication</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>http://verba_MX_address/verba/phoneservice.do</td>
<td>Enters to the Verba Phone Service App.</td>
</tr>
<tr>
<td>http://verba_MX_address/verba/phoneservice.do?manual=1</td>
<td>Enters to the recording control menu, where the user can start / stop the recording.</td>
</tr>
<tr>
<td>http://verba_MX_address/verba/phoneservicesm.do</td>
<td>Enters to the silent monitoring menu.</td>
</tr>
<tr>
<td>http://verba_MX_address/verba/phoneservice.do?type=manualRecord</td>
<td>Quick action for starting the recording.</td>
</tr>
<tr>
<td>http://verba_MX_address/verba/phoneservice.do?type=manualRecord&amp;unmark=1</td>
<td>Quick action for stopping the recording.</td>
</tr>
<tr>
<td>http://verba_MX_address/verba/phoneservice.do?onLogin=Record</td>
<td>Quick action for marking the recording for keeping.</td>
</tr>
<tr>
<td>http://verba_MX_address/verba/phoneservice.do?onLogin=Protect</td>
<td>Quick action for marking the call as protected.</td>
</tr>
<tr>
<td>http://verba_MX_address/verba/phoneservice.do?onLogin=Protect&amp;unmark=1</td>
<td>Quick action for removing the protected mark.</td>
</tr>
<tr>
<td>http://verba_MX_address/verba/phoneservice.do?onLogin=Delete</td>
<td>Quick action for stopping the recording, and delete it.</td>
</tr>
<tr>
<td>http://verba_MX_address/verba/phoneservice.do?onLogin=Mute</td>
<td>Quick action for muting the recording.</td>
</tr>
<tr>
<td>http://verba_MX_address/verba/phoneservice.do?onLogin=Unmute</td>
<td>Quick action for unmuting the recording.</td>
</tr>
<tr>
<td>http://verba_MX_address/verba/phoneservice.do?onLogin=Private</td>
<td>Quick action for marking the call as private.</td>
</tr>
<tr>
<td>URL</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>http://verba_MR_address/verba/phoneservice.do?onLogin=Private&amp;unmark=1</td>
<td>Quick action for removing the private mark.</td>
</tr>
<tr>
<td>http://verba_MR_address/verba/phoneservice.do?onLogin=Important</td>
<td>Quick action for marking the call as important.</td>
</tr>
<tr>
<td>http://verba_MR_address/verba/phoneservice.do?onLogin=Important&amp;unmark=1</td>
<td>Quick action for removing the important mark.</td>
</tr>
<tr>
<td>http://verba_MR_address/verba/phoneservice.do?onLogin=AddTag</td>
<td>Quick action for adding a comment.</td>
</tr>
<tr>
<td>http://verba_MR_address/verba/phoneservice.do?onLogin=EmailMe</td>
<td>Quick action for emailing a link to the user.</td>
</tr>
<tr>
<td>http://verba_MR_address/verba/phoneservice.do?onLogin=EmailBoss</td>
<td>Quick action for emailing a link to the group supervisor.</td>
</tr>
</tbody>
</table>

**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.

**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](image1)

**Step 5** - Press the **Next** button.

**Step 6** - Provide the necessary parameters if required.

![Service Information](image2)

**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.
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).

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 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 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.
Configuring the Verba Cisco MediaSense connector

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.

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.

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 in ip: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.

<table>
<thead>
<tr>
<th>Cisco MediaSense</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basics</td>
</tr>
<tr>
<td>Automatic Gain Control Enabled:</td>
</tr>
<tr>
<td>Audio Format: Microsoft GSM-Fullrate (LPC-RPE) in WAV</td>
</tr>
<tr>
<td>Bidirectional/Stereo Recording:</td>
</tr>
<tr>
<td>Call event listening port:</td>
</tr>
<tr>
<td>Scheduled offline call import interval start time (hh:mm):</td>
</tr>
<tr>
<td>Scheduled offline call import interval end time (hh:mm):</td>
</tr>
<tr>
<td>Central Recorder DB Service address:</td>
</tr>
<tr>
<td>Central Recorder DB Service port:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MediaSense Cluster</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frontends:</td>
</tr>
<tr>
<td>User:</td>
</tr>
<tr>
<td>Password:</td>
</tr>
</tbody>
</table>

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:

1. Activate and start Cisco AXL web service. MediaSense uses AXL for administration and configuration tasks.
2. Create or modify an application super user to grant AXL access permission. Application user should have Standard CCM Super Users group rights.
3. Create Media Sense API user (standard End user, no special rights required), Verba is going to use the user to connect MediaSense.
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 MediaSense.
5. Create a recording profile used by the recorded lines / extensions.
6. Configure call routing that let the Cisco UCM to direct calls to the MediaSense cluster.
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.
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.
9. Verify if transcoding is required and available (recommended).
10. Configure a recording notification tone (optional).

Cisco MediaSense configuration

The initial Cisco MediaSense configuration includes the following steps:

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.
2. In the configuration wizard or Administration/MediaSense API user configuration menu add the end user to be used for API access.
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.
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.
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.

**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.
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**
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**: open-compliance.cups21
- **Port**: 10042
- **Password**: ********

Click **Save**.

**Step 7** - Expand the **IM Recording** node, and set the **Enable Recorder** setting to **Yes**, and set the **Internal Domain, Number Pattern** setting according to the internal 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.

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.

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.
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.
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.

<table>
<thead>
<tr>
<th>Presence Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Component Name</td>
</tr>
<tr>
<td>Port</td>
</tr>
<tr>
<td>Password</td>
</tr>
</tbody>
</table>

Click **Save**.

**Step 7** - Expand the **IM Recording** node, and set the **Enable Recorder** setting to **Yes**, and set the **Internal Domain, Number Pattern** setting according to the internal 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 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 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 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.

The license could not be verified: License Certificate has expired!

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.

   Stage 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.
Step 6 - In RTP Proxy section set Enabled to Yes.

Step 7 - In RTP Proxy / Advanced section set the Enforce ACL on Relay Sessions to Yes.
Step 8 - In SIP Proxy section set ‘Enabled’ to Yes.

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.

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 uploaded 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 11 (Optional) - Add additional incoming SIP connections if there are multiple incoming connections, by clicking on the icon.

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.
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.

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.
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.

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 SBSs. 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

<table>
<thead>
<tr>
<th>Configuration Parameter Name</th>
<th>Description</th>
<th>Sample Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recorder connection \ Listening Port</td>
<td>API port used with the Verba passive recording service.</td>
<td>11111</td>
</tr>
<tr>
<td>Recorder connection \ Secure Listening Port</td>
<td>API port over TLS used with the Verba passive recording service.</td>
<td>11112</td>
</tr>
<tr>
<td>Recorder connection \ Certificate File Path</td>
<td>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.</td>
<td>c:\verba.crt</td>
</tr>
<tr>
<td>Recorder connection \ Certificate Authority Certificate File Path</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Recorder connection \ Private Key File Path</td>
<td>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.</td>
<td>c:\verba.key</td>
</tr>
<tr>
<td>Recorder connection \ Private Key File Password</td>
<td>Password for the private key file used by the recorder proxy service to establish the TLS connection with the passive recorder service.</td>
<td></td>
</tr>
<tr>
<td>Recorder connection \ Authentication User</td>
<td>User account name to authenticate the passive recorder service accessing the proxy service.</td>
<td>verba</td>
</tr>
<tr>
<td>Recorder connection \ Authentication Password</td>
<td>Password for the user account.</td>
<td></td>
</tr>
<tr>
<td>Announcement Service UrIs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assign Call To Recorder only on First RTP</td>
<td>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.</td>
<td>No</td>
</tr>
<tr>
<td>Call Timeout (sec)</td>
<td>Defines the call timeout value in seconds, which is used to terminate the call recording automatically if the last RTP</td>
<td>60</td>
</tr>
<tr>
<td>Configuration Parameter Name</td>
<td>Description</td>
<td>Sample Value</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Enabled</td>
<td>Enable or disable the remote capture module in the service.</td>
<td>Yes</td>
</tr>
<tr>
<td>Interfaces</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Capture Buffer Size (megabytes)</td>
<td>Ethernet-level capture buffer size in megabytes.</td>
<td>90</td>
</tr>
<tr>
<td>Skinny Support Enabled</td>
<td>Turns on SCCP/Skinny support. By enabling this settings, you can record any type of calls using SCCP signaling.</td>
<td>Yes</td>
</tr>
<tr>
<td>SIP Support Enabled for Recording</td>
<td>Enable or disable SIP signaling support for the service.</td>
<td>Yes</td>
</tr>
<tr>
<td>RTP Address Translation Enabled</td>
<td>Enable or disable RTP address translation hint to detect the address of translated RTP streams.</td>
<td>Yes</td>
</tr>
<tr>
<td>Use RTP source address in call - RTP</td>
<td>Allows to use RTP source address in</td>
<td>No</td>
</tr>
<tr>
<td>mapping</td>
<td>internal stream map tables.</td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------------</td>
<td></td>
</tr>
</tbody>
</table>

SIP Capture Filter  
Capcure filter for SIP packets  
\[ ip[2]<5120 \text{ and } (ip[6:2]\&0x3F!=0 \text{ or } (tcp[0:2]=5060 \text{ or } tcp[2:2]=5060 \text{ or } udp[0:2]=5060 \text{ or } udp[2:2]=5060) \]  

Skinny Capture Filter  
Capcure filter for Skinny packets  

Media Capture Filter  
Capcure filter for RTP packets  
\[ ip[2]<2048 \text{ and } (udp \text{ and } ip[6:2]\&0x3F!=0 \text{ or } tcp \text{ src port } 443 \text{ or } ((udp[8:2]=0x0115 \text{ and } udp[24:4]=0x00000000) \text{ or } (udp[8:2]=0x0004 \text{ and } udp[12:4]=0x2112a442)) \text{ or } (udp[8]\&0xC0=0x80 \text{ and } (udp[9]\&0x7f <35 \text{ or } udp[9]\&0x7f >95))) \]  

TCP Media Capture Filter  
Capcure filter for TCP Media packets  
\( (tcp \text{ dst portrange } 1024-65535 \text{ or } tcp \text{ port } 443) \)  

Base Capture Filter  

**Lync Connector settings**

<table>
<thead>
<tr>
<th>Configuration Parameter Name</th>
<th>Description</th>
<th>Sample Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection \ Listening Port</td>
<td>API port number used by the Lync Filter services.</td>
<td>10201</td>
</tr>
<tr>
<td>Connection \ Certificate File Path</td>
<td>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.</td>
<td>C:\Program Files (x86)\Verba\bin\recordercert.crt</td>
</tr>
<tr>
<td>Connection \ Certificate Authority Certificate File Path</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Connection \ Private Key File Path</td>
<td>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.</td>
<td>C:\Program Files (x86)\Verba\bin\recorderkey.key</td>
</tr>
<tr>
<td>Connection \ Private Key File Password</td>
<td>Password for the private key file used by the recorder proxy service to establish the TLS connection with the Lync filter service.</td>
<td></td>
</tr>
<tr>
<td>Enabled</td>
<td>Enable or disable the Lync Filter connection. This setting needs to enabled when Lync recording is used.</td>
<td>Yes</td>
</tr>
<tr>
<td>Act as RTP Proxy</td>
<td>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.</td>
<td>Yes</td>
</tr>
<tr>
<td>Legacy Mode</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Enable Luware LUCS Integration</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Contact Center UCMA B2B Agents</td>
<td>RTCC/5.0.0.0 ACE RTCC/5.0.0.0 ICH RTCC/5.0.0.0 ICH-1.0.0 RTCC/5.0.0.0 TM-ICH RTCC/6.0.0.0 UCC</td>
<td></td>
</tr>
</tbody>
</table>

**RTP Proxy settings**
<table>
<thead>
<tr>
<th>Configuration Parameter Name</th>
<th>Description</th>
<th>Sample Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced \ Enforce ACL on Relay Sessions</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>Advanced \ Enforce ACL Modalities on Relay Sessions</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Advanced \ Relay Media from Public Address</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Advanced \ Advanced Relay Mode</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>Advanced \ Drop Unsolicited Packets</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>Advanced \ Support RTCP Mux</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>Advanced \ Support Late Media Negotiation</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>Advanced \ Banned IP Subnets</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advanced \ Codecs To Remove From Media Offer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advanced \ Crypto To Remove From Media Offer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advanced \ Redirect SfB/Lync Application Sharing Streams (RDP)</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Advanced \ Redirect SfB/Lync File Transfer</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Advanced \ Force Non-Secure RTP</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>Advanced \ Try To Avoid Double-Edge Relaying</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>Advanced \ Enable Address Translation for NAT Traversing</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>Advanced \ Merge B2B Call Legs to One Relay Session</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Advanced \ Enable relaying of TCP sessions</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Enabled</td>
<td>Enable or disable the RTP proxy module in the service.</td>
<td>Yes</td>
</tr>
<tr>
<td>Relay video streams</td>
<td>Enables the relaying of the video streams.</td>
<td>Yes</td>
</tr>
<tr>
<td>A/V Port Range Begin</td>
<td>RTP port range starting number to receive media streams.</td>
<td>16384</td>
</tr>
<tr>
<td>A/V Port Range End</td>
<td>RTP port range ending number to receive media streams.</td>
<td>65535</td>
</tr>
<tr>
<td>Separated Video Port Range Begin</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>Separated Video Port Range End</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>Appshare Port Range Begin</td>
<td></td>
<td>42000</td>
</tr>
<tr>
<td>Appshare Port Range End</td>
<td></td>
<td>44999</td>
</tr>
<tr>
<td>Filetransfer Port Range Begin</td>
<td></td>
<td>45000</td>
</tr>
<tr>
<td>Filetransfer Port Range End</td>
<td></td>
<td>49999</td>
</tr>
<tr>
<td>Block the calls if there is no online</td>
<td></td>
<td>No</td>
</tr>
</tbody>
</table>
### SIP Proxy settings

<table>
<thead>
<tr>
<th>Configuration Parameter Name</th>
<th>Description</th>
<th>Sample Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection \ Listening Port</td>
<td>SIP listening port.</td>
<td>5060</td>
</tr>
<tr>
<td>Connection \ Secure Listening Port</td>
<td>Secure SIP listening port.</td>
<td>5061</td>
</tr>
<tr>
<td>Connection \ Certificate File Path</td>
<td>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.</td>
<td>c:/verba.crt</td>
</tr>
<tr>
<td>Connection \ Certificate Authority Certificate File Path</td>
<td>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.</td>
<td>c:/verba.crt</td>
</tr>
<tr>
<td>Connection \ Private Key File Path</td>
<td>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).</td>
<td>c:/verba.key</td>
</tr>
<tr>
<td>Connection \ Private Key File Password</td>
<td>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).</td>
<td></td>
</tr>
<tr>
<td>Enabled</td>
<td>Enable or disable SIP Proxy module in the service.</td>
<td>Yes</td>
</tr>
<tr>
<td>Operation mode</td>
<td>The following valid values apply:</td>
<td>Outbound Proxy</td>
</tr>
<tr>
<td></td>
<td>• Outbound Proxy - the SIP proxy server acts as a standard outbound proxy.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SIP Router - the SIP proxy server uses its own routing rules to route calls.</td>
<td></td>
</tr>
</tbody>
</table>

### Overload Thresholds

<table>
<thead>
<tr>
<th>Configuration Parameter Name</th>
<th>Description</th>
<th>Sample Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concurrent Calls</td>
<td>Maximum concurrent calls threshold.</td>
<td>1250</td>
</tr>
<tr>
<td>Concurrent Media Relay Sessions</td>
<td>Maximum media relay sessions threshold. Every call consists of multiple relay sessions</td>
<td>1250</td>
</tr>
<tr>
<td>CPU (%)</td>
<td>Maximum CPU utilization threshold.</td>
<td>75</td>
</tr>
<tr>
<td>Network (%)</td>
<td>Maximum network utilization threshold.</td>
<td>75</td>
</tr>
</tbody>
</table>
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.

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: Example CSS
Description: 

**Route Partitions for this Calling Search Space**

<table>
<thead>
<tr>
<th>Available Partitions**</th>
</tr>
</thead>
<tbody>
<tr>
<td>AnalogPorts</td>
</tr>
<tr>
<td>Directory URI</td>
</tr>
<tr>
<td>Global Learned Enterprise Patterns</td>
</tr>
<tr>
<td>VerbaDev-SfB</td>
</tr>
<tr>
<td>Global Learned E164 Numbers</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Selected Partitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lab-Internal</td>
</tr>
<tr>
<td>VerbaDev-Cisco</td>
</tr>
</tbody>
</table>

---

**- 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 form the list, than 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 form the list, than 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 form the list, than 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 clickin 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.

