Operation and Maintenance Guide

This guide is for system managers working with monitoring, troubleshooting, SQL administration and backup/restore operations.

System Monitoring

Troubleshooting

System backup

SQL Server administration and maintenance

Moving the database to another SQL Server

Failure scenarios and procedures

How to change service log level

How to replace a service executable

System Monitoring

Introducing monitoring procedures

Verba solutions depend on a number of external factors that might cause degradation of the recording, replay and archiving functionality:

1. Server hardware failures
2. Operating system failures or configuration errors
3. Network failures or configuration errors (both access and traffic spanning related)
4. Database server problems
5. Storage network failures
6. System overload

The Verba Call Recording System is built to provide call recording and replay functionality around the clock.
Verba Technologies constantly improves the reliability of Verba software and builds active monitoring and automatic intervention solutions to cope with failure situations due to software and other external problems.

In this topic the **monitoring and maintenance best practices** are summarized that will help you operate Verba safely.

> This topic does not deal with regular hardware, operating system and database monitoring and maintenance procedures. Your IT organization should take care of those parts according to respective product documentation or your existing processes.

We recommend designing and introducing monitoring procedures based on this article to ensure that problems are detected as early as possible to minimize downtime.

The following table shows a typical **Verba Monitoring Plan**:

Monitoring procedure		**Recommended frequency**
HW, OS and database (not detailed here)		Ongoing
Automated monitoring functions in Verba	Service health checks	Ongoing
	Memory monitoring	Ongoing
	Volume monitoring	Ongoing
	Idle monitoring	Ongoing
Manual monitoring procedures for Verba	Test calls	Weekly (if security policies does not allow listening to actual recorded calls)
	Simple system inspection	Monthly

Configuring SNMP Alert Traps

Overview

The built-in Verba monitoring solution supports **SNMP traps (v2),** using a Verba specific set of SNMP Trap OIDs. Please refer to the following article: Alerts

In order for it to work, you need to configure it on **all servers and desktop components** installed in your Verba system, such as:

- Verba Recording Servers
- Verba Media Repository
- Verba Desktop Recorders
- Verba Remote Components (e.g. Lync Filters, Remote Capture Providers)

Step 1 - Activate the Verba System Monitor Service

ⓘ **Verba System Monitor Service** is activated **by default** on all Verba systems and is configured for email sending. However it still worth checking that the service is not disabled and is actually running.

The SNMP traps are sent by the **Verba System Monitor Service**. In order to configure and use it, the service should be activated and started.

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 or desktop recorder from the list.

Step 3 - Click on the **Service Activation** tab.

Step 4 - Activate the **Verba System Monitor Service** using the ⚙ icon.

Step 5 - Verify under the **Service Control** tab that it is running. If not, start it with the ▶ icon.

Step 2 - Configure SNMP Traps

The following steps should be done for all servers and desktop components in your system. You can simplify the configuration of multiple servers and desktop components by using Verba server configuration profiles.

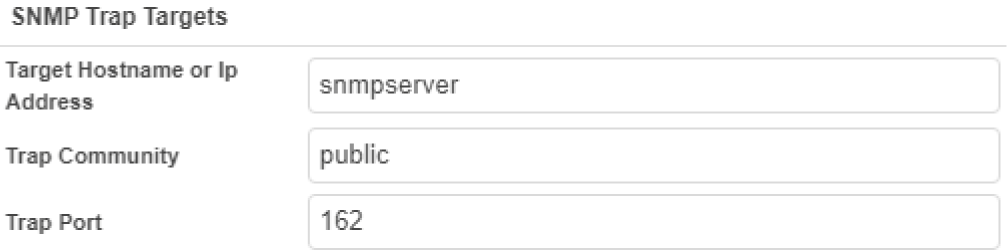
Step 1 - Go to the **Change Configuration Settings** tab of the server/desktop you want to configure

Step 2 - Open the **System Monitoring / SNMP Notification Target** category in the tree

Step 3 - Click on the ➕

icon for adding a new **SNMP Trap Target**.

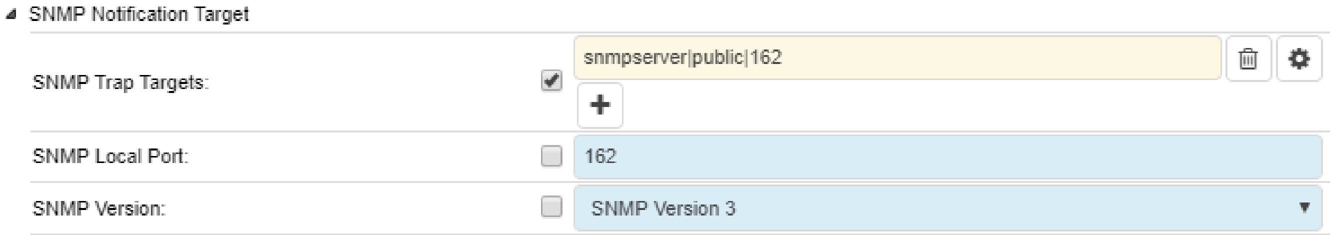
Step 4 - In the right panel, provide the **Target Hostname or Ip Address**, **Trap Communitiy** and **Trap Port** settings. Click **Save**.



SNMP Trap Targets

Target Hostname or Ip Address	snmpserver
Trap Community	public
Trap Port	162

Step 5 - After making the changes clicking on the **Save** button in top right corner of the configuration tree.

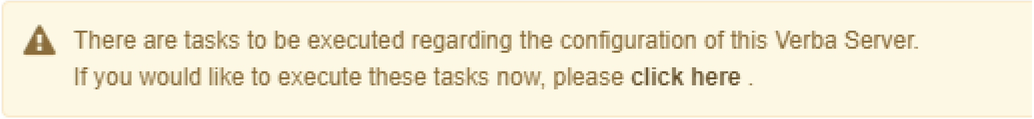


SNMP Notification Target

SNMP Trap Targets:	☑	snmpserver|public|162
SNMP Local Port:	□	162
SNMP Version:	□	SNMP Version 3

Step 6 - Set the **SNMP Version**.

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** .

SCOM Management Pack

Available in version 8.2 and later

The Verba SCOM Management Pack allows customers in a Microsoft Server Environment to monitor the health of their system using SCOM. SCOM (System Center Operations Manager) is an infrastructure/system monitoring solution form Microsoft standardized at many organizations: https://technet.microsoft.com/en-us/library/hh205987.aspx.

This page guides you through the import and installation procedure of the Verba SCOM Management Pack onto the Microsoft System Center Operations Manager tool.

Downloading the Verba SCOM Management Pack

The unsealed management pack, compatible with SCOM 2007 R2,2012, and 2019 can be downloaded from Verba support site at https://support.verba.com.

Importing the Management Pack

Follow the steps below to import the Verba management pack into Operations Manager:

Step 1 - Log on to the computer with an account that is a member of the Operations Manager Administrators role.

Step 2 - In the Operations console, click **Administration**.

Step 3 - Right-click **Management Packs**, and then click **Import Management Packs**.

Step 4 - The **Import Management Packs** wizard opens. Click **Add**, and then click **Add from disk**.

Step 5 - The **Select Management Packs to import** dialog box appears. If necessary, change to the directory that holds your management pack file. Click on the management packs to import from that directory, and then click **Open**.

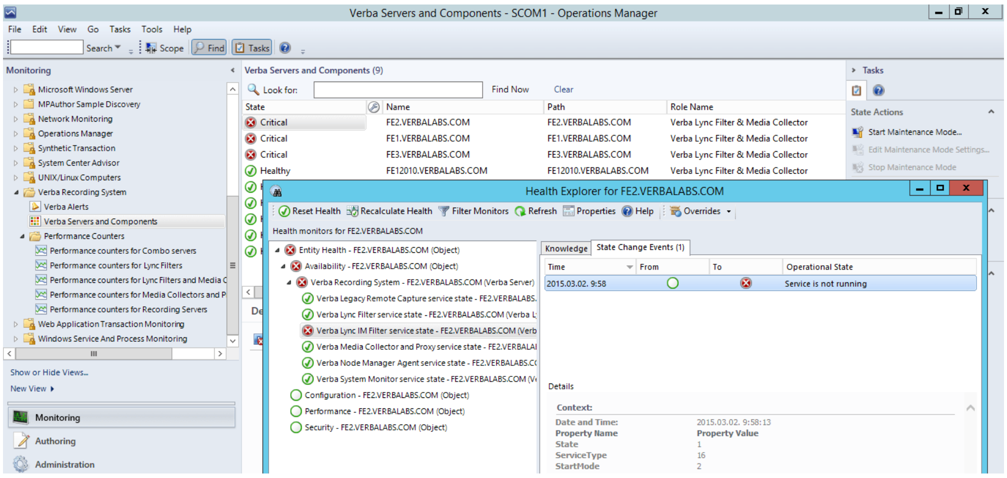
Step 6 - On the **Select Management Packs** page, the management packs that you selected for import are listed. Click **Import.**

Step 7 - The **Import Management Packs** page appears and shows the progress for each management pack. Each management pack is downloaded to a temporary directory, imported to Operations Manager, and then deleted from the temporary directory. If there is a problem at any stage of the import process, select the management pack in the list to view the status details. Click **Close**.

Verifying the installation

After importing the management pack, a Verba Recording System folder should appear in the Monitoring page. The discovery interval is one hour by default, so you may see all the Verba servers under the Verba Servers and Components view after an hour. The performance counters only appears when the corresponding services are running on the servers. If you can't see the counters please see the Troubleshooting performance counter access article.

SCOM sample screens


Verba Servers and Components - SCOM1 - Operations Manager
File Edit View Go Tasks Tools Help
Search Scope Find Tasks
Monitoring
Microsoft Windows Server
MPAuthor Sample Discovery
Network Monitoring
Operations Manager
Synthetic Transaction
System Center Advisor
UNIX/Linux Computers
Verba Recording System
Verba Alerts
Verba Servers and Components
Performance Counters
Performance counters for Combo servers
Performance counters for Lync Filters
Performance counters for Lync Filters and Media C
Performance counters for Media Collectors and P
Performance counters for Recording Servers
Web Application Transaction Monitoring
Windows Service And Process Monitoring
Show or Hide Views...
New View
Monitoring
Authoring
Administration
Tasks
State Actions
Start Maintenance Mode...
Edit Maintenance Mode Settings...
Stop Maintenance Mode
Reset Health
Recalculate Health
Filter Monitors
Refresh
Properties
Help
Overrides
Knowledge
State Change Events (1)

Verba Servers and Components (9)

Look for: Find Now Clear

State	Name	Path	Role Name
Critical	FE2.VERBALABS.COM	FE2.VERBALABS.COM	Verba Lync Filter & Media Collector
Critical	FE1.VERBALABS.COM	FE1.VERBALABS.COM	Verba Lync Filter & Media Collector
Critical	FE3.VERBALABS.COM	FE3.VERBALABS.COM	Verba Lync Filter & Media Collector
Healthy	FE12010.VERBALABS.COM	FE12010.VERBALABS.COM	Verba Lync Filter & Media Collector

Health Explorer for FE2.VERBALABS.COM

Health monitors for FE2.VERBALABS.COM

- Entity Health - FE2.VERBALABS.COM (Object)
  - Availability - FE2.VERBALABS.COM (Object)
    - Verba Recording System - FE2.VERBALABS.COM (Verba Server)
      - Verba Legacy Remote Capture service state - FE2.VERBALABS.
      - Verba Lync Filter service state - FE2.VERBALABS.COM (Verba L
      - Verba Lync IM Filter service state - FE2.VERBALABS.COM (Verb
      - Verba Media Collector and Proxy service state - FE2.VERBALAI
      - Verba Node Manager Agent service state - FE2.VERBALABS.C(
      - Verba System Monitor service state - FE2.VERBALABS.COM (V
  - Configuration - FE2.VERBALABS.COM (Object)
  - Performance - FE2.VERBALABS.COM (Object)
  - Security - FE2.VERBALABS.COM (Object)

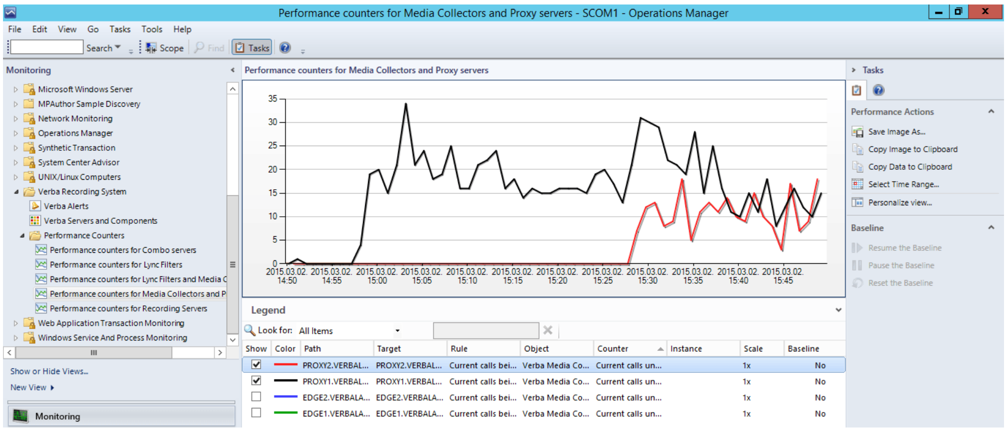
Time	From	To	Operational State
2015.03.02. 9:58	○	☒	Service is not running

Details

Context:

Date and Time:	2015.03.02. 9:58:13
Property Name	Property Value
State	1
ServiceType	16
StartMode	2

Verba Services and Components in SCOM

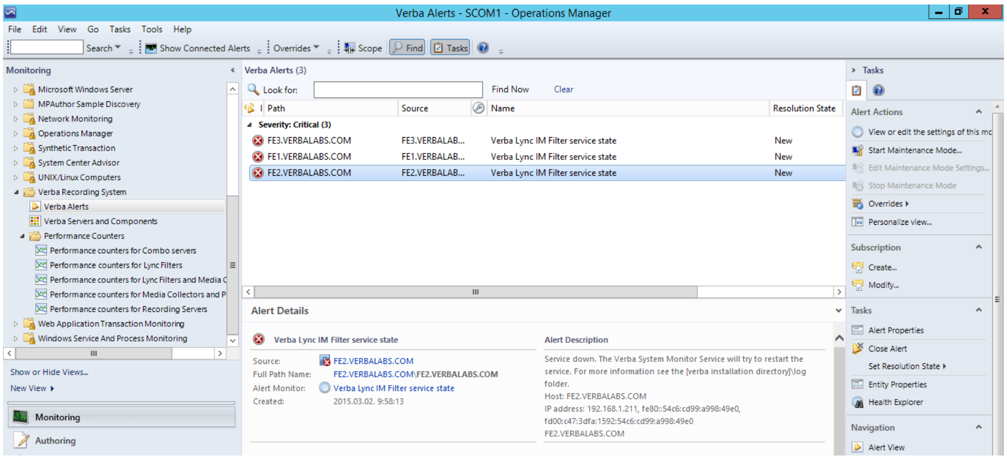


Legend

Look for: All Items

Show	Color	Path	Target	Rule	Object	Counter	Instance	Scale	Baseline
☑	🟥	PROXY2.VERBAL...	PROXY2.VERBAL...	Current calls bei...	Verba Media Co...	Current calls un...		1x	No
☑	⬛	PROXY1.VERBAL...	PROXY1.VERBAL...	Current calls bei...	Verba Media Co...	Current calls un...		1x	No
□	🟦	EDGE2.VERBALA...	EDGE2.VERBALA...	Current calls bei...	Verba Media Co...	Current calls un...		1x	No
□	🟩	EDGE1.VERBALA...	EDGE1.VERBALA...	Current calls bei...	Verba Media Co...	Current calls un...		1x	No

Verba Performance counters in SCOM


Verba Alerts - SCOM1 - Operations Manager
File Edit View Go Tasks Tools Help
Search Show Connected Alerts Overrides Scope Find Tasks
Monitoring
Microsoft Windows Server
MPAuthor Sample Discovery
Network Monitoring
Operations Manager
Synthetic Transaction
System Center Advisor
UNIX/Linux Computers
Verba Recording System
Verba Alerts
Verba Servers and Components
Performance Counters
Performance counters for Combo servers
Performance counters for Lync Filters
Performance counters for Lync Filters and Media C
Performance counters for Media Collectors and P
Performance counters for Recording Servers
Web Application Transaction Monitoring
Windows Service And Process Monitoring
Show or Hide Views...
New View
Monitoring
Authoring
Tasks
Alert Actions
View or edit the settings of this mo
Start Maintenance Mode...
Edit Maintenance Mode Settings...
Stop Maintenance Mode
Overrides
Personalize view...
Subscription
Create...
Modify...
Tasks
Alert Properties
Close Alert
Set Resolution State
Entity Properties
Health Explorer
Navigation
Alert View

Verba Alerts (3)

Look for: Find Now Clear

Path	Source	Name	Resolution State
Severity: Critical (3)			
FE3.VERBALABS.COM	FE3.VERBALAB...	Verba Lync IM Filter service state	New
FE1.VERBALABS.COM	FE1.VERBALAB...	Verba Lync IM Filter service state	New
FE2.VERBALABS.COM	FE2.VERBALAB...	Verba Lync IM Filter service state	New

Alert Details

Verba Lync IM Filter service state

Source: FE2.VERBALABS.COM
Full Path Name: FE2.VERBALABS.COM\FE2.VERBALABS.COM
Alert Monitor: Verba Lync IM Filter service state
Created: 2015.03.02. 9:58:13

Alert Description

Service down. The Verba System Monitor Service will try to restart the service. For more information see the [verba installation directory]\log folder.
Host: FE2.VERBALABS.COM
IP address: 192.168.1.211, fe80::54c6:cd99:a998:49e0, fd00:c47:3dfa:1592:54c6:cd99:a998:49e0
FE2.VERBALABS.COM

Verba Alerts in SCOM

Troubleshooting performance counter access

Performance counter access troubleshooting tips

Sometimes SCOM cannot access the custom performance counters generated by 3rd party applications. In order to sort this issue please check the following.

Collector service privileges and conectivity

Make sure that the collector service has **Local Administrator** privilege on the host where it wants to access to the performance counters. The **TCP** port **135** and **445** is has to be open.

Local services

Start the following services, and set the startup type to **Automatic** for the

- Remote Procedure Call (RPC)
- Remote Registry

services, and set at least **Manual** for the

- WMI Performance Adapter
- Performance Counter DLL Host
- Performance Logs and Alerts
- Remote Procedure Call (RPC) Locator

services.

Local Service privileges

If the issue still present, please do the following:

Step 1 - Open a **regedit** and navigate to the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Window NT\CurrentVersion\Perflib

Step 2 - Right click on **Perflib** key and select permissions

Step 3 - Click **Add** and add Local Service with full control

Step 4 - Save and exit

Step 5 - Restart the **Remote Registry Service**

Rebuilding Perfmon Performance Counters

If the steps above didn't help and you still can't see the performance counters in SCOM, you have to rebuild the performance counters and restart the server. Open an administrator command prompt and enter the following commands:

```
cd c:\windows\system32
lodctr /R
cd c:\windows\sysWOW64
lodctr /R
WINMGMT.EXE /RESYNCPERF
```

After this, restart the server. Don't forget to start the services specified above.

Accessing performance counters on Windows Server 2008 R2

Windows Server 2012 can only manage Windows Server 2012 and Hyper-V Server 2012 servers by default. For the other servers, the Windows Managemement Framework have to be installed. In order to access the performance counters on these servers please follow these steps:

Step 1 - Download and Install the Windows Management Framework 3.0 for Windows Server 2008 SP2 and Windows Server 2008 R2 SP1. The .Net Framework 4 is a prerequisite for this.

Step 2 - Install this hotfix: http://support.microsoft.com/kb/2682011

Step 3 - Execute the following PowerShell commands as administrator:

```
Set-ExecutionPolicy -ExecutionPolicy RemoteSigned
Configure-SMRemoting.ps1 -force -enable
```

Windows Performance Counters

Available in version 8.2 and later

Verba services offer performance counters to provide information as to how well the system or a service is performing. The counter data can help determine system bottlenecks and fine-tune system and service performance. The service counters are available as standard Windows Performance Counters on the servers.

Follow this guide to get familiar with Windows Performance Counters: https://technet.microsoft.com/en-us/library/cc749249.aspx

Service performance counters are also available through SCOM Management Pack.

Configuring email alerts

In order to send email alerts and SMTP server account need to be configured. Follow the steps below to configure an SMTP server and account:

Step 1 - In the Verba web interface click on **System \ Servers** and select your Media Repository server, or select the appropriate Configuration Profile at **System \ Configuration Profiles**.

Step 2 - Click on the **Change Configuration Settings** tab.

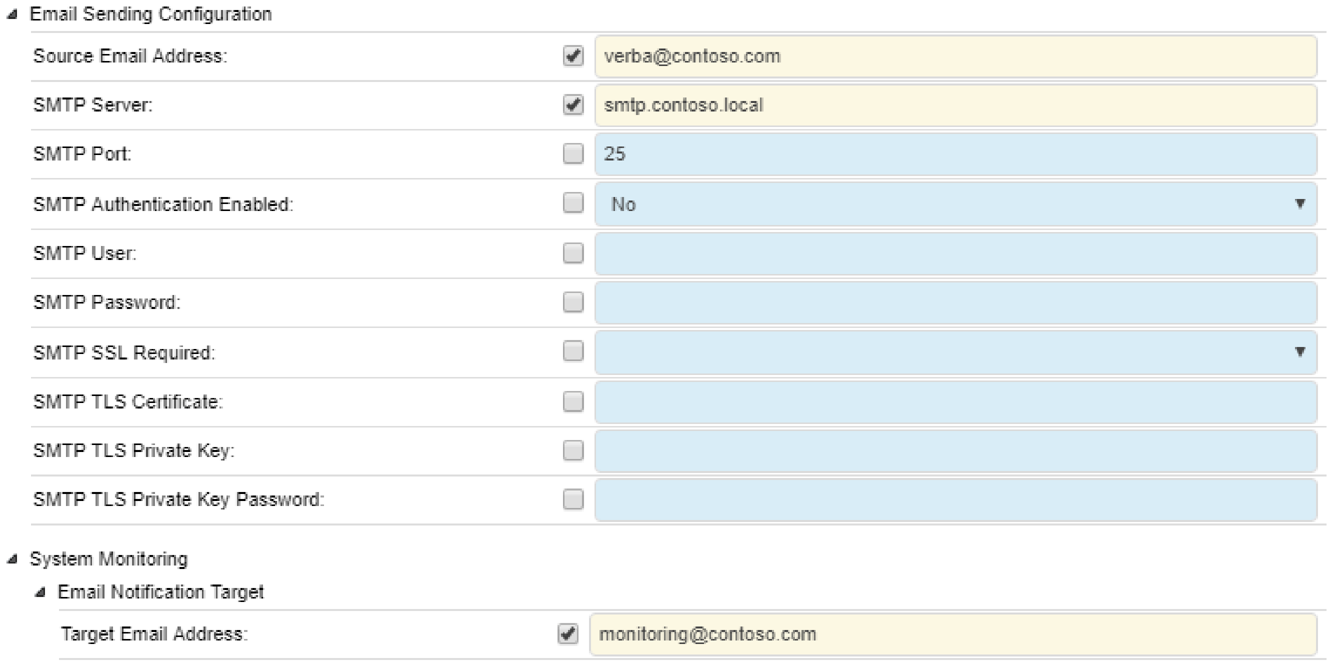
Step 3 - Expand **Email Sending Configuration**.

Step 4 - Configure settings based on your environment. See description below for more details.

Step 5 - Expand **System Monitoring / Email Notification Target**.

Step 6 - Configure **Target Email Address** to the email address of the recipient of the alerts.

Step 7 (Optional) - If required, change the SMTP Port and provide the other settings for the authentication and/or secure connection.



Email Sending Configuration

Source Email Address:	☑	verba@contoso.com
SMTP Server:	☑	smtp.contoso.local
SMTP Port:	□	25
SMTP Authentication Enabled:	□	No ▾
SMTP User:	□	
SMTP Password:	□	
SMTP SSL Required:	□	▾
SMTP TLS Certificate:	□	
SMTP TLS Private Key:	□	
SMTP TLS Private Key Password:	□	

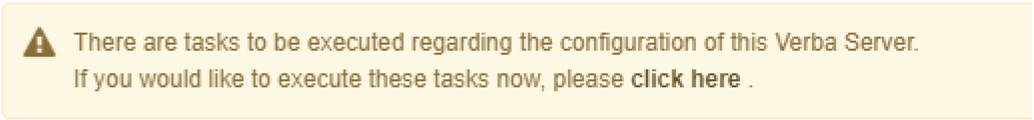
System Monitoring

Email Notification Target

Target Email Address:	☑	monitoring@contoso.com

Step 8 - Click the **Save** icon to save your settings

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.

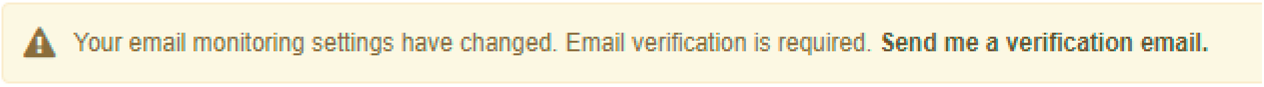


There are tasks to be executed regarding the configuration of this Verba Server.
If you would like to execute these tasks now, please **click here** .

Verifying the email settings

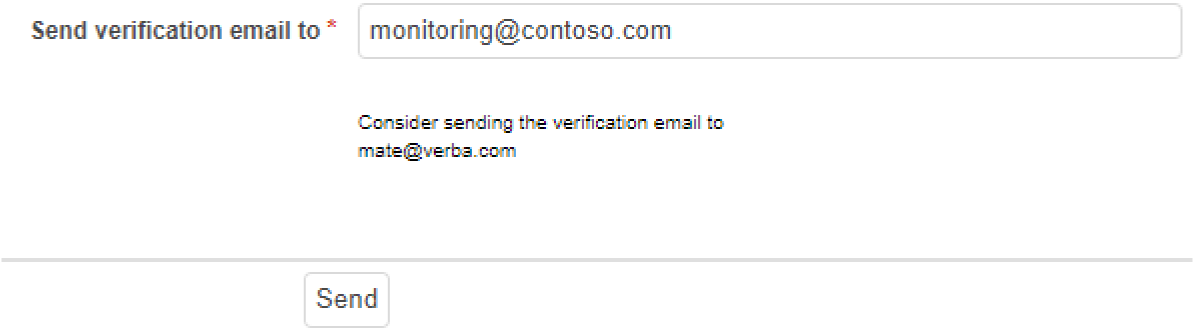
After the initial installation of the Verba system, a notification on the top shows that the email configuration is missing. Once the configuration is done, and the web application restarted this notification changes to a verification notification.

Step 1 - Click on the **Send me a verification email** link in the notification.



⚠ Your email monitoring settings have changed. Email verification is required. **Send me a verification email.**

Step 2 - Click on the Send button for sending out the notification email.



Send verification email to * monitoring@contoso.com

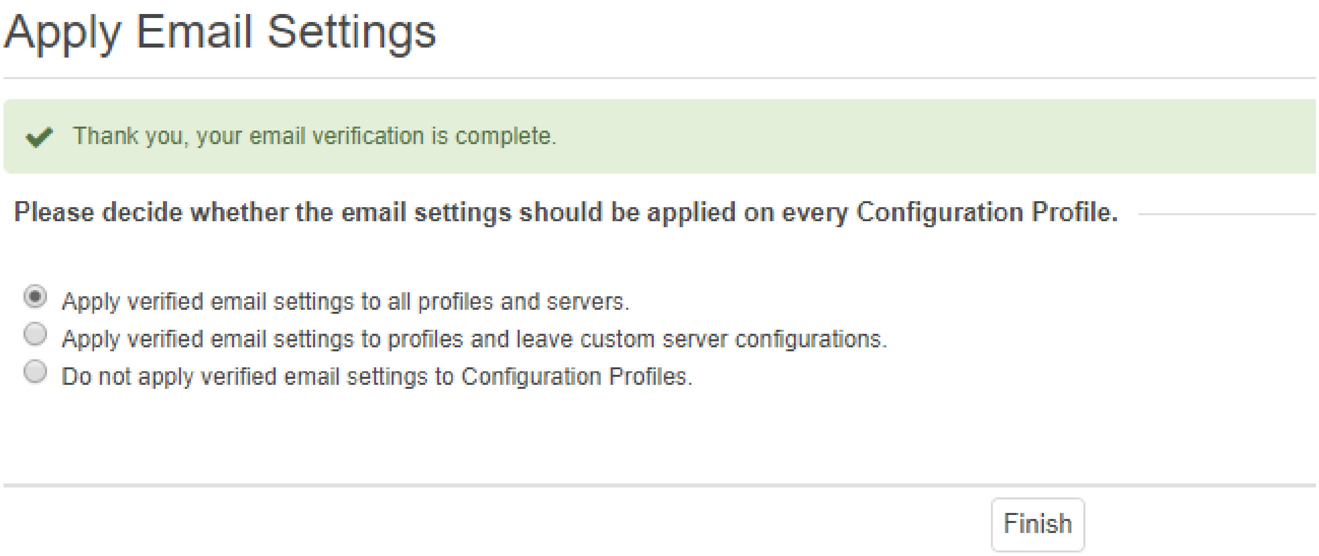
Consider sending the verification email to mate@verba.com

Step 3 - If the email settings are correct, then you will receive the verification email. Click on the link within this email.

Step 4 - The Verba Web Application opens. In order to use the same email configuration all Verba servers, select the **Apply verified email settings to all profiles and servers** option. (Recommended)

If you want to use the same email configuration on all Verba servers, except the ones where a server-specific configuration is being used, then select the **Apply verified email settings to profiles and leave custom server configurations** option.

If you have only one Verba server, or you want the other servers to keep intact, then select **Do not apply verified email settings to Configuration Profiles** setting.



Apply Email Settings

✓ Thank you, your email verification is complete.

Please decide whether the email settings should be applied on every Configuration Profile.

● Apply verified email settings to all profiles and servers.
○ Apply verified email settings to profiles and leave custom server configurations.
○ Do not apply verified email settings to Configuration Profiles.

Step 5 - Click **Finish**.

Configuration refence

Configuration Parameter Name	Description

Source Email Address	Verba sends notification emails using this address (from:email header).
SMTP Server	Hostname or IP address of SMTP server used for email sending.
SMTP Port	SMTP server port number.
SMTP Authentication Enabled	If enabled, Verba will try to authenticate with the SMTP server for email sending.
SMTP User	User to authenticate on the SMTP server.
SMTP Password	Password used to authenticate on the SMTP server.
SMTP SSL Required	Indicates if SSL based encryption is required or not for the connection with the SMTP server.
SMTP TLS Certificate	Thumbprint of the certificate being used for TLS connection. The certificate has to be found in the Windows Certificate Store. Alternatively, a path to a .crt file can be used.
SMTP TLS Private Key	If a path is being used at the SMTP TLS Certificate setting, then this setting has to contain the path to the corresponding .key file.
SMTP TLS Private Key Password	Password for the .key file.

Alerts

IANA Enterprise Number

The Verba Technologies assigned enterprise number at IANA is **39067**.

The official list of IANA Enterprise Numbers can be found here: http://www.iana.org/assignments/enterprise-numbers

MIB of Verba SNMP Traps

SNMP trap OIDs are under our enterprise prefix **1.3.6.1.4.1.39067**. The SNMP Traps follow **SNMP Version 2c**.

Here is the SMIv2 Verba MIB file.

Overriding alerts

It is possible to customize the alert severities and their targets. For the configuration guide, see: Customizing Alert Severities and Selective Alert Sending

General alerts

Alert Name	Severity	Trap OID	Event ID	Resolved by
Free Memory Low	Fatal	1.3.6.1.4.1.39067.**100.0.1**	1	Free Memory OK
Free Memory OK	Fatal	1.3.6.1.4.1.39067.**100.0.2**	2	-
Disk Space Low	Fatal	1.3.6.1.4.1.39067.**100.0.3**	3	Disk Space OK
Disk Space OK	Fatal	1.3.6.1.4.1.39067.**100.0.4**	4	-
Service Down	Fatal	1.3.6.1.4.1.39067.**100.0.5**	5	Service Up
Service Up	Fatal	1.3.6.1.4.1.39067.**100.0.6**	6	-
Recording Inactivity	Fatal	1.3.6.1.4.1.39067.**100.0.7**	7	Recording Inactivity Over
Database Connection Down	Critical	1.3.6.1.4.1.39067.**100.0.10**	10	Database Connection Up
Database Connection Up	Critical	1.3.6.1.4.1.39067.**100.0.11**	11	-
Database Error	Critical	1.3.6.1.4.1.39067.**100.0.12**	12	-
Prerequisite Missing	Fatal	1.3.6.1.4.1.39067.**100.0.13**	13	-
Recording Inactivity Over	Fatal	1.3.6.1.4.1.39067.**100.0.14**	14	-
Certificate is not accessible	Fatal	1.3.6.1.4.1.39067.**100.0.15**	15	-
Certificate expires	Warning	1.3.6.1.4.1.39067.**100.0.16**	16	-
Certificate expired	Critical	1.3.6.1.4.1.39067.**100.0.17**	17	-
Certificate not trusted	Critical	1.3.6.1.4.1.39067.**100.0.18**	18	-
Certificate revoked	Critical	1.3.6.1.4.1.39067.**100.0.19**	19	-
Certificate key is not accessible	Critical	1.3.6.1.4.1.39067.**100.0.20**	20	-
Configuration Error	Fatal	1.3.6.1.4.1.39067.**100.0.21**	21	-

Undefined	Critical	1.3.6.1.4.1.39067.**100.0.999**	999	-
Folder access problem	Error	1.3.6.1.4.1.39067.**999.10**	910	Folder access problem resolved
Folder access problem resolved	Notification	1.3.6.1.4.1.39067.**999.11**	911	-

Service-specific alerts

Service	Alert name	Severity	Trap OID	Event ID	Resolved by
Verba Storage Management Service	Policy Error	Error	1.3.6.1.4.1.39067**.101.0.1**	1001	Policy Continues
	Policy Continues	Critical	1.3.6.1.4.1.39067**.101.0.2**	1002	-
	Policy Finished	Warning	1.3.6.1.4.1.39067**.101.0.3**	1003	-
	Centera Privileged Delete Allowed	Critical	1.3.6.1.4.1.39067**.101.0.4**	1004	-
	PolicyVQError	Error	1.3.6.1.4.1.39067**.101.0.5**	1005	-
	VerintMissingAgentAssociations	Critical	1.3.6.1.4.1.39067**.101.0.6**	1006	-
Verba Passive Recorder Service	CaptureDown	Critical	1.3.6.1.4.1.39067**.102.0.1**	2001	CaptureUp
	CaptureUp	Critical	1.3.6.1.4.1.39067**.102.0.2**	2002	-
	CallProcError	Error	1.3.6.1.4.1.39067**.102.0.3**	2003	-
Verba Legacy Cisco Central Recorder Service	JTAPIServiceDown	Critical	1.3.6.1.4.1.39067**.103.0.1**	3001	JTAPIServiceUp
	JTAPIServiceUp	Critical	1.3.6.1.4.1.39067**.103.0.2**	3002	-
	CallProcError	Critical	1.3.6.1.4.1.39067**.103.0.3**	3003	-
Verba Cisco JTAPI Service	CUCMDown	Fatal	1.3.6.1.4.1.39067**.104.0.1**	4001	CUCMUp
	CUCMUp	Critical	1.3.6.1.4.1.39067**.104.0.2**	4002	-
	Genesys connection down	Error	1.3.6.1.4.1.39067**.123.0.1**	23001	Genesys connection up
	Genesys connection up	Error	1.3.6.1.4.1.39067**.123.0.2**	23002	-
Verba Dial-in Recorder Service	CallProcError	Error	1.3.6.1.4.1.39067**.105.0.1**	5001	-
Verba General Media Recorder Service	CallProcError	Error	1.3.6.1.4.1.39067**.106.0.1**	6001	-
Verba Avaya Recorder Service	AESDown	Fatal/Critical	1.3.6.1.4.1.39067**.107.0.1**	7001	AESUp

	AESUp	Critical	1.3.6.1.4.1.39067**.107.0.2**	7002	-
	MediaRecDown	Fatal	1.3.6.1.4.1.39067**.107.0.3**	7003	MediaRecUp
	MediaRecUp	Critical	1.3.6.1.4.1.39067**.107.0.4**	7004	-
	CallProcError	Fatal	1.3.6.1.4.1.39067**.107.0.5**	7005	-
Verba Legacy Cisco UC Gateway Recorder Service	XCCServiceDown	Critical	1.3.6.1.4.1.39067**.108.0.1**	8001	XCCServiceUp
	XCCServiceUp	Critical	1.3.6.1.4.1.39067**.108.0.2**	8002	-
	CallProcError	Critical	1.3.6.1.4.1.39067**.108.0.3**	8003	-
Verba Cisco MediaSense Connector Service	ConnectionDown	Critical	1.3.6.1.4.1.39067**.109.0.1**	9001	ConnectionUp
	ConnectionUp	Critical	1.3.6.1.4.1.39067**.109.0.2**	9002	-
	CallProcError	Critical	1.3.6.1.4.1.39067**.109.0.3**	9003	-
Verba Screen Capturing Service	ConnectionDown	Critical	1.3.6.1.4.1.39067**.110.0.1**	10001	ConnectionUp
	ConnectionUp	Critical	1.3.6.1.4.1.39067**.110.0.2**	10002	-
	CapturingError	Critical	1.3.6.1.4.1.39067**.110.0.3**	10003	-
Verba SfB/Lync Call Filter Service	RecorderTimeout	Critical	1.3.6.1.4.1.39067**.111.0.1**	11001	RecorderBack
	RecorderBack	Critical	1.3.6.1.4.1.39067**.111.0.2**	11002	-
	LyncDown	Critical	1.3.6.1.4.1.39067**.111.0.3**	11003	LyncUp
	LyncUp	Critical	1.3.6.1.4.1.39067**.111.0.4**	11004	-
	LyncInactive	Critical	1.3.6.1.4.1.39067**.111.0.9**	11009	Lync Connection Active
	MediaCollectorTimeout	Critical	1.3.6.1.4.1.39067**.111.0.5**	11005	MediaCollectorBack
	MediaCollectorBack	Critical	1.3.6.1.4.1.39067**.111.0.6**	11006	-
	AnnouncementTimeout	Critical	1.3.6.1.4.1.39067**.111.0.7**	11007	AnnouncementBack
	AnnouncementBack	Critical	1.3.6.1.4.1.39067**.111.0.8**	11008	-
	CallProcessingError	Error	1.3.6.1.4.1.39067**.111.0.10**	11010	-
	ConfigurationError	Critical	1.3.6.1.4.1.39067**.111.0.11**	11011	-

	Lync Connection Active	Critical	1.3.6.1.4.1.39067**.111.0.12**	11012	-
Verba SfB/Lync IM Recorder Service	Lync filter down	Critical	1.3.6.1.4.1.39067**.112.0.1**	12001	Lync filter up
	Lync filter up	Critical	1.3.6.1.4.1.39067**.112.0.2**	12002	-
Verba Node Manager Agent	RegistrationFailed	Fatal	1.3.6.1.4.1.39067**.113.0.1**	13001	RegistrationReady
	RegistrationReady	Fatal	1.3.6.1.4.1.39067**.113.0.2**	13002	-
Verba CDR Importer Service	ImportFailure	Critical	1.3.6.1.4.1.39067**.114.0.1**	14001	-
	RecordFailure	Error	1.3.6.1.4.1.39067**.114.0.2**	14002	-
	RecheckFailure	Critical	1.3.6.1.4.1.39067**.114.0.3**	14003	-
	MediaLengthMismatch	Error	1.3.6.1.4.1.39067**.114.0.4**	14004	-
	Metadata Filesize Too Big	Fatal	1.3.6.1.4.1.39067**.114.0.5**	14005	-
	Bad configuration	Critical	1.3.6.1.4.1.39067**.114.0.6**	14006	-
	CiscoWebex Token error	Fatal	1.3.6.1.4.1.39067**.114.0.7**	14007	-
	Approaching API throttling limit	Warning	1.3.6.1.4.1.39067**.114.0.8**	14008	-
	API throttling limit reached	Error	1.3.6.1.4.1.39067**.114.0.9**	14009	-
	General Notification	Notification	1.3.6.1.4.1.39067**.114.0.11**	14011	-
Verba Centile Connector Service	DiskAccess	Critical	1.3.6.1.4.1.39067**.150.0.1**	50001	-
	DatabaseAccessDown	Critical	1.3.6.1.4.1.39067**.150.0.2**	50002	DatabaseAccessUp
	DatabaseAccessUp	Critical	1.3.6.1.4.1.39067**.150.0.3**	50003	-
	UnidentifiedEnterprise	Critical	1.3.6.1.4.1.39067**.150.0.4**	50004	-
	CallProcessingError	Critical	1.3.6.1.4.1.39067**.150.0.5**	50005	-
Verba Unified Call Recorder Service	RecProviderDown	Critical	1.3.6.1.4.1.39067**.115.0.1**	15001	RecProviderUp
	RecProviderUp	Critical	1.3.6.1.4.1.39067**.115.0.2**	15002	-
	MediaRecDown	Warning	1.3.6.1.4.1.39067**.115.0.3**	15003	MediaRecUp
	MediaRecUp	Warning	1.3.6.1.4.1.39067**.115.0.4**	15004	-

JTAPIServiceDown	Critical	1.3.6.1.4.1.39067.115.0.5	15005	JTAPIServiceUp
JTAPIServiceUp	Critical	1.3.6.1.4.1.39067.115.0.6	15006	-
CallProcError	Error	1.3.6.1.4.1.39067.115.0.7	15007	-
SipTrunkDown	Critical	1.3.6.1.4.1.39067.115.0.8	15008	SipTrunkUp
SipTrunkUp	Critical	1.3.6.1.4.1.39067.115.0.9	15009	-
RecorderOverloadBegin	Warning	1.3.6.1.4.1.39067.115.0.10	15010	RecorderOverloadEnd
RecorderOverloadEnd	Warning	1.3.6.1.4.1.39067.115.0.11	15011	-
RecorderStandbyBegin	Warning	1.3.6.1.4.1.39067.115.0.12	15012	RecorderStandbyEnd
RecorderStandbyEnd	Warning	1.3.6.1.4.1.39067.115.0.13	15013	-
RecordingDirectorDown	Warning	1.3.6.1.4.1.39067.115.0.14	15014	RecordingDirectorUp
RecordingDirectorUp	Warning	1.3.6.1.4.1.39067.115.0.15	15015	-
IPCCTIPassive	Error	1.3.6.1.4.1.39067.115.0.16	15016	-
IPCCTIActive	Error	1.3.6.1.4.1.39067.115.0.17	15017	IPCCTIPassive
BT Heartbeat & Directory Service Down	Critical	1.3.6.1.4.1.39067.115.0.18	15018	BT Heartbeat & Directory Service Up
BT Heartbeat & Directory Service Up	Critical	1.3.6.1.4.1.39067.115.0.19	15019	-
BT ITSLink Down	Critical	1.3.6.1.4.1.39067.115.0.20	15020	BT ITSLink Up
BT ITSLink Up	Critical	1.3.6.1.4.1.39067.115.0.21	15021	-
BT TTP Down	Critical	1.3.6.1.4.1.39067.115.0.22	15022	BT TTP Up
BT TTP Up	Critical	1.3.6.1.4.1.39067.115.0.23	15023	-
BT Voice LAN0 Down	Critical	1.3.6.1.4.1.39067.115.0.24	15024	BT Voice LAN0 Up
BT Voice LAN0 Temporarily Down	Critical	1.3.6.1.4.1.39067.115.0.25	15025	BT Voice LAN0 Up
BT Voice LAN0 Partially Down	Critical	1.3.6.1.4.1.39067.115.0.26	15026	BT Voice LAN0 Up
BT Voice LAN0 Up	Critical	1.3.6.1.4.1.39067.115.0.27	15027	-
BT Voice LAN1 Down	Critical	1.3.6.1.4.1.39067.115.0.28	15028	BT Voice LAN1 Up

	BT Voice LAN1 Temporarily Down	Critical	1.3.6.1.4.1.39067**.115.0.29**	15029	BT Voice LAN1 Up
	BT Voice LAN1 Partially Down	Critical	1.3.6.1.4.1.39067**.115.0.30**	15030	BT Voice LAN1 Up
	BT Voice LAN1 Up	Critical	1.3.6.1.4.1.39067**.115.0.31**	15031	-
	BT TFTP0 Down	Warning	1.3.6.1.4.1.39067**.115.0.32**	15032	BT TFTP0 Up
	BT TFTP0 Up	Warning	1.3.6.1.4.1.39067**.115.0.33**	15033	-
	BT TFTP1 Down	Warning	1.3.6.1.4.1.39067**.115.0.34**	15034	BT TFTP1 Up
	BT TFTP1 Up	Warning	1.3.6.1.4.1.39067**.115.0.35**	15035	-
	BT TMS Access Down	Critical	1.3.6.1.4.1.39067**.115.0.36**	15036	BT TMS Access Up
	BT TMS Access Up	Critical	1.3.6.1.4.1.39067**.115.0.37**	15037	-
	Failover Between TTP Managers	Critical	1.3.6.1.4.1.39067**.115.0.38**	15038	-
	BT LDAP access down	Critical	1.3.6.1.4.1.39067**.115.0.39**	15039	BT LDAP access up
	BT LDAP access up	Critical	1.3.6.1.4.1.39067**.115.0.40**	15040	-
	BT TMS Cache access down	Critical	1.3.6.1.4.1.39067**.115.0.41**	15041	BT TMS Cache access up
	BT TMS Cache access up	Critical	1.3.6.1.4.1.39067**.115.0.42**	15042	-
	BT TTP packet loss started	Critical	1.3.6.1.4.1.39067**.115.0.43**	15043	BT TTP packet loss ended
	BT TTP packet loss ended	Critical	1.3.6.1.4.1.39067**.115.0.44**	15044	.
	IPC media channel went down	Error	1.3.6.1.4.1.39067**.115.0.45**	15045	IPC media channel went up
	IPC media channel went up	Error	1.3.6.1.4.1.39067**.115.0.46**	15046	-
Verba Cisco Compliance Service	IMPNodeUp	Critical	1.3.6.1.4.1.39067**.116.0.1**	16001	-
	IMPNodeDown	Fatal	1.3.6.1.4.1.39067**.116.0.2**	16002	IMPNodeUp
	MessageQueueThreshold	Fatal	1.3.6.1.4.1.39067**.116.0.5**	16005	-
	Processing Error	Error	1.3.6.1.4.1.39067**.116.0.6**	16006	-
	DLP Server Error	Error	1.3.6.1.4.1.39067**.116.0.7**	16007	-
Verba Media Collector and Proxy Service	RecorderUp	Critical	1.3.6.1.4.1.39067**.117.0.1**	17001	-