<table>
<thead>
<tr>
<th>Central Cisco Silent Monitoring Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Features</td>
</tr>
<tr>
<td>Silent Monitoring Enabled: Yes</td>
</tr>
<tr>
<td>Whisper Coaching Enabled: Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco UCM IP Address(es): 10.1.20</td>
</tr>
<tr>
<td>JTAPI User Name: VerbaJTAPI</td>
</tr>
<tr>
<td>JTAPI User Password:</td>
</tr>
<tr>
<td>Play Tone: No tone play</td>
</tr>
<tr>
<td>Work Folder: C:\Program Files\Verba\work\ciscocentralism</td>
</tr>
<tr>
<td>API Port: 10013</td>
</tr>
</tbody>
</table>

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 clicking 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 server 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.
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
Verint Verba Collaboration Compliance Platform

---

```
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, 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 redirects the call to the Verba Announcement server.
6. When the call established, the announcement played.
7. The Verba Announcement service calls the original callee.
8. The Verba Announcement service connects the two calls, then leaves the call.

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.

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:

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/

Step 4 - Set the Call Treatment on Failures setting to Block 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.

**Step 4** - Click on the **Save** button then on the **Apply Config**.

**Step 5** - Repeat Step 1-4 at all phone devices where the inbound announcement is 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 the port the SIP Trunk connecting to the Verba server on.

---

**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.
Step 6 - Provide a directory number at the Service’s Phone Number setting. This directory number must be a number not used by anything else.

Step 7 - Set the Internal Number Pattern setting. This has to be a regex which matches to all internal line numbers.

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 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 Inbound Calls setting.
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.
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
- 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**.
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.

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.
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.

![Warning](image1.png)

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.
Step 11 - Save the changes by clicking on the icon.

Step 12 - A notification banner will appear on the top. Click on the link, so you will be redirected to the Configuration Tasks tab. Click on the button in order to execute the changes.

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.
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.

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.
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.

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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:  
  - Master IP Address  
  - Master Port  
  - Slave IP Address  
  - Slave Port |
| CTI Server Protocol Version | 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. Protocol versions based on UCCE version: |
| 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 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, 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 route pattern.
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 redirects the call to the Verba Announcement server.
6. The Verba Announcement service calls the original callee.
7. When the call established, the announcement played.
8. The Verba Announcement service connects the two calls, then leaves the call.

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 SIP Trunk Security Profile, since it needs a separate incoming port at the UCM side. The same SIP Trunk can be used for inbound and outbound announcement.

Configuring Cisco for Recording Announcement

Creating routing to the Announcement Service:

Creating the External Call Control Profile:

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/

Step 4 - Set the Call Treatment on Failures setting to Block Calls.
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.

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 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.
Step 6 - Provide a directory number at the **Service's Phone Number** setting. This directory number must be a number not used by anything else.

Step 7 - Set the **Internal Number Pattern** setting. This has to be a regex which matches to all internal line numbers.

### Cisco Recording Announcement

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CURRI Listening Port:</td>
<td>10205</td>
</tr>
<tr>
<td>CURRI 'TLS Certificate:</td>
<td></td>
</tr>
<tr>
<td>CURRI TLS Key:</td>
<td></td>
</tr>
<tr>
<td>CURRI TLS Key Password:</td>
<td></td>
</tr>
<tr>
<td>RTP Port Range Start:</td>
<td>16384</td>
</tr>
<tr>
<td>RTP Port Range End:</td>
<td>65535</td>
</tr>
<tr>
<td>SIP Ports:</td>
<td></td>
</tr>
<tr>
<td>SIP URI Modification:</td>
<td></td>
</tr>
<tr>
<td>Service's Phone Number:</td>
<td>8888</td>
</tr>
<tr>
<td>Internal Number/Domain's Pattern:</td>
<td>id(\d)</td>
</tr>
<tr>
<td>Enable Service Alerts:</td>
<td>Yes</td>
</tr>
</tbody>
</table>

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 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.
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.
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.
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:
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:
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: Use rs / 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.

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Genesys T-Server IP(s)</td>
<td>After clicking on the gear icon at the end of the line, the following fields can be configured:</td>
</tr>
<tr>
<td></td>
<td>• User</td>
</tr>
<tr>
<td></td>
<td>• Password</td>
</tr>
<tr>
<td></td>
<td>• IP Address(es) and ports the port should be separated by a</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Target Genesys Field for Verba Call ID</td>
<td>Verba will attach the Verba Call ID to this Genesys User Data Field.</td>
</tr>
</tbody>
</table>

**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 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.

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 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 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 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 be 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 SIB - 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 SIB / 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


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:

<table>
<thead>
<tr>
<th>Configuration Parameter Name</th>
<th>Description</th>
<th>Sample Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Service FQDN</strong></td>
<td>Fully Qualified Domain Name (FQDN) of the server running the application. It has to match the value entered during the trusted application pool registration.</td>
<td>TrustedApplicationServer.yourDomain.com</td>
</tr>
<tr>
<td><strong>Service Port</strong></td>
<td>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.</td>
<td>6000</td>
</tr>
<tr>
<td><strong>Lync Pool FQDN</strong></td>
<td>Fully Qualified Domain Name (FQDN) of the Front End pool where the application is registered.</td>
<td>fepool.yourDomain.com</td>
</tr>
<tr>
<td><strong>Lync Port</strong></td>
<td>SIP port on the Front End pool.</td>
<td>5061</td>
</tr>
<tr>
<td><strong>Service certificate</strong></td>
<td>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.</td>
<td>yourTrustedApplicationPool.yourDomain.com</td>
</tr>
<tr>
<td><strong>Service certificate password</strong></td>
<td>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 another server then imported to the store.</td>
<td></td>
</tr>
<tr>
<td><strong>Application URI</strong></td>
<td>SIP address of the announcement service endpoint created by the New-CsTrustedApplicationEndpoint command. 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 ID is 'verbaAppID'. You can check these parameters by simply running the Get-CsTrustedApplication command:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>$a = Get-CsTrustedApplication -identity &quot;verbaapps.contoso.com/urn:application:verbaAppID&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>$a.ComputerGruus</td>
<td></td>
</tr>
<tr>
<td></td>
<td>sip:<a href="mailto:TrustedApplicationServer.yourDomain.com@yourDomain.com">TrustedApplicationServer.yourDomain.com@yourDomain.com</a>;gruu;opaque= srvr:verbaAppID:BiusNAOGF-VGcGpM-LG-gAA</td>
<td></td>
</tr>
<tr>
<td><strong>Application GRUU</strong></td>
<td>Computer Routable User Agent URI (GRUU) of the announcement application. Use * to enable the API on all local network.</td>
<td>sip:<a href="mailto:VerbaAnnouncement@yourDomain.com">VerbaAnnouncement@yourDomain.com</a></td>
</tr>
<tr>
<td></td>
<td>http://*:12222/</td>
<td></td>
</tr>
<tr>
<td><strong>HTTP API URL</strong></td>
<td>Recorder API address and port number. Use * to enable the API on all local network.</td>
<td>http://*:12222/</td>
</tr>
</tbody>
</table>
The service uses this API to communicate with the recorder service(s) to obtain events like call recording getting started/stopped.

<table>
<thead>
<tr>
<th>IM notification message</th>
<th>The instant messaging text displayed when recording is started by one of the participants in the conference. The message is only displayed in the group chat when recording is started. If a new participant joins the conference, the message is not displayed again.</th>
<th>This meeting is being recorded</th>
</tr>
</thead>
</table>

**Default Voice 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 not hear the prompt again.

<table>
<thead>
<tr>
<th>Default voice prompt for inbound calls</th>
<th>The audio prompt played when receiving an inbound call.</th>
<th>C:\Program Files\Verba\resources\announcement\recording.wma</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default voice prompt for outbound calls</td>
<td>The audio prompt played when making an outbound call.</td>
<td>C:\Program Files\Verba\resources\announcement\pstin. wma</td>
</tr>
</tbody>
</table>

**Enable voice announcement for inbound and outbound calls**
Enable voice announcement for inbound and outbound calls.

<table>
<thead>
<tr>
<th>Enable caller impersonation for outbound calls</th>
<th>Yes</th>
</tr>
</thead>
</table>

**On hold prompt for outbound calls**
The audio played to the caller when making an outbound call.

<table>
<thead>
<tr>
<th>Announcement Prompt Store Path</th>
<th>The store of the audio files used for announcement.</th>
<th>C:\Program Files\Verba\resources\announcement\</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice Prompt Delay for PSTN Conference Joiners (msec)</td>
<td>The delay for the conference announcement for PSTN joiners.</td>
<td>15000</td>
</tr>
</tbody>
</table>

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)

- **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.
If you selected one of the localhost's interfaces hit the 'Save' button.

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

<table>
<thead>
<tr>
<th>Configuration Parameter Name</th>
<th>Description</th>
<th>Sample Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Email Protocol</strong></td>
<td>POP3 or IMAP</td>
<td>POP3</td>
</tr>
<tr>
<td><strong>Email Server</strong></td>
<td>Host name or IP address of the POP3 or IMAP server.</td>
<td>pop.mailserver.com</td>
</tr>
<tr>
<td><strong>Email Server Folder for Invites</strong></td>
<td>Logical name of the Inbox folder. Usually it should be set to INBOX.</td>
<td>INBOX</td>
</tr>
<tr>
<td><strong>Email Account User Name</strong></td>
<td>User name of the email server account.</td>
<td>verba_account</td>
</tr>
<tr>
<td><strong>Email Account Password</strong></td>
<td>Password for the email server account.</td>
<td>secret_pwd</td>
</tr>
<tr>
<td><strong>Authentication Required for Email Account</strong></td>
<td>If the email server requires authentication, this should be set to Yes.</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Email Server Port Number</strong></td>
<td>Default ports:</td>
<td>110</td>
</tr>
<tr>
<td></td>
<td>• POP3: 110</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• POP3+SSL: 995</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• IMAP: 143</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• IMAP+SSL: 993</td>
<td></td>
</tr>
<tr>
<td><strong>SSL Required for Email Server</strong></td>
<td>If the email server requires the use of SSL, this should be set to Yes.</td>
<td>No</td>
</tr>
<tr>
<td><strong>Archive Invites in Folder</strong></td>
<td>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.</td>
<td>PROCESSED</td>
</tr>
<tr>
<td><strong>Delete Invites After (days)</strong></td>
<td>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.</td>
<td>0</td>
</tr>
<tr>
<td><strong>Meeting URLs in Invites</strong></td>
<td>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 &quot;<a href="https://meet.mycompany.com/myuser/QOP2XV3S">https://meet.mycompany.com/myuser/QOP2XV3S</a>&quot;, then set this setting to &quot;meet.mycompany.com&quot;. Multiple values separated by new lines are accepted.</td>
<td>meet.mycompany.com</td>
</tr>
<tr>
<td><strong>Store Invite Message Bodies</strong></td>
<td>For debugging purposes the invitation message body can be stored in the database. Requires more storage but can be handy if anything went wrong.</td>
<td>No</td>
</tr>
<tr>
<td><strong>Check for New Invites Period (sec)</strong></td>
<td>Frequency of email server polling.</td>
<td>15</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-----------------------------------</td>
<td>--</td>
</tr>
<tr>
<td><strong>Send Notification Emails</strong></td>
<td>If it is set to &quot;Yes&quot;, Verba will send an email after each recording to the meeting organizer and participants.</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Email Subject</strong></td>
<td>The subject of the notification email sent by Verba. Available reference strings:</td>
<td>Meeting (${MEETING_SUBJECT} - ${CONFERENCE_ID} - ${MEETING_ID}) recording available</td>
</tr>
<tr>
<td>Referenc...</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>${MEETING_ID}</td>
<td>Meeting ID parsed from the meeting URL.</td>
<td></td>
</tr>
<tr>
<td>${CONFERENCE_ID}</td>
<td>Conference ID found in the meeting email after &quot;Conference ID:&quot;</td>
<td></td>
</tr>
<tr>
<td>${MEETING_SUBJECT}</td>
<td>Subject of the invitation email.</td>
<td></td>
</tr>
<tr>
<td>${USER_NAME}</td>
<td>Name of the user the email will be sent to.</td>
<td></td>
</tr>
<tr>
<td>${ORGANIZER_NAME}</td>
<td>Name of the meeting organizer.</td>
<td></td>
</tr>
<tr>
<td>${ORGANIZER_EMAIL}</td>
<td>Email address of the meeting organizer.</td>
<td></td>
</tr>
<tr>
<td>${LINK}</td>
<td>Direct access link to the recording (pointing to Verba web application)</td>
<td></td>
</tr>
<tr>
<td><strong>Email Body for Attendees</strong></td>
<td>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.</td>
<td>Dear ${USER_NAME},&lt;br/&gt;&lt;br/&gt;The recorded media of your Lync Meeting (${MEETING_SUBJECT} - ${CONFERENCE_ID} - ${MEETING_ID}), organized by ${ORGANIZER_NAME} (${ORGANIZER_EMAIL}) is now shared with you on the following link: &lt;a href='${LINK}'&gt;${LINK}&lt;/a&gt; &lt;br/&gt; You can also access it by looking for it under the Sharing / View Shared Items menu. &lt;br/&gt;Sincerely,&lt;br/&gt;Verba Recording System</td>
</tr>
<tr>
<td><strong>Email Body for Organizer</strong></td>
<td>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.</td>
<td>Dear ${USER_NAME},&lt;br/&gt;&lt;br/&gt;The recorded media of your Lync Meeting (${MEETING_SUBJECT} - ${CONFERENCE_ID} - ${MEETING_ID}) is now available on the following link: &lt;a href='${LINK}'&gt;${LINK}&lt;/a&gt; &lt;br/&gt; You can also access it by looking for it under the Search menu. &lt;br/&gt;Sincerely,&lt;br/&gt;Verba Recording System</td>
</tr>
<tr>
<td><strong>Share Recordings to Participants</strong></td>
<td>If it is &quot;Yes&quot;, 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.</td>
<td></td>
</tr>
</tbody>
</table>
Configuring Verba for Skype for Business / Lync IM recording

Prerequisites

The Verba SfB / Lync Filter 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 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 - 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](image)

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.

![Warning](image)

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

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.

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

<table>
<thead>
<tr>
<th>Interface Name</th>
<th>SCCP</th>
<th>SIP</th>
<th>RTP</th>
<th>Total</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>fe80::31e0:9628:94fb:6f12 10.4.0.42</td>
</tr>
<tr>
<td>Ethernet 2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>fe80::f45ff332:190a:40d 192.108.167.65</td>
</tr>
</tbody>
</table>

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.
Step 11 - Save the changes by click 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 Media Collector and Proxy Service** by clicking on the **play** 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.

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 **gear** 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 **add** 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**

<table>
<thead>
<tr>
<th>Host</th>
<th>TESTFE1SFB.VERBATEST.LOCAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>10201</td>
</tr>
<tr>
<td>Public IP</td>
<td></td>
</tr>
</tbody>
</table>

**Step 9** - Repeat Steps 7-8 for every Mediation / AVMCU Server in your system.
**Verint Verba Collaboration Compliance Platform**

---

**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.**

---

**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.**

**Step 14** - Repeat these steps for every Lync Front End / Filter in your system.
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.

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|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 have the same priority) |

| 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, remove 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".

**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.

**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.
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 belong 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 Filter 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 clicking on the icon.

Step 7 - A notification banner will appear on the top. Click on the link, so you will be redirected to the Configuration Tasks tab. Click on the Execute button in order to execute the changes.

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 SIB/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.)
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|adalum.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 is 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.
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 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.

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 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:** 1514 (Phone number) / 1234 (extension)
- **User:** Jerry Jones (Jerry)
- **Type:** Number/Address

If a user is missing from the list, please verify the Valid Until and Valid From fields of that user.

**Update User Information on Existing Conversations:**
- Select options:
  - Apply to: new conversations, unassigned conversations, all conversations, or update conversations within the user's validity period only.

**Description:**

### Recording Settings

- **Recording Mode:** Full
- **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/UC/Teams 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.

**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.
**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.

Changes can be execute at once at the end. In that case don't forget to click on 'Check All'.
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.

<table>
<thead>
<tr>
<th>Verba Proxy Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
</tr>
<tr>
<td>Proxy Host</td>
</tr>
<tr>
<td>Proxy Port</td>
</tr>
<tr>
<td>Priority or Subnets</td>
</tr>
<tr>
<td>Pool Name</td>
</tr>
</tbody>
</table>

Step 9 - Repeat Steps 7-8 for every Proxy Server in your system.
Step 10 - Save the changes by clicking on the icon.

Step 11 - A notification banner will appear on the top. Click on the 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.
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 - 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 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.

<table>
<thead>
<tr>
<th>Verba Proxy Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
</tr>
<tr>
<td>Proxy Host</td>
</tr>
<tr>
<td>Proxy Port</td>
</tr>
<tr>
<td>Priority or Subnets</td>
</tr>
<tr>
<td>Pool Name</td>
</tr>
</tbody>
</table>

**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.

**Advanced**

- **RTP Proxy**
  - Enabled: Yes
  - Relay video streams: Yes
  - A/V Port Range Begin: 10304
  - A/V Port Range End: 05535
  - Separated Video Port Range Begin: 0
  - Separated Video Port Range End: 0
  - AppShare Port Range Begin: 42800
  - AppShare Port Range End: 44999
  - Filetransfer Port Range Begin: 45900
  - Filetransfer Port Range End: 49999
  - Block the calls if there is no online recorder: No
  - Proxy pool name: 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 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 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 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.

<table>
<thead>
<tr>
<th>Choose Recording Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
</tr>
<tr>
<td>---</td>
</tr>
<tr>
<td>Interface Name</td>
</tr>
<tr>
<td>Ethernet</td>
</tr>
<tr>
<td>Ethernet 2</td>
</tr>
<tr>
<td>Ethernet 2</td>
</tr>
</tbody>
</table>

**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.
### 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.

---

**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.

**Attention** 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.
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 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.
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:

<table>
<thead>
<tr>
<th>Configuration Parameter Name</th>
<th>Description</th>
<th>Sample Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recording announcement</td>
<td>Enable the announcement feature</td>
<td>Yes</td>
</tr>
<tr>
<td>Recording announcement for incoming PSTN calls</td>
<td>Enable voice announcement for incoming PSTN calls.</td>
<td>Yes</td>
</tr>
<tr>
<td>Enable Announcement for Outgoing PSTN calls</td>
<td>Enable voice announcement for outgoing PSTN calls.</td>
<td>Yes</td>
</tr>
<tr>
<td>Enable Announcement for Incoming Federated calls</td>
<td>Enable voice announcement for incoming Federated calls.</td>
<td>Yes</td>
</tr>
<tr>
<td>Enable Announcement for Outgoing Federated calls</td>
<td>Enable voice announcement for outgoing Federated calls.</td>
<td>Yes</td>
</tr>
<tr>
<td>Apply announcement to forwarded calls</td>
<td>Enable voice announcement for forwarded calls.</td>
<td>Yes</td>
</tr>
<tr>
<td>Enable announcement for Team calls</td>
<td>Sets whether the announcement should be played in the case of all users in the team, or to none of them.</td>
<td>Yes</td>
</tr>
<tr>
<td>Remove route information from SIP INVITE messages</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Verba Announcement URI</td>
<td>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.</td>
<td>sip:<a href="mailto:VerbaAnnouncement@yourDomain.com">VerbaAnnouncement@yourDomain.com</a></td>
</tr>
<tr>
<td>Internal Number Pattern</td>
<td>Defines the internal numbers</td>
<td>^((4-9)(0-9)[3])(*{0,}?[0-9][5])$</td>
</tr>
<tr>
<td>Internal SIP Domains</td>
<td>Defines the internal SIP domains. One at each line.</td>
<td>yourDomain.com</td>
</tr>
<tr>
<td>Verba Announcement services</td>
<td>Configure the installed announcement services</td>
<td>announcementserver: 10210</td>
</tr>
<tr>
<td>Lync/SfB Contact Center UCMA B2B Agents</td>
<td>List of user agents where the announcement should not be played, separated by a new line.</td>
<td>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</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Configuration Parameter Name</th>
<th>Description</th>
<th>Sample Value</th>
</tr>
</thead>
</table>

- **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.

- **Configuration for large multi-site deployments**
  The configuration should consist of two parts:

- **Load balancing and failover configuration with FE / AVMCU preference (1 announcement server per data center):**

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://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

So for example, the final configuration for Site1 should be something like this:
https://announcement1:12222|FE_IP1,FE_IP2
https://announcement3:12222|FE_IP6
https://announcement4:12222|FE_IP7,FE_IP8
https://announcement2:12222|3
https://announcement3:12222|2
https://announcement4:12222|1

| Announcement Service Uris | 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)**
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)

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)
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.

<table>
<thead>
<tr>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:john_doe@adatum.com">john_doe@adatum.com</a></td>
</tr>
<tr>
<td><a href="mailto:peter_parker@adatum.com">peter_parker@adatum.com</a></td>
</tr>
<tr>
<td><a href="mailto:bruce_wayne@adatum.com">bruce_wayne@adatum.com</a></td>
</tr>
</tbody>
</table>

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](https://en.wikipedia.org/wiki/List_of_SIP_response_codes)

**Step 4** - Click the **Save** 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 Topolgy 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 of your Announcement Server** and enter the **FQDN of your new trusted application pool**.

Click on the **Next**.

**Step 5.** If you selected the Multiple computer pool, add the **FQDNs of your Announcement Servers**. Click on the **Next**.

**Step 6.** Enable the **Associate next hop pool** checkbox and select your Lync pool where you creating the **Trusted Application Pool** from the dropdown list. Click on the **Finish**.

**Step 7.** Click on the **Action -> Topolog -> 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'.