	RecorderDown	Critical	1.3.6.1.4.1.39067**.117.0.2**	17002	RecorderUp
	LyncFilterUp	Critical	1.3.6.1.4.1.39067**.117.0.3**	17003	-
	LyncFilterDown	Critical	1.3.6.1.4.1.39067**.117.0.4**	17004	LyncFilterUp
	RecorderOverloadBegin	Warning	1.3.6.1.4.1.39067**.117.0.5**	17005	RecorderOverloadEnd
	RecorderOverloadEnd	Warning	1.3.6.1.4.1.39067**.117.0.6**	17006	-
	RecorderStandbyBegin	Warning	1.3.6.1.4.1.39067**.117.0.7**	17007	RecorderStandbyEnd
	RecorderStandbyEnd	Warning	1.3.6.1.4.1.39067**.117.0.8**	17008	-
	CallProcError	Error	1.3.6.1.4.1.39067**.117.0.9**	17009	-
Verba Web Application Service	FailedLogin	Warning	1.3.6.1.4.1.39067**.118.0.1**	18001	-
	ApplyACLFailed	Error	1.3.6.1.4.1.39067**.118.1.1**	18101	-
	ApplyCommPoliciesFailed	Error	1.3.6.1.4.1.39067**.118.1.2**	18102	-
	Could not send license usage to RLS	Error	1.3.6.1.4.1.39067**.118.1.3**	18103	-
	Database Maintenance Completed	Info	1.3.6.1.4.1.39067**.118.1.4**	18104	-
	Database Maintenance Error	Error	1.3.6.1.4.1.39067**.118.1.5**	18105	-
	License Issue	Error	1.3.6.1.4.1.39067**.118.1.6**	18106	-
	Report Upload Failed	Error	1.3.6.1.4.1.39067**.118.1.7**	18107	-
	License Warning	Warning	1.3.6.1.4.1.39067**.118.1.8**	18108	-
	ADSyncError	Error	1.3.6.1.4.1.39067**.118.2.1**	18201	ADSyncExecutedOK
	ADSyncExecutedOK	Info	1.3.6.1.4.1.39067**.118.2.2**	18202	-
	ADSyncUsersDecreasedSignificantly	Warning	1.3.6.1.4.1.39067**.118.2.3**	18203	-
	AD Synchronization Added New Site	Warning	1.3.6.1.4.1.39067**.118.2.4**	18204	-
	Data Management Policy Created	Notification	1.3.6.1.4.1.39067**.118.3.1**	18301	-
	Data Management Policy Updated	Notification	1.3.6.1.4.1.39067**.118.3.2**	18302	-
	Data Management Policy Deleted	Notification	1.3.6.1.4.1.39067**.118.3.3**	18303	-

	Users without Ethical Wall User permission	Warning	1.3.6.1.4.1.39067**.118.4.1**	18401	-
	Audit Log Fatal	Fatal	1.3.6.1.4.1.39067**.118.9.1**	18901	-
	Audit Log Critical	Critical	1.3.6.1.4.1.39067**.118.9.2**	18902	-
	Audit Log Error	Error	1.3.6.1.4.1.39067**.118.9.3**	18903	-
	Audit Log Warning	Warning	1.3.6.1.4.1.39067**.118.9.4**	18904	-
	Audit Log Info	Info	1.3.6.1.4.1.39067**.118.9.5**	18905	-
Verba SMS Recorder Service	SMS-C connection up	Critical	1.3.6.1.4.1.39067**.119.0.1**	19001	-
	SMS-C connection down	Critical	1.3.6.1.4.1.39067**.119.0.2**	19002	SMS-C up
	SMS Processing Error	Error	1.3.6.1.4.1.39067**.119.0.3**	19003	-
Verba SfB/Lync IM Filter Service	Recorder connection down	Critical	1.3.6.1.4.1.39067**.120.0.1**	20001	Recorder connection up
	Recorder connection up	Critical	1.3.6.1.4.1.39067**.120.0.2**	20002	-
	Lync connection down	Critical	1.3.6.1.4.1.39067**.120.0.3**	20003	Lync connection up
	Lync connection up	Critical	1.3.6.1.4.1.39067**.120.0.4**	20004	-
	Lync connection inactive	Critical	1.3.6.1.4.1.39067**.120.0.5**	20005	Lync Connection Active
	Call Processing error	Error	1.3.6.1.4.1.39067**.120.0.6**	20006	-
	Configuration error	Error	1.3.6.1.4.1.39067**.120.0.7**	20007	-
	Lync Connection Active	Critical	1.3.6.1.4.1.39067**.120.0.8**	20008	-
Verba SfB/Lync Ethical Wall Service	Announcement connection down	Critical	1.3.6.1.4.1.39067**.121.0.1**	21001	Announcement connection up
	Announcement connection up	Critical	1.3.6.1.4.1.39067**.121.0.2**	21002	-
	Lync connection down	Critical	1.3.6.1.4.1.39067**.121.0.3**	21003	Lync connection up
	Lync connection up	Critical	1.3.6.1.4.1.39067**.121.0.4**	21004	-
	Lync connection inactive	Critical	1.3.6.1.4.1.39067**.121.0.5**	21005	Lync Connection Active
	Call Processing error	Error	1.3.6.1.4.1.39067**.121.0.6**	21006	-
	Configuration error	Error	1.3.6.1.4.1.39067**.121.0.7**	21007	-

	Lync Connection Active	Critical	1.3.6.1.4.1.39067.121.0.8	21008	-
Verba Microsoft Teams Bot Service	Recorder connection down	Critical	1.3.6.1.4.1.39067.122.0.1	22001	Recorder connection up
	Recorder connection up	Warning	1.3.6.1.4.1.39067.122.0.2	22002	-
	User is not configured in Verba	Warning	1.3.6.1.4.1.39067.122.0.3	22003	-
	Could not join call	Critical	1.3.6.1.4.1.39067.122.0.4	22004	-
	No available recorder	Critical	1.3.6.1.4.1.39067.122.0.5	22005	-
	Unexpected call termination	Critical	1.3.6.1.4.1.39067.122.0.6	22006	
	Could not authenticate	Critical	1.3.6.1.4.1.39067.122.0.7	22007	
	Call timed out	Warning	1.3.6.1.4.1.39067.122.0.8	22008	
	Recorder overloaded	Critical	1.3.6.1.4.1.39067.122.0.9	22009	
Verba Genesys CTI Service	Genesys connection down	Error	1.3.6.1.4.1.39067.123.0.1	23001	Genesys connection up
	Genesys connection up	Error	1.3.6.1.4.1.39067.123.0.2	23002	-
Verba Unified IM Recorder Service	Message queue is up	Critical	1.3.6.1.4.1.39067.124.0.1	24001	-
	Message queue is down	Critical	1.3.6.1.4.1.39067.124.0.2	24002	Message queue is up
	Message queue is in active state	Critical	1.3.6.1.4.1.39067.124.0.3	24003	-
	Message queue is in standby state	Critical	1.3.6.1.4.1.39067.124.0.4	24004	Message queue is in active state
	Teams subscription is up	Warning	1.3.6.1.4.1.39067.124.0.5	24005	-
	Teams subscription is down	Warning	1.3.6.1.4.1.39067.124.0.6	24006	Teams subscription is up
	Attachment download failed	Error	1.3.6.1.4.1.39067.124.0.7	24007	-
	No provider is configured for message processing	Critical	1.3.6.1.4.1.39067.124.0.8	24008	-
	Subscription lifecycle event	Warning	1.3.6.1.4.1.39067.124.0.9	24009	-
	Recording inactivity	Critical	1.3.6.1.4.1.39067.124.0.10	24010	Recording activity
	Recording activity	Critical	1.3.6.1.4.1.39067.124.0.11	24011	-
	Teams Export API connection is up	Critical	1.3.6.1.4.1.39067.124.0.12	24012	-

	Teams Export API connection is down	Critical	1.3.6.1.4.1.39067**.124.0.13**	24013	Teams Export API connection is up
	Teams Export API license issue	Critical	1.3.6.1.4.1.39067**.124.0.14**	24014	-

Variables used in SNMP Traps

The following variables are used in various Verba traps to describe the event:

OID	Variable Name	Description
1.3.6.1.4.1.39067**.200.1**	Description	Human readable description of the trap
1.3.6.1.4.1.39067**.200.2**	ServiceName	Name of the affected service
1.3.6.1.4.1.39067**.200.3**	HostName	Host name of an affected server
1.3.6.1.4.1.39067**.200.4**	DiskSpaceLowPath	Path of an affected disk
1.3.6.1.4.1.39067**.200.5**	CallId	ID of the affected recording
1.3.6.1.4.1.39067**.200.6**	ServiceDisplayName	Display name of the affected service
1.3.6.1.4.1.39067**.200.7**	Path	Affected path
1.3.6.1.4.1.39067**.200.8**	Interface	Recording capture interface
1.3.6.1.4.1.39067**.200.9**	CertThumbprint	Certificate thumbprint
1.3.6.1.4.1.39067**.200.10**	CertFriendlyName	Certificate friendly name
1.3.6.1.4.1.39067**.200.11**	CertExpirationDate	Certificate expiration date
1.3.6.1.4.1.39067**.200.12**	CertSubject	Certificate subject
1.3.6.1.4.1.39067**.200.13**	Severity	Event Severity
1.3.6.1.4.1.39067**.200.14**	Title	Title
1.3.6.1.4.1.39067**.200.15**	Userid	User id
1.3.6.1.4.1.39067**.200.16**	TenantId	Tenant id
1.3.6.1.4.1.39067**.200.17**	EventID	Event ID

Avaya DMCC-JTAPI Service: AESDown

Application Enabled Services (AES) Down Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#

Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the Verba DMCC/JTAPI Service is not able to connect to the AES.

Resolution

If you receive such an alert, please check the connections between the recording server(s) and the AES. Please note that if you received the "AESUp" alert as well, the communication between the Verba component and the AES is back in normal, the connection lost state was temporary.

If there's no connection between the server and the AES, please contact your IT team.

If the connection is up, but the Avaya DMCC/JTAPI Service and the AES still can not communicate with each other, check at the AES side if the application user still exists.
Also, on Verba side check/update the AES user credentials.
Follow these steps:

Step 1 - On the web interface go to **Administration** and choose **Verba Servers**.
Step 2 - Choose the server from which you received the alert from the server list.
Step 3 - Click on the **Change Configuration Settings** tab, and search for **Avaya DMCC/JTAPI**.
Step 4 - Under **Avaya connection** set the correct credentials for **AES IP address**, **AES user name** and **AES user password.**
Step 5 - Click 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.

If the problem is not solved, please contact the support service and send the log files of the related service(s) - avaya_recorder.log file(s). Log files are available under ""APPLICATION_FOLDER\log"" (by default C:\Program Files\Verba\log) folder on each server.

Avaya DMCC-JTAPI Service: AESUp

Application Enabled Services (AES) Up Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#

Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the connection between Verba DMCC/JTAPI Service and the AES is up again.

Resolution

No further action required.
However, if you receive this pair of alerts on a regular basis, please contact the support service and send the log files of the related service (s) - avaya_recorder.log file(s).
Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files (x86)\Verba\log) folder on each server.

Avaya DMCC-JTAPI Service: CallProcError

Call Processing Error Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
Call processing error: <Information>

Alert attributes:
Call id (OID: .200.5): <CALL_ID>

Cause

This alert is sent if the Verba Avaya Recorder Service encountered some error during call processing.

Resolution

If you receive such an alert, please check the configuration according to the description part of the alert - e.g. invalid access code.

If there is no configuration issue, or you need assistance, contact the support service and send the log files of the Verba Avaya DMCC/JTAPI Service - avaya_recorder.log
Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Avaya DMCC-JTAPI Service: MediaRecDown

Media Recorder Down Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#

Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the Verba Avaya DMCC/JTAPI Service can not connect to one of the Verba Media Recorder(s). The not reachable Media Recorder's IP address is mentioned in the alert email.

Resolution

Please note, that you need to restart the Avaya DMCC/JTAPI Service after this alert.

Before that, please check if the server machine (running the Verba Media Recorder role - which is provided by Verba Unified Call Recorder Service) is reachable. If not, contact your IT team.

If the server is reachable, please check if the Unified Call Recorder Service is running on that Server. If not, start that service and restart the Avaya DMCC/JTAPI Service as well.

If MediaRecUp alert is still not received, contact the support service and send the following log files from each Verba Server: Unified Call Recorder Service - unifiedrec.log. Verba Avaya DMCC/JTAPI Service - avaya_recorder.log.
Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files (x86)\Verba\log) folder on each server.

Avaya DMCC-JTAPI Service: MediaRecUp

Media Recorder Up Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#

Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the communication is restored between the Verba components - Avaya DMCC/JTAPI Service and Verba Unified Call Recorder Service.

Resolution

No further action required, the issue was probably caused by a network glitch.
However, if you receive this pair of alerts on a regular basis, your network is probably overloaded.

If that is not the case, contact the support service and send the following log files from each Verba Server: Unified Call Recorder Service - unifiedrec.log. Verba Avaya DMCC/JTAPI Service - avaya_recorder.log.
Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

CDR Importer Service: ImportFailure Alert

Import Failure Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
Import run failed for connection #ID#: #DESCRIPTION#

Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the importing failed.

Resolution

If you receive such an alert, please contact the support service and send the log files of the related service - cdrimporter.log.

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

CDR Importer Service: Media Length Mismatch

Media Length Mismatch Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#

Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if during the comparison there's a difference in Media Length.

Resolution

If you receive such an alert, please contact the support service and send the log files of the related service - cdrimporter.log.

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

CDR Importer Service: RecheckFailure

Recheck Failure Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
Recheck run failed: #DESCRIPTION#

Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

CDR reconciliation allows to find conversations which were not recorded for some reason, and conversation which were not recorded correctly. This alert is sent if during the recheck process, the service has encountered an error.

Resolution

If you receive such an alert, please contact the support service and send the log files of the related service - cdrimporter.log.

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files (x86)\Verba\log) folder on each server.

CDR Importer Service: RecordFailure Alert

Record Failure Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
Number of calls found not recorded in current reporting session: <NUMBER>. Number of calls having media length mismatch in current reporting session : <NUMBER>

Alert attributes:
<CUSTOM_ATTRIBUTES>

Cause

CDR reconciliation allows to find conversations which were not recorded for some reason, and conversation which were not recorded correctly. This alert is sent if processing not recorded calls fails.

Resolution

If you receive such an alert, please contact the support service and send the log files of the related service - cdrimporter.log. Also please send the lynfilter.log file from the Lync/SfB Frontend servers of the pool where the recorded user is homed.

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Centile Connector Service: CallProcessingError Alert

Call Processing Error Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
Call processing error. #DESCRIPTION#

Alert attributes:
Call id (OID: .200.5): <CALL_ID>

Cause

This alert is sent if a call could not be imported due to a processing error.

Resolution

If you receive such an alert, please contact the support service and send the log files of the related service.

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files (x86)\Verba\log) folder on each server.

Centile Connector Service: DatabaseAccessDown Alert

Database Access Down Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#
Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the service is not able to connect to the database.

Resolution

If you receive such an alert, please contact the support service and send the log files of the related service(s).

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Centile Connector Service: DatabaseAccessUp Alert

Database Access Up Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#
Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the service is able to connect to the database again.

Resolution

No further action required.

However, if you receive this pair of alerts on a regular basis, please contact the support service and send the log files of the related service(s).

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Centile Connector Service: DiscAccess Alert

Disk Access Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#
Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if Centile Completed Recordings share is not accessible.

Resolution

If you receive such an alert, please contact the support service and send the log files of the related service(s).

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files (x86)\Verba\log) folder on each server.

Centile Connector Service: UnidentifiedEnterprise Alert

Unidentified Enterprise Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#
Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if recording from non-provisioned tenant/enterprise is processed.

Resolution

If you receive such an alert, please contact the support service and send the log files of the related service(s).

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files (x86)\Verba\log) folder on each server.

Cisco Central Recorder Service: CallProcError

Call Processing Error Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
Call processing error: <INFORMATION>

Alert attributes:
Call id (OID: .200.5): <CALL_ID>

Cause

This alert is sent if the Verba Cisco Central Recorder Service encountered some error during call processing.

Resolution

If you receive such an alert, please contact the support service and send the log files of the related service - nativerecorder.log.

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files (x86)\Verba\log) folder on each server.

Cisco Central Recorder Service: JTAPIServiceDown

JTAPI Service Down Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
JTAPI service went down

Alert attributes:
Hostname (OID: .200.3): <IP>

Cause

This alert is sent if JTAPI Service is not reachable for the Cisco Central Recorder service.

Resolution

If you receive such an alert, please check that the Verba JTAPI service is running.
If yes, contact the support service and send the log files of the related service - nativerecorder.log, native_recorder_dbservice.log.

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Please note, if you received the JTAPI/DB service up alert as well, the connection loss was temporary.

Cisco Central Recorder Service: JTAPIServiceUp

JTAPI Service Up Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
JTAPI service went up

Alert attributes:
Hostname (OID: .200.3): <IP>

Cause

This alert is sent if JTAPI Service is reachable for the Cisco Central Recorder service again.

Resolution

No further action required.

However, if you receive this pair of alert on a regular basis, contact the support service and send the log files of the related services: nativerecorder.log, native_recorder_dbservice.log.

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files (x86)\Verba\log) folder on each server.

Cisco Complience Service: IMPNodeDown Alert

IMP Node Down Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#
Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent when the connection between the Verba server and the Cisco IM&P server is down.

Resolution

If you receive such an alert, please check if the Cisco IM&P server is reachable from the Verba server. If not, contact your IT team to search for a network issue, and check the firewall configuration as well.

If the Cisco IM&P server is reachable from the Verba server, please contact the support service and send the log files of the related service(s).

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files (x86)\Verba\log) folder on each server.

Cisco Complience Service: IMPNodeUpAlert

IMP Node Up Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#
Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent after a connection down state, when the Cisco IM&P server connected to the Verba server again.

Resolution

No further action required after this notification.

Cisco Complience Service: JabberLoginTimeout Alert

Jabber Login Timeout Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#
Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

NOT USED

Resolution

If you receive such an alert, please contact the support service and send the log files of the related service(s).

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Cisco Complience Service: JabberMessageTimeout

Jabber Message Timeout Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#
Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

NOT USED

Resolution

If you receive such an alert, please contact the support service and send the log files of the related service(s).

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Cisco Complience Service: MessageQueueThreshold Alert

Message Queue Threshold Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#
Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if one of the XMPP event processing threads reaches the queue threshold.

Resolution

Queue threshold can be reached if the load is too much on the Verba server and the current configuration is not able to handle the mount of the received XMPP events.
Review the CPU load and the Memory usage of the Cisco Compliance service. It is running as a java.exe.

If you need any assistance, please contact the support service and send the log files of the related service(s).

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Cisco JTAPI Service: CallProcError

Call Processing Error

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
Call processing error: <INFORMATION>

Alert attributes:
Call id (OID: .200.5): <CALL_ID>

Cause

This alert is sent if the Cisco JTAPI Service encountered an error during call processing.

Resolution

If you receive such an alert, please contact the support service and send the log files of the related service(s) - native_recorder_dbservice.log.log file(s).

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files (x86)\Verba\log) folder on each server.

Cisco JTAPI Service: CUCMDown

CUCM Down Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
Connection to CUCM lost.

Alert attributes:
Service name (OID: .200.2): <SERVICE_NAME>

Cause

This alert is sent if the Verba JTAPI Service is not able to connect to the CUCM.

Resolution

If you receive such an alert, please check the connections between the server(s) and the CUCM. Please note that if you received the "CUCMUp" alert as well, the communication between the Verba component and the CUCM is back in normal, the connection lost state was temporary.

If there's no connection between the server and the CUCM, contact your IT team.

If the connection is up, but the JTAPI Service(s) and the CUCM still can not communicate with each other, check at the CUCM side if the application user still exists.

Also, on Verba side update the JTAPI credentials. Follow these steps:

Step 1 - On the web interface go to **Administration** and choose **Verba Servers.**
Step 2 - Choose the server from which you received the alert from the server list.
Step 3 - Click on the **Change Configuration Settings** tab, and search for **Cisco JTAPI Configuration.**
Step 4 - Under **Basics** set the correct credentials.
Step 5 - Click 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.

If the problem is not solved, please contact the support service and send the log files of the related service(s) - native_recorder_dbservice.log(s).

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Cisco JTAPI Service: CUCMUp

CUCM Up Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#

Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the Verba JTAPI Service is able to connect to the CUCM again.

Resolution

No further action required.
However, if you receive this pair of alerts on a regular basis, please contact the support service and send the log files of the related service (s) - native_recorder_dbservice.log file(s).

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files (x86)\Verba\log) folder on each server.

Cisco MediaSense Connector Service: CallProcError

Call Processing Error Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description: í
Call processing error: <Information>

Alert attributes:
Call id (OID: .200.5): <CALL_ID>

Cause

This alert is sent if the Verba Cisco MediaSense Connector Service encountered some error during call processing.

Resolution

If you receive such an alert, please contact the support service and send the log files of the related service.

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Cisco MediaSense Connector Service: ConnectionDown

Connection Down Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#

Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if connection to MediaSense is lost.

Resolution

If you receive such an alert, please check if the connection is up between the Verba server and the MediaSense. If not, contact your IT team.

If the connection is up, please contact the support service and send the log files of the related service - mediasense-connector.log.
Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files (x86)\Verba\log) folder on each server.

Cisco MediaSense Connector Service: ConnectionUp

Connection Up Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#

Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if connection to MediaSense is reestablished.

Resolution

No further action required.

However, if you receive this pair of alerts on a regular basis, please contact the support service and send the log files of the related services - mediasense-connector.log.

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files (x86)\Verba\log) folder on each server.

Cisco UC Gateway Recorder Service: CallProcError

Call Processing Error Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
Media processing error: <Information>

Alert attributes:
Call id (OID: .200.5): <CALL_ID>

Cause

This alert is sent if the Verba Cisco UC Gateway Recorder Service encountered some error during call processing.

Resolution

If you receive such an alert, please contact the support service and send the log files of the related service.

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files (x86)\Verba\log) folder on each server.

Cisco UC Gateway Recorder Service: XCCServiceDown

Extended Call Control Provider Down Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#

Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if connection to the gateway went down.

Resolution

If you receive such an alert, please check if the connection is up between the Verba server and the Gateway. If not, contact your IT team.

If the connection is up, please contact the support service and send the log files of the related service - ciscogatewayrec.log.

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Cisco UC Gateway Recorder Service: XCCServiceUp

Extended Call Control Provider Up Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#

Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the connection to the gateway is up again.

Resolution

No further action required.

Desktop Agent: ConnectionDown

Connection Down Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#
Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if connection to a recorder service is lost.

Resolution

If you receive such an alert, please check if the connection is up between the the server and the user's computer. If not, contact your IT team.

If the connection is up, please contact the support service and send the log files of the related service - agentcontroller.log, captureagent.log.
Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files (x86)\Verba\log) folder on each server.

Desktop Agent: ConnectionUp

Connection Up Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#
Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if connection to a recorder service is reestablished.

Resolution

No further action required.

However, if you receive this pair of alerts on a regular basis, your network is probably overloaded.

If that is not the case, please contact the support service and send the log files of the related service - agentcontroller.log, captureagent.log.
Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Dial-in Recorder Service: CallProcError

Call Processing Error Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description: Call processing error: <Information>

Alert attributes:
Call id (OID: .200.5): <CALL_ID>

Cause

This alert is sent if the Verba Dial-in Recorder Service encountered some error during call processing.

Resolution

If you receive such an alert, please contact the support service and send the log files of the related service.

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files (x86)\Verba\log) folder on each server.

General Alerts: Database Connection Down

- Database Connection Down Alert
- Database Down Alert from Service
- Database Connection Up Alert

Database Connection Down Alert

Content

Verba System Monitor has detected that the database is not accessible.

Computer name: <COMPUTER_NAME>
SQL server name: <DB_HOST>
User name: <DB_LOGIN_NAME>

Cause

This alert is sent if the Verba server mentioned in the alert email cannot connect to the database.

Resolution

If you receive such an alert, please check the connections between the servers and the database. Please note that if you received the "Database Connection Up" alert as well, the communication between the Verba component and the database is back in normal, the connection lost state was temporary.

If you didn't receive the "Connection Up" alert, and there's no connection between the server and the database, contact your IT team.
If the connection is up, but Verba components still can not communicate with the Database, please contact the support service and send the log files of the related service(s).

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Database Down Alert from Service

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#

Alert attributes:

#CUSTOM_ATTRIBUTES#

Cause

This alert is a service specific alert. It is sent if the Verba service mentioned in the alert email cannot connect to the database.

Resolution

If you receive such an alert, please check the connections between the servers and the database. If there is no connection between the server and the database, contact your IT team.
If the connection is up, but a Verba service still can not communicate with each other, please contact the support service and send the log files of the mentioned service(s).

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Database Connection Up Alert

Content

Verba System Monitor detected that the database is now accessible.

Computer name: <COMPUTER_NAME>
SQL server name: <DB_HOST>
User name: <DB_LOGIN_NAME>

Cause

This alert is sent if the communication is up and running again.

Resolution

No further action required, the issue was probably caused by a network glitch. However, if you receive this pair of alerts on a regular basis, your network is probably overloaded.

General Alerts: Database Error

Database Error Alert

Content

Verba System Monitor has encountered a database error.

Computer name: <COMPUTER_NAME>
SQL server name: #DBMSHOST#
User name: #DBMSLOGIN#

Cause

This alert is sent if the service mentioned in the email cannot execute an SQL statement in the database. The alert is sent if the execution of the database command failed three times in a row.

Resolution

If you receive such an alert, please contact the support service and send the log files of the related service(s).
Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files (x86)\Verba\log) folder on each server.

General Alerts: Folder Access Problem

Folder Access Problem Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#

Alert attributes:

#CUSTOM_ATTRIBUTES#

Cause

This alert is sent when a service failed to access a folder.

Resolution

Verify if the service has the necessary rights to access the folder. The service could run under a specific service user account or using the built-in LocalSystem account (default).

If the problem cannot be resolved, please contact the support service and send the log files of the related service(s).
Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

General Alerts: Free Memory Low

- Free Memory Low Alert
- Free Memory OK Alert

Free Memory Low Alert

Content

Verba System Monitor has detected a low memory state on server: <COMPUTER_NAME>

```
Computer Name:              <COMPUTER_NAME>
Total physical memory:        <TOTAL_PHYSICAL_MEMORY> MB
Available physical memory:     <AVAILABLE_PHYSICAL_MEMORY> MB
```

Process id: <Process_id> Process name:<Process_name> Memory usage: <Memory_Usage> MB

Process id: <Process_id> Process name:<Process_name> Memory usage: <Memory_Usage> MB

Process id: <Process_id> Process name:<Process_name> Memory usage: <Memory_Usage> MB

Process id: <Process_id> Process name:<Process_name> Memory usage: <Memory_Usage> MB

Process id: <Process_id> Process name:<Process_name> Memory usage: <Memory_Usage> MB

Process id: <Process_id> Process name:<Process_name> Memory usage: <Memory_Usage> MB

Process id: <Process_id> Process name:<Process_name> Memory usage: <Memory_Usage> MB

Process id: <Process_id> Process name:<Process_name> Memory usage: <Memory_Usage> MB

Process id: <Process_id> Process name:<Process_name> Memory usage: <Memory_Usage> MB

Process id: <Process_id> Process name:<Process_name> Memory usage: <Memory_Usage> MB

Cause

This alert is sent if the available physical memory on the server machine is less than the given threshold value - by default 200 megabytes. The alert email lists the top 10 memory consuming processes.

Resolution

If you receive such an alert, please check the server machine - if one of the Verba services consuming too much memory, please contact the support service and send the log files of the related service(s). Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files (x86)\Verba\log) folder on each server.

Please note that if you received the "Free Memory OK" alert as well, the server is back in normal, the low memory state was temporary.

Follow the steps below to change the threshold value:

Step 1 - On the web interface go to **Administration** and choose **Verba Servers**
Step 2 - Choose the server from which you received an alert from the server list

Step 3 - Click on the **Change Configuration Settings** tab, and search for **System Monitoring**

Step 4 - Under System Monitoring you can edit the **Minimum Physical Memory** field

Step 5 - Click the 💾 icon to save your settings.

Step 6 - The system will notify you that the changes need to applied to the server by restarting the involved services or rereading the new configuration. Execute the required tasks.

Free Memory OK Alert

Content

Verba System Monitor has detected that the available physical memory on the server machine - <COMPUTER_NAME> - is more than the given threshold value again.

Computer Name: <COMPUTER_NAME>
Total physical memory: <TOTAL_PHYSICAL_MEMORY> MB

Cause

This alert is sent if the available physical memory on the server machine is more than the given threshold value again.

Resolution

No further action required. However, if you receive this pair of alert on a regular basis, consider installing more physical memory into your server.

General Alerts: Low Disk Space

- Low Disk Space Alert
- Disk Space OK Alert

Low Disk Space Alert

Content

Verba System Monitor has detected low disk space condition on the server: <COMPUTER_NAME>

Computer Name: <COMPUTER_NAME>
Volume path: <VOLUME_PATH>
Total disk space: <TOTAL_DISK_SPACE> MB
Available disk space: <AVAILABLE_DISK_SPACE> MB

Cause

This alert is sent if the available space on one of the disks of the server machine is less than the given threshold value - by default 5000 megabytes.

Resolution

If you receive such an alert, please check the server machine.

After freeing some space, the "Disk Space OK" alert should be received.

Follow the steps below to change the threshold value:

Step 1 - On the web interface go to **Administration** and choose **Verba Servers**
Step 2 - Choose the server from which you received an alert from the server list
Step 3 - Click on the **Change Configuration Settings** tab, and search for **Low Disk Space Monitoring - 1st Disk Volume**
Step 4 - Under each "Low Disk Space Monitoring - X Disk Volume System" you can edit the "**Alert Threshold**" field
Step 5 - Click 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.

Disk Space OK Alert

Content

Verba System Monitor has detected that the available disk space on the server machine - <COMPUTER_NAME> - is more than the given threshold value again.

Computer Name:<COMPUTER_NAME>
Volume path: <VOLUME_PATH>
Total disk space: <TOTAL_DISK_SPACE> MB
Available disk space: <AVAILABLE_DISK_SPACE> MB

Cause

This alert is sent if the available space on the disk of the server machine is over than the given threshold value.

Resolution

No further action required.

General Alerts: Prerequisite Missing

Prerequisite Missing Alert

Content

Verba System Monitor has detected a missing prerequisite.

Computer name: <COMPUTER_NAME>
Application name: <MISSING_APPLICATION>

Cause

This alert is sent if one of the required prerequisite is missing.

Resolution

If you receive such an alert, please install the missing application mentioned in the alert email.

General Alerts: Recording Inactivity

- Recording Inactivity Alert
- Recording Inactivity Over Alert

Recording Inactivity Alert

Content

Verba System Monitor has detected there are no calls recorded since <AT_TIME>
Computer name: <COMPUTER_NAME>

Cause

This alert is sent if the number of calls is less than the given value during the window. By default this function is disabled.

Resolution

If you receive such an alert, please check if the number of the to be recorded calls truly was under the threshold value in the monitored window. If that is the case, consider changing the values. Also check for other alerts from your Verba system.

If there should have been more recorded calls in the given time window, please contact the support service and send the log files of the related service(s).
Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Enabling/Disabling monitoring feature, or changing the given values:

Step 1 - On the web interface go to **System** and under **Configuration** choose **Servers**
Step 2 - Choose and click on the Media Repository server from the server list
Step 3 - Click on the **Change Configuration Settings** tab, and search for **Database Monitoring**
Step 4 - Under Database Monitoring, you can enable/disable notification, change the monitored time window, and set the threshold value for number of recordings
Step 5 - Click 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.

Recording Inactivity Over Alert

Content

Verba System Monitor has detected there are <NUMBER_OF_CALLS> calls recorded since <TIME>
Computer name: <COMPUTER_NAME>

Cause

This alert is sent if the system has recorded call(s) again after the Recording Inactivity Alert was sent.

Resolution

No further action needed. However, if you receive this pair of alerts on a regular basis, consider changing the threshold values.

General Alerts: Service Down

Service Down Alert

Content

Verba System Monitor has detected that a service is not running.

Computer name: <COMPUTER_NAME>
Service: <SERVICE_NAME>

Cause

This alert is sent if the service mentioned in the alert email is stopped.

Resolution

Please note that if you received the Service Up Alert as well, the system already restarted the service. If you received the Service Down Alert only, please contact the support service and send the log files of the related service(s).
Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Also, please check the "APPLICATION_FOLDER\bin" (by default C:\Program Files\Verba\bin) folder and search for .cab files. If you find any, please send us that file and the log file also.

Service Up Alert

Content

Verba System Monitor has restarted a service.

Computer name: <COMPUTER_NAME>
Service: <SERVICE_NAME>

Cause

This alert is sent if the service mentioned in the alert email is up and running again.

Resolution

No further action required. However, if you receive this pair of alert on a regular basis, please contact the support service and send the log files of the related service(s).
Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Also, please check the "APPLICATION_FOLDER\bin" (by default C:\Program Files\Verba\bin) folder and search for .cap files. If you find any, please send us that file and the log file also.

General Media Recorder Service: CallProcError

Call Processing Error Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
Call processing error: <Information>

Alert attributes:
Call id (OID: .200.5): <CALL_ID>

Cause

This alert is sent if the Verba General Media Recorder Service encountered some error during call processing.

Resolution

If you receive such an alert, please contact the support service and send the log files of the related service.

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Media Collector and Proxy Service: CallProcError

Call Processing Error Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
Call processing error. <Information>
Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the Verba Media Collector and Proxy Service encountered some error during call processing.

Resolution

If you receive such an alert, please contact the support service and send the log files of the related service.

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files (x86)\Verba\log) folder on each server.

Media Collector and Proxy Service: LyncFilterDown

SfB/Lync Filter Down Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#
Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the communication is down between the Verba components - Lync Filter and Media Collector and Proxy.

Resolution

Please note, if the Lync Filter Up alert was sent as well, the connection loss was temporary only.

If only the Lync Filter Down alert was sent, please check if the Front End server (running the Verba Lync filter role) is reachable. If not, contact your IT team.

If the server is reachable, and the Lync Filter Up alert was still not received, please contact the support service and send the log file of the related services - recorderproxy.log, lyncfilter.log
Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Media Collector and Proxy Service: LyncFilterUp

SfB/Lync Filter Up Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#
Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the communication is restored between the Verba components - Lync Filter and Media Collector and Proxy.

Resolution

No further action required, the issue was probably caused by a network glitch.

However, if you receive this pair of alerts on a regular basis, please contact the support service and send the log files of the related service (s).

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files (x86)\Verba\log) folder on each server.

Media Collector and Proxy Service: RecorderDown

Recorder Down Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: CRITICAL

Description:
Recorder '<COMPUTER>' disconnected, remote port: <PORT_NUMBER>

Alert attributes:
Hostname (OID: .200.3): <COMPUTER>

Cause

This alert is sent if one of the Recorder server(s) disconnects.

Resolution

Please note, if the Recorder Up alert was sent as well, the connection loss was temporary only.

If only the Recorder Down alert was sent, please check if the server machine (mentioned in the description) is reachable. If not, contact your IT team.

If the server is reachable, and the RecorderUp alert was still not received, please contact the support service and send the log files of the related service(s) - recorderproxy.log, engine.log (from the recorder server).

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Media Collector and Proxy Service: RecorderOverloadBegin

Recorder Overload Begin Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#
Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent by the Proxy Server(s); if the Overload Thresholds limits (number of concurrent calls, CPU load, Network load, etc..) on one the Recorder Server(s) are reached. By default this function is disabled.

Resolution

If you receive such an alert, consider changing the threshold values, or upgrade the server machine.

If the Overall Threshold limits are reached on one the Recorder Servers, the Proxy will assign the call to a recorder when it's load become normal the Proxy will route the next call to another available Recorder Server with normal load.

Enabling/Disabling monitoring feature, or changing the given values:

Step 1 - On the web interface go to **Administration** and choose **Configuration Profiles**.

Step 2 - Choose and click on each of the **Default Media Collector & Proxy Server Configuration Profile** from the list

Step 3 - Click on the **Change Configuration Settings** tab, and search for **Media Collector and Proxy**.

Step 4 - Under **Media Collector and Proxy/Overload Thresholds** you can set the threshold values

Step 5 - Click the
💾
icon to save your settings.

Step 6 - The system will notify you that the changes need to applied to the server by restarting the involved services or rereading the new configuration. Execute the required tasks.

Media Collector and Proxy Service: RecorderOverloadEnd

Recorder Overload End Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#
Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the load on the Recorder Server is under the Overload Thresholds limits again.

Resolution

No further action needed.

However, if you receive this pair of alerts on a regular basis, consider improving the hardware, or changing the threshold values.

Media Collector and Proxy Service: RecorderStandbyBegin

Recorder Stand-by Begin Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#
Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if a Recorder Server is switched to maintenance mode.

Resolution

If you receive such an alert, and the start of the maintenance mode was not on purpose, follow the steps below to switch the Recorder to active mode:

Step 1 - On the web interface go to **Administration** and choose **Verba Servers**
Step 2 - Choose the **Media Repository** from the server list
Step 3 - Click on the **Service Contro**l tab, and search for **Verba Media Collector and Proxy Service**
Step 4 - In the row of **Verba Media Collector and Proxy Service**, under **Operations** you can stop the Maintenance Mode by clicking on the icon
.

After those steps, you should receive the Recorder Standby End alert.

If the service won't switch to Normal Operation please contact the support service and send the log files of the related service - recorderproxy.log
Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files (x86)\Verba\log) folder on each server.

Media Collector and Proxy Service: RecorderStandbyEnd

Recorder Stand-by End Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: WARNING

Description:
Recorder <COMPUTER> returned from maintenance mode

Alert attributes:
Hostname (OID: .200.3): <COMPUTER>

Cause

This alert is sent if the Verba Media Collector and Proxy Service back at Normal Operation state.

Resolution

No further action required.

Media Collector and Proxy Service: RecorderUp

Recorder Up Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: CRITICAL

Description:
Recorder '<COMPUTER>' connected, remote port: <PORT_NUMBER>
Alert attributes:
Hostname (OID: .200.3): <COMPUTER>

Cause

This alert is sent if the Recorder server (mentioned in the description) is reachable again.

Resolution

No further action required, the issue was probably caused by a network glitch.

However, if you receive this pair of alerts on a regular basis, please contact the support service and send the log files of the related service (s) - recorderproxy.log, engine.log (from the recorder server).
Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files (x86)\Verba\log) folder on each server.

Node Manager Service: RegistrationFailed

Registration Failed Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
Node registration failed: Could not connect to database.
#DESCRIPTION#

Alert attributes:
<CUSTOM_ATTRIBUTES>

Cause

This alert is sent if the Node Manager service can not register the server in the Verba management system. The cause can be connectivity issue or database connection configuration issue in Verba. This doesn't affects the recording.

Resolution

Check the connectivity between the database and server provided at the "Computer Name". Check the databse connection configuration in Verba: Configuring database connection

If you need additional help, please contact the support service and send the log files of the related service(s).

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Node Manager Service: RegistrationReady

Registration Ready Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#
Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if after a failure the Node Manager service can register the server in the Verba management system

Resolution

If you receive such an alert, please contact the support service and send the log files of the related service(s).

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Passive Recorder Service: CallProcError

Call Processing Error Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
Failed to record new call: #DESCRIPTION#

Alert attributes:
Call id (OID: .200.5): #ID#

Cause

This alert is sent if the Verba Passive Recorder Service encountered an error during call processing.

Resolution

If you receive such an alert, please contact the support service and send the log files of the related service - engine.log file.

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files (x86)\Verba\log) folder on each server.

Passive Recorder Service: Capture Down Alert

Capture Interface Down Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
Capture device went down:
#DESCRIPTION#

Alert attributes:
Capture interface url (OID: .200.8): <HOSTNAME|PORT|USERNAME|PW_ENC|#|#|#>

Cause

This alert is sent if the Passive Recorder Service loses connection to Media Collector or Network Interface which causes stop of recording calls.

Resolution

If you receive such an alert, please contact the support service and send the log files of the Passive Recorder Service - engine.log file.

Also, if you have a Lync/Skype for Business environment, please send the log files of the related media collector services as well - recorderproxy.log and lyncfilter.log files from each server where a Verba component is present.

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files (x86)\Verba\log) folder on each server.

Please note, that if you received the Capture Interface Up alert as well, then the recording continues.

Passive Recorder Service: Capture Up

Capture Interface Up Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
Capture device is up

Alert attributes:
Capture interface url (OID: .200.8): <HOSTNAME|PORT|USERNAME|PW_ENC|#|#|#>

Cause

This alert is sent if the Media Collector connection or Network Interface capturing is reopened and recording is up again.

Resolution

This is not an error condition, no further action required.
However, if you receive this pair of alerts on a regular basis, please contact the support service and send the log files of the Passive Recorder Service - engine.log file.

Also, if you have a Lync/Skype for Business environment, please send the log files of the related media collector services as well - recorderproxy.log and Lyncfilter.log files from each server where a Verba component is present.

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files (x86)\Verba\log) folder on each server.

SfB-Lync Call Filter Service: AnnouncementBack Alert

Announcement Back Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#
Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the announcement connection is restored after a recorder timeout.

Resolution

No further action required.

However, if you receive this pair of alerts on a regular basis, your network is probably overloaded.

If that is not the case, please contact the support service and send the log files of the related services - LyncFilter.log from The Front End(s) and announcement.log from the Verba Server.
Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files (x86)\Verba\log) folder on each server.

SfB-Lync Call Filter Service: AnnouncementTimeout Alert

Announcement Timeout Alert

Content

Verba System Monitor has received an alert from Call Filter Service.

Computer name: <COMPUTER_NAME>
Alert id: <ID>
Alert timestamp: <TIME> UTC
Alert: <ERROR_TYPE> (OID: <OID>)
Alert severity: <SEVERITY>

Description:

Alert attributes:
<CUSTOM_ATTRIBUTES>

Cause

This alert is sent if the announcement does not answer for a keepalive request for a certain time (10 sec).

Resolution

If you receive such an alert, please check if the connection is up between the affected Front End server and the Verba Announcement server (TCP 10210). If not, contact your IT team.

If the connection is up, and the Recorder Back alert was not received, please contact the support service and send the log files of the related service - LyncFilter.log from The Front End(s) and announcement.log from the Verba Server.
Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

SfB-Lync Call Filter Service: LyncDown Alert

SfB/Lync Down Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#

Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the Lync API connection is closed by Lync Server.

Resolution

If you receive such an alert, please contact the support service and send the log files of the related service(s).

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files (x86)\Verba\log) folder on each server.

Please note, if you received the Lync Up alert as well, the connection lost was temporary only.

SfB-Lync Call Filter Service: LyncInActive Alert

Sfb/Lync Inactive Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#
Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the filter service does not get SIP message from the Lync Server for a certain time.

Resolution

If you receive such an alert, please contact the support service and send the log files of the related service(s).

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

SfB-Lync Call Filter Service: LyncUp

SfB/Lync Up Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#
Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the Lync API connection is restored after a Lync Down event.

Resolution

No further action required.

However, if you receive this pair of alerts on a regular basis, please contact the support service and send the log files of the related service(s).

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files (x86)\Verba\log) folder on each server.

SfB-Lync Call Filter Service: MediaCollectorBack Alert

Media Collector Back Alert

Content

Verba System Monitor has received an alert from Call Filter Service.

Computer name: <COMPUTER_NAME>
Alert id: <ID>
Alert timestamp: <TIME> UTC
Alert: <ERROR_TYPE> (OID: <OID>)
Alert severity: <SEVERITY>

Description:

Alert attributes:
<CUSTOM_ATTRIBUTES>

Cause

This alert is sent if the medica collector connection is restored after a recorder timeout.

Resolution

No further action required.

However, if you receive this pair of alerts on a regular basis, your network is probably overloaded.

If that is not the case, please contact the support service and send the log files of the related services - LyncFilter.log from the Front End(s) and recorderproxy.log from the Verba Server.

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

SfB-Lync Call Filter Service: MediaCollectorTimeout Alert

Media Collector Timeout Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#
Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the media collector does not answer for a keepalive request for a certain time (10 sec).

Resolution

If you receive such an alert, please check if the connection is up between the the mentioned Front End server and the Verba server (TCP 10201). If not, contact your IT team.

If the connection is up, and the Media Collector Back alert was not received, please contact the support service and send the log files of the related service - LyncFilter.log from The Front End(s) and recorderproxy.log from the Verba Servers.
Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files (x86)\Verba\log) folder on each server.

SfB-Lync Call Filter Service: RecorderBack Alert

Recorder Back Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#

Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the recorder connection is restored after a recorder timeout.

Resolution

No further action required.

However, if you receive this pair of alerts on a regular basis, please contact the support service and send the log files of the related services - LyncFilter.log from The Front End(s) and engine.log from the Verba Server.

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files (x86)\Verba\log) folder on each server.

SfB-Lync Call Filter Service: RecorderTimeout Alert

Recorder Time-out Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#

Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the recorder does not answer for a keepalive request for a certain time (10 sec).

Resolution

If you receive such an alert, please check if the connection is up between the affected Front End server and the Verba server (TCP, port: 10201). If not, contact your IT team.

If the connection is up, and the Recorder Back alert was not received, please contact the support service and send the log files of the related services - LyncFilter.log from The Front End(s) and engine.log from the Verba Server.
Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

SfB-Lync Call Filter Sevice: CallProcessingError

Call Processing Error Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#
Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the filter cannot process a SIP message.

Resolution

If you receive such an alert, please contact the support service and send the log files of the related service(s).

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

SfB-Lync IM Filter Service: LyncDown Alert

SfB/Lync Down Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#
Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the Lync API connection is closed by Lync Server.

Resolution

If you receive such an alert, please contact the support service and send the log files of the related service(s).

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

SfB-Lync IM Filter Service: LyncUpAlert

SfB/Lync Up Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#
Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the Lync API connection is restored after a Lync Down event.