```powershell
New-CsTrustedApplicationPool -Identity verbaannouncement.contoso.com -Registrar sfbpool1.yourdomain.com -RequiresReplication $false -Site 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'.

```powershell
New-CsTrustedApplicationComputer -Identity
```
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 verbaannouncement.contoso.com -Port 6000
```

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
```

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 FQDM 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 -DisplayName "Announcement Service" -TrustedApplicationPoolFqdn verbaannouncement.contoso.com -ApplicationId verbaannouncementapplication
```
(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 display name"
```

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 policy display name"
```
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 SIB/Lync version. Provide a Work Folder for the data source (recommended: C:\Program Files\Verba\work\archive_importer), then click Save.
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.
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 |
| Proxy connection 2 setting | 192.168.3.0/24,192.168.4.0/24 |
| 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.
- If you are expecting more than 100 simultaneous recorded calls in your tenant(s), the bot has to be whitelisted by Microsoft to remove the throttling limits in the Graph API

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](#).

**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](#).
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.

Step 6 - Provide a Tab name (it can be anything), then provide the URL of the Verba Web Application.
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:

  ```powershell
  Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force
  ```

- **Step 4** - Install the Microsoft Teams module by running the following command:

  ```powershell
  Install-Module MicrosoftTeams
  ```

**Accessing the tenant via PowerShell**

Follow the steps below to assign a compliance policy to a user:

- **Step 1** - Open **PowerShell** as administrator.
- **Step 2** - Execute the following command:

  ```powershell
  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)

  ```powershell
  Grant-CsTeamsComplianceRecordingPolicy -Identity '<User’s UPN>' -PolicyName '<PolicyName>'
  ```

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.
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 'TeamsComplianceRecordingPolicy'
```

**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 'TeamsComplianceRecordingPolicy'
```
Binding the SSL certificate to the Ports of the Verba Microsoft Teams Bot Server

In order to complete the steps below, you must have Local Administrator rights on the VMs.

A publicly signed certificate is required for the virtual machine. The SAN configuration of the certificate must include the hostname of the virtual machine with the domain where the Teams tenant resides. Using asterisk in the SAN is accepted. The private key of the certificate has to be exportable.

**Step 1** - Log in to the Verba Bot virtual machine in Azure, and open an administrator command prompt.

**Step 2** - Bind the 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, and insert the thumbprint of the SSL certificate at the `certificate_thumbprint_without_spaces` part. The `appid` is just a random GUID.

```
netsh http add sslcert ipport=ip_address:9440
certhash=certificate_thumbprint_without_spaces appid="{00000000-0000-0000-0000-000000000001}"  
netsh http add sslcert ipport=ip_address:10100
certhash=certificate_thumbprint_without_spaces appid="{00000000-0000-0000-0000-000000000001}"  
```
Verint Verba Collaboration Compliance Platform

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
- 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 / 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 7 - Under **Microsoft Teams**, configure the following settings (see configuration reference for more details):

<table>
<thead>
<tr>
<th>Setting Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bot Service DNS Name</td>
<td>The FQDN of the virtual machine</td>
</tr>
<tr>
<td>Bot Service CName</td>
<td>The CNAME DNS entry created for the server</td>
</tr>
<tr>
<td>Service Certificate Thumbprint</td>
<td>The thumbprint of the publicly signed certificate used previously for binding the ports</td>
</tr>
<tr>
<td>Bot Application ID</td>
<td>The App ID of the bot (see related step at Registering the Microsoft Teams Bot in Azure)</td>
</tr>
<tr>
<td>Bot Application Secret</td>
<td>The secret created for the bot (see related step at Registering the Microsoft Teams Bot in Azure)</td>
</tr>
<tr>
<td>Microsoft Teams Tenant ID</td>
<td>The ID of the Azure tenant where the bot was created (see related step at Registering the Microsoft Teams Bot in Azure)</td>
</tr>
<tr>
<td>Query Hosting Tenant's Azure AD</td>
<td>Defines if the bot service will query the Azure Active Directory for User Principal Names (UPN)</td>
</tr>
<tr>
<td>Public IP Address</td>
<td>The public IP address of the virtual machine</td>
</tr>
</tbody>
</table>
Configuring the Verba Unified Call Recorder service

**Step 8** - Expand the Unified Call Recorder \ Media Recorder \ Microsoft Teams node.

**Step 9** - At the Teams Bot Servers setting, click on the icon to add a new connection.

**Step 10** - 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.

**Step 11** - Click on the Save button at the bottom. You will see the bot connection added to the configuration.
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.

Starting the services

Step 14 - Click on the Service Control tab.

Step 15 - Start the Verba Microsoft Teams Bot Service and the Verba Unified Call Recorder Service by clicking on the icon.

Configuration reference

<table>
<thead>
<tr>
<th>Setting Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General/Recorder Connection</strong></td>
<td></td>
</tr>
<tr>
<td>Recording Director Listening Port</td>
<td>The TCP/TLS port where the bot service is listening for the Recording Director connections from the Verba Unified Call Recorder Service</td>
</tr>
<tr>
<td>Media Recorder Listening Port</td>
<td>The TCP/TLS port where the bot service is listening for the Media Recorder connections from the Verba Unified Call Recorder Service.</td>
</tr>
<tr>
<td>Authentication User</td>
<td>Username for authenticating with the Verba Unified Call Recorder Service.</td>
</tr>
<tr>
<td>Authentication Password</td>
<td>Password for authenticating with the Verba Unified Call Recorder Service.</td>
</tr>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td>Record Non-configured Extensions</td>
<td>Defines if the bot service has to record non-configured extensions.</td>
</tr>
<tr>
<td>Compress RAW audio to G.711</td>
<td>Defines if the bot service transcodes the original PCM audio stream to G.711 before sending the data to the recorder.</td>
</tr>
<tr>
<td>Bidirectional/Stereo Recording</td>
<td>Defines if the bot service subscribes for unmixed audio stream in the Microsoft Teams call. Note: The unmixed audio has to be whitelisted on the Microsoft Teams side.</td>
</tr>
<tr>
<td>Number of Recorded Video Participants</td>
<td>Defines how many video streams are recorded per call, including the video streams of the recorded user.</td>
</tr>
<tr>
<td>Preferred Video Resolution</td>
<td>The video resolution used when the bot</td>
</tr>
<tr>
<td><strong>Verint Verba Collaboration Compliance Platform</strong></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td></td>
</tr>
<tr>
<td>subscribes to the video streams of the participants. Microsoft Teams streams the video up to the resolution requested during the subscription. The resolution can be lower based on network conditions/capacity.</td>
<td></td>
</tr>
</tbody>
</table>

**Preferred Screen Share Resolution**
The video resolution used when the bot subscribes to the screen share streams of the participants. Microsoft Teams streams the video up to the resolution requested during the subscription. The resolution can be lower based on network conditions/capacity.

**Separated Screen Share Record**
Defines if a separated record is created for the screen share modality. The separate call includes the audio stream too.

**Start Recording After Recorded User Joined**
Defines if the bot waits for the join event of the recorded user before it starts the recording session.

**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 then it will prevent the establishment of the call. If the bot cannot fail-over to another recorder mid-call, the bot will leave 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 replace the recorder with 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 replace the recorder with another online Unified Call Recorder service/server.

**Microsoft Teams**

<p>| <strong>Bot Service DNS Name</strong> | The FQDN of the virtual machine hosting the bot service. |
|---|
| <strong>Bot Service Public CNAME</strong> | CNAME entry on the public trusted domain which points to the public IP (ILPIP) of the virtual machine hosting the bot service. |
| <strong>Service Certificate</strong> | The thumbprint or the file path of the public domain's certificate. If the certificate in the WCS, it has to have an exportable private key. Only CSP certificates are supported (CNG/KSP certificates are not supported!) |
| <strong>Service Certificate Key File</strong> | The key file if the certificate is files based. |
| <strong>Service Certificate Key File Password</strong> | Password for the key file |
| <strong>Bot Application ID</strong> | The Application ID generated during the bot registration. Format: GUID |
| <strong>Bot Application Secret</strong> | The Application secret generated during the bot registration. |
| <strong>Bot Application Authentication Certificate</strong> | The authentication certificate uploaded on the Certificates and Secrets page of the Azure AD App registration. If configured the application secret is ignored. |
| <strong>Authentication Certificate Key File</strong> | The key file if the certificate is files based |
| <strong>Authentication Certificate Key File</strong> | Password for the key file |</p>
<table>
<thead>
<tr>
<th><strong>Password</strong></th>
<th><strong>Microsoft Teams Tenant ID</strong></th>
<th>The ID of the Microsoft Teams Tenant where the bot is hosted. Format: GUID</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Query Hosting Tenant’s Azure AD</strong></td>
<td>Defines if the bot will query the Azure Active Directory of the tenant for additional user information such as User Principal Name.</td>
<td></td>
</tr>
<tr>
<td><strong>Public IP Address</strong></td>
<td>The public IP address assigned to the virtual machine hosting the bot service.</td>
<td></td>
</tr>
<tr>
<td><strong>Bot Service Port</strong></td>
<td>HTTPS port where the bot is listening for call invites from Microsoft Teams.</td>
<td></td>
</tr>
<tr>
<td><strong>Call Control Port</strong></td>
<td>HTTPS port where the bot is listening for call control messages from Microsoft Teams.</td>
<td></td>
</tr>
<tr>
<td><strong>Media Control Port</strong></td>
<td>HTTPS port used by the Microsoft Media SDK for media control messages.</td>
<td></td>
</tr>
<tr>
<td><strong>Media Port Range Begin</strong></td>
<td>Beginning of the UDP port range for the media streams.</td>
<td></td>
</tr>
<tr>
<td><strong>Media Port Range End</strong></td>
<td>End of the UDP port range for the media stream.</td>
<td></td>
</tr>
<tr>
<td><strong>Advanced</strong></td>
<td><strong>Microsoft API Endpoint</strong></td>
<td>Base URL of the Microsoft Graph API. All API messages from the bot are sent to the URL.</td>
</tr>
</tbody>
</table>
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-csteamscompliancerecordingpolicy

The policy configuration consists of the following steps:

- **Prerequisites**
  - Accessing the tenant via PowerShell
  - 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** - 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.

**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. Replace the `<TenantId>` part with your Azure Tenant ID (Creating the Microsoft Teams Recording Bot - Step 29).
At the `<Policy Description>` part, provide some description. At the `<PolicyName>` part, provide a name.

```
New-CsTeamsComplianceRecordingPolicy -Tenant '<TenantId>' -Enabled $true -Description '<Policy Description>' -Identity '<PolicyName>'
```

**Step 6** - Execute the following command. Replace the `<TenantId>` parts with your Azure Tenant ID (Creating the Microsoft Teams Recording Bot - Step 29). 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 -Tenant '<TenantId>' -Identity '<PolicyName>' -ComplianceRecordingApplications @(New-CsTeamsComplianceRecordingApplication -Tenant '<TenantId>' -Parent '<PolicyName>' -Id '<ObjectId>'
```

**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>' -ComplianceRecordingPairedApplications @(New-CsTeamsComplianceRecordingPairedApplication -Id '<ObjectId_of_Bot2>
```

### Changing the Compliance Recording Policy settings

The Teams Compliance Recording Policy allows the following configuration options:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>RequiredBeforeMeetingJoin</td>
<td>Defines if the bot has to join the call before the recorded user can join the meetings</td>
<td>1 (On)</td>
</tr>
<tr>
<td>RequiredBeforeCallEstablishment</td>
<td>Defines if the bot has to join the call before the recorded user can place or receive calls</td>
<td>1 (On)</td>
</tr>
<tr>
<td>RequiredDuringMeeting</td>
<td>Defines if the recorded user will be disconnected from the meetings if the recorder bot connection is lost</td>
<td>1 (On)</td>
</tr>
<tr>
<td>RequiredDuringCall</td>
<td>Defines if the recorded user will be disconnected from the call if the recorder bot connection is lost</td>
<td>1 (On)</td>
</tr>
</tbody>
</table>

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 : {Ids`.

```
Get-CsTeamsComplianceRecordingPolicy
```
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.

```powershell
Set-CsTeamsComplianceRecordingApplication -Identity '<PolicyName>/<ComplianceApplicationId>' -RequiredBeforeMeetingJoin 0 - RequiredBeforeCallEstablishment 0 -RequiredDuringMeeting 0 -RequiredDuringCall 0
```

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 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 Bot Channels Registration 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, and the Location of the bot channel registration. The Location should be the same region where the Verba Bot virtual machine resides in Azure.