Resolution

No further action required.

However, if you receive this pair of alerts on a regular basis, please contact the support service and send the log files of the related service (s).

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Storage Management Service: Centera Privileged Delete Allowed

Centera Privileged Delete Allowed Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
Privileged delete is allowed! Remove this capability.
Alert attributes:
Description (OID: .200.1): Centera address: primary=192.168.1.153?C:\auth.PEA

Cause

This alert is sent when we have privileged delete right, which means we could delete files which are locked against normal delete.

Resolution

This is an error condition. Verba will not use the Centera storage target until the issue is resolved.

To resolve the issue you should generate another PEA authorization file in your Centera system, but without the Privileged delete right, then add this new PEA file on the Centera Storage Target configuration page.

Storage Management Service: PolicyContinues

Policy Continues Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:

Policy processing continues after error: <ERROR>
Affected policy was: <POLICY_NAME>
Affected target was: <TARGET_NAME>

Alert attributes:
<CUSTOM_ATTRIBUTES>

Cause

This alert is sent after policy processing can be contiued after an error.

Resolution

This is not an error condition, no further action required.

Storage Management Service: PolicyError

Policy Error Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
Policy processing Error: #Description#
Affected policy: <POLICY_NAME>
Affected target: <TARGET_NAME>
Affected call: <CALL_CDR_ID>

Alert attributes:

#CUSTOM_ATTRIBUTES#

Cause

This alert is sent out when there is a recording on the Recording Server, but there is no corresponding recording in the database. In this case, the Verba Storage Management service cannot upload the file to any storage targets. This usually happens when the recording was successful, but the recorder service couldn't insert the record into the database. In cases like this, the recorder service keeps trying until it succeeds. The Verba Storage Management service does the same, it keeps trying until it finds a corresponding record in the database.

Resolution

Since the services keep trying, first the media file should be checked on the Recording Server. Go to the server specified in the "Computer name" field of the alert, and search for the call ID specified in the "Affected call" field of the alert in the local media folder. The local media folder specified in the server configuration (Administration->Verba Servers) under the Directories \ Media Folder setting. If the call cannot be found, then the recorder service managed to insert the record and the Verba Storage Management service succeeded to upload the file to a storage target.

If the file is still there then please contact the support service and send the recorder log (engine.log in case of SfB/Lync, unifiedrec.log in case of Cisco/SIPREC, nativerecorder.log in case of legacy Cisco) files from the "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder, so we can find out why the database record is missing.

Storage Management Service: PolicyFinished

Policy Finished Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:

Policy processing finished.
Policy: <POLICY_NAME>
Total processed calls: <NUMBER_OF_CALLS>, failed calls: <NUMBER_OF_CALLS>

Alert attributes:
<CUSTOM_ATTRIBUTES>

Cause

This alert is sent when a policy processing finished.

Resolution

This is not an error condition, no further action required.

Undefined Error

Undefined Error Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#

Alert attributes:

#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the service mentioned in the email encountered some unexpected error.

Resolution

If you receive such an alert, please contact the support service and send the log files of the related service(s).
Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files (x86)\Verba\log) folder on each server.

Unified Call Recorder Service: CallProcessingError Alert

Call Processing Error Alert

Content

Alert: Call processing error
Service: Unified Recorder
Computer name: <COMPUTER_NAME>
Alert id: .115.0.7
Time: <TIME> (UTC)
Severity: ERROR

Description:
Cannot start recording of call since media recorder is not available currently

Alert attributes:
Call id (OID: .200.5): <CALL_ID>

Cause

This alert is sent if there are no media recorder available.

Resolution

If you receive such an alert, please contact the support service and send the log files of the related service.

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

If BT IP Trade recording is configured, check the Configuration limitation section of BT IP Trade.

Unified Call Recorder Service: JTAPIServiceDown Alert

JTAPI Service Down Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
JTAPI service went down

Alert attributes:
Hostname (OID: .200.3): <IP>

Cause

This alert is sent if JTAPI Service is not reachable for the Unified Call Recorder service.

Resolution

If you receive such an alert, please check that the Verba Cisco JTAPI service is running. If yes, contact the support service and send the log files of the related service(s). Please note, if you received the JTAPI/DB service up alert as well, the connection loss was temporary.

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Unified Call Recorder Service: JTAPIServiceUp Alert

JTAPI Service Up Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
JTAPI service went up

Alert attributes:
Hostname (OID: .200.3): <IP>

Cause

This alert is sent if JTAPI Service is reachable for the Unified Call Recorder service again.

Resolution

No further action required.

However, if you receive this pair of alert on a regular basis, contact the support service and send the log files of the related services: unified.log, nativedbrecorder.log.

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files (x86)\Verba\log) folder on each server.

Unified Call Recorder Service: MediaRecDown Alert

Media Recorder Down Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
Media recorder went down (vrp://"USERNAME":"PASSWORD"@"MEDIAREC_IP_ADDRESS":"MEDIAREC_PORT")

Alert attributes:
<CUSTOM_ATTRIBUTES>

Cause

This alert is sent if the Verba Recording Director component can not connect to one of the Verba Media Recorder(s). The not reachable Media Recorder's IP address is mentioned in the alert email.

Resolution

Please note, if the MediaRecUp alert was sent as well, the connection loss was temporary only.

If only the MediaRecDown alert was sent, please check if the server machine (running the Verba Media Recorder role) is reachable. If not, contact your IT team.

If the server is reachable, and the MediaRecUp alert was still not received, please contact the support service and send the log files of the Unified Call Recorder service.

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files (x86)\Verba\log) folder on each server.

Unified Call Recorder Service: MediaRecUp Alert

Media Recording Up Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
Media recorder went up (vrp://"USERNAME":"PASSWORD"@"MEDIAREC_IP_ADDRESS":"MEDIAREC_PORT")

Alert attributes:
<CUSTOM_ATTRIBUTES>

Cause

This alert is sent if the communication is restored between the Verba components - Recording Director and Media Recorder.

Resolution

No further action required, the issue was probably caused by a network glitch. However, if you receive this pair of alerts on a regular basis, your network is probably overloaded.

Unified Call Recorder Service: RecorderOverloadBegin

Recorder Overload Begin Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
Recorder <COMPUTER> become overloaded

Alert attributes:
Hostname (OID: .200.3): <COMPUTER>

Cause

This alert is sent by the Recording Director; if the Overload Thresholds limits (number of concurrent calls, CPU load, Network load, etc..) on one the Media Recorder(s) are reached. By default this function is disabled.

Resolution

If you receive such an alert, consider changing the threshold values, or upgrade the server machine. If the Overall Threshold limits are reached on one the Media Recorder(s), the Recording Director will route the next call to another available Media Recorder.

Enabling/Disabling monitoring feature, or changing the given values:

On Recording Director:

Step 1 - On the web interface go to **Administration** and choose **Verba Servers**.

Step 2 - Choose and click on each of the Recording Director server(s) from the server list

Step 3 - Click on the **Change Configuration Settings** tab, and search for **Unified Call Recorder**.

Step 4 - Under **Unified Call Recorder/Recording Providers/General** you can enable/disable **Performance Based Load balancing for Recorders**.

Step 5 - Click the
💾
icon to save your settings.

Step 6 - The system will notify you that the changes need to applied to the server by restarting the involved services or rereading the new configuration. Execute the required tasks.

On Media Recorder:

Step 1 - On the web interface go to **Administration** and choose **Verba Servers**.

Step 2 - Choose and click on each of the Media Recorder server(s) from the server list

Step 3 - Click on the **Change Configuration Settings** tab, and search for **Unified Call Recorder**.

Step 4 - Under **Unified Call Recorder/Media Recorder/Overload Thresholds** you can set the threshold values

Step 5 - Click the
💾
icon to save your settings.

Step 6 - The system will notify you that the changes need to applied to the server by restarting the involved services or rereading the new configuration. Execute the required tasks.

Unified Call Recorder Service: RecorderOverloadEnd

Recorder Overload End Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
Recorder <COMPUTER> become normal

Alert attributes:
Hostname (OID: .200.3): <COMPUTER>

Cause

This alert is sent if the load on the Media Recorder is under the Overload Thresholds limits again.

Resolution

No further action needed.

However, if you receive this pair of alerts on a regular basis, consider improving the hardware, or changing the threshold values.

Unified Call Recorder Service: RecorderStandbyBegin

Recorder Stand-by Begin Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
Recorder <COMPUTER> switched to maintenance mode

Alert attributes:
Hostname (OID: .200.3): <COMPUTER>

Cause

This alert is sent if a Verba Component is switched to maintenance mode.

Resolution

If you receive such an alert, and the start of the maintenance mode was not on purpose follow the steps below to switch the Recorder to active mode:

Step 1 - On the web interface go to **Administration** and choose **Verba Servers**.

Step 2 - Choose the Media Repository from the server list

Step 3 - Click on the **Service Control** tab, and search for **Verba Unified Call Recorder Service**.

Step 4 - In the row of **Verba Unified Call Recorder Service,** under **Operations** you can stop the Maintenance Mode by clicking on the ⬆ icon

After those steps, you should receive the RecorderStandbyEnd alert

If the service won't switch to **Normal Operation** please contact the support service and send the log files of the related service.

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Unified Call Recorder Service: RecorderStandbyEnd

Recorder Stand-by End Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
Recorder <COMPUTER> returned from maintenance mode

Alert attributes:
Hostname (OID: .200.3): <COMPUTER>

Cause

This alert is sent if the Verba Unified Recorder Service back at Normal Operation state.

Resolution

No further action required.

Unified Call Recorder Service: Recording Director Down

Recording Director Down Alert

Content

Alert: Recording director down
Service: Unified Recorder
Computer name: <COMPUTER_NAME>
Alert id: .115.0.14
Time: <TIME> (UTC)
Severity: WARNING

Description:
Recording director (RD) disconnected

Alert attributes:
Hostname (OID: .200.3):

Cause

This alert is sent if a Recording Director component is not reachable for a Media Recorder component.

Resolution

If the connection should be on (you are sure that the connection is up between the two servers), and you did not receive a Recording Director Up alert, please contact the support service and send the log files of the related service(s) - unified.log. If you received Recording Provider Up alert, the connection down state was temporary only.

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Unified Call Recorder Service: Recording Director Up

Recording Director Up Alert

Content

Alert: Recording director up
Service: Unified Recorder
Computer name: <COMPUTER_NAME>
Alert id: .115.0.15
Time: <TIME> (UTC)
Severity: WARNING

Description:
Recording director (RD) connected

Alert attributes:
Hostname (OID: .200.3):

Cause

This alert is sent if a Recording Director component is reachable again for the Media Recorder component.

Resolution

No further action required.

However, if you receive this pair of alert on a regular basis, contact the support service and send the log files of the related services: unified.log.

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Unified Call Recorder Service: RecProviderDown Alert

Recording Provider Down Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#
Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if a Cisco Gateway XCC connector or Speakerbus iCDS or Iptrade turret disconnects from the recorder.

Resolution

> ⓘ Confirm that the alert is from an UC platform that is recorded. In case it is from a not recorded platform, it is a false alert most likely generated by a port scanning application

If the connection should be on, and you did not receive a Recording Provider Up alert, please contact the support service and send the log files of the related service(s) - unified.log. If you received Recording Provider Up alert, the connection down state was temporary only.

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Unified Call Recorder Service: RecProviderUp Alert

Recording Provider Up Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#
Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if a Cisco Gateway XCC connector or Speakerbus iCDS or Iptrade turret connects back to the recorder.

Resolution

This is not an error condition, no further action required. Please note that these alerts are on Warning level. If you don't want to receive that level of errors, you can change the alert sending level from Warning to Error level, so this alert won't be sent anymore. You can do that by following these steps:

Step 1 - On the web interface go to **Administration** menu, and choose **Verba servers**
Step 2 - Choose the server from the server list from which you receive such alerts
Step 3 - Click on the **Change Configuration** tab, and search for **System Monitoring**
Step 4 - Under **System Monitoring/Service Alerts/Email Notification Level** change the level from Warning to Error, and click on the Save button
Step 5 - Click the
💾
icon to save your settings.
Step 6 - The system will notify you that the changes need to applied to the server by restarting the involved services or rereading the new configuration. Execute the required tasks.

Unified Call Recorder Service: SipTrunkDown Alert

SIP Trunk Down Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
SIP trunk is down

Alert attributes:
Hostname (OID: .200.3): <CUCM_IP_ADDRESS>

Cause

This alert is sent if the Recording Director did not receive any SIP messages from the given CUCM IP address. By default this function is disabled.

Resolution

If you receive such an alert, please check the connection between the server and the CUCM. If the connection is down, contact your IT team. If the connection is alive, please check the trunk settings from the CUCM's web page.

> ⓘ **Timeout configuration**
> The time set in Verba should be higher than the value set in CUCM.
> The default values are 120 seconds for Verba timeout and 60 seconds for CUCM Options Ping interval.

Enabling/Disabling monitoring feature:

Required setting in Cisco UCM side: Use a SIP Trunk with a **SIP Profile in** which has the **SIP Options Ping** configured.

Required setting in Verba side:

Step 1 - On the web interface go to **Administration** and choose **Verba Servers**.

Step 2 - Choose and click on each of the Recording Director server(s) from the server list

Step 3 - Click on the **Change Configuration Settings** tab, and search for **Unified Call Recorder**.

Step 4 - Under **Unified Call Recorder/Recording Providers/SIP/SIPREC/SIP Trunk Status Monitoring** you can add a stup by clicking on the + icon.

Step 5 - On the right side of the window, set the CUCM IP address, and the threshold value for timeout. Note that it should be greater then the Options Ping interval set on the CUCM side.

Step 6 - Click the 💾 icon to save your settings.

Step 7 - The system will notify you that the changes need to applied to the server by restarting the involved services or rereading the new configuration. Execute the required tasks.

Unified Call Recorder Service: SipTrunkUp Alert

SIP Trunk Up Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
SIP trunk is up

Alert attributes:
Hostname (OID: .200.3): <CUCM_IP_ADDRESS>

Cause

This alert is sent if the Recording Director received SIP messages from the CUCM again.

Resolution

No further action required. However, if you receive this pair of alerts on a regular basis, your network is probably overloaded.

Web Application Service: AD Synchronization Error

AD Synchronization Error alert

Content

Alert: AD Synchronization Error
Service: Web Application
Computer name: <COMPUTER_NAME>
Alert id: .118.2.1
Time: <TIME> (UTC)
Severity: ERROR

Description:
#DESCRIPTION#

Alert attributes:

Service name (OID: .200.2): VerbaWebApp

Cause

This alert is sent when too many users (based on the setting) would be deactivated during an Active Directory Synchronization.

Resolution

By default that function is disabled.

To enable that function, follow the steps below:

Step 1 - On the web interface go to **System** and choose **Servers**
Step 2 - Choose the Media Repository server from the server list
Step 3 - Click on the **Change Configuration Settings** tab, and search for **Web Application**
Step 4 - Under Web Application search for **Active Directory Synchronization/Automatic Rollback Threshold on Invalidated Users [%]:,** and set how many users can be invalidated during a single AD synchronization (in percent).
Step 5 - Click the
💾
icon to save your settings.
Step 6 - The system will notify you that the changes need to apply to the server by restarting the involved services or rereading the new configuration. Execute the required tasks.

Web Application Service: Could not apply recording rules

Could not apply recording rules alert

Content

Alert: Could not apply recording rules (ACL)
Service: Web Application
Computer name: <COMPUTER_NAME>
Alert id: .118.1.1
Time: <TIME> (UTC)
Severity: ERROR

Description:
#DESCRIPTION#

Alert attributes:

Service name (OID: .200.2): VerbaWebApp

Cause

This alert is sent when Verba failed to apply extension configuration after Active Directory Synchronization.

Resolution

If you receive such an alert, please check if the Verba Node Manager Agent service is running on the server mentioned in the description part.

If the Verba Node Manager Agent service is running, please check if that server is reachable from the Media Repository server through port 4433.

If yes, please contact the support service and send the log files of the related service(s).
Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Web Application Service: Failed Login Attempt

Failed Login Attempt Alert

Content

Alert: Failed Login Attempt
Service: Web Application
Computer name: <COMPUTER_NAME>
Alert id: .118.0.1
Time: <TIME> (UTC)
Severity: WARNING

Description:
Failed Login Attempt

Alert attributes:

#CUSTOM_ATTRIBUTES#

Cause

This alert is sent when a user login attempt is failed.

Configuration

By default that function is disabled.

To enable that function, follow the steps below:

Step 1 - On the web interface go to **Administration** and choose **Verba Servers**
Step 2 - Choose the Media Repository server from the server list
Step 3 - Click on the **Change Configuration Settings** tab, and search for **Web Application**
Step 4 - Under Web Application search for **Miscellaneous/Send System Alert On Failed Login Attempts,** and choose **Yes**
Step 5 - Click the
💾
icon to save your settings.
Step 6 - The system will notify you that the changes need to applied to the server by restarting the involved services or rereading the new configuration. Execute the required tasks.

General Alerts: Certificate is not accessible

Certificate is not accessible

Content

Verba System Monitor has detected there are no calls recorded since <AT_TIME>
Computer name: <COMPUTER_NAME>

Cause

This alert is sent when a certificate is not accessible due to various reasons. Most of the certificates used by the system are stored in the Windows Certificate Store and access should be provided for the services. This could prevent the communication between internal system components and with external systems completely.

Resolution

Ensure the services have access to the certificate. The system uses certificates at various places for internal communication (server certificate), encryption and signing, web application, etc.

If the problem remains, please contact the support service and send the log files of the related service(s).
Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

General Alerts: Certificate expires

Certificate expires

Content

Verba System Monitor has detected there are no calls recorded since <AT_TIME>
Computer name: <COMPUTER_NAME>

Cause

This alert is sent when a certificate is about to expire in 30 days. An expired certificate could prevent the communication between internal system components and with external systems completely.

Resolution

The certificate has to be renewed or replaced with a valid certificate. The system uses certificates at various places for internal communication (server certificate), encryption and signing, web application, etc.

If the problem remains, please contact the support service and send the log files of the related service(s).
Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

General Alerts: Certificate expired

Certificate expired

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#

Alert attributes:

#CUSTOM_ATTRIBUTES#

Cause

This alert is sent when a certificate is expired and can no longer be used. This could prevent the communication between internal system components and with external systems completely.

Resolution

The certificate has to be renewed or replaced with a valid certificate. The system uses certificates at various places for internal communication (server certificate), encryption and signing, web application, etc.

If the problem remains, please contact the support service and send the log files of the related service(s).
Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

General Alerts: Certificate not trusted

Certificate not trusted

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#

Alert attributes:

#CUSTOM_ATTRIBUTES#

Cause

This alert is sent when a certificate is not trusted. An untrusted certificate could prevent the communication between internal system components and with external systems completely.

Resolution

The certificate configuration have to reviewed and verified to ensure the other components can trust them. The system uses certificates at various places for internal communication (server certificate), encryption and signing, web application, etc.

If the problem remains, please contact the support service and send the log files of the related service(s).
Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

General Alerts: Certificate revoked

Certificate revoked

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#

Alert attributes:

#CUSTOM_ATTRIBUTES#

Cause

This alert is sent when a certificate is revoked and can no longer be used. This could prevent the communication between internal system components and with external systems completely.

Resolution

The certificate has to be renewed or replaced with a valid certificate. The system uses certificates at various places for internal communication (server certificate), encryption and signing, web application, etc.

If the problem remains, please contact the support service and send the log files of the related service(s).
Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

General Alerts: Certificate key is not accessible

Certificate key is not accessible

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#

Alert attributes:

#CUSTOM_ATTRIBUTES#

Cause

This alert is sent when a certificate key is not trusted. An untrusted certificate could prevent the communication between internal system components and with external systems completely.

Resolution

The certificate configuration have to reviewed and verified to ensure the service have access to the key in the certificate. The system uses certificates at various places for internal communication (server certificate), encryption and signing, web application, etc.

If the problem remains, please contact the support service and send the log files of the related service(s).
Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

General Alerts: Configuration Error

Configuration Error

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#

Alert attributes:

#CUSTOM_ATTRIBUTES#

Cause

This alert is sent when a service cannot start due to configuration error(s).

Resolution

Check the alert message and review the service configuration.

If the problem remains, please contact the support service and send the log files of the related service(s).
Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Desktop Agent: Capturing Error

Capturing Error Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#
Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if connection to a recorder service is lost.

Resolution

If you receive such an alert, please check if the connection is up between the the server and the user's computer. If not, contact your IT team.

If the connection is up, please contact the support service and send the log files of the related service - agentcontroller.log, captureagent.log.
Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files (x86)\Verba\log) folder on each server.

SfB-Lync Call Filter Sevice: Configuration Error

Configuration Error Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#
Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if there is a problem in the service configuration.

Resolution

If you receive such an alert, please contact the support service and send the log files of the related service(s).

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Web Application Service: Apply Communication Policies Failed

Apply Communication Policies Failed alert

Content

Alert: AD Synchronization Error
Service: Web Application
Computer name: <COMPUTER_NAME>
Alert id: .118.2.1
Time: <TIME> (UTC)
Severity: ERROR

Description:
#DESCRIPTION#

Alert attributes:

Service name (OID: .200.2): VerbaWebApp

Cause

This alert is sent when too many users (based on the setting) would be deactivated during an Active Directory Synchronization.

Resolution

By default that function is disabled.

To enable that function, follow the steps below:

Step 1 - On the web interface go to **Administration** and choose **Verba Servers**
Step 2 - Choose the Media Repository server from the server list
Step 3 - Click on the **Change Configuration Settings** tab, and search for **Web Application**
Step 4 - Under Web Application search for **Active Directory Synchronization/Automatic Rollback Threshold on Invalidated Users [%]:,** and set how many users can be invalidated during a single AD synchronization (in percent).
Step 5 - Click the
💾
icon to save your settings.
Step 6 - The system will notify you that the changes need to applied to the server by restarting the involved services or rereading the new configuration. Execute the required tasks.

Unified Call Recorder Service: IPCCTIActive Alert

IPC CTI Active Alert

Content

IPC CTI Passive -> Active role change

Alert: IPC CTI Passive -> Active role change
Service: Unified Recorder
Computer name: <COMPUTER_NAME>
Alert id: .115.0.17
Time: <TIME> (UTC)
Severity: CRITICAL

Description:
Changing role to active CTI due to primary become offline

Alert attributes:
Hostname (OID: .200.3): <COMPUTER_NAME>

Cause

This alert is sent if the role is changed from passive to active - this suggests that the primary component is down.

Resolution

Please check the status of the primary component.

Unified Call Recorder Service: IPCCTIPassive Alert

IPC CTI Passive Alert

Content

IPC CTI Active -> Passive role change

Alert: IPC CTI Active -> Passive role change
Service: Unified Recorder
Computer name: <COMPUTER_NAME>
Alert id: .115.0.16
Time: <TIME> (UTC)
Severity: CRITICAL

Description:
Changing role back to passive CTI due to primary become online

Alert attributes:
Hostname (OID: .200.3): <COMPUTER_NAME>

Cause

This alert is sent if the role is changed from active to passive - this suggests that the primary component is available again, so the operation is back to normal.

Resolution

No further action needed.

Verba SMS Recorder Service: SMS-C Up

SMS-C Up Alert

Content

Alert: SMS-C up
Service: SMS Recorder
Computer name: <COMPUTER_NAME>
Alert id: .119.0.1
Time: <TIME> (UTC)
Severity: CRITICAL

Description:
#DESCRIPTION#

Alert attributes:
Hostname (OID: .200.3):

Cause

This alert is sent after a connection down state.