---

Registering the MS 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 "[password]
```
Step 4 - Click on the Create button. Creating the Bot Channel Registration may take some seconds. Azure will automatically create an App Registration and a Bot Service assigned to it.

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 Bot management section, click on the Channels menu.

Step 8 - Under the Add featured channel section select the Teams icon (Configure Microsoft Teams channel).

Step 9 - Select the Calling tab, then tick the Enable calling checkbox.

Step 10 - 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 11 - Click on the Save button. Agree with the terms of service.

Configuring authentication for the bot

Step 12 - 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 13 - Select the App Registration from the list that was created previously using the name provided at Step 3 (Bot handle).

Step 14 - Take a note of the Application (client) ID and the Directory (tenant) ID. They will be needed later.

Step 15 - Select the Certificates & secrets menu in the left panel.

Step 16 - Under the Client secrets section, click on the New Client Secret button.

Step 17 - Provide a Description, set when the secret Expires, then click on the Add button.
Step 18 - Take a note of the new Client secret. It will be needed later.

Step 19 - In the left panel, under the Manage section, click on the Authentication menu.

Step 20 - Under the Platform configuration sections, click on the Add a platform button.

Step 21 - In the right panel, select Web.

Step 22 - Provide a Redirect URI. It can be any website. Take a note of the URI provided, it will be needed later.

Step 23 - Click on the Configure button in the bottom.

Configure Web

All platforms

Quickstart

Docs

Redirect URIs

The URIs that we will accept as destinations when returning authentication responses (tokens) after successfully authenticating users. Also referred to as reply URIs. Learn more about redirect URIs and the restrictions

https://www.verba.com

Step 4 (Optional) - Assign an user to the App registration as owner using the az ad app app owner add command:

```
az ad app owner add
```

Step 5 - Add permissions to the App registration using the az ad app permission add command:

```
az ad app permission add
```
Configuring permissions to the bot

Step 24 - In the left panel, under the Manage section, click on the API permissions menu.

Step 25 - Click on the Add a permission button.

Step 26 - Select Microsoft Graph, then select Application permissions.

Step 27 - Select the following permissions:
- Calendars.Read
- Calls.AccessMedia.All
- Calls.Initiate.All
- Calls.InitiateGroupCall.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 28 - 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
Step 29 - Build the consent URL. The format is the following:

https://login.microsoftonline.com/{tenant_id}/adminconsent?client_id={microsoft_app_id}&state=12345&redirect_uri={redirect_uri}

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 30 - 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

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

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.
Step 6 (Optional) - If the same App Registration will be used for Chat recording also, then add the following permissions also:

- az
- ad
- ap
- p
- pe
- rm
- is
Step 7 - Grant admin consent using the **az ad app permission admin-consent** command:

```bash
az ad app permission ison ad min-con sen t -- id $a pp ID
```

Step 8 - Create the Bot channels
registration using the `az bot create` command:

```
az bot create
-n "[bot_channel_name]"
-k "registration_name"
--appid $app_id
--subscription
```
Step 9 - Add the Teams channel to the Bot channels registration using the `az bot msteams create` command:

```bash
az bot msteams create
```
Step 10 (Optional) - 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.
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** - Install the NuGet package provider module by running the following command:

```bash
Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force
```

**Step 4** - Install the Microsoft Teams module by running the following command:

```bash
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:

```bash
Update-Module MicrosoftTeams
```

**Step 3** - Execute the following command:

```bash
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).
Verint Verba Collaboration Compliance Platform

New-CsOnlineApplicationInstance -UserPrincipalname <UPN> -DisplayName '<displayName>' -ApplicationId <botAppId>

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 Microsoft Teams Chat Recording

In order to complete the steps below, you must have System Administrator role in Verba.

The registration consists of the following steps:

- Recording architecture
  - File queue setup for failover and load-balancing
- Configuration
  - Prerequisites
    - Assigning a Public IP Address
    - Creating an App Registration in Azure
    - Creating the File Queue folder
    - Assigning Certificates
  - Configuring a single-recorder setup
  - Configuring a highly-available setup
    - Co-located Recording Directors and Media Recorders in a highly available setup

Recording architecture

The following diagram shows the connections in a highly available Microsoft Teams IM recording environment.

File queue setup for failover and load-balancing

In a highly available environment, only one of the Recording Director servers is writing into the file queues at once, depending on which one receives the events from the Application Gateway. The "Number of Receiving Queues Owned by Director Role" setting has to be the same on all Recording Director servers. This setting has to be the same as the total Media Recorder cores (without redundancy) multiplied by two.

In the Media Recorder configuration, the "Number of Processing Queues Owned by Recorder Role" setting has to be specified, and it has to be the same on all the Media Recorder servers. When there is no load-balancing (1+1 servers), then the "Number of Processing Queues Owned by Recorder Role" configuration will be equal to the total number of file queues. When load-balancing is
being used (N+1), the file queues have to be distributed between the (active or N) Media Recorders, so the "Number of Processing Queues Owned by Recorder Role" configuration will be the quantity of the file queues divided by the quantity of the (active or N) recorders.

In the case of N+1 setup, an extra Media Recorder has to be added. When a Media Recorder (N) is started, it will pick up X queues depending on its "Number of Processing Queues Owned by Recorder Role" configuration. When the last Media Recorder (+1) is starting up, all the file queues will be taken already, so the last recorder will be the standby recorder. If a Media Recorder goes down, the standby recorder picks up its queues, and becomes an active recorder. When the Media Recorder comes back, it will be the new standby recorder.

Highly available setup with load-balancing:

Highly available setup without load-balancing:

**Configuration**

**Prerequisites**

**Assigning a Public IP Address**

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]media\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

A **publicly signed certificate** is required. 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 asterisk in the SAN is accepted. The **private key** of the certificate has to be **exportable**.

**Configuring a single-recorder setup**

The configuration steps of the single-recorder setup can be found here:

[Configuring the Verba Unified IM Recorder Service for Microsoft Teams Chat Recording](#)

**Configuring a highly-available setup**

The following configuration steps needs 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**

**Co-located Recording Directors and Media Recorders in a highly available setup**

Alternatively, the Recording Director and the Media Recorder servers can be **co-located**. In this case, do the **single-recorder setup** for each servers, but use the file queues on the network location instead of creating them on the local disks, and use the common certificate for the Teams connections.
Configuring the Verba Unified IM Recorder Service for Microsoft Teams Chat Recording

This configuration guide described 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 Recoding 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 **Activate** 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 = "Number of Receiving Queues Owned by 
Director Role" setting value
```

**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 **Add** icon to add a new connection.

**Step 13** - In the left panel, provide the following settings:
<table>
<thead>
<tr>
<th>Setting Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application (Client) ID</td>
<td>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)</td>
</tr>
<tr>
<td>Application (Client) Secret</td>
<td>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)</td>
</tr>
<tr>
<td>Directory (Tenant) ID</td>
<td>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)</td>
</tr>
<tr>
<td>Notification URL</td>
<td>The notification URL of the Unified IM Recorder service. The format is the following: <a href="https://server_CNAME.domain.com:3333/msteams">https://server_CNAME.domain.com:3333/msteams</a>. 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.</td>
</tr>
<tr>
<td>Event Listener Port</td>
<td>The event listener port of the Unified IM Recorder service. Set it to 3333.</td>
</tr>
<tr>
<td>Connection Encryption Certificate</td>
<td>The thumbprint of the certificate being 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. This has to be a publicly signed certificate. Only CSP certificate 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 asterisk in the SAN is accepted. The private key of the certificate has to be exportable. 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.</td>
</tr>
<tr>
<td>Connection Encryption Key file</td>
<td>If the file path is provided at the Connection Encryption Certificate setting, then the path to the .key file has to be provided here.</td>
</tr>
<tr>
<td>Connection Encryption Key file password</td>
<td>If the file path is provided at the Connection Encryption Certificate setting, then the password of the .key file has to be provided here</td>
</tr>
<tr>
<td>Connection Encryption trust list</td>
<td>The thumbprint of the incoming connection certificates that should be trusted, or the thumbprint of the CA certificates whom certificates should be trusted. If left empty, all certificates will be trusted.</td>
</tr>
<tr>
<td>Disable P2P/Group Chat Subscription</td>
<td>Sets whether the P2P or group chats should be recorded or not.</td>
</tr>
<tr>
<td>Disable Team/Channel Chat Subscription</td>
<td>Sets whether the Team or Channel chats should be recorded or not.</td>
</tr>
</tbody>
</table>
### Microsoft Teams IM

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application (Client) ID</td>
<td>76e11d9e-571c-47af-9b35-0c49686b2f2b</td>
</tr>
<tr>
<td>Application (Client) Secret</td>
<td>..........................</td>
</tr>
<tr>
<td>Directory (Tenant) ID</td>
<td>df88a583-9017-4f7d-8232-f9ef6409d7d7</td>
</tr>
<tr>
<td>Notification URL</td>
<td><a href="https://imrecorder.contoso.com:3333/msteams">https://imrecorder.contoso.com:3333/msteams</a></td>
</tr>
<tr>
<td>Event Listener Port</td>
<td>3333</td>
</tr>
<tr>
<td>Connection Encryption Certificate</td>
<td>9b28ae65169aa477c5783d6480f296ef48cf14d</td>
</tr>
<tr>
<td>Connection Encryption Key file</td>
<td>..........................</td>
</tr>
<tr>
<td>Connection Encryption Key file password</td>
<td>............</td>
</tr>
<tr>
<td>Connection Encryption trust list</td>
<td></td>
</tr>
<tr>
<td>Disable P2P/Group Chat Subscription</td>
<td>No</td>
</tr>
<tr>
<td>Disable Team/Channel Chat Subscription</td>
<td>No</td>
</tr>
</tbody>
</table>

**Step 14** - Click Save.

**Step 15** - Repeat steps 12-14 for every Microsoft Teams connection.

**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.

### 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 on the Media Recorder Servers

This configuration guide described 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:

<table>
<thead>
<tr>
<th>Setting Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application (Client) ID</td>
<td>The ID of the App Registration</td>
</tr>
<tr>
<td></td>
<td>(Registering an App for Chat Recording in Azure - Step 6 or Registering the Microsoft Teams Bot in Azure - Step 13)</td>
</tr>
<tr>
<td>Application (Client) Secret</td>
<td>The secret created for the App Registration</td>
</tr>
<tr>
<td></td>
<td>(Registering an App for Chat Recording in Azure - Step 10 or Registering the Microsoft Teams Bot in Azure - Step 17)</td>
</tr>
<tr>
<td>Directory (Tenant) ID</td>
<td>The ID of the Azure tenant where the App Registration was created</td>
</tr>
<tr>
<td></td>
<td>(Registering an App for Chat Recording in Azure - Step 6 or Registering the Microsoft Teams Bot in Azure - Step 29)</td>
</tr>
<tr>
<td><strong>Notification URL</strong></td>
<td>The notification URL of the Unified IM Recorder service. The format is the following: <a href="https://server_CNAME.domain.com:3333/msteams">https://server_CNAME.domain.com:3333/msteams</a>. <em>Note:</em> 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.</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Event Listener Port</strong></td>
<td>The event listener port of the Unified IM Recorder service. Set it to 3333.</td>
</tr>
<tr>
<td><strong>Connection Encryption Certificate</strong></td>
<td>The thumbprint of the certificate being 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. This has to be a <strong>publicly signed</strong> certificate. Only CSP certificate are supported (CNG/KSP certificates are not supported). The SAI 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 asterisk in the SAN is accepted. The <strong>private key</strong> of the certificate has to be <strong>exportable</strong>. 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.</td>
</tr>
<tr>
<td><strong>Connection Encryption Key file</strong></td>
<td>If the file path is provided at the Connection Encryption Certificate setting, then the path to the .key file has to be provided here.</td>
</tr>
<tr>
<td><strong>Connection Encryption Key file password</strong></td>
<td>If the file path is provided at the Connection Encryption Certificate setting, then the password of the .key file has to be provided here.</td>
</tr>
<tr>
<td><strong>Connection Encryption trust list</strong></td>
<td>The thumbprint of the incoming connection certificates that should be trusted, or the thumbprint of the CA certificates whom certificates should be trusted. If left empty, all certificates will be trusted.</td>
</tr>
<tr>
<td><strong>Disable P2P/Group Chat Subscription</strong></td>
<td>Sets whether the P2P or group chats should be recorded or not.</td>
</tr>
<tr>
<td><strong>Disable Team/Channel Chat Subscription</strong></td>
<td>Sets whether the Team or Channel chats should be recorded or not.</td>
</tr>
</tbody>
</table>
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 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 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:

\[ \text{"Number of Processing Queues Owned by Recorder Role" setting value on the Media Recorders} \times \text{Number of Media Recorders} = \text{"Number of Receiving Queues Owned by Director Role" setting value} \]

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:

<table>
<thead>
<tr>
<th>Setting Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application (Client) ID</td>
<td>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)</td>
</tr>
<tr>
<td>Application (Client) Secret</td>
<td>The secret created for the App Registration</td>
</tr>
<tr>
<td><strong>Directory (Tenant) ID</strong></td>
<td>The ID of the Azure tenant where the App Registration was created.</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Notification URL</strong></td>
<td>The notification URL of the Unified IM Recorder service. The format is the following: <a href="https://server_CNAME.domain.com:3333/msteams">https://server_CNAME.domain.com:3333/msteams</a>. 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.</td>
</tr>
<tr>
<td><strong>Event Listener Port</strong></td>
<td>The event listener port of the Unified IM Recorder service. Set it to 3333.</td>
</tr>
</tbody>
</table>
| **Connection Encryption Certificate** | The thumbprint of the certificate being 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.  
This has to be a **publicly signed** certificate. Only CSP certificates are supported (CNG/KSP certificates are not supported). The SAI 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 asterisk in the SAN is accepted. The **private key** of the certificate has to be **exportable**.  
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 whom 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. |
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 Recorder Director servers.

Step 19 - A notification banner will appear on the top. Click on the 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 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.
Registering an App for Microsoft Teams Chat Recording 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.

**Step 5** - Click Register.

**Step 6** - Take a note of the Application (client) ID and the Directory (tenant) ID. They will be needed later.
Step 7 - Select the **Certificates & secrets** menu in the left panel.

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**

**verba_bot_secret**

**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 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.

```bash
$app = az ad app create --display-name "[app_display_name]" --app-credentials --app-allowed-all-devices
```
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.

Contoso Ltd.

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=12345&redirect_uri={redirect_uri}

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.

---

**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 $appID --owner-obj-id "["user_object_id"]"
```

**Step 5** - Add permissions to the App registration using the `az ad app permission add` command:
Step 6 - Grant admin consent using the `az ad app permission admin-consent` command:

```
az
ad
app
perm
is
si
on
ad
mi
n-
con
sent
--
id
$appp
ID
```

Step 7 - The protected API access has to be requested. See the [Protected API Access for Chat Recording](#) section at the bottom.
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**

<table>
<thead>
<tr>
<th>Secure Recording</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring secure communication is required to record turrets which are configured to use secure connections/media encryption</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Provisioning recorded agents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agents/traders are identified by Unigy End User’s personal extension. This should be added as Agent Id type extension</td>
</tr>
</tbody>
</table>
Configuring secure recorder communication for IPC Unigy

Unigy authenticates the recorder service via TLS, i.e., 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=US/ST=/L=/O=/CN=10.7.0.8"
```

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**

<table>
<thead>
<tr>
<th>Select</th>
<th>Name</th>
<th>Description</th>
<th>Duplicate Of</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔️</td>
<td>All Channels</td>
<td>All Channels</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DUPLICATE - All Channels</td>
<td>All Channels</td>
<td>All Channels</td>
</tr>
</tbody>
</table>

**Step 4 - Assign recording profile to the users (System Designer/End User Configuration)**

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
    - Preparation
    - Configure the 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](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](icon) under Unigy Zones. On the right panel, configure the zone configuration settings as described below:

<table>
<thead>
<tr>
<th>IPC Zone</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Zone VIP CTI URL</strong></td>
</tr>
<tr>
<td><img src="url" alt="url" /></td>
</tr>
<tr>
<td><strong>Local CTI port (leave empty for random port)</strong></td>
</tr>
<tr>
<td>2320</td>
</tr>
<tr>
<td><strong>CCM SIP port (leave empty if default is used)</strong></td>
</tr>
<tr>
<td>5060</td>
</tr>
<tr>
<td><strong>Secondary Recorder (2N)</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
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.

If secure communication is required the URL should be `https://...`. If HTTPS is configured recorder establishes recording channels via SIP over TLS as well.

If secure communication is configured, Verba should be configured to use a Unigy trusted certificate.

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 (i.e. other applications should not use it).

If for some reason Unigy does not use the standard/default 5060/5061 ports, then the SIP port number should be configured here.

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.