Resolution

No further action required after this notification.

However, if you receive this pair of alerts on a regular basis, please contact the support service and send the log files of the related service (s) - smsrecorder.log.

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Verba SMS Recorder Service: SMS-C Down

SMS-C Down Alert

Content

Alert: SMS-C Down
Service: SMS Recorder
Computer name: <COMPUTER_NAME>
Alert id: .119.0.2
Time: <TIME> (UTC)
Severity: CRITICAL

Description:
#DESCRIPTION#

Alert attributes:
Hostname (OID: .200.3):

Cause

This alert is sent when the connection between the Verba server and the SMS-C is down.

Resolution

If you receive such an alert, please check if the SMS-C is reachable from the Verba server. If not, contact your IT team to search for a network issue, and check the firewall configuration as well.

If the SMS-C is reachable from the Verba server, please contact the support service and send the log file of the Verba SMS Recorder Service.

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Web Application Service: Could not send license usage to RLS

Could not send license usage to RLS alert

Content

Alert: Could not send license usage to RLS
Service: Web Application
Computer name: <COMPUTER_NAME>
Alert id: .118.1.3
Time: <TIME> (UTC)
Severity: ERROR

Description:
Could not send license usage to <REMOTE_LICENSE_SERVER_URL>
<ERROR_DETAILS>

Alert attributes:
Service name (OID: .200.2): VerbaWebApp

Cause

This alert is sent when a Remote License Subscriber web application failed to send its usage to the Remote License Server.

Resolution

Please check the Remote License settings on the server in the System / License menu, and verify that the Remote License Server URL is accessible from the server using a browser.

Storage Management Service: Verint Missing Agent Associations

Verint Missing Agent Associations Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
Missing agent association in the Verint System
Alert attributes:
Description (OID: .200.1): Action required. Employee <employee> is not configured in the Verint system. To be able to use the ingested media on the Verint side please add the employee <employee> to the Verint system and ingest the media again for this agent from Verba to Verint.

Cause

This alert is sent when the Verint system cannot assign the sent media to an employee in their system.

Resolution

This is not an error condition. Verba can successfully send the media. However, the sent media will only be visible with a superuser on the Verint side.

To resolve the issue you should follow the instructions from here to create the missing employee.

Storage Management Service: PolicyVQError

Voice Quality Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:

Policy processing error: Voice quality issues found;

Affected policy: #<POLICY_ID> - <POLICY_NAME>" (action: <ACTION>)
Affected target: <TARGET_ID>
Affected calls:
<CDR_ID> - <VQ_SCORE>

Alert attributes:
<CUSTOM_ATTRIBUTES>

Cause

This alert is sent when a Voice Quality Check find potential bad quality records according to policy's threshold setting. The alert contains the list of affected calls and their scores, alerts are generated if list size exceeds configured size or configured time to wait for bad calls elapses or policy finishes.

Resolution

This is not an error condition, no further action required.

Web Application Service: AD Synchronization Executed OK

AD Synchronization Error alert

Content

Alert: AD Synchronization Executed OK
Service: Web Application
Computer name: <COMPUTER_NAME>
Alert id: .118.2.2
Time: <TIME> (UTC)
Severity: ERROR

Description:
#DESCRIPTION#

Alert attributes:

Service name (OID: .200.2): VerbaWebApp

Cause

This alert is sent when the Active Directory Synchronization executed successfully. A short summary is included.

Resolution

By default that function is disabled.

To enable that function, follow the steps below:

Step 1 - On the web interface go to **System** and choose **Servers**
Step 2 - Choose the Media Repository server from the server list
Step 3 - Click on the **Change Configuration Settings** tab, and search for **Web Application**
Step 4 - Under Web Application search for **Active Directory Synchronization/Send Email Notification on Successful AD Sync Runs:,** and set it to Yes.
Step 5 - Click the
💾
icon to save your settings.
Step 6 - The system will notify you that the changes need to applied to the server by restarting the involved services or rereading the new configuration. Execute the required tasks.

SfB-Lync IM Filter Service: LyncInActive Alert

Sfb/Lync Inactive Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#
Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the filter service does not get SIP message from the Lync Server for a certain time.

Resolution

If you receive such an alert, please contact the support service and send the log files of the related service(s).

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

SfB-Lync Ethical Wall Service: LyncInActive Alert

Sfb/Lync Inactive Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#
Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the filter service does not get SIP message from the Lync Server for a certain time.

Resolution

If you receive such an alert, please contact the support service and send the log files of the related service(s).

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

SfB-Lync Ethical Wall Service: AnnouncementTimeout Alert

Announcement Timeout Alert

Content

Verba System Monitor has received an alert from Call Filter Service.

Computer name: <COMPUTER_NAME>
Alert id: <ID>
Alert timestamp: <TIME> UTC
Alert: <ERROR_TYPE> (OID: <OID>)
Alert severity: <SEVERITY>

Description:

Alert attributes:
<CUSTOM_ATTRIBUTES>

Cause

This alert is sent if the announcement does not answer for a keepalive request for a certain time (10 sec).

Resolution

If you receive such an alert, please check if the connection is up between the affected Front End server and the Verba Announcement server (TCP 10210). If not, contact your IT team.

If the connection is up, and the Recorder Back alert was not received, please contact the support service and send the log files of the related service - LyncFilter.log from The Front End(s) and announcement.log from the Verba Server.
Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

SfB-Lync Ethical Wall Service: AnnouncementBack Alert

Announcement Back Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#
Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the announcement connection is restored after a recorder timeout.

Resolution

No further action required.

However, if you receive this pair of alerts on a regular basis, your network is probably overloaded.

If that is not the case, please contact the support service and send the log files of the related services - LyncFilter.log from The Front End(s) and announcement.log from the Verba Server.
Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files (x86)\Verba\log) folder on each server.

SfB-Lync Ethical Wall Service: LyncDown Alert

SfB/Lync Down Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#

Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the Lync API connection is closed by Lync Server.

Resolution

If you receive such an alert, please contact the support service and send the log files of the related service(s).

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files (x86)\Verba\log) folder on each server.

Please note, if you received the Lync Up alert as well, the connection lost was temporary only.

SfB-Lync Ethical Wall Service: LyncUp

SfB/Lync Up Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#
Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the Lync API connection is restored after a Lync Down event.

Resolution

No further action required.

However, if you receive this pair of alerts on a regular basis, please contact the support service and send the log files of the related service (s).

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files (x86)\Verba\log) folder on each server.

SfB-Lync IM Filter Service: RecorderTimeout Alert

Recorder Time-out Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#

Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the recorder does not answer for a keepalive request for a certain time (10 sec).

Resolution

If you receive such an alert, please check if the connection is up between the affected Front End server and the Verba server (TCP, port: 10201). If not, contact your IT team.

If the connection is up, and the Recorder Back alert was not received, please contact the support service and send the log files of the related services - LyncFilter.log from The Front End(s) and engine.log from the Verba Server.
Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

SfB-Lync IM Filter Service: RecorderBack Alert

Recorder Back Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#

Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the recorder connection is restored after a recorder timeout.

Resolution

No further action required.

However, if you receive this pair of alerts on a regular basis, please contact the support service and send the log files of the related services - LyncFilter.log from The Front End(s) and engine.log from the Verba Server.

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files (x86)\Verba\log) folder on each server.

SfB-Lync IM Filter Sevice: CallProcessingError

Call Processing Error Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#
Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the filter cannot process a SIP message.

Resolution

If you receive such an alert, please contact the support service and send the log files of the related service(s).

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

SfB-Lync Ethical Wall Filter Sevice: CallProcessingError

Call Processing Error Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#
Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the filter cannot process a SIP message.

Resolution

If you receive such an alert, please contact the support service and send the log files of the related service(s).

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

SfB Lync Chat Recorder Service: LyncFilterDown

SfB/Lync Filter Down Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#
Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the communication is down between the Verba components - Lync Filter and Chat Recorder.

Resolution

Please note, if the Lync Filter Up alert was sent as well, the connection loss was temporary only.

If only the Lync Filter Down alert was sent, please check if the Front End server (running the Verba Lync filter role) is reachable. If not, contact your IT team.

If the server is reachable, and the Lync Filter Up alert was still not received, please contact the support service and send the log file of the related services - lyncimrecorder.log, lyncimfilter.log
Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

SfB Lync Chat Recorder Service: LyncFilterUp

SfB/Lync Filter Up Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#
Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the communication is restored between the Verba components - Lync Filter and Chat Recorder.

Resolution

No further action required, the issue was probably caused by a network glitch.

However, if you receive this pair of alerts on a regular basis, please contact the support service and send the log files of the related service (s).

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files (x86)\Verba\log) folder on each server.

SfB-Lync IM Filter Sevice: Configuration Error

Configuration Error Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#
Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if there is a problem in the service configuration.

Resolution

If you receive such an alert, please contact the support service and send the log files of the related service(s).

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

SfB-Lync Ethical Wall Sevice: Configuration Error

Configuration Error Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#
Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if there is a problem in the service configuration.

Resolution

If you receive such an alert, please contact the support service and send the log files of the related service(s).

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Web Application Service: Data Management Policy Created

Data Management Policy Created alert

Content

Alert: Data Management Policy Created
Service: Web Application
Computer name: <COMPUTER_NAME>
Alert id: .118.2.2
Time: <TIME> (UTC)
Severity: NOTIFICATION

Description:
#DESCRIPTION#

Alert attributes:

Service name (OID: .200.2): VerbaWebApp

Cause

This alert is sent when a Data Management Policy was created.

Resolution

Newly created policies can be checked in the Data \ Data Management Policies menu.

Web Application Service: Data Management Policy Updated

Data Management Policy Updated alert

Content

Alert: Data Management Policy Updated
Service: Web Application
Computer name: <COMPUTER_NAME>
Alert id: .118.2.2
Time: <TIME> (UTC)
Severity: NOTIFICATION

Description:
#DESCRIPTION#

Alert attributes:

Service name (OID: .200.2): VerbaWebApp

Cause

This alert is sent when a Data Management Policy was updated.

Resolution

Policies can be checked in the Data \ Data Management Policies menu.

Web Application Service: Data Management Policy Deleted

Data Management Policy Deleted alert

Content

Alert: Data Management Policy Deleted
Service: Web Application
Computer name: <COMPUTER_NAME>
Alert id: .118.2.2
Time: <TIME> (UTC)
Severity: NOTIFICATION

Description:
#DESCRIPTION#

Alert attributes:

Service name (OID: .200.2): VerbaWebApp

Cause

This alert is sent when a Data Management Policy was deleted.

Resolution

Policies can be checked in the Data \ Data Management Policies menu.

SfB-Lync Call Filter Service: LyncActive Alert

Sfb/Lync Active Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#
Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the filter service gets SIP message again from the Lync Server.

Resolution

If you receive such an alert, please contact the support service and send the log files of the related service(s).

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

SfB-Lync IM Filter Service: LyncActive Alert

Sfb/Lync Active Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#
Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the filter service gets SIP message again from the Lync Server.

Resolution

If you receive such an alert, please contact the support service and send the log files of the related service(s).

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

SfB-Lync Ethical Wall Service: LyncActive Alert

Sfb/Lync Active Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#
Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the filter service gets SIP message again from the Lync Server.

Resolution

If you receive such an alert, please contact the support service and send the log files of the related service(s).

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Web Application Service: Number of AD synchronized users decreased significantly

AD Synchronization Warning alert

Content

Alert: Number of AD synchronized users decreased significantly
Service: Web Application
Computer name: <COMPUTER_NAME>
Alert id: .118.2.3
Time: <TIME> (UTC)
Severity: Warning

Description:
#DESCRIPTION#

Alert attributes:

Service name (OID: .200.2): VerbaWebApp

Cause

This alert is sent when the Active Directory Synchronization deactivated more users than the 15% threshold.

Resolution

Double check the LDAP query provided in the AD Search Filter setting of the Active Directory Synchronization profile

Avaya DMCC-JTAPI Service: CallProcError Resolved

Call Processing Error Resolved Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
Call processing error: <Information>

Alert attributes:
Call id (OID: .200.5): <CALL_ID>

Cause

This alert is sent if the Verba Avaya Recorder Service encountered some error during call processing, but it is resolved now.

Resolution

If you receive such an alert, please check the configuration according to the description part of the previous CallProcError alert - e.g. invalid access code.

If there is no configuration issue, or you need assistance, contact the support service and send the log files of the Verba Avaya DMCC/JTAPI Service - avaya_recorder.log
Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

CDR Importer Service: Metadata Filesize Too Big

Metadata Filesize Too Big Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#

Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the metadata csv / xml / json file provided in the general import is bigger than 100 MB.

Resolution

Fragment the metadata file, and do the import in multiple runs.

Cisco Compliance Service: Processing Error

Processing Error Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
Call processing error. <Information>
Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the Cisco Compliance Service encountered some error during processing.

Resolution

If you receive such an alert, please contact the support service and send the log files of the related service.

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Cisco Compliance Service: DLP Server Error

DLP Server Error Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
Call processing error. <Information>
Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the Cisco Compliance Service encountered some error during contacting the DLP server.

Resolution

If you receive such an alert, please contact the support service and send the log files of the related service.

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

SMS Recorder Service: SMS ProcessingError

SMS Processing Error Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
Call processing error. <Information>
Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the SMS Recorder Service encountered some error during SMS processing.

Resolution

If you receive such an alert, please contact the support service and send the log files of the related service.

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Web Application Service: Database Maintenance Completed

Database Maintenance Completed alert

Content

Alert: Database Maintenance Completed
Service: Web Application
Computer name: <COMPUTER_NAME>
Alert id: .118.1.3
Time: <TIME> (UTC)
Severity: INFO

Description:
<ERROR_DETAILS>

Alert attributes:
Service name (OID: .200.2): VerbaWebApp

Cause

This alert is sent when the daily database maintenance job is completed.

Resolution

No further actions are required.

Web Application Service: Database Maintenance Error

Database Maintenance Error alert

Content

Alert: Database Maintenance Error
Service: Web Application
Computer name: <COMPUTER_NAME>
Alert id: .118.1.3
Time: <TIME> (UTC)
Severity: ERROR

Description:
<ERROR_DETAILS>

Alert attributes:
Service name (OID: .200.2): VerbaWebApp

Cause

This alert is sent when an error occurred during the daily maintenance job.

Resolution

If you receive such an alert, please contact the support service and send the log files of the related service.

Additional information is available within the alert.

Web Application Service: Users without Ethical Wall User permission

Users without Ethical Wall User permission alert

Content

Alert: Users without Ethical Wall User permission
Service: Web Application
Computer name: <COMPUTER_NAME>
Alert id: .118.4.1
Time: <TIME> (UTC)
Severity: NOTIFICATION

Description:
#DESCRIPTION#

Alert attributes:

Service name (OID: .200.2): VerbaWebApp

Cause

This alert is sent when there are users who are configured in communication policy, but their Communication Policies right is set to "no access".

Resolution

Go to the Users \ Roles menu, select the role which is assigned to these users, and set the Communication Policies right accordingly.

Web Application Service: License Issue

License Issue alert

Content

Alert: License Issue
Service: Web Application
Computer name: <COMPUTER_NAME>
Alert id: .118.1.3
Time: <TIME> (UTC)
Severity: ERROR

Description:
<ERROR_DETAILS>

Alert attributes:
Service name (OID: .200.2): VerbaWebApp

Cause

This alert is sent when there is an issue with the license.

Resolution

Go to the System \ License menu in order to check the license issue.

Web Application Service: Audit Log Fatal

Audit Log Fatal alert

Content

Alert: Audit Log Fatal
Service: Web Application
Computer name: <COMPUTER_NAME>
Alert id: .118.9.1
Time: <TIME> (UTC)
Severity: FATAL

Description:
#DESCRIPTION#

Alert attributes:

Service name (OID: .200.2): VerbaWebApp

Cause

This alert is sent when there is a new Fatal level alert event is logged in the Audit Log.

Resolution

Web Application Service: Audit Log Critical

Audit Log Critical alert

Content

Alert: Audit Log Critical
Service: Web Application
Computer name: <COMPUTER_NAME>
Alert id: .118.9.2
Time: <TIME> (UTC)
Severity: CRITICAL

Description:
#DESCRIPTION#

Alert attributes:

Service name (OID: .200.2): VerbaWebApp

Cause

This alert is sent when there is a new Critical level alert event is logged in the Audit Log.

Resolution

Web Application Service: Audit Log Error

Audit Log Error alert

Content

Alert: Audit Log Error
Service: Web Application
Computer name: <COMPUTER_NAME>
Alert id: .118.9.3
Time: <TIME> (UTC)
Severity: ERROR

Description:
#DESCRIPTION#

Alert attributes:

Service name (OID: .200.2): VerbaWebApp

Cause

This alert is sent when there is a new Error level alert event is logged in the Audit Log.

Resolution

Web Application Service: Audit Log Warning

Audit Log Warning alert

Content

Alert: Audit Log Warning
Service: Web Application
Computer name: <COMPUTER_NAME>
Alert id: .118.9.4
Time: <TIME> (UTC)
Severity: WARNING

Description:
#DESCRIPTION#

Alert attributes:

Service name (OID: .200.2): VerbaWebApp

Cause

This alert is sent when there is a new Warning level alert event is logged in the Audit Log.

Resolution

Web Application Service: Audit Log Notification

Audit Log Notification alert

Content

Alert: Audit Log Notification
Service: Web Application
Computer name: <COMPUTER_NAME>
Alert id: .118.9.5
Time: <TIME> (UTC)
Severity: NOTIFICATION

Description:
#DESCRIPTION#

Alert attributes:

Service name (OID: .200.2): VerbaWebApp

Cause

This alert is sent when there is a new Notification level alert event is logged in the Audit Log.

Resolution

Unified Call Recorder Service: BT Heartbeat and Directory Service Down

BT Heartbeat and Directory Service Down Alert

Content

Alert: BT Heartbeat and Directory Service Down
Service: Unified Recorder
Computer name: <COMPUTER_NAME>
Alert id: .115.0.18
Time: <TIME> (UTC)
Severity: CRITICAL

Description:
BT Heartbeat and Directory Service Down

Alert attributes:
Hostname (OID: .200.3): <COMPUTER_NAME>

Cause

The BT Heartbeat and Directory services are not running.

Resolution

Check if the BT Voice Recorder Heartbeat service is installed, if the services are running, and if the localip_config.txt is properly configured.

Unified Call Recorder Service: BT ITSLink Down

BT ITSLink Down Alert

Content

Alert: BT ITSLink Down
Service: Unified Recorder
Computer name: <COMPUTER_NAME>
Alert id: .115.0.20
Time: <TIME> (UTC)
Severity: CRITICAL

Description:
BT ITSLink Down

Alert attributes:
Hostname (OID: .200.3): <COMPUTER_NAME>

Cause

The Verba Recording Server is unable to reach the BT CTI server.

Resolution

Check the state of the ITSLink service and the network connectivity between the servers.

Unified Call Recorder Service: BT TTP Down

BT TTP Down Alert

Content

Alert: BT TTP Down
Service: Unified Recorder
Computer name: <COMPUTER_NAME>
Alert id: .115.0.22
Time: <TIME> (UTC)
Severity: CRITICAL

Description:
BT TTP Down

Alert attributes:
Hostname (OID: .200.3): <COMPUTER_NAME>

Cause

The Verba Recording Server lost the TTP media stream. This happens when the Recording Server doesn't receive any media for more time than the configured media timeout.

Resolution

Check the state of the IPSI card, and the network connectivity between the Verba Recording Server and the IPSI network interface(s).

Unified Call Recorder Service: BT Voice LAN0 Down

BT Voice LAN0 Down Alert

Content

Alert: BT Voice LAN0 Down
Service: Unified Recorder
Computer name: <COMPUTER_NAME>
Alert id: .115.0.24
Time: <TIME> (UTC)
Severity: CRITICAL

Description:
BT Voice LAN0 Down

Alert attributes:
Hostname (OID: .200.3): <COMPUTER_NAME>

Cause

The BT Heartbeat service reported losing both the Voice VLANs A and B

Resolution

Check the state of the IPSI card, and the network connectivity of the VLANs

Unified Call Recorder Service: BT Voice LAN1 Down

BT Voice LAN1 Down Alert

Content

Alert: BT Voice LAN1 Down
Service: Unified Recorder
Computer name: <COMPUTER_NAME>
Alert id: .115.0.28
Time: <TIME> (UTC)
Severity: CRITICAL

Description:
BT Voice LAN1 Down

Alert attributes:
Hostname (OID: .200.3): <COMPUTER_NAME>

Cause

The BT Heartbeat service reported losing both the Voice VLANs A and B

Resolution

Check the state of the IPSI card, and the network connectivity of the VLANs

Unified Call Recorder Service: BT Voice LAN0 Temporarily Down

BT Voice LAN0 Temporarily Down Alert

Content

Alert: BT Voice LAN0 Temporarily Down
Service: Unified Recorder
Computer name: <COMPUTER_NAME>
Alert id: .115.0.25
Time: <TIME> (UTC)
Severity: CRITICAL

Description:
BT Voice LAN0 Temporarily Down

Alert attributes:
Hostname (OID: .200.3): <COMPUTER_NAME>

Cause

The BT Heartbeat service reported losing the Voice VLAN A, and expecting failover to the standby IPSI.

Resolution

Check the state of the IPSI card, and the network connectivity of the VLAN.

Unified Call Recorder Service: BT Voice LAN1 Temporarily Down

BT Voice LAN1 Temporarily Down Alert

Content

Alert: BT Voice LAN1 Temporarily Down
Service: Unified Recorder
Computer name: <COMPUTER_NAME>
Alert id: .115.0.29
Time: <TIME> (UTC)
Severity: CRITICAL

Description:
BT Voice LAN1 Temporarily Down

Alert attributes:
Hostname (OID: .200.3): <COMPUTER_NAME>

Cause

The BT Heartbeat service reported losing the Voice VLAN B, and expecting failover to the standby IPSI.

Resolution

Check the state of the IPSI card, and the network connectivity of the VLAN.

Unified Call Recorder Service: BT Voice LAN0 Partially Down

BT Voice LAN0 Partially Down Alert

Content

Alert: BT Voice LAN0 Partially Down
Service: Unified Recorder
Computer name: <COMPUTER_NAME>
Alert id: .115.0.26
Time: <TIME> (UTC)
Severity: CRITICAL

Description:
BT Voice LAN0 Partially Down

Alert attributes:
Hostname (OID: .200.3): <COMPUTER_NAME>

Cause

The BT Heartbeat service reported losing the Voice VLAN A. VLAN B is still up.

Resolution

Check the state of the IPSI card, and the network connectivity of the VLAN.

Unified Call Recorder Service: BT Voice LAN1 Partially Down

BT Voice LAN1 Partially Down Alert

Content

Alert: BT Voice LAN1 Partially Down
Service: Unified Recorder
Computer name: <COMPUTER_NAME>
Alert id: .115.0.30
Time: <TIME> (UTC)
Severity: CRITICAL

Description:
BT Voice LAN1 Partially Down

Alert attributes:
Hostname (OID: .200.3): <COMPUTER_NAME>

Cause

The BT Heartbeat service reported losing the Voice VLAN B. VLAN A is still up.

Resolution

Check the state of the IPSI card, and the network connectivity of the VLAN.