Configure certificate

**Step 5 - Configure the certificate settings if secure communication is used in zone configuration:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL/TLS Certificate</td>
<td>Specify the certificate file/certificate thumbprint (a certificate store in the Windows Certificate Store or PEM/PFX certificate file path). The certificate must be signed by Unigy.</td>
</tr>
<tr>
<td>SSL/TLS Key</td>
<td>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.</td>
</tr>
<tr>
<td>SSL/TLS Key Password</td>
<td>Specify the password for the file that contains the certificate keys</td>
</tr>
<tr>
<td>SSL/TLS Trust List</td>
<td>Specify the list of certificates validating Unigy’s certificate:</td>
</tr>
<tr>
<td></td>
<td>• empty: no validation on Verba side</td>
</tr>
<tr>
<td></td>
<td>• thumbprint: either self-signed certificate with the thumbprint or CA-signed certificate where CA certificate matches the thumbprint is accepted</td>
</tr>
<tr>
<td></td>
<td>• “*: use windows top-level CA store</td>
</tr>
<tr>
<td></td>
<td>• PEM file path: the file should contain the certificate chain for Unigy Enterprise</td>
</tr>
</tbody>
</table>

Revise optional settings and save the configuration

**Step 6 - Review the following optional configuration settings:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDR/Agent Event Subscription Keepalive (seconds)</td>
<td>The keepalive timer for the subscription. The lower value detects failure quicker but causes more load on Unigy.</td>
</tr>
<tr>
<td>Agent State Polling Period (seconds)</td>
<td>The timer for agent state polling, lower value detects failure quicker but causes more load on Unigy.</td>
</tr>
<tr>
<td>Start Recording by RTP (not by CTI)</td>
<td>By default Verba starts recording and waiting for media based on CTI call start/stop events. For more reliability this can be changed</td>
</tr>
</tbody>
</table>
Verint Verba Collaboration Compliance Platform

Unigy Controlled Recording

Recording decision from IPC should or not override Verba decision.

to start recording based on arriving media and update the record based on CTI events (if they are arriving).

Step 7 - Save the changes by clicking on the icon.

Step 8 - A notification banner will appear on the top. Click on the 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.

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**

<table>
<thead>
<tr>
<th>Zone VIP CTI URL</th>
<th><a href="http://10.0.1.2/ctisvc/recording/CSTAService">http://10.0.1.2/ctisvc/recording/CSTAService</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Local CTI port (leave empty for random port)</td>
<td>2320</td>
</tr>
<tr>
<td>CCM SIP port (leave empty if default is used)</td>
<td>5060</td>
</tr>
<tr>
<td>Secondary Recorder (2N)</td>
<td></td>
</tr>
</tbody>
</table>
**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**

<table>
<thead>
<tr>
<th>Zone VIP CTI URL</th>
<th><a href="http://10.0.1.2/ctisvc/recording/CSTAService">http://10.0.1.2/ctisvc/recording/CSTAService</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Local CTI port (leave empty for random port)</td>
<td>2320</td>
</tr>
<tr>
<td>CCM SIP port (leave empty if default is used)</td>
<td>5060</td>
</tr>
<tr>
<td>Secondary Recorder (2N)</td>
<td>[ ]</td>
</tr>
</tbody>
</table>

**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**

**Preparation**

For this setup two Recording Directors needed. One should be set as active CTI service, for this server, no additional configuration required, the other as passive.

**Configure the 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 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 collocated 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

![General Settings](image)

Configure the recording server according to the following table:

<table>
<thead>
<tr>
<th>Item</th>
<th>Example value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>HU-BUDLAB-MR</td>
<td>Descriptive name of the recording server</td>
</tr>
<tr>
<td>Recorder Brand</td>
<td>Verba</td>
<td>Type of the recorder</td>
</tr>
<tr>
<td>Primary URI</td>
<td>vrc://10.110.77.129:8000</td>
<td>vrc://&lt;IP address&gt;:port number</td>
</tr>
<tr>
<td>Secondary URI</td>
<td>vrc://10.110.77.128:8001</td>
<td></td>
</tr>
<tr>
<td>Recorder mixing mode</td>
<td>Mixed</td>
<td>The recording mixing mode used</td>
</tr>
</tbody>
</table>
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.
Verint Verba Collaboration Compliance Platform

配置冗余

步骤 1 在录制服务器配置中，应提供两个录制服务器。
- 对于 2N 录制：vrc://192.168.2.1:8000;vrc://192.168.2.2:8001
- 对于 N+1 录制：vrc://192.168.2.1:8000

步骤 2 在 TPO 或 turret 基于录制配置中，选择步骤 4。

步骤 3 转到 Expert 模式标签，选择 Recorder 设置。

步骤 4 选择冗余双流模式设置。设置为 true 对于 2N 或 false 对于 N+1 录制模式。

步骤 5 点击更新按钮以保存更改。

TSS 9.2 以及更早

系统级配置

步骤 1 登录到基于 web 的“TSS 控制台”管理界面。

步骤 2 转到 Device Management -> Zones -> System (或自定义 zone) -> Turret Boot Settings (标签)

Zone: System

Turret Boot Settings

步骤 3 转到 Recorder (左键/标签) 并在 Basic (标签) 中检查 Recorder 兼容性为“iptrade”。

步骤 4 转到 Expert (标签) 仍在 Recorder 设置，并启用 Keep-Alive 在所有录制 turret上。

步骤 5 转到 Advanced Mode (标签)，并添加以下键：

```
profile.setting.disablerecorder = false
```

Turret 基于录制配置

步骤 1 创建一个 Shared Profile，该配置将被附加到所有录制 turret 上（如果有 existing shared profile，则可以用于这些设置，并确保它被分配给所有录制 turret）。
Step 2  
In the **Shared Profile** (created above) apply the following settings:

**Account Management: Shared Profile Edition (Mixed Mode)**

### Settings

**Basic Mode**

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recording channel 10 devices</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recording channel 11 devices</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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.

**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 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.

**Step 2**  
Set the **ReplayBox URL** to [http://192.168.5.69:8000](http://192.168.5.69:8000) (Verba recorder IP)

**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
```

Step 6  Make sure to reboot all recorded turrets after the configuration changes.

Recorder configuration

Keep alive configuration
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.

<table>
<thead>
<tr>
<th>Configuration Name and Key</th>
<th>Location</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recorder compatibility</td>
<td>FTP</td>
<td>iptrade</td>
<td>Defines which type of recorder is in use.</td>
</tr>
<tr>
<td>application.recorder.compatibility</td>
<td></td>
<td></td>
<td>For Verba Recording System it has to be the default value: iptrade.</td>
</tr>
<tr>
<td>profile.setting.activerecording</td>
<td></td>
<td></td>
<td>Format: vrc://recorder_address:port</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For redundancy, add the second recorder after “;” Example: vrc://192.168.2.1:8000;vrc://192.168.2.2:8001</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The port number is configured in the Verba Recording System, see I P Trade Recorder settings.</td>
</tr>
<tr>
<td>Recording mixing mode</td>
<td>Shared Profile</td>
<td>separated</td>
<td>Indicates the mixing mode:</td>
</tr>
<tr>
<td>profile.setting.recording.mixingmode</td>
<td></td>
<td></td>
<td>• separated: each call is recorded separately by recorder channel at the same time. We use one recorder channel per call.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td>Default recording channel</td>
<td>Shared Profile</td>
<td>0</td>
<td>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 &quot;mixed&quot;.</td>
</tr>
<tr>
<td>profile.setting.recording.default.channel</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recording channel 0..9 devices</td>
<td>Shared Profile</td>
<td></td>
<td>Devices recorded on channel 0 (mixing mode only). Multiple devices may be listed separated by &quot;.&quot; character. For advanced GUI editions, applet may be referenced in this key.</td>
</tr>
<tr>
<td>profile.setting.recording.channel.0..9.devices</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Default Value</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>----------------------------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Authorize replay</td>
<td>true</td>
<td>Defines if recorder replay is authorized on the turret.</td>
<td></td>
</tr>
</tbody>
</table>
| ReplayBox URL                    | 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 I P Trade Recorder settings.  
If you have a 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                      | FTP/ TCP      | Defines the replay mode.                                                    |
| Disable recorder                 | 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        | 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 > 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 Force Recording Media on Director is set to Yes.

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 - Click on the Service Control tab.

Step 9 - 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

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](image.png).

*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 - 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.

Step 13 - Start the Verba Unified Call Recorder Service by clicking on the icon.

Step 14 - 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 /IPS

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
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>Recording Server Role</td>
<td>Defines the role of the server:</td>
</tr>
<tr>
<td></td>
<td>• Recording Director: deals only with TTP management only, it distributes and moves TTPs across media recorders</td>
</tr>
<tr>
<td></td>
<td>• 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</td>
</tr>
<tr>
<td></td>
<td>• Recording Director + Media Recorder: includes both functionality</td>
</tr>
<tr>
<td></td>
<td>For Recording Director functionality either TMS or LDAP based BT ITS platform provisioning and Voice Recorder IDs must be configured</td>
</tr>
<tr>
<td>Voice Recorder IDs</td>
<td>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.</td>
</tr>
<tr>
<td>TTP Codec</td>
<td>Voice codec which is being used to compress voice streams, it can be G.711 A-Law or U-Law</td>
</tr>
<tr>
<td>IPSI / Media 2N Recording Mode</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>• Disabled</td>
</tr>
<tr>
<td></td>
<td>• Primary</td>
</tr>
<tr>
<td></td>
<td>• Secondary</td>
</tr>
<tr>
<td>Active TTP Manager</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>In case the default API port (10031) is configured on the active Recording Director, only the IP address /hostname has to be defined.</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td>Management VLAN IP</td>
<td>IPv4 address of the NIC connecting IPSI management LAN. If it is not defined, it defaults to Server Local IPv4 address configuration.</td>
</tr>
<tr>
<td>Voice VLAN1 IP</td>
<td>IPv4 address of the NIC connecting IPSI VLAN A. If it is not defined, it defaults to Server Local IPv4 address configuration.</td>
</tr>
<tr>
<td>Voice VLAN2 IP</td>
<td>IPv4 address of the NIC connecting IPSI VLAN B. If it is not defined, it defaults to Server Local IPv4 address configuration.</td>
</tr>
<tr>
<td>Number of Media Processing Threads</td>
<td>Number of media processing threads to be used by the Media Recorder component</td>
</tr>
<tr>
<td>BT Heartbeat Listening Port</td>
<td>UDP port on which the Media Recorder listens to BT Heartbeat Service requests</td>
</tr>
<tr>
<td>TTP Timeout (seconds)</td>
<td>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.</td>
</tr>
<tr>
<td>TTP Distribution Timer (seconds)</td>
<td>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.</td>
</tr>
<tr>
<td>BT Heartbeat Service Timeout (seconds)</td>
<td>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</td>
</tr>
<tr>
<td>IPSI TFTP 1 URL</td>
<td>BT service is not responding within the configured timeout value, the BT services will be restarted to recover from error states.</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IPSI TFTP 2 URL</td>
<td>TFTP address on the IT Profile server where the global_ipconfig.txt is downloaded from. tftp://itslnksserver/global_ipconfig.txt</td>
</tr>
<tr>
<td></td>
<td>TFTP address on the IT Profile server where the global_ipconfig.txt is downloaded from. tftp://itslnksserver/global_ipconfig.txt</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITS Links</td>
<td>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.</td>
</tr>
<tr>
<td>ITSLink Server</td>
<td>FQDN or IP address of the BT ITSLink server</td>
</tr>
<tr>
<td>Port</td>
<td>port on which the BT ITSLink server listens (defaults to 3001)</td>
</tr>
<tr>
<td>Secondary</td>
<td>defines if the CTI/CDR record is primary or secondary when multiple Recording Directors are deployed.</td>
</tr>
<tr>
<td>ITS Link Timeout (seconds)</td>
<td>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.</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trader Provisioning Source</td>
<td>Defines the source of information for provisioning BT ITS configuration. The following valid values apply:</td>
</tr>
<tr>
<td>LDAP/TMS Polling Timer (seconds)</td>
<td>Defines how often the TMS files are read and the data is synchronized</td>
</tr>
<tr>
<td>TMS Files SMB Folder Path</td>
<td>The path of the DataFiles folder on the ITS Profile server</td>
</tr>
<tr>
<td>TMS Files SMB User</td>
<td>The username configured for SMB authentication</td>
</tr>
<tr>
<td>TMS Files SMB Password</td>
<td>The password configured for SMB authentication</td>
</tr>
</tbody>
</table>

**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.
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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trader Provisioning Source</td>
<td>Defines the source of information for provisioning BT ITS configuration. The following valid values apply:</td>
</tr>
<tr>
<td></td>
<td>• TMS Share</td>
</tr>
<tr>
<td></td>
<td>• LDAP</td>
</tr>
<tr>
<td>LDAP/TMS Polling Timer</td>
<td>Defines how often the LDAP directory is read and the data is synchronized</td>
</tr>
<tr>
<td>LDAP Server</td>
<td>Hostname or IP address of the BT ITS LDAP server</td>
</tr>
<tr>
<td>LDAP User</td>
<td>Username for the LDAP server user</td>
</tr>
<tr>
<td>LDAP Password</td>
<td>Password for the LDAP server user</td>
</tr>
<tr>
<td>LDAP Base DN</td>
<td>Base DN for the data in the LDAP directory</td>
</tr>
</tbody>
</table>

**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.

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 client connecting to configured iCDS services or act as server accepting connection from any iCDS service.

Verba side settings

- 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 model for trader voice recordings which is important if silence suppression is utilized.

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 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 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 Enpoints? 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 ctl-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.

Step 8 - 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:

<table>
<thead>
<tr>
<th>Setting Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES IP Address</td>
<td>The IP Address of the AES server. One Recording Server can only connect to one AES server</td>
</tr>
<tr>
<td>AES Port Number</td>
<td>Communication port of the AES server</td>
</tr>
<tr>
<td>AES User Name</td>
<td>The user in AES that has the rights for DMCC to execute the necessary commands</td>
</tr>
<tr>
<td>AES User Password</td>
<td>The password of the AES User</td>
</tr>
<tr>
<td>AES Secure Connection</td>
<td>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</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>AES JKS Trust Store File</td>
<td>Location of the Trust Store. This needs to contain the public certificate of the AES</td>
</tr>
<tr>
<td>AES JKS Trust Store File Password</td>
<td>The password of the Trust Store</td>
</tr>
<tr>
<td>AES JKS Key Store File</td>
<td>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</td>
</tr>
<tr>
<td>AES JKS Key Store File Password</td>
<td>The password of the Key Store</td>
</tr>
<tr>
<td>Communication Manager IP Address</td>
<td>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)</td>
</tr>
<tr>
<td>Communication Manager Name</td>
<td>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)</td>
</tr>
<tr>
<td>AES API Version</td>
<td>Define the version of the AES</td>
</tr>
<tr>
<td>Preferred Codec</td>
<td>The comma (,) separated list of supported codecs</td>
</tr>
<tr>
<td>Dependency Mode for Multiple Registration</td>
<td>DEPENDENT or INDEPENDENT</td>
</tr>
<tr>
<td>Registration Retry Interval (seconds)</td>
<td>Upon failed registration, the component will wait for this amount of time before trying again</td>
</tr>
<tr>
<td>Default Device Password</td>
<td>The default password for extensions</td>
</tr>
<tr>
<td>Internal Domain, Number Pattern</td>
<td>A regex pattern that should match the internal directory numbers</td>
</tr>
<tr>
<td>Secondary Recording Server</td>
<td>Sets whether the Recording Server should be considered as secondary or not</td>
</tr>
<tr>
<td>Ignore Recording Rule Entries Without Device Password</td>
<td>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</td>
</tr>
<tr>
<td>Advanced Recording Rules Enabled</td>
<td>Enables XML-based advanced recording rules</td>
</tr>
<tr>
<td>Enable Beep Tones</td>
<td>Enables recording beep tones</td>
</tr>
<tr>
<td>Worker Thread Count</td>
<td>Amount of worker threads</td>
</tr>
<tr>
<td>Work Folder</td>
<td>The system will place temporary files into this folder</td>
</tr>
</tbody>
</table>
Step 6 - Configure the settings under the Avaya JTAPI node:

<table>
<thead>
<tr>
<th>Setting Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avaya Tlink Name</td>
<td>Tlink name to the Communication Manager. This is displayed on the interface of the AES</td>
</tr>
<tr>
<td>JTAPI User Name</td>
<td>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)</td>
</tr>
<tr>
<td>JTAPI User Password</td>
<td>The password of the AES user</td>
</tr>
<tr>
<td>JTAPI JKS Trust Store File</td>
<td>Location of the Trust Store. This is needed if the AVAYA Tlink is configured for secure communication. This needs to contain the public certificate of the AES.</td>
</tr>
</tbody>
</table>
**Verint Verba Collaboration Compliance Platform**

<table>
<thead>
<tr>
<th><strong>JTAPI JKS Trust Store File Password</strong></th>
<th>The password of the Trust Store</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Disable Agent ID Handling</strong></td>
<td>The use of agent IDs can be disabled</td>
</tr>
<tr>
<td><strong>Hunt Group for Monitored Agent(s)</strong></td>
<td>special/&quot;dummy&quot; group that includes all agents. This is needed for JTAPI to gather additional information on the users</td>
</tr>
<tr>
<td><strong>Agent Status Check Interval (seconds)</strong></td>
<td>The system queries the agents for their status with a time interval that is set here</td>
</tr>
</tbody>
</table>

### Avaya Recorder
- **Avaya DMCC**
- **Avaya JTAPI**

<table>
<thead>
<tr>
<th><strong>Avaya Tlink Name</strong></th>
<th>AVAYAECM658C5AAAE585</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>JTAPI User Name</strong></td>
<td>verba.spi_user</td>
</tr>
<tr>
<td><strong>JTAPI User Password</strong></td>
<td>*********</td>
</tr>
<tr>
<td><strong>JTAPI JKS Trust Store File</strong></td>
<td></td>
</tr>
<tr>
<td><strong>JTAPI JKS Trust Store File Password</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Disable Agent ID Handling</strong></td>
<td>No</td>
</tr>
<tr>
<td><strong>Hunt Group for Monitored Agent(s)</strong></td>
<td>45676</td>
</tr>
<tr>
<td><strong>Agent Status Check Interval (seconds)</strong></td>
<td>3600</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th><strong>Protocol</strong></th>
<th>vrp</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User</strong></td>
<td>verba</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>*********</td>
</tr>
<tr>
<td><strong>Host</strong></td>
<td>TESTRS1.VERBATEST.LOCAL</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td></td>
</tr>
</tbody>
</table>

**Step 9** - Click on the Save button at the bottom.
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

<table>
<thead>
<tr>
<th>Section Name</th>
<th>Parameter</th>
<th>Required Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TServer</td>
<td>msml-support</td>
<td>true</td>
<td>Set to true to enable support of the call recording solution.</td>
</tr>
<tr>
<td>TServer</td>
<td>resource-management-by-rm</td>
<td>true</td>
<td>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.</td>
</tr>
<tr>
<td>TServer</td>
<td>record-consult-calls</td>
<td>true</td>
<td>Specifies whether to record consult calls:</td>
</tr>
</tbody>
</table>
|              |                             |                |  - 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

![Configuration of MSML DN Object](image)

**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

<table>
<thead>
<tr>
<th>Section Name</th>
<th>Parameter</th>
<th>Required Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>gvp.service-parameters</td>
<td>recordingclient.recdest</td>
<td>fixed.sip:&lt;recording-server-ip&gt;:&lt;recording-server-sip-port&gt;</td>
<td>Recording servers URI, where the SIP Server sends the invite.</td>
</tr>
<tr>
<td>gvp.service-parameters</td>
<td>recordingclient.recmediactl</td>
<td>fixed,1</td>
<td>This value represents the number of invites</td>
</tr>
</tbody>
</table>

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 8.

**Step 10** - Add or modify the following options in the gvp.rm section
### 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.
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

Step 12 - Configure the MCP application and corresponding Resource Group

<table>
<thead>
<tr>
<th>Section Name</th>
<th>Parameter</th>
<th>Required Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrmrecorder</td>
<td>sip.routeset</td>
<td>sip:&lt;[rm-ip or FQDN]:[rm-port]&gt;</td>
<td>Host and port of Resource Manager</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Genesys T-Server IP(s)</td>
<td>After clicking on the gear icon at the end of the line, the following fields can be configured:</td>
</tr>
<tr>
<td></td>
<td>- User</td>
</tr>
<tr>
<td></td>
<td>- Password</td>
</tr>
<tr>
<td></td>
<td>- IP Address(es) and ports</td>
</tr>
<tr>
<td></td>
<td>the port should be separated by a</td>
</tr>
<tr>
<td>Internal Domain, Number Pattern</td>
<td>See Conversation direction detection using internal domain and number patterns</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Target Genesys Field for Verba Call ID</td>
<td>Verba will attach the Verba Call ID to this Genesys User Data Field.</td>
</tr>
<tr>
<td>Secondary Recording Service</td>
<td>Defines if the Recording Server is a secondary server when duplicate / 2N recording is configured</td>
</tr>
</tbody>
</table>

**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.

![Warning: 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 controlled 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

Configuring SPAN on Catalyst 5000

Configuring SPAN and RSPAN on Catalyst 4000 Running Hybrid Mode

Configuring SPAN and RSPAN on Catalyst 3550

Configuring SPAN and RSPAN on Catalyst 2950

Configuring SPAN on Catalyst 2900XL/3500XL

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.

![IP phone diagram]

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.

![Diagram](image)

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.

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.


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]
```

<table>
<thead>
<tr>
<th>name</th>
<th>The name of the recording platform. (1-80 characters)</th>
</tr>
</thead>
<tbody>
<tr>
<td>netAddress</td>
<td>This is the FQDN, host, or IP address of the recording platform.</td>
</tr>
<tr>
<td>port</td>
<td>This is the address port of the recording platform. (Integer 1 to 65535).</td>
</tr>
<tr>
<td>transportType</td>
<td>This is the SIP interface type (“UDP”, “TCP”, “Unspecified”)</td>
</tr>
<tr>
<td>mediaStream</td>
<td>This is the type of media stream defined either as “dual” or “stream”.</td>
</tr>
<tr>
<td>description value</td>
<td>This is the description of this recording platform.</td>
</tr>
</tbody>
</table>

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:

- ServiceProvider/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:


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) pass-through 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**

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.

<table>
<thead>
<tr>
<th>Conference Profile Setting</th>
<th>Recording Link Connection Status according to flag: ALLOW_NON_ENCRYPT_RECORDING_LINK_IN_ENCRYPT_CONF</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>YES</td>
</tr>
<tr>
<td>Encrypt All</td>
<td>Connected encrypted if possible, otherwise connected non-encrypted.</td>
</tr>
<tr>
<td>No Encryption</td>
<td>Connected non-encrypted.</td>
</tr>
<tr>
<td>Encrypt when possible</td>
<td>Connected encrypted if possible, otherwise connected non-encrypted.</td>
</tr>
<tr>
<td></td>
<td>NO</td>
</tr>
<tr>
<td></td>
<td>Connected only if encrypted, otherwise disconnected.</td>
</tr>
<tr>
<td></td>
<td>Connected non-encrypted.</td>
</tr>
<tr>
<td></td>
<td>Connected encrypted if possible, otherwise connected non-encrypted.</td>
</tr>
</tbody>
</table>

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.

Step 3 - Set configuration (an API Key and API User has to be set in advance on the RLS).

If the configuration is correct and the RLS was accessible, then the RLS information will be shown on the License screen.
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:

- 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

1. Customer dials the video call center
2. Incoming call from the Cisco Unified Border Element (CBE) gateway to Unified CVP
3. Incoming call to Unified CCE/Package CCE/HC for Contact Center from Unified CVP
4. Play Unified CVP studio video application
5. Unified CVP sends the call to the Cisco Unified Border Element/VXML Gateway
6. Unified CVP VXML Server application instructs VXML Gateway to connect to a specific dialed number (DN)
7. Cisco Unified Border Element sends the call to Verba Server with that DN
8. Caller receives video stream from the Verba Server
9. Agent is now available, Unified CVP sends the call to an agent

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:

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 the media files)
```

During processing the tool provides progress information and estimated time to finish processing.
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:

**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

To define a call rule, you need to specify the following:

- **Address (incoming number):** This should be the same as the VOH server's "Default Video Content Identifier." This is based on which Verba can associate the video clip to the VOH server.
- **Action:**
  - **Once:** If the video clip ends, Verba will terminate the call.
  - **Continuously:** Repeat video clip playback until the caller terminates.
- **Media file:** Select the 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 the changes, it will:

- Download media files on Verba servers running the Announcement service.
- Refresh services' configuration with changes in clip - incoming number association.

### Incoming Call Rule Configuration

Select the configuration with the following parameters:

- **Address:** 3000
- **Action:** Once
- **Media File:** Video-In-Queue-Clip1.vmf

Click **Save** to apply changes.
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)**

- 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**

**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

- 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)

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

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 sequence**: 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.
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**.

**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.

**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 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

**Step 1** - After starting the installer, select **Typical**

Please select the feature that you want to install.

- **Typical**
  - Install SynCTI Driver, most users use this option.

- **Advance**
  - Install SynCTI Driver, SynlPAnalyzer, SynlPRecorder Master, SynHMP

- **Full**
  - SynCTI Driver, SynlPAnalyzer, SynlPRecorder Master, SynlPRecorder Slaver, SynHMP, SynHMPCodec

- **SpecialOnly**
  - Install SynlPRecorder Slaver & SynHMPCodec

**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
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](http://www.synway.net/Download/Manual/HardwareManual/Rec_ATP006.pdf).

**Step 2** - To configure a channel for recording, add the following lines:

```xml
<Channel type="analog" id="" eid=""
<Device id="" name="" tapPort="" continuousRecord=""/>
</Channel>
```

**Step 3** - Fill in the properties of the channels and save the file.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
</table>

### Channel

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>type</strong></td>
<td>analog/voip: for Synway ATP recording use the &quot;analog&quot; value.</td>
</tr>
<tr>
<td><strong>id</strong></td>
<td>It can be a random string, you have to change it every configuration change in the channel.</td>
</tr>
<tr>
<td><strong>eid</strong></td>
<td>4char: Optional. For multi-tenant system this attribute shows the tenant id of the channel.</td>
</tr>
</tbody>
</table>

### Device

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>id</strong></td>
<td>The phone number of the agent.</td>
</tr>
<tr>
<td><strong>name</strong></td>
<td>The name of the agent.</td>
</tr>
<tr>
<td><strong>tapPort</strong></td>
<td>The tap port number where the line is plugged in.</td>
</tr>
<tr>
<td><strong>continuousRecord</strong></td>
<td>true/false: For continuous recording set it to &quot;true&quot;. For onhook-offhook based recording set it to &quot;false&quot;.</td>
</tr>
</tbody>
</table>

**NOTE:** It only works with normal analog PSTN lines.

### Example:

```xml
<?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:\Sh\C\ShConfig.ini
  - 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.

Step 8 - Click on the Service Control tab, and start the Verba Analogue and Radio Recorder Service by clicking on the icon.
Configuring the Verba Desktop Agent

The Verba Desktop Agent enables several advanced features:

- Agent View
- Recording pop-up
- Screen recording
- Auto-pause for PCI DSS

Prerequisites

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.

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, ITrade, 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.
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. 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", "facebookcom", "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.
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 database 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.

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 Repositroy (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.

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 Verba 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.
Step 3 - Click on the **Generate** button.

Step 4 - In the upper right corner click on the **Download CA Certificate** link.

**Stage 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:


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 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 prefered, 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 metadate**: 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

<table>
<thead>
<tr>
<th>Configuration Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local SIP Port Number</td>
<td>Port number used for SIP signaling communication. This port number has to match the configuration in other systems connecting to the service.</td>
</tr>
<tr>
<td>Silent Monitoring Enabled</td>
<td>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/disables the silent monitoring feature on the web application for calls recorded by this service.</td>
</tr>
<tr>
<td>Called Party Name</td>
<td>Display name of the service, which will be displayed as called party name on the caller phone device.</td>
</tr>
<tr>
<td>Default Menu Language</td>
<td>Default language setting for the voice menu.</td>
</tr>
<tr>
<td>SIP Transport Protocol</td>
<td>SIP signaling transport protocol configured in the SIP proxy. Values can be TCP or UDP. TCP is recommended.</td>
</tr>
<tr>
<td>Audio Format</td>
<td>The recorder application will use the selected file format and codec option to create the audio files.</td>
</tr>
<tr>
<td>PIN Entry Retries</td>
<td>Number of allowed PIN code entry attempts. After exceeding this number, the system plays an error prompt and disconnects the caller.</td>
</tr>
<tr>
<td>Public Recorder Access Number</td>
<td>Entry point (directory number) used to access the recording functionality. If you do not want to allow unauthenticated access to the recording service, do not configure this access number, leave it empty.</td>
</tr>
<tr>
<td>Authenticated Recorder Access Number</td>
<td>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.</td>
</tr>
<tr>
<td>Authenticated Recorder Access Number without Prompt</td>
<td>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.</td>
</tr>
<tr>
<td>Authenticated and Unauthorized Playback Access Number</td>
<td>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.</td>
</tr>
</tbody>
</table>
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.

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.

**Authenticated and Authorized Playback Access Number**

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.

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.

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.

### Advanced settings

The following table provides detailed instructions on each configuration setting:

<table>
<thead>
<tr>
<th>Configuration Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process Unicode Names</td>
<td>If enabled, the system treats the calling party names as Unicode characters.</td>
</tr>
<tr>
<td>Store Call Time in UTC/GMT</td>
<td>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 in displaying inaccurate date and time values.</td>
</tr>
<tr>
<td>Strip Domain from SIP Phone Numbers</td>
<td>If enabled, the system automatically strips the domain information from the SIP addresses and leaves the phone number information only.</td>
</tr>
<tr>
<td>Menu Timeout (seconds)</td>
<td>The system waits 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.</td>
</tr>
<tr>
<td>Call Timeout (seconds)</td>
<td>Defines the call timeout value in seconds, which is used to terminate the call if the reinvite was not successful.</td>
</tr>
<tr>
<td>Database Cache Folder</td>
<td>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.</td>
</tr>
<tr>
<td>Automatic Gain Control Enabled</td>
<td>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.</td>
</tr>
<tr>
<td>IVR Prompt Path</td>
<td>The path to the folder containing the prompt files used by the IVR. Network drives are not supported, because of reliability and performance issues.</td>
</tr>
</tbody>
</table>
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 Micorosoft 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. It’s 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.
Define the PSTN Gateway FQDN

Define the fully qualified domain name (FQDN) for the PSTN gateway.

FQDN: *

192.168.1.205
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.
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.

  ![On-demand Calls Buffer](image)

- 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 DTM 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 Fallback 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.

<table>
<thead>
<tr>
<th>Settings Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Hostname</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>- (local) - (SQL Server running co-hosted on the Verba server using the default 1433 port)</td>
</tr>
<tr>
<td></td>
<td>- verba-db-server.acme.com - (SQL Server using the default 1433 port)</td>
</tr>
<tr>
<td></td>
<td>- verba-db-server.acme.com:15001 - (SQL Server using the 15001 port)</td>
</tr>
<tr>
<td></td>
<td>- verba-db-server.acme.com\InstanceName - (SQL Server named instance using the default 1433 port)</td>
</tr>
<tr>
<td>Database Name</td>
<td>The name of the Verba database.</td>
</tr>
<tr>
<td>Database Windows Authentication</td>
<td>Set to Yes if Windows authentication used.</td>
</tr>
<tr>
<td>Database Login</td>
<td>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.</td>
</tr>
<tr>
<td>Database Password</td>
<td>The password for the SQL/Windows user.</td>
</tr>
<tr>
<td>Database Failover Partner</td>
<td>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.</td>
</tr>
</tbody>
</table>
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.**

<table>
<thead>
<tr>
<th><strong>Database Multi-Subnet Failover</strong></th>
<th>Set to Yes if Always-on database used with Multi-Subnet Failover configuration. <strong>Please note that in this case the ODBC 13.1 have to be used as Database Driver.</strong></th>
</tr>
</thead>
</table>
| **Database Driver**           | 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:  
  - SQL Server (default driver)  
  - Microsoft ODBC Driver 13.1, certain advanced features requires this driver instead of the default:  
    - Mirroring  
    - Always-on with multi-subnet failover  
    - SSL based connection encryption and when TLS 1.0 is disabled on the OS level  
  Microsoft ODBC Driver 13.1 download |
| **Enable SSL Encryption**     | Set to Yes if you want to set up SSL encryption. For more information see: [Configuring SSL encryption for database connections](https://docs.microsoft.com/en-us/sql/sql-server/install/configure-the-windows-firewall-to-allow-sql-server-access?view=sql-server-2016) |
| **Java Trust Store Path**     | Java Trust Store path used for SSL encryption. For more information see: [Configuring SSL encryption for database connections](https://docs.microsoft.com/en-us/sql/sql-server/install/configure-the-windows-firewall-to-allow-sql-server-access?view=sql-server-2016) |
| **Java Trust Store Password** | The password for the Java Trust Store. For more information see: [Configuring SSL encryption for database connections](https://docs.microsoft.com/en-us/sql/sql-server/install/configure-the-windows-firewall-to-allow-sql-server-access?view=sql-server-2016) |

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](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

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


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 truststore.ks
```

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 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


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:

- 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/altered 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.

```sql
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.


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.

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.

```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>
/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 model for trader voice recordings 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**

<table>
<thead>
<tr>
<th>Protocol</th>
<th>vrp</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>verba</td>
</tr>
<tr>
<td>Password</td>
<td>*********</td>
</tr>
<tr>
<td>Host</td>
<td>DEVFE1SFB</td>
</tr>
<tr>
<td>Port</td>
<td>10500</td>
</tr>
<tr>
<td>Priority</td>
<td>1</td>
</tr>
</tbody>
</table>

**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.

**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.

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).

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

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.

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.
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.

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:

```xml
<Connector
    SSLEnabled="true"
    port="443"
    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 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-1.0.2q-i386-win32.zip](https://indy.fulgan.com/SSL/openssl-1.0.2q-i386-win32.zip)

**Step 2** - Extract the downloaded .zip file and start the openssl.exe

**Step 3** - Execute the following commands:

<table>
<thead>
<tr>
<th>For .p12 files</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>pkcs12 -in yourP12File.p12 -nocerts -out privateKey.pem</code></td>
</tr>
<tr>
<td><code>pkcs12 -in yourP12File.p12 -clcerts -nokeys -out publicCert.pem</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>For .pfx files</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>pkcs12 -in yourPfxFile.pfx -nocerts -out privateKey.pem</code></td>
</tr>
<tr>
<td><code>pkcs12 -in yourPfxFile.pfx -out publicCert.pem</code></td>
</tr>
<tr>
<td><code>x509 -inform pem -in publicCert.pem -pubkey -out publicCert.pem -outform pem</code></td>
</tr>
</tbody>
</table>

When it asks for password enter the password of the certificate

**Step 4** - Change the created privateKey.pem to .key and publicCert.pem to .crt
# 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.