Unified Call Recorder Service: BT TFTP0 Down

BT TFTP0 Down Alert

Content

Alert: BT TFTP0 Down
Service: Unified Recorder
Computer name: <COMPUTER_NAME>
Alert id: .115.0.32
Time: <TIME> (UTC)
Severity: WARNING

Description:
BT TFTP0 Down

Alert attributes:
Hostname (OID: .200.3): <COMPUTER_NAME>

Cause

The Verba Recording Server cannot connect to the ITSProfile server TFTP0, and cannot download the grlobalip_config.txt file.

Resolution

Check the state of ITSProfile server and the network connectivity between the Verba Recording Server and the ITSProfile server.

Unified Call Recorder Service: BT TFTP1 Down

BT TFTP1 Down Alert

Content

Alert: BT TFTP0 Down
Service: Unified Recorder
Computer name: <COMPUTER_NAME>
Alert id: .115.0.34
Time: <TIME> (UTC)
Severity: WARNING

Description:
BT TFTP1 Down

Alert attributes:
Hostname (OID: .200.3): <COMPUTER_NAME>

Cause

The Verba Recording Server cannot connect to the ITSProfile server TFTP1, and cannot download the grlobalip_config.txt file.

Resolution

Check the state of ITSProfile server and the network connectivity between the Verba Recording Server and the ITSProfile server.

Unified Call Recorder Service: BT TMS Access Down

BT TMS Access Down Alert

Content

Alert: BT TMS Access Down
Service: Unified Recorder
Computer name: <COMPUTER_NAME>
Alert id: .115.0.36
Time: <TIME> (UTC)
Severity: CRITICAL

Description:
BT TMS Access Down

Alert attributes:
Hostname (OID: .200.3): <COMPUTER_NAME>

Cause

The Verba Recording Server cannot reach the TMS share on the ITSProfile server, and cannot update the turret / vertical / line information.

Resolution

Check the state of ITSProfile server and the network connectivity between the Verba Recording Server and the ITSProfile server.

Unified Call Recorder Service: Failover Between TTP Managers

Failover Between TTP Managers Alert

Content

Alert: Failover Between TTP Managers
Service: Unified Recorder
Computer name: <COMPUTER_NAME>
Alert id: .115.0.38
Time: <TIME> (UTC)
Severity: CRITICAL

Description:
Failover Between TTP Managers

Alert attributes:
Hostname (OID: .200.3): <COMPUTER_NAME>

Cause

The Recording Director with the active TTP Manager role has changed to passive, and the Recording Director with the passive TTP Manager role has changed to active.

Resolution

Unified Call Recorder Service: BT LDAP access down

BT LDAP access down Alert

Content

Alert: BT LDAP access down
Service: Unified Recorder
Computer name: <COMPUTER_NAME>
Alert id: .115.0.39
Time: <TIME> (UTC)
Severity: CRITICAL

Description:
BT LDAP access down

Alert attributes:
Hostname (OID: .200.3): <COMPUTER_NAME>

Cause

The Verba Recording Server cannot reach the LDAP, and cannot update the turret / vertical / line information.

Resolution

Check the state of ITSProfile server and the network connectivity between the Verba Recording Server and the ITSProfile server.

Unified Call Recorder Service: BT TMS Cache access down

BT TMS Cache access down Alert

Content

Alert: BT TMS Cache access down
Service: Unified Recorder
Computer name: <COMPUTER_NAME>
Alert id: .115.0.41
Time: <TIME> (UTC)
Severity: CRITICAL

Description:
BT TMS Cache access down

Alert attributes:
Hostname (OID: .200.3): <COMPUTER_NAME>

Cause

The Verba Recording Server cannot access the local cache for the TMS / LDAP information.

Resolution

Check if the [Verba_Application_Folder]\settings\bt tms\ folder is accessible for the Verba Unified Call Recorder service on the Recording Server. To cleanup the cache, stop the Verba Unified Call Recorder service, clear the contents of the cache folder, then start the service again.

Web Application Service: Report Upload Failed

Report Upload Failed alert

Content

Alert: Report Upload Failed
Service: Web Application
Computer name: <COMPUTER_NAME>
Alert id: .118.2.4
Time: <TIME> (UTC)
Severity: Error

Description:
#DESCRIPTION#

Alert attributes:

Service name (OID: .200.2): VerbaWebApp

Cause

This alert is sent when the Web Application was unable to upload the generated report to the given network path using the credentials provided.

Resolution

Check the Web Application log in the [APPLICATION_FOLDER]\log\webapp.log file. Check if the network path is accessible, and the credentials are correct.

Web Application Service: AD Synchronization Added New Site

AD Synchronization Added New Site

Content

Alert: AD Synchronization Added New Site
Service: Web Application
Computer name: <COMPUTER_NAME>
Alert id: .118.2.4
Time: <TIME> (UTC)
Severity: Warning

Description:
#DESCRIPTION#

Alert attributes:

Service name (OID: .200.2): VerbaWebApp

Cause

This alert is sent when a new site has been added during AD synchronization.

Resolution

No further action needed.

Genesys T-Server: Genesys connection down

Genesys connection down

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
Genesys connection down.

Alert attributes:
Service name (OID: .123.0.1): <SERVICE_NAME>

Cause

This alert is sent if Verba is not able to connect to Genesys.

Resolution

If you receive such an alert, please check the connections between the server(s) and Genesys. Please note that if you received the "Genesys connection up" alert as well, the communication between the Verba component and Genesys is back in normal, the connection lost state was temporary.

If there's no connection between the server and Genesys, contact your IT team.

Genesys T-Server: Genesys connection up

Genesys connection up

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
Genesys connection up.

Alert attributes:
Service name (OID: .123.0.2): <SERVICE_NAME>

Cause

This alert is sent if Verba is able to connect to Genesys again.

Resolution

If you receive such an alert, please check the connections between the server(s) and Genesys. Please note that if you received the "Genesys connection up" alert as well after the "Genesys connection down", the communication between the Verba component and Genesys is back in normal, the connection lost state was temporary.

If there's no connection between the server and Genesys, contact your IT team.

Unified Call Recorder Service: BT TTP packet loss started

BT TTP packet loss started Alert

Content

Alert: BT TTP packet loss started
Service: Unified Recorder
Computer name: <COMPUTER_NAME>
Alert id: .115.0.43
Time: <TIME> (UTC)
Severity: CRITICAL

Description:
BT TTP packet loss started

Alert attributes:
Hostname (OID: .200.3): <COMPUTER_NAME>

Cause

The Verba Recording Server noticed packet loss at the incoming streams from the TTPs.

Resolution

Verify the network connectivity.

Unified Call Recorder Service: BT TTP packet loss ended

BT TTP packet loss ended Alert

Content

Alert: BT TTP packet loss ended
Service: Unified Recorder
Computer name: <COMPUTER_NAME>
Alert id: .115.0.44
Time: <TIME> (UTC)
Severity: CRITICAL

Description:
BT TTP packet loss ended

Alert attributes:
Hostname (OID: .200.3): <COMPUTER_NAME>

Cause

The Verba Recording Server noticed packet loss at the incoming streams from the TTPs.

Resolution

Verify the network connectivity.

Web Application Service: License Warning

License Warning Alert

Content

Alert: License Warning
Service: Web Application
Computer name: <COMPUTER_NAME>
Alert id: .118.1.8
Time: <TIME> (UTC)
Severity: WARNING

Description:
License Warning

Alert attributes:

#CUSTOM_ATTRIBUTES#

Cause

This alert is sent when there is a license item that will expire soon.

Microsoft Teams Bot Service: Recorder Connection Down Alert

Recorder Connection Down Alert

Content

Alert: Recorder Connection Down
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: .122.0.1
Time: <TIME> (UTC)
Severity: Critical

Description:
#DESCRIPTION#

Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the recorder does not answer for a keepalive request for a certain time (10 sec).

Resolution

If you receive such an alert, please check if the connection is up between the affected Bot server and the Verba Recording Server (TCP, port: 10501). If not, contact your IT team.

If the connection is up, and the Recorder Connection Up alert was not received, please contact the support service and send the log files of the related services - teamsbot.log from the Bot server and unifiedrec.log from the Verba Recording Server.
Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Microsoft Teams Bot Service: Recorder Connection Up Alert

Recorder Connection Up Alert

Content

Alert: Recorder Connection Up
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: .122.0.2
Time: <TIME> (UTC)
Severity: Warning

Description:
#DESCRIPTION#

Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the recorder connection was down, but now it is back again.

Resolution

If you receive such an alert, please check if the connection is up between the affected Bot server and the Verba Recording Server (TCP, port: 10501). If not, contact your IT team.

If the connection is up, and the Recorder Connection Up alert was not received, please contact the support service and send the log files of the related services - teamsbot.log from the Bot server and unifiedrec.log from the Verba Recording Server.
Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Microsoft Teams Bot Service: User is not configured in Verba Alert

User is not configured in Verba Alert

Content

Alert: User is not configured in Verba
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: .122.0.3
Time: <TIME> (UTC)
Severity: Warning

Description:
#DESCRIPTION#

Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the Bot service was invited into a recording session, but none of the users were found in the ACL.

Resolution

This alert is received when a Teams compliance policy is assigned to a user, but the User ID is not added as a recorded extension on the Verba side.

Microsoft Teams Bot Service: Could not join call Alert

Could not join call Alert

Content

Alert: Could not join call
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: .122.0.4
Time: <TIME> (UTC)
Severity: Critical

Description:
#DESCRIPTION#

Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the Bot service was invited into a recording session, but was not able to join.

Resolution

If you receive such an alert, please contact the support service and send the teamsbot.log from the Verba Bot Server.

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Microsoft Teams Bot Service: No available recorder Alert

No available recorder Alert

Content

Alert: No available recorder
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: .122.0.5
Time: <TIME> (UTC)
Severity: Critical

Description:
#DESCRIPTION#

Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the Bot service was invited into a recording session, but there is no available Media Recorder server/service.

Resolution

If you receive such an alert, please check the availability of the Verba Recording Servers. Contact the support service and send the unifiedrec.log from the server.

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Verba Unified IM Recorder Service: Message queue is up Alert

Message queue is up Alert

Content

Alert: Message queue is up
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: .124.0.1
Time: <TIME> (UTC)
Severity: Critical

Description:
#DESCRIPTION#

Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the message queue storage was inaccessible, but now it is back again.

Resolution

If you receive such an alert, please check if the connection is up between the affected Verba server and the storage location. If not, contact your IT team.

If the connection is up, and the Message queue is up alert was not received, please contact the support service and send the log files of the related services - unifiedimrec.log from the Verba server.
Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Verba Unified IM Recorder Service: Message queue is down Alert

Message queue is down Alert

Content

Alert: Message queue is down
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: .124.0.2
Time: <TIME> (UTC)
Severity: Critical

Description:
#DESCRIPTION#

Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the message queue storage is inaccessible.

Resolution

If you receive such an alert, please check if the connection is up between the affected Verba server and the storage location. If not, contact your IT team.

If the connection is up, and the Message queue is up alert was not received, please contact the support service and send the log files of the related services - unifiedimrec.log from the Verba server.
Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Verba Unified IM Recorder Service: Message queue is in active state Alert

Message queue is in active state Alert

Content

Alert: Message queue is in active state
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: .124.0.3
Time: <TIME> (UTC)
Severity: Critical

Description:
#DESCRIPTION#

Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the Media Recorder role was in standby state previously, and now it is active. This indicates that another active server went down, and this server took over the processing.

Resolution

If you receive such an alert, please check the network connectivity of the server that went down.

If the connection is up, please contact the support service and send the log files of the related services - unifiedimrec.log from the Verba server.
Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Verba Unified IM Recorder Service: Message queue is in standby state Alert

Message queue is in standby state Alert

Content

Alert: Message queue is in standby state
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: .124.0.4
Time: <TIME> (UTC)
Severity: Critical

Description:
#DESCRIPTION#

Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the Media Recorder tried to lock message queues for processing, but all of them were locked already. This is normal in the case of redundant server(s).

Resolution

If there is no redundant server(s), please contact the support service and send the log files of the related services - unifiedimrec.log from the Verba server.

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Verba Unified IM Recorder Service: Teams subscription is up Alert

Teams subscription is up Alert

Content

Teams subscription is up
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: .124.0.5
Time: <TIME> (UTC)
Severity: Warning

Description:
#DESCRIPTION#

Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the Verba server was unable to connect to Teams, but now the connection is up.

If you have a highly available setup with 2 Recording Directors

If you see "Microsoft Teams subscription is down" and "Microsoft Teams subscription is up" alerts in rapid succession, please check the service configuration of the servers that are recording on the same Tenant with the same AppID. They must have the same **Notification URL** and **Connection Encryption Certificate** configured. If they are different, the two servers will constantly delete the other's subscription and create their own, because only one subscription can exist for the same Tenant and AppId (Microsoft API limitation).

Resolution

If you receive such an alert, please check the network connectivity of the affected Verba server. If there is no internet connection, contact your IT team.

If the connection is up, and the Teams subscription is up alert was not received, please contact the support service and send the log files of the related services - unifiedimrec.log from the Verba server.

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Verba Unified IM Recorder Service: Teams subscription is down Alert

Teams subscription is down Alert

Content

Teams subscription is down
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: .124.0.6
Time: <TIME> (UTC)
Severity: Warning

Description:
#DESCRIPTION#

Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the Verba server is unable to connect to Teams.

Resolution

If you receive such an alert, please check the network connectivity of the affected Verba server. If there is no internet connection, contact your IT team.

If the connection is up, and the Teams subscription is up alert was not received, please contact the support service and send the log files of the related services - unifiedimrec.log from the Verba server.

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Verba Unified IM Recorder Service: Attachment download failed Alert

Attachment download failed Alert

Content

Attachment download failed
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: .124.0.7
Time: <TIME> (UTC)
Severity: Error

Description:
#DESCRIPTION#

Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the Verba server is unable to download an attachment.

Resolution

If you receive such an alert, please check the network connectivity of the affected Verba server. If there is no internet connection, contact your IT team.

If the connection is up, please contact the support service and send the log files of the related services - unifiedimrec.log from the Verba server.

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Verba Unified IM Recorder Service: No provider is configured for message processing Alert

No provider is configured for message processing Alert

Content

No provider is configured for message processing
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: .124.0.8
Time: <TIME> (UTC)
Severity: Critical

Description:
#DESCRIPTION#

Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent if the Verba server is unable to process a message, because there is no provider is configured.

Resolution

If you receive such an alert, please contact the support service and send the log files of the related services - unifiedimrec.log from the Verba server.

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

CDR Importer Service: Bad configuration

CDR Importer Service: CiscoWebex Token error

CiscoWebex Token error Alert

Content

Alert: <ALERT_ERROR>
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: <ID>
Time: <TIME> (UTC)
Severity: <SEVERITY>

Description:
#DESCRIPTION#

Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

The CiscoWebex Import Source could not **automatically** update the Refresh token. This alert only triggers on automatic updates, user-initiated updates will not cause the alert to trigger.
Causes could include configuration inconsistencies between CiscoWebex Import Source and CiscoWebex Integration configurations, intermittent networking issues, or corruption of the local token.json file.

Resolution

Step 1 - Stop the **Verba Import Service**.

Step 2- Navigate to your local Verba installation directory then find: [APPLICATION_DIRECTORY]\work\cdrimport\cisco_webex_teams [import_source_id]\token.json

Step 3 - Delete the file.

Step 4 - Restart **Verba Import Service**.

Step 5 - In your browser open [Redirect URI]:[Listener Port] set up according to Cisco Webex Import Source Configuration

Step 6 - Follow the instructions for authenticating the Import Source, after which a fresh set of tokens will be collected and written to the aforementioned token.json file.

Unified Call Recorder Service: IPC media channel went down Alert

IPC media channel went down Alert

Content

IPC media channel went down

Alert: IPC media channel went down
Service: Unified Recorder
Computer name: <COMPUTER_NAME>
Alert id: .115.0.45
Time: <TIME> (UTC)
Severity: CRITICAL

Description:
The IPC media channel is not available

Alert attributes:
Hostname (OID: .115.0.45): <COMPUTER_NAME>

Cause

The recorder service didn't manage to build up or lose the SIP session for the media stream. There will be no media record for the mix.

Resolution

No further action is needed.

Unified Call Recorder Service: IPC media channel went up Alert

IPC media channel went up Alert

Content

IPC media channel went up

Alert: IPC media channel went up
Service: Unified Recorder
Computer name: <COMPUTER_NAME>
Alert id: .115.0.46
Time: <TIME> (UTC)
Severity: CRITICAL

Description:
The IPC media channel is available again

Alert attributes:
Hostname (OID: .115.0.46): <COMPUTER_NAME>

Cause

The recorder service managed to build up the SIP session for the media stream.

Resolution

No further action needed.

Verba Unified IM Recorder Service: Subscription lifecycle event Alert

Subscription lifecycle event Alert

Content

Subscription lifecycle event
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: .124.0.9
Time: <TIME> (UTC)
Severity: Warning

Description:
#DESCRIPTION#

Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent when something is changed on the MS subscription side. It is sent when the subscription is removed, reauthorized, or missed.

Resolution

No further action is needed.

Verba Unified IM Recorder Service: Recording inactivity Alert

Recording inactivity Alert

Content

Recording inactivity
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: .124.0.10
Time: <TIME> (UTC)
Severity: Critical

Description:
#DESCRIPTION#

Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent when no activity is detected on the Webhook API for a long time.

Resolution

Check the network connectivity and user activity.

Verba Unified IM Recorder Service: Recording activity Alert

Recording activity Alert

Content

Recording activity
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: .124.0.11
Time: <TIME> (UTC)
Severity: Critical

Description:
#DESCRIPTION#

Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent when activity is detected again on the Webhook API.

Resolution

Check the network connectivity and user activity.

Verba Unified IM Recorder Service: Teams Export API connection is up Alert

Teams Export API connection is up Alert

Content

Teams Export API connection is up
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: .124.0.12
Time: <TIME> (UTC)
Severity: Critical

Description:
#DESCRIPTION#

Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent when the service is successfully connected again to the Teams Export API.

Resolution

Check the network connectivity.

Verba Unified IM Recorder Service: Teams Export API connection is down Alert

Teams Export API connection is down Alert

Content

Teams Export API connection is down
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: .124.0.13
Time: <TIME> (UTC)
Severity: Critical

Description:
#DESCRIPTION#

Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent when the service lost the connection to the Teams Export API.

Resolution

Check the network connectivity.

Verba Unified IM Recorder Service: Teams Export API license issue Alert

Teams Export API license issue Alert

Content

Teams Export API license issue
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: .124.0.14
Time: <TIME> (UTC)
Severity: Critical

Description:
#DESCRIPTION#

Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent when there is a user recording license issue on the Microsoft side.

Resolution

Check the user license assignment. For more information, see: https://kb.verba.com/display/docs/Microsoft+Teams

CDR Importer Service: General Notification Alert

General Notification Alert

Content

Alert: General Notification
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: 14011
Time: <TIME> (UTC)
Severity: Notification

Description:
#DESCRIPTION#

Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

A generic notification about the state of the recording.

Resolution

No further action is needed.

CDR Importer Service: Bad configuration Alert

Bad configuration Alert

Content

Alert: Bad configuration
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: 14006
Time: <TIME> (UTC)
Severity: Critical

Description:
#DESCRIPTION#

Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent when the configuration of one of the import sources is not correct, and the import cannot start.

Resolution

Check the import source configuration.

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

CDR Importer Service: API throttling limit reached Alert

API throttling limit reached Alert

Content

Alert: API throttling limit reached
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: 14009
Time: <TIME> (UTC)
Severity: Error

Description:
#DESCRIPTION#

Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent when the throttling is reached in the case of an integration endpoint. The import will stop, and wait till the provided amount of time.

Resolution

Open a support ticket at the Verba support site, so the configuration can be reviewed.

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

CDR Importer Service: Approaching API throttling limit Alert

Approaching API throttling limit Alert

Content

Alert: Approaching API throttling limit
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: 14008
Time: <TIME> (UTC)
Severity: Warning

Description:
#DESCRIPTION#

Alert attributes:
#CUSTOM_ATTRIBUTES#

Cause

This alert is sent when the service is reaching the throttling in the case of an integration endpoint. The import will stop, and wait till the provided amount of time.

Resolution

Open a support ticket at the Verba support site, so the configuration can be reviewed.

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Microsoft Teams Bot Service: Unexpected call termination Alert

Unexpected call termination Alert

Content

```
Alert: Unexpected call termination
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: .122.0.6
Time: <TIME> (UTC)
Severity: Critical

Description:
#DESCRIPTION#

Alert attributes:
#CUSTOM_ATTRIBUTES#
```

Cause

This alert is sent if the call between Teams and the bot service was terminated with an end reason code other than 200 OK.

Resolution

If you receive such an alert, please contact the support service and send the teamsbot.log from the Verba Bot Server.

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Microsoft Teams Bot Service: Could not authenticate Alert

Could not authenticate Alert

Content

```
Alert: Could not authenticate
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: .122.0.7
Time: <TIME> (UTC)
Severity: Critical

Description:
Could not authenticate

Alert attributes:
Description (OID: .200.1): Could not request OAuth token for tenant: <TENANT_ID>. Check the credentials.
<ERROR_MESSAGE>
Tenant id (OID: .200.16): <TENANT-ID>

– OR –

Description (OID: .200.1): Could not validate JWT Token of inbound request for tenant: <TENANT_ID>

JWT Token: <JWT_TOKEN>

<ERROR_MESSAGE>
Tenant id (OID: .200.16): <TENANT_ID>
```

Cause

This alert is sent if the Bot service is not able to retrieve an OAuth token for the outbound HTTP requests or the bot service is not able to validate the inbound HTTP requests.

Resolution

If you receive such an alert, please contact the support service and send the teamsbot.log from the Verba Bot Server.

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Microsoft Teams Bot Service: Call timed out Alert

Call timed out Alert

Content

```
Alert: Call timed out
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: .122.0.8
Time: <TIME> (UTC)
Severity: Warning

Description:
#DESCRIPTION#

Alert attributes:
#CUSTOM_ATTRIBUTES#
```

Cause

This alert is sent if the call between Teams and the bot service didn't receive any updates or media packets in the configured amount of time. (Default timeout is 45 mintues)

Resolution

If you receive such an alert, please contact the support service and send the teamsbot.log from the Verba Bot Server.

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Microsoft Teams Bot Service: Recorder overloaded Alert

Recorder overloaded Alert

Content

```
Alert: Recorder overloaded
Service: <SERVICE_NAME>
Computer name: <COMPUTER_NAME>
Alert id: .122.0.9
Time: <TIME> (UTC)
Severity: Critical

Description:
Recorder overloaded

Alert attributes:
Description (OID: .200.1): Verba Unified Call Recorder Service has overloaded at <Hostname>

Performance metrics in keep-alive: CallCount: <int>
MediaCallCount: <int>
MediaDiskFreeMbytes: <int>
MediaDiskFreePercent: <int>
NetworkUtilizationMbps: <int>
NetworkUtilizationPercent: <int>
OndemandDiskFreeMbytes: <int>
OndemandDiskFreePercent: <int>
Overloaded: <int>
ProcCpuUtilizationPercent: <int>
TotalCpuUtilizationPercent: <int>

Hostname (OID: .200.3): <Hostname>
```

Cause

This alert is sent if any of the underlying recorder services became overloaded.

Resolution

If you receive such an alert, please contact the support service and send the teamsbot.log from the Verba Bot Server.