<table>
<thead>
<tr>
<th>Component</th>
<th>How to Configure TLS 1.2</th>
</tr>
</thead>
</table>
| Internal communication between Verba servers and components | **Step 1** - Ensure that TLS 1.2 is not disabled on the Verba servers  
**Step 2** - Open the Web Application and navigate to **System**\**Server**  
and select the server  
**Step 3** - Select the **Change Configuration Settings** tab, **Server Certificate** - **Advanced TLS Settings** node  
**Step 4** - Set **Enable TLSv1** and **Enable TLSv1.1** to **No**, and **Enable TLSv1.2** to **Yes**  
**Step 5** - Save the changes and click on the **click here** link to apply the changes |
| 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 | **Step 1** - Go to the Java home directory  
**Step 2** - Open the **conf/security/java.security** or **lib/security/java.security** (JDK 8 and earlier) file using notepad with elevated permissions  
**Step 3** - Change the **jdk.tls.disabledAlgorithms** property by appending ", TLSv1, TLSv1.1"  
As an example:  
`jdk.tls.disabledAlgorithms=SSLv3, RC4, DES, MD5withRSA, DH keySize < 1024, \ 
EC keySize < 224, 3DES_EDE_CBC, anon, NULL, TLSv1, TLSv1.1`  
**Step 4** - Save the changes  
**Step 5** - Restart the impacted Verba Service |
| HTTPS connection with the Web Application | Follow the instructions on all Media Repository Servers:  
**Step 1** - Go to **C:\Program Files\Verba\tomcat\conf**  
**Step 2** - Create a backup of the **server.xml** file  
**Step 3** - Open the **server.xml** file using notepad with elevated permissions  
**Step 4** - Change the value of the **SSLProtocol** from "TLSv1+TLSv1.1" to "TLSv1.1+TLSv1.2"  
**Step 5** - Save the changes  
**Step 6** - Restart the Verba Web Application Service |
| Encrypted SQL Server communication | Follow the information in the following article: [https://support.microsoft.com/en-gb/help/3135244/tls-1-2-support-for-microsoft-sql-server](https://support.microsoft.com/en-gb/help/3135244/tls-1-2-support-for-microsoft-sql-server)  
To enable encrypted communication with the SQL Server in Verba, follow [Configuring encryption for database connections](https://support.microsoft.com/en-gb/help/3135244/tls-1-2-support-for-microsoft-sql-server) |
| 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 | |
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 1.0 and TLS 1.1 protocols on Windows follow the instructions:

**Step 1 - Add the following registries on all bot servers:**

```plaintext
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Client]
"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

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Client]
"DisabledByDefault"=dword:00000001
"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server]
"DisabledByDefault"=dword:00000001
"Enabled"=dword:00000000
```

The following .reg file contains the above registries and it can be simply run on the servers:
Step 2 - Restart the Verba Microsoft Teams Bot Service

Disable TLS10-11.reg
Configuring the Monthly License Summary Email

AVAILABLE IN 8.4 AND LATER

Overview

Your Verba platform can send License Summary emails every month to a set of email addresses. This can be sent to your admin/license team or (if needed) directly to Verba. The included information is similar to the contents of the System / License menu in the Verba web application.

Steps

Follow these steps to configure

1. Login to the Windows server running the Verba system
2. Run regedit.exe to configure the Windows registry
3. Go to HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Verba\Web
   (note: on your system Wow6432Node might not be in the key path)
4. Write a comma separated email list into the following STRING key: LicenseSendMonthlyTo (create if does not exist)
5. Set day of month for sending (default is 1), set the following DWORD key: LicenseSendMonthlyOnDay (create if does not exist)

The email will be sent according to the hour (in UTC timezone) defined in HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Verba\RunDailyJobsAtHour key (DWORD), default value is 1.
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 **execute** 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
Network settings

System

The following table provides detailed instructions on each configuration setting:

<table>
<thead>
<tr>
<th>Configuration Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server IP Address</td>
<td>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.</td>
</tr>
<tr>
<td>Server S-NAT/Public IPv4 Address</td>
<td>The IPv4 address of the server which is visible from outside network. This is required in several cases when the recorder has to advertise its external IP address also, so the remote party can connect.</td>
</tr>
<tr>
<td>Server IPv6 Address</td>
<td>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.</td>
</tr>
<tr>
<td>Server S-NAT/Public IPv6 Address</td>
<td>The IPv6 address of the server which is visible from outside 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.</td>
</tr>
<tr>
<td>Multi-Tenant Mode</td>
<td>If set to Yes, then the server will be in Multi-Tenant mode. For more information see: Multitenancy</td>
</tr>
</tbody>
</table>

Recording

The following table provides detailed instructions on each configuration setting:

<table>
<thead>
<tr>
<th>Configuration Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telephony Gateway IP Addresses</td>
<td>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.</td>
</tr>
</tbody>
</table>
## Directory settings

The following table provides detailed instructions on each configuration setting:

<table>
<thead>
<tr>
<th>Configuration Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media Folder</td>
<td>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.</td>
</tr>
<tr>
<td>Log Folder</td>
<td>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.</td>
</tr>
<tr>
<td>Application Folder</td>
<td>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.</td>
</tr>
<tr>
<td>Temporary Folder</td>
<td>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.</td>
</tr>
</tbody>
</table>
Cisco Central Silent Monitoring Configuration settings

Features

The following table provides detailed instructions on each configuration setting:

<table>
<thead>
<tr>
<th>Configuration Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Silent Monitoring Enabled</td>
<td>Sets whether the silent monitoring is enabled or not.</td>
</tr>
<tr>
<td>Whisper Coaching Enabled</td>
<td>Sets whether the whisper coaching is enabled or not.</td>
</tr>
</tbody>
</table>

Settings

The following table provides detailed instructions on each configuration setting:

<table>
<thead>
<tr>
<th>Configuration Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco UCM IP Address(es)</td>
<td>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.</td>
</tr>
<tr>
<td>JTAPI User Name</td>
<td>Login name of the user configured in Cisco Unified Communications Manager allows monitoring the recorded phones via JTAPI.</td>
</tr>
<tr>
<td>JTAPI User Password</td>
<td>Password of the user configured in Cisco Unified Communications Manager, which monitoring the recorded phones via JTAPI.</td>
</tr>
<tr>
<td>Play Tone Setting</td>
<td>Indicates whether the tone needs to be played to the target, to the caller, or both during the silent monitoring session.</td>
</tr>
<tr>
<td>Work Folder</td>
<td>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.</td>
</tr>
<tr>
<td>API Port</td>
<td>Sets the incoming API port of the Verba Cisco Central Silent Monitoring service.</td>
</tr>
</tbody>
</table>
Cisco JTAPI Configuration settings

Basics

The following table provides detailed instructions on each configuration setting:

<table>
<thead>
<tr>
<th>Configuration Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco UCM Cluster(s)</td>
<td></td>
</tr>
<tr>
<td>Cisco UCM IP Address(es)</td>
<td>Comma (,) separated list of the IP Addresses of the CUCM servers. All CUCM addresses need to be configured where the CTIManager service is enabled. The system will always use the first address, and fail over to the next one in the list if the primary CTIManager is down. Only a single CUCM cluster can be configured.</td>
</tr>
<tr>
<td>JTAPI User Name</td>
<td>The name of the user configured in the CUCM as an Application user.</td>
</tr>
<tr>
<td>JTAPI User Password</td>
<td>The password of the user configured in the CUCM as an Application user.</td>
</tr>
</tbody>
</table>

Cisco UCCX Integration

The following table provides detailed instructions on each configuration setting:

<table>
<thead>
<tr>
<th>Configuration Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco UCCX IP Address(es)</td>
<td>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.</td>
</tr>
</tbody>
</table>

Cisco UCCE Integration

The following table provides detailed instructions on each configuration setting:

<table>
<thead>
<tr>
<th>Configuration Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco UCCE PG CTI Server IP(s) and port(s)</td>
<td></td>
</tr>
<tr>
<td>CTI Server Protocol Version</td>
<td></td>
</tr>
<tr>
<td>Peripheral ID</td>
<td></td>
</tr>
</tbody>
</table>

Genesys Integration

The following table provides detailed instructions on each configuration setting:

<table>
<thead>
<tr>
<th>Configuration Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Genesys T-Server IP(s)</td>
<td></td>
</tr>
<tr>
<td>Target Genesys Field for Verba Call ID</td>
<td>Verba will attach the Verba Call ID to this Genesys User Data Field.</td>
</tr>
</tbody>
</table>

Advanced

The following table provides detailed instructions on each configuration setting:

<table>
<thead>
<tr>
<th>Configuration Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Service Port</td>
<td>Port number for the service.</td>
</tr>
<tr>
<td>Work Folder</td>
<td>Work folder path.</td>
</tr>
<tr>
<td>Advanced Recording Rules Enabled</td>
<td>When enabled, the service uses a special XML file for recording rules. For more information, see Advanced Call Recording Rules.</td>
</tr>
</tbody>
</table>
### Unified Call Recorder service configuration reference for Cisco network based recording

<table>
<thead>
<tr>
<th>Configuration Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secondary Recording Service</td>
<td>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.</td>
</tr>
</tbody>
</table>

### Media Recorder

The following table provides detailed instructions on each configuration setting:

<table>
<thead>
<tr>
<th>Configuration Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Unified Call Recorder \ Media Recorder \ Incoming Connection</strong></td>
<td></td>
</tr>
<tr>
<td>User</td>
<td>The username for authenticating the connection between the local Media Recorder and the Recording Directors.</td>
</tr>
<tr>
<td>Password</td>
<td>The user password for authenticating the connection between the local Media Recorder and the Recording Directors.</td>
</tr>
<tr>
<td>Priority</td>
<td>Defines the priority of the local Media Recorder to provide weighted load balancing among the configured recorders.</td>
</tr>
<tr>
<td>Port</td>
<td>The port number used for the Recording Director connections.</td>
</tr>
<tr>
<td><strong>Unified Call Recorder \ Media Recorder \ Basic</strong></td>
<td></td>
</tr>
<tr>
<td>Media Recorder Enabled</td>
<td>Enables the Media Recorder component in the service. If the server is deployed as a Recording Director, this component need to be disabled.</td>
</tr>
<tr>
<td>Automatic Gain Control Enabled</td>
<td>The application automatically controls the gain in the audio file to provide more convenient user experience while listening back recordings.</td>
</tr>
<tr>
<td>Audio Format</td>
<td>The recorder application will use the selected file format and codec option to store the audio/voice conversations.</td>
</tr>
<tr>
<td>Video Format</td>
<td>The recorder application will use the selected file format and codec option to store the video conversations.</td>
</tr>
<tr>
<td>Bidirectional/Stereo Recording</td>
<td>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.</td>
</tr>
<tr>
<td>Call Timeout (seconds)</td>
<td>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.</td>
</tr>
<tr>
<td>Media Port Range Begin</td>
<td>Defines the beginning of the media port range used by the application to receive RTP streams from the UC platform.</td>
</tr>
<tr>
<td>Media Port Range End</td>
<td>Defines the end of the media port range used by the application to receive RTP streams from the UC platform.</td>
</tr>
<tr>
<td>Voice Activity Statistics</td>
<td>Enabled silence and talk-over detection.</td>
</tr>
<tr>
<td><strong>Unified Call Recorder \ Media Recorder \ Advanced</strong></td>
<td></td>
</tr>
<tr>
<td>Database Cache Folder</td>
<td>The path to the database cache folder without the name of the file. Use the</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Skip Calls Without Media</td>
<td>When enabled, the system will not create a database record for calls without any media.</td>
</tr>
<tr>
<td>Media Format Fallback Enabled</td>
<td>When enabled, the system is able to fall back to raw stream recording if certain codecs are detected to avoid drastic decrease in quality.</td>
</tr>
<tr>
<td>PCM Mixer Buffer Length (milliseconds)</td>
<td>Length of the mixer buffer in milliseconds.</td>
</tr>
<tr>
<td>RTP Stream Reorder Buffer Length (packets)</td>
<td>Size of the RTP packet capture/receiver buffer in packets used for RTP packet reordering.</td>
</tr>
<tr>
<td>Write XML Metadata</td>
<td>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.</td>
</tr>
<tr>
<td>SSL/TLS Certificate</td>
<td>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.</td>
</tr>
<tr>
<td>SSL/TLS Key</td>
<td>Path to the SSL/TLS key file.</td>
</tr>
<tr>
<td>SSL/TLS Key Password</td>
<td>Password for the SSL/TLS key.</td>
</tr>
</tbody>
</table>

**Unified Call Recorder \ Media Recorder \ JTAPI Integration**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco JTAPI Integration Enabled</td>
<td>Enables the integration with the Cisco JTAPI Service component.</td>
</tr>
<tr>
<td>Cisco JTAPI Services</td>
<td>The IP address or hostname of the Recording Director servers where the Cisco JTAPI Service is enabled. Multiple addresses can be configured.</td>
</tr>
</tbody>
</table>

**Unified Call Recorder \ Media Recorder \ Overload Thresholds**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concurrent Calls</td>
<td>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.</td>
</tr>
<tr>
<td>CPU (%)</td>
<td>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.</td>
</tr>
<tr>
<td>Network (%)</td>
<td>Limitation on the maximum network load (%) on the server. When</td>
</tr>
</tbody>
</table>
the threshold is reached, the system will notify the Recording Director component to stop assigning calls to the server.

<table>
<thead>
<tr>
<th>Disk Space (%)</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk Space (mbyte)</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Recording Providers**

The following table provides detailed instructions on each configuration setting:

<table>
<thead>
<tr>
<th>Configuration Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Unified Call Recorder \ Recording Providers \ General</strong></td>
<td></td>
</tr>
<tr>
<td>Internal Domain, Numbers Pattern</td>
<td>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).</td>
</tr>
</tbody>
</table>
| SIP URI Modification | The following valid value apply:  
  - **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 |

<table>
<thead>
<tr>
<th>Use Recording Rules</th>
<th>When enabled, the system will only record configured extensions.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Unified Call Recorder \ Recording Providers \ Remote Media Recorders</strong></td>
<td></td>
</tr>
<tr>
<td>Remote Media Recording Servers</td>
<td>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.</td>
</tr>
</tbody>
</table>
- **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.

<table>
<thead>
<tr>
<th>Connection Keepalive Interval (seconds)</th>
<th>Keep alive interval in milliseconds between the Media Recorder and the Recording Director.</th>
</tr>
</thead>
</table>

**Unified Call Recorder \ Recording Providers \ SIP/SIPREC**

<table>
<thead>
<tr>
<th>SIP Port</th>
<th>The port number used for SIP communication. It has to match the value configured at the UC platform.</th>
</tr>
</thead>
</table>

**Secure SIP Ports**

<table>
<thead>
<tr>
<th>Secure SIP Ports</th>
<th>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.</th>
</tr>
</thead>
</table>

**Cisco Partition Based Multitenant Processing**

<table>
<thead>
<tr>
<th>Cisco Partition Based Multitenant Processing</th>
<th>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.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Prefer Session Local Refreshing</th>
<th>SIP keepalive preferred role.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Expires Timer (seconds)</td>
<td>SIP session keep alive timer.</td>
</tr>
<tr>
<td>SIP Trunk Status Monitoring</td>
<td>When enabled, the system sends alerts if there is no SIP OPTIONS ping request on the SIP trunk.</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Configuration Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verba Web Application HTTP Port</td>
<td>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.</td>
</tr>
</tbody>
</table>

Password policy

Various settings for rules applied to Database Credentials passwords.

The following table provides detailed instructions on each configuration setting:

<table>
<thead>
<tr>
<th>Configuration Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Password Length</td>
<td>Defines the minimum length of the password fields in the system. The setting applies for all users configured on the web interface.</td>
</tr>
<tr>
<td>Passwords Expire after (days)</td>
<td>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.</td>
</tr>
<tr>
<td>Passwords Must Include Capital Letter</td>
<td>Password phrases must include at least one capital letter or not. The setting applies for all users configured on the web interface.</td>
</tr>
<tr>
<td>Passwords Must Include Numeric Character</td>
<td>Password phrases must include at least one numeric character or not. The setting applies for all users configured on the web interface.</td>
</tr>
<tr>
<td>Passwords Must Include Special Character</td>
<td>Password phrases must include at least one special character or not. The setting applies for all users configured on the web interface.</td>
</tr>
<tr>
<td>Password History Count</td>
<td>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.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Configuration Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Lockout Attempts Threshold</td>
<td>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.</td>
</tr>
<tr>
<td>User Lockout Threshold Reset After (minutes)</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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:

<table>
<thead>
<tr>
<th>Configuration Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strip Domain Information from Login ID</td>
<td>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.</td>
</tr>
<tr>
<td>Domain User Account Format</td>
<td>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.</td>
</tr>
<tr>
<td>Allow Single Sign-On for System Administrators</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Reporting**

Configuration settings for the Verba Reporting module.

The following table provides detailed instructions on each configuration setting:

<table>
<thead>
<tr>
<th>Configuration Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allowed Reporting Interval Start Time</td>
<td>Start time value for allowed reporting time period in hour: minute format.</td>
</tr>
<tr>
<td>Allowed Reporting Interval End Time</td>
<td>End time value for allowed reporting time period in hour: minute format.</td>
</tr>
<tr>
<td>Scheduled Reports Folder</td>
<td>Directory where the report scheduler service saves reports to.</td>
</tr>
<tr>
<td>Enable External Reporting Database</td>
<td>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.</td>
</tr>
<tr>
<td>External Reporting Database Name</td>
<td>Name of the database.</td>
</tr>
<tr>
<td>External Reporting Database Hostname or IP Address</td>
<td>Hostname or IP address of the external Verba Recording System reporting database.</td>
</tr>
</tbody>
</table>
### 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:

<table>
<thead>
<tr>
<th>Configuration Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Access Enabled</td>
<td>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.</td>
</tr>
<tr>
<td>Font Setting</td>
<td>The name of the font used on the entire web interface. The following valid values apply: Arial, Arial Narrow, Tahoma, Verdana, etc.</td>
</tr>
<tr>
<td>Event Log Purging Threshold (days)</td>
<td>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.</td>
</tr>
<tr>
<td>Default List Page Size</td>
<td>The number of listed records on one page.</td>
</tr>
<tr>
<td>Maximum Active Sessions</td>
<td>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.</td>
</tr>
<tr>
<td>Maximum Query Rows</td>
<td>Sets the maximum number of rows to retrieve in the result set of the call lists (results of the search screen).</td>
</tr>
<tr>
<td>Support Site URL</td>
<td>URL of the support site, which is available as a link in the menu of the web interface.</td>
</tr>
<tr>
<td>Click2Dial Enabled</td>
<td>Enable or disable Click2Dial feature.</td>
</tr>
<tr>
<td>Cisco Unified Communications Manager IP Address or Hostname</td>
<td>IP address or Hostname of the Cisco Unified Communications Manager. This parameter is used in the Click2dial feature.</td>
</tr>
<tr>
<td>Video Transcoding Enabled</td>
<td>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.</td>
</tr>
<tr>
<td>Hide Menu Item(s)</td>
<td>Comma(,) separated list of menu items, which has to be disabled on the web interface.</td>
</tr>
<tr>
<td>Configuration Parameter Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Hostname or IP Address of Waveform Service</td>
<td>Hostname or IP address of the Wave Formatter service. It is installed on the Verba Media Repository server by default.</td>
</tr>
<tr>
<td>HTTP Port</td>
<td>HTTP port number for accessing the Wave Formatter service.</td>
</tr>
<tr>
<td>Sampling Rate</td>
<td>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.</td>
</tr>
<tr>
<td>Call Segment Export Codec</td>
<td>Call segments exported are saved using the configured codec.</td>
</tr>
</tbody>
</table>

**Wave formatter settings**

Configuration settings for the Verba Wave Formatter service.

The following table provides detailed instructions on each configuration setting:

<table>
<thead>
<tr>
<th>Configuration Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname or IP Address of Waveform Service</td>
<td>Hostname or IP address of the Wave Formatter service. It is installed on the Verba Media Repository server by default.</td>
</tr>
<tr>
<td>HTTP Port</td>
<td>HTTP port number for accessing the Wave Formatter service.</td>
</tr>
<tr>
<td>Sampling Rate</td>
<td>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.</td>
</tr>
<tr>
<td>Call Segment Export Codec</td>
<td>Call segments exported are saved using the configured codec.</td>
</tr>
</tbody>
</table>

**Recording notification settings**
If this feature is enabled than 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 than 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:

<table>
<thead>
<tr>
<th>Configuration Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Recording Notification Display Enabled</strong></td>
<td>Enables or disables the sending of recording notification messages to XML capable IP phones. If this setting is enabled than 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 than this service is not available.</td>
</tr>
<tr>
<td><strong>Cisco Unified Communications Manager Push XML User ID</strong></td>
<td>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).</td>
</tr>
<tr>
<td><strong>Cisco Unified Communications Manager Push XML User Password</strong></td>
<td>The password of that Cisco Unified Communications Manager user, which is used to send recording notification messages to XML capable IP phones.</td>
</tr>
<tr>
<td><strong>Recording Notification Language</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Recording Notification Display Timeout</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
# CDR and Archived Content Importer settings

## General

The following table provides detailed instructions on each configuration setting:

<table>
<thead>
<tr>
<th>Configuration Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wait Time Between Query Cycles [sec]</td>
<td>If the schedule is set to No Schedule at any of the settings, this setting defines the time interval between the runs.</td>
</tr>
</tbody>
</table>

## CDR Import

The following table provides detailed instructions on each configuration setting:

<table>
<thead>
<tr>
<th>Configuration Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco CDR Column Filters</td>
<td>Sets which CDR records should be excluded from the CDR Import. Column names and values can be provided in &quot;column_name:value&quot; format, on at each line. The value is a regex.</td>
</tr>
<tr>
<td>Cisco External Device/IP Criteria</td>
<td>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.</td>
</tr>
<tr>
<td>Import Schedule</td>
<td>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.</td>
</tr>
<tr>
<td>Wait Time for Recorder's CDR [sec]</td>
<td>The CDR Reconciliation won't check the calls which are not older than the time specified in this setting.</td>
</tr>
<tr>
<td>Recheck Schedule</td>
<td>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.</td>
</tr>
</tbody>
</table>
Number of Days to Recheck Imported Records Set the number of days to recheck in case of CDR Import Recheck.

### Archive Import

The following table provides detailed instructions on each configuration setting:

<table>
<thead>
<tr>
<th>Configuration Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import Schedule</td>
<td>Sets the schedule of the Archive Import. The configuration can be changed by clicking on the icon, then following the wizard in the right panel.</td>
</tr>
<tr>
<td>Import Query Wait Time [sec]</td>
<td>The Archive importing won’t check the calls which are not older than the time specified in this setting.</td>
</tr>
</tbody>
</table>
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\Verba\ActiveRecorder\OutboundProxy:
    - The IP address of the PBX.
  - HKLM\SOFTWARE\Verba\ActiveRecorder\OutboundProxyPort:
    - The incoming SIP port of the PBX.

- Service Configuration:
  - \SIP\SIP User:
    - The login address of the user created for the recorder.
  - \SIP\SIP User Password:
    - The password
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
<?xml version="1.0" encoding="UTF-8"?>
<VerbaApi>
  <Request type="StartDialOutRecording" id="0" persistent="0">
    <CallId>random_guid</CallId>
  </Request>
</VerbaApi>
```
Step 6 - The recorder can be commanded by the following API call for hanging up the outgoing call:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<VerbaApi>
  <Request type="StopDialOutRecording" id="0" persistent="0">
    <CallId>sip_call_id</CallId>
  </Request>
</VerbaApi>
```
Integrated Windows Authentication

Overview

The web application can authenticate users using Microsoft Windows domain authentication information. If a user is logged into the Windows Domain on a PC, the same user can access the web application without authenticating again.

When the domain user opens the web interface the system automatically authenticates the Windows user against the AD and logs in him/her to the recording system seamlessly. However this still requires a user created in the Verba Recording System due to the need for configuration settings not available in active directory.

Do not confuse this SSO functionality with the separate Single Sign-On API, that allows Single Sign-on integration with any systems/portals using a simple web protocol.

This SSO function helps you stop managing user passwords and user deletions in the Verba Recording System. You will still need to create the users in Verba, configure access rights and assign phone numbers to them.

Configuring Integrated Windows Authentication

Follow three steps to enable/configure SSO.

**Step 1** - Make sure your Verba web app server in the same domain where your users are.

**Step 2** - Configure the web app for SSO. With System Administrator rights you fill find these under Administration menu / Verba Servers / (select your server) / Change Configuration Settings / Web Application Configuration / Single sign on settings. See the parameters in the Web application settings topic.

<table>
<thead>
<tr>
<th>Configuration Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strip Domain Information from Login ID</td>
<td>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.</td>
</tr>
<tr>
<td>Domain User Account Format</td>
<td>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.</td>
</tr>
<tr>
<td>Allow Single Sign-On for System Administrators</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Step 3** - Configure users with the login name in the Verba Recording System as in Active Directory

If you have problems with SSO verify the following:

- Integrated Windows Authentication browser requirements
- Integrated Windows Authentication server requirements

Accessing the web interface with IWA

In order to access the web interface using SSO, use the following URL:

http://ServerNameorIPAddress/verba/sso

When Verba is configured to use the secured SSL (HTTPS) protocol, to access the web interface, the following must be in the address bar: https://ServerNameorIPAddress/verba/sso

If a user already logged in to the domain of the web application, they can just access the system. If they are not logged in, the browser will automatically asks for the Windows user credentials.
You can use Active Directory / Windows Domain based authentication and standard Verba authentication at the same time on one system. Your users need to access the web interface using the above links to use SSO. Other web links do not provide this capability.

Forcing non-IWA login when IWA is enabled

It is possible to force a non SSO login by visiting the following URL:

https://ServerNameorIPAddress/verba/login.do

Changing the default login procedure to single sign-on

You can change the above behaviour, where SSO requires a separate link.

Step 1 - If you have not already done that, please follow the above steps to enable SSO

Step 2 - Access the Verba server using Remote desktop

Step 3 - Open the <PROGRAM FILES>Verba\tomcat\webapps\ROOT\index.html file where <PROGRAM FILES> is e.g. "C:\Program Files (x86)"

Step 4 - Change the META line from

```
  <META HTTP-EQUIV="Refresh" CONTENT="0; URL=/verba">
```

To

```
  <META HTTP-EQUIV="Refresh" CONTENT="0; URL=/verba/sso">
```

Step 5 - This change goes live without any restart, point your browser to http://ServerNameorIPAddress
Integrated Windows Authentication browser requirements

If you have problems with IWA, verify the following:

- **For all types of browsers**
  - Use the hostname of the server instead of the IP address
  - Use https, make sure the server’s certificate is trusted by the browser
  - Add the URL to Local intranet zone in IE even if you use Chrome or Firefox

  AD SSO might not work if Internet Explorer does not consider the server as a Local Intranet site. Make sure you add your service domain URL (e.g. verba.company.com) to the Local intranet zone in Internet Explorer.

  Use the hostname of the server instead of the IP address
  Use https, make sure the server's certificate is trusted by the browser
  Add the URL to Local intranet zone in IE even if you use Chrome or Firefox

  Internet Explorer
  - Strange error pages with HTTP Status 401

  Internet Explorer users may occasionally receive strange error pages after logged in to Verba using Single Sign On. Unfortunately, the cause of the issue is an Internet Explorer feature and can be solved on the client computer only. Microsoft has confirmed that this is a problem with the Microsoft products.

  The only workaround currently is to disable NTLM Pre-Authentication on the client computer:

  Internet Explorer users may occasionally receive strange error pages after logged in to Verba using Single Sign On. Unfortunately, the cause of the issue is an Internet Explorer feature and can be solved on the client computer only. Microsoft has confirmed that this is a problem with the Microsoft products.

  The only workaround currently is to disable NTLM Pre-Authentication on the client computer:

  Use Registry Editor (RegEdt32.exe) to add a value to the following registry key: HKEY_CURRENT_USER/Software/Microsoft /Windows/CurrentVersion/Internet Settings/

  Add the following registry value:

  Value Name: DisableNTLMPreAuth
  Data Type: REG_DWORD
  Value: 1

  A description and the same workaround from Microsoft can be read here: [http://support.microsoft.com/kb/2749007](http://support.microsoft.com/kb/2749007)

  - Ensure that “Enable Integrated Windows Authentication” is checked (by default it is).
  
  Go to Tools > Internet Options > Advanced
  
  Scroll down to the Security section
  
  Find “Enable Integrated Windows Authentication” and ensure that it is checked.

  - Firefox
  
  If SSO does not work (i.e. an unexpected login box appears, or HTTP 401 error comes up), probably the Verba server has to be added to the trusted SSO servers.

  At the address field, type about:config

  In the Filter, type network.n

  Double click on network.negotiate-auth.trusted-uris

  This preference lists the sites that are permitted to engage in SPNEGO Authentication with the browser

  Enter a comma-delimited list of trusted domains or URLs (for example: http://verbaserver.com).

  - Chrome

  - Everything should work properly without any further configuration.
Integrated Windows Authentication server requirements

- **Add the server to Windows Domain** - The server running the Verba web app (Media Repository component) has to be added to the Windows Domain where your users are. Currently, there is no simple SSO solution for organizations with multiple domains.
- **Tomcat has to be run as a service with Local System or Network Service account** to enable all types of authentication. Or **alternatively**, use the following `setspn` commands in your AD:

  ```
  setspn -S HTTP/Verbaserver-name.domain.com verba-service-user
  setspn -S HTTP/Verbaserver-name domain\verba-service-user
  setspn -S HTTP/Verbaserver-name.domain.com domain\verba-service-user
  ```

  You should wait one day for the `setspn` commands to take effect!

- If you have done the client side requirements as well and you are still having issues with SSO then navigate to `C:\Program Files\Verba\tomcat\webapps\verba\META-INF\context.xml` and uncomment the following line:

  ```
  <!-- By default, this parameter is not set -->
  <Parameter name="onlyntlm" value="" override="false"/>
  ```

- **To enable logging** add this to the end of `C:\Program Files\Verba\tomcat\conf\logging.properties`:

  ```
  fr.doume.level = FINE
  ```
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.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channel</td>
<td></td>
</tr>
<tr>
<td>type</td>
<td>The type of the channel. The options are &quot;telex_roip&quot; or &quot;voip&quot;.</td>
</tr>
<tr>
<td>id</td>
<td>Unique ID for the channel. Can be anything.</td>
</tr>
<tr>
<td>eid</td>
<td>The Verba tenant environment ID for the channel. Required only in the case of multi-tenant Verba deployment.</td>
</tr>
<tr>
<td>Caller / Called</td>
<td></td>
</tr>
<tr>
<td>id</td>
<td>The ID of the caller / called. This field will populate the &quot;From&quot; or &quot;To&quot; (phone number) fields of the record.</td>
</tr>
<tr>
<td>name</td>
<td>The name of the caller / called. This field will populate the &quot;From Info&quot; or &quot;To Info&quot; fields of the record.</td>
</tr>
<tr>
<td>multicast</td>
<td>The multicast IP address of the recorder. Required only in the case of multicast listening.</td>
</tr>
<tr>
<td>port</td>
<td>The incoming port for the channel. In the case of single-channel RTP recording, the caller and called ports are the same.</td>
</tr>
<tr>
<td>codec</td>
<td>The codec of the incoming RTP stream. The options are &quot;G726_32&quot;, &quot;VOX&quot; or &quot;DV14&quot;. Required only in the case of Bosch Telex recording.</td>
</tr>
</tbody>
</table>

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:
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, 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.

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 - 2nd 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 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 filed 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 storage medium 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 download 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.
• Uploaded related features, such as retention period configuration, encryption/singing, 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 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 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 Disable server registration and API user configuration 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 is 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 policy 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** - 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.

**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.

#### 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 set 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:

<table>
<thead>
<tr>
<th>Call Direction</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal</td>
<td>Both participants are a match for the defined pattern</td>
</tr>
<tr>
<td>External</td>
<td>Neither of the participants is a match for the defined pattern</td>
</tr>
<tr>
<td>Incoming</td>
<td>Only the called party is a match for the defined pattern</td>
</tr>
<tr>
<td>Outgoing</td>
<td>Only the caller party is a match for the defined pattern</td>
</tr>
</tbody>
</table>

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


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 |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Match your domain</td>
<td>.*@yourdomain.com</td>
</tr>
<tr>
<td>Match SIP URI that starts with &quot;verba&quot; plus one or more characters and ends with &quot;@yourdomain.com&quot;</td>
<td>verba(w+)@yourdomain.com</td>
</tr>
<tr>
<td>Match extension name that starts with &quot;ext&quot; plus one or more characters and ends with &quot;@128.144.122.12:5080&quot;</td>
<td>ext(w+)@128:144:122:12:5080</td>
</tr>
<tr>
<td>Match one digit numbers</td>
<td>[0-9]</td>
</tr>
<tr>
<td>Match four digit numbers</td>
<td>[0-9][4]</td>
</tr>
<tr>
<td>Match numbers that start with 1213 and has one or more numbers at the end</td>
<td>1213[0-9]+</td>
</tr>
<tr>
<td>Match numbers that start with +1213 and has one or more</td>
<td>+1213[0-9]+</td>
</tr>
<tr>
<td>numbers at the end</td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------------------------------------------</td>
<td>---</td>
</tr>
<tr>
<td>Match numbers that start with 1213 and has 3 additional numbers at the end</td>
<td>1213[0-9]{3}</td>
</tr>
<tr>
<td>Match optional + sign at the beginning of a number</td>
<td>+1213</td>
</tr>
<tr>
<td>Multiple conditions, match numbers that start with +12 or +13 plus one or more numbers at the end</td>
<td>+(12</td>
</tr>
<tr>
<td>Multiple conditions, SIP URI / numbers</td>
<td>.*@yourdomain.com</td>
</tr>
<tr>
<td>Multiple conditions, multiple numbers</td>
<td>1213</td>
</tr>
</tbody>
</table>