Log files are available under "APPLICATION_FOLDER\log" (by default C:\Program Files\Verba\log) folder on each server.

Customizing Alert Severities and Selective Alert Sending

AVAILABLE IN VERSION 9.6.4 AND LATER

Verba alert priorities can be overridden by a provided severity. The alerts can be also turned off for specific alert targets or turned off entirely. For this, a rule XML file has to be created on the server(s).

Creating an Alert Rule XML

Step 1 - Create the **alert_rules.xml** file under the **[APPLICATION_FOLDER]\settings** folder, then open it for editing.

Step 2 - Paste in the following template for the XML file:

```
<?xml version="1.0" encoding="UTF-8"?>
<alert_rules>
 <rule oid_filter="oid_regexp" severity="" disabled_targets=""/>
</alert_rules>
```

Step 3 - Configure the rules the following way:

Property	Description
oid_filter	A regex filter that has to match the last three numbers of the alert OID. For example: "\.115\.0\.1" matches to the alert OID 1.3.6.1.4.1.39067.115.0.1 "\.115\.0\.." or "\.115\.0\.\d" matches to alert OIDs 1.3.6.1.4.1.39067.115.0.1-9 "\.115\.0\.\d{2}" matches to alert OIDs 1.3.6.1.4.1.39067.115.0.10-99
severity	Sets the new severity for the alert(s). If not specified, the default severity of the alert(s) will be used. Possible values: • 0 - Disables the alert(s) • 1 - Fatal • 2 - Critical • 3 - Error • 4 - Warning • 5 - Notification
disabled_targets	Specifies to which alert targets should not the alert be sent. If not specified, the alert(s) will be sent to all targets. Possible values: • snmp - The alert(s) will not be sent to the SNMP target • db - The alert(s) will not be inserted into the Verba database, so they won't be available in the Alert Management menu • mail - The alert(s) will not be sent to the email target • eventlog - The alert(s) will not be inserted into the Windows Event Log • all - Disables the alert(s) • none - The alert(s) will be sent to all targets Multiple values can be provided, separated by a comma.

Examples:

<rule oid_filter="\.115\.0\.1" severity="0"/> - Diables the alert 1.3.6.1.4.1.39067.115.0.1.

<rule oid_filter="\.115\.0\.1" severity="5"/> - Sets the severity to NOTIFICATION level for the alert 1.3.6.1.4.1.39067.115.0.1.

<rule oid_filter="\.115\.0\.1" disabled_targets="all"/> - Diables the alert 1.3.6.1.4.1.39067.115.0.1.

<rule oid_filter="\.115\.0\.1" disabled_targets="mail"/> - The alert 1.3.6.1.4.1.39067.115.0.1 will be sent to all targets, except to email.

<rule oid_filter="\.115\.0\.1" disabled_targets="mail,snmp"/> - The alert 1.3.6.1.4.1.39067.115.0.1 will be sent to all targets, except to email and SNMP.

<rule oid_filter="\.115\.0\.1" severity="5" disabled_targets="mail"/> - Sets the severity to NOTIFICATION level for the alert 1.3.6.1.4.1. 39067.115.0.1, and it will not be sent to email.

Step 4 - Save the file, then **restart the Verba System Monitor service**.

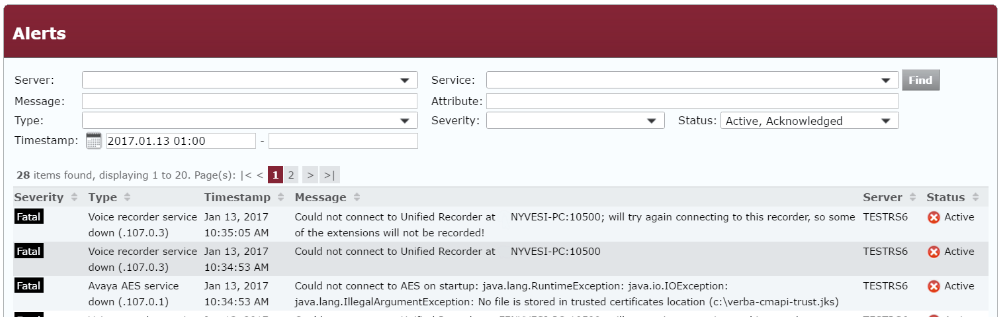
Step 5 - Repeat the steps on each server where you want to change the default alert sending.

Alert Management

The Alert Management tool displays all alerts that are being generated by any of the Verba services on any of the servers.

These alerts are sent out in emails or SNMP traps are used, but they are always displayed on the Alert Management page as well. For more information on what types of alerts exist in Verba, refer to the Alerts article. To see how SNMP traps can be configured or how SCOM can be used among others, refer to the System Monitoring article.

The tool can be accessed by navigating to the System -> Alert Management menu.



Alerts

Server:

Service:

Message:

Attribute:

Type:

Severity:

Status: Active, Acknowledged

Timestamp: 2017.01.13 01:00 -

28 items found, displaying 1 to 20. Page(s): |< < 1 2 > >|

Severity	Type	Timestamp	Message	Server	Status
Fatal	Voice recorder service down (.107.0.3)	Jan 13, 2017 10:35:05 AM	Could not connect to Unified Recorder at NYVESI-PC:10500; will try again connecting to this recorder, so some of the extensions will not be recorded!	TESTRS6	Active
Fatal	Voice recorder service down (.107.0.3)	Jan 13, 2017 10:34:53 AM	Could not connect to Unified Recorder at NYVESI-PC:10500	TESTRS6	Active
Fatal	Avaya AES service down (.107.0.1)	Jan 13, 2017 10:34:53 AM	Could not connect to AES on startup: java.lang.RuntimeException: java.io.IOException: java.lang.IllegalArgumentException: No file is stored in trusted certificates location (c:\verba-cmapi-trust.jks)	TESTRS6	Active

The alerts have different severity values:

- **Warning**
- **Error**
- **Critical**
- **Fatal**

When an alert is raised, it automatically enters the **Active** state. This means that it is a new alert, which has not been seen by any of the administrators, yet. Upon receiving a notification of an alert being raised, the administrators have the ability to change the status of the alert to either of the following 2 options:

- **Acknowledged** - This state suggests, that the administrators have seen and are aware of the issue and are working on solving the problem.
- **Cleared** - This state shows, that the issue has been resolved either automatically by the system (i.e. Database connection went down and up because of network issues) or manually by the system administrators. The status, however, always needs to be changed manually, even if the issue has been solved by the system.

> ✓ The alerts can be restored to Active, Acknowledged or Cleared state, from any of the other states.

Handling Alerts

To change the state of an individual alert, click on the alert, then at the bottom of the page, select the desired state.

Two bulk status change of alerts are possible on the alert list page:

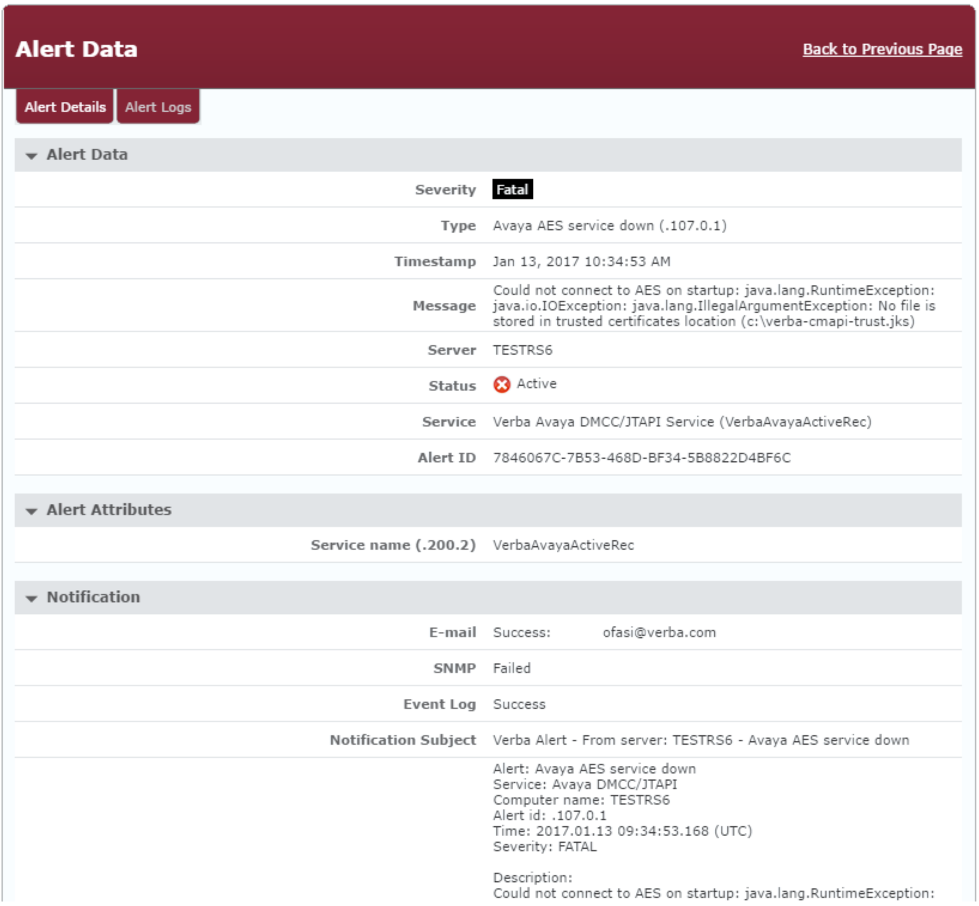
- Top right URLs which are changing the state of the entire search result through the paging as well
- Checkboxes at each alert, if any of the checkboxes checked three buttons appear at the bottom of the list which can be used for changing the selected alerts. On the top of the list Check All option is also available which checks or unchecks the displayed alerts.

Searching Alerts

By default, all alerts are shown, but the search options at the top of the page can be used to narrow down the results. The following search criteria exist:

Criterion	Description
Timestamp	Select a time range. This refers to the time when an alert was raised
Server	This can be used to only show alerts generated on a certain machine
Service	This can be used to only show alerts generated by a certain service
Message	Searches in the message content of the alerts, which describes the exact
Attribute	Different alerts can have different attributes, such as a Call ID for a failed call. The field can be used to search for these values
Type	There are a certain number of existing alert types, the search can be narrowed down to show only the selected events
Severity	The severity types, going from least severe to most severe are: Warning, Error, Critical, Fatal
Status	The options are: Active, Acknowledged, Cleared

Upon selecting an alert, the Alert Details page opens up.



Alert Data

Severity	Fatal
Type	Avaya AES service down (.107.0.1)
Timestamp	Jan 13, 2017 10:34:53 AM
Message	Could not connect to AES on startup: java.lang.RuntimeException: java.io.IOException: java.lang.IllegalArgumentException: No file is stored in trusted certificates location (c:\verba-cmapi-trust.jks)
Server	TESTRS6
Status	✖ Active
Service	Verba Avaya DMCC/JTAPI Service (VerbaAvayaActiveRec)
Alert ID	7846067C-7B53-468D-BF34-5B8822D4BF6C

Alert Attributes

Service name (.200.2)	VerbaAvayaActiveRec

Notification

E-mail	Success: ofasi@verba.com
SNMP	Failed
Event Log	Success
Notification Subject	Verba Alert - From server: TESTRS6 - Avaya AES service down
	Alert: Avaya AES service down Service: Avaya DMCC/JTAPI Computer name: TESTRS6 Alert id: .107.0.1 Time: 2017.01.13 09:34:53.168 (UTC) Severity: FATAL Description: Could not connect to AES on startup: java.lang.RuntimeException:

This page shows all of the details on the alert, including which server it was raised on, by which service. It also shows if an email or an SNMP trap has been successfully sent and if the system managed to write the events into the Windows Event Log. This is also visible on the Alert Logs page, which can be accessed by clicking on the Alert Logs tab at the top left corner.

Web interface session monitor

The administrator and the system administrators can view real-time session status for the Verba Web Application by selecting the **System / Monitoring / Session Monitor** menu.

This page provides real-time information about current user sessions, which are using the Web Application. The session register, which stores the session information, automatically puts a session into the register, if a client computer starts using the Verba Web Application (can be an IP phone XML service user or a standard web client user). If a session terminates, the register deletes the given entry.

The following table describes the available fields in the monitor pane:

Name	Description
Login Time	Date and time of the user login event.
Duration	Time elapsed since the user has logged in. Format: HH:mm:ss
Protocol	HTTP protocol version used by the client computer.
User-Agent	HTTP header User-Agent parameter, that defines the client application, which has called the Web Application. Internet Explorer sends: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322) Mozilla Firefox sends: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.7.12) Gecko/20050919 Firefox/1.0.7 (ax) Cisco IP phone sends: Allegro-Software-WebClient/xxx
Client	IP address and host name of the client computer.
Original URL	The original URL, which has started the session.
Request	Full URL request.

You can reset/clear the session register by clicking the **Clear Session Register** button. After clearing the register only new session will be stored.

Log File Names

Service or Job Name	Function	Log Name	Default Path: C:\Program Files\Verba\log
Verba Avaya DMCC/JTAPI Service	Service Log	avaya_recorder.log	APPLICATION_FOLDER\log
Verba Centile Connector Service	Service Log	centile-connector.log	APPLICATION_FOLDER\log
Verba Legacy Cisco Central Recorder Service	Service Log	nativerecorder.log	APPLICATION_FOLDER\log
Verba Cisco Central Silent Monitoring Service	Service Log	cisco-central-sm.log	APPLICATION_FOLDER\log
Verba Cisco Announcement Service	Service Log	ciscoannouncement.log	APPLICATION_FOLDER\log
Verba Cisco Compliance Service	Service Log	ciscocompliance.log	APPLICATION_FOLDER\log
	Component Connection Listener	ciscocompliance-op-recServername_1.cupsServername.log	APPLICATION_FOLDER\log
	Database Connection	ciscocompliance_dbconnbroker.log	APPLICATION_FOLDER\log
	Recorder Module	ciscocompliance-recorder.log	APPLICATION_FOLDER\log
	Ethical Wall Module	ciscocompliance-ethicalwall.log	APPLICATION_FOLDER\log
	XMPP Client	ciscocompliance-xmppclient.log	APPLICATION_FOLDER\log
Verba Cisco JTAPI Service	Service Log	native_recorder_dbservice.log	APPLICATION_FOLDER\log
Verba Cisco MediaSense Connector Service	Service Log	mediasense-connector.log	APPLICATION_FOLDER\log
Verba Legacy Cisco UC Gateway Recorder Service	Service Log	ciscogatewayrec.log	APPLICATION_FOLDER\log
Verba Dial-in Recorder Service	Service Log	activerecorder.log	APPLICATION_FOLDER\log
Verba General Media Recorder Service	Service Log	media_receiver.log	APPLICATION_FOLDER\log
Verba Importer Service	Service Log	cdrimport.log	APPLICATION_FOLDER\log
Verba Legacy IP Trade Recorder Service	Service Log	iptrade.log	APPLICATION_FOLDER\log
Verba Label Processor Service	Service Log	label-processor.log	APPLICATION_FOLDER\log
Verba Media Collector and Proxy Service	Service Log	recorderproxy.log	APPLICATION_FOLDER\log
Verba Media Streamer and Content Server Service	Service Log	mediastreamer.log	APPLICATION_FOLDER\log
Verba Media Transcoder Service	Service Log	transcoder.log	APPLICATION_FOLDER\log
Verba Media Utility Service	Service Log	waveform.log	APPLICATION_FOLDER\log
Verba Node Manager Agent	Service Log	nmagent.log	APPLICATION_FOLDER\log
Verba Passive Recorder Service	Service Log	engine.log	APPLICATION_FOLDER\log
Screen Capture Multiplexer	Service Log	multiplexer.log	APPLICATION_FOLDER\log
Screen Capturing	Service Log	captureagent.log	APPLICATION_FOLDER\log
	User Session Monitor	agentcontroller.log	APPLICATION_FOLDER\log

Verba SfB/Lync Announcement Service	Service Log	announcement.log	APPLICATION_FOLDER\log
Verba SfB/Lync Call Filter Service	Service Log	LyncFilter.log	APPLICATION_FOLDER\log
Verba SfB/Lync Communication Policy Service	Service Log	ethicalwall.log	APPLICATION_FOLDER\log
Verba SfB/Lync IM Filter Service	Service Log	LyncIMFilter.log	APPLICATION_FOLDER\log
Verba SfB/Lync IM Recorder Service	Service Log	LyncIMRecorder.log	APPLICATION_FOLDER\log
Verba Microsoft Teams Bot Service	Service Log	teamsbot.log	APPLICATION_FOLDER\log
Verba Unified IM Recorder Service	Service Log	unifiedimrec.log	APPLICATION_FOLDER\log
Verba Speech Analytics Service	Service Log	speech-analytics.log	APPLICATION_FOLDER\log
Verba Storage Management Service	Service Log	storage.log	APPLICATION_FOLDER\log
	Data Retention	policy_number.log	APPLICATION_FOLDER\log\storage policies
	Audit Log	type_number_date.log	APPLICATION_FOLDER\log\storage audit
Verba System Monitor Service	Service Log	sysmon.log	APPLICATION_FOLDER\log
Verba Unified Call Recorder Service	Service Log	unifiedrec.log	APPLICATION_FOLDER\log
Verba Web Application Service	Service Log	webapp.log	APPLICATION_FOLDER\log
	Database Connection	webapp_dbconnbroker.log	APPLICATION_FOLDER\log
	Web Application Report	webapp_rep.log	APPLICATION_FOLDER\log

Audit Log Alerts

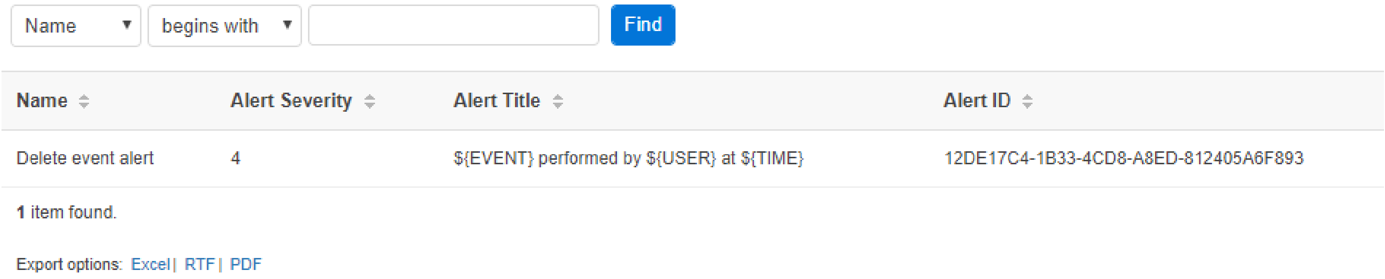
Verba provides the capability to configure alerts based on specific user actions in the web interface. The Audit Log Alerts feature can be found under the **System \ Audit Log Alerts** menu (under the **Monitoring** section).

In order to access this menu item, the user must have at least Read level access at the **Audit Log Alerts permission**. For further details, see User roles and User permissions.

Audit Log Alert Rules List

Once a user goes to the System \ Audit Log Alerts menu, it lands on the Audit Log Alert Rules list page. On this page, it's possible to filter the rules based on name or alert title, or order based on several properties.

The list of the rules can be also exported as XLS, RTF or PDF on the bottom of the page.



Name	Alert Severity	Alert Title	Alert ID
Delete event alert	4	${EVENT} performed by ${USER} at ${TIME}	12DE17C4-1B33-4CD8-A8ED-812405A6F893

1 item found.

Export options: Excel | RTF | PDF

Adding a new Audit Log Alert Rule

A new Audit Log Alert Rule can be added by clicking on the Add New Audit Log Alert Rule link in the upper right corner ow the Audit Log Alert Rules List page.

The following table describes the properties of the Audit Log Alert Rules:

Property name	Description
Name	The name of the Audit Log Event Rule.
Alert Severity	The alert will be created with the severity selected here. The severity also defines the Trap OID and Event ID (see the section below). The available severities are: - Fatal - Critical - Error - Warning - Notification
Alert Title	In the Windows Event Log, the alert data will contain a custom title provided here. This title will be picked up, and will be shown in SCOM as the title of the alert. Different properties of the Audit Log Events can be provided as variables: - ${EVENT} - ${USER} - ${TIME}

Alert Message	The alert will be created with the message provided here. Different properties of the Audit Log Events can be provided as variables: • ${EVENT} • ${USER} • ${TIME} • ${DETAILS}
Event Regexes	The alert will be triggered when the name of the Audit Log Event matches the regex provided here. Besides this, the alert will be triggered also based on the values provided in the Events list (below).
Events	The alert will be triggered when one of the selected events happen. Events can be added with the **>>** icon, or removed from the list with the **<<** icon. Besides this, the alert will be triggered also based on the regex provided in the Event Regexes (above).
Users	The alert will be triggered only for the users provided here.
Groups	The alert will be triggered only for the groups provided on the list. Groups can be added with the **>>** icon, or removed from the list with the **<<** icon.
Event Detail Content Filters	The alert will be triggered only if the Audit Log Event details are matching to the filters provided here. A new filter can be added with the + icon. If multiple filters are provided, then there will be **AND** logic between them. The **Regex** checkbox defines whether the provided values are regexes or not. The filter will match if the details of the Audit Log Event contain the value provided in the **Matches Any of These** textbox. If multiple lines are provided, then there will be **OR** logic between the lines.

Once the Audit Log Event Rule is configured, it can be saved by clicking on the **Save** button.

Alerts generated based on the Audit Log Alert Rules

There are five types of alerts defined, based on the severity of the alert:

Alert Name	Severity	Trap OID	Event ID
Audit Log Fatal	Fatal	1.3.6.1.4.1.39067.**118.9.1**	18901
Audit Log Critical	Critical	1.3.6.1.4.1.39067.**118.9.2**	18902
Audit Log Error	Error	1.3.6.1.4.1.39067.**118.9.3**	18903
Audit Log Warning	Warning	1.3.6.1.4.1.39067.**118.9.4**	18904
Audit Log Info	Info	1.3.6.1.4.1.39067.**118.9.5**	18905

Troubleshooting

Troubleshooting voice recording or import failures

There can be various reasons why a conversation was not recorded or imported. It is recommended to establish a process to investigate the issues after recognizing missing recordings (e.g. receiving the alerts). The following table provides a detailed description of the recommended troubleshooting process.

Troubleshooting Step	Description
Try to reproduce the call scenario to see if the issue can be reproduced	It is important to understand if the issue can be reproduced or not. Try to reproduce the same scenario which failed with the same participants, using the same infrastructure, etc.
Check if the recorded extensions are configured properly in the system	Most integrations require recorded extensions to be configured in the system, otherwise, the system will not record or import the conversation. • Check if the extension is added in the right format and with the right settings. The deployment guide includes information about the requirements for each integration. For more information, see Integrations • Check if the extension configuration is applied on the Recording Servers: • Check if there are no pending configurations tasks • Check if the local copy of the extension configuration is up to date
Check if recording is enabled in the communication system	Certain platforms require additional configuration to enable recording for a device, user or line. The deployment guide includes information about the requirements for each integration. For more information, see Integrations
Check if the Recording Servers are up and running and if there are no errors in the server logs	In order to verify the Recording Servers (or servers with recording or import services enabled) are up and running, follow the check below: • Check if the server is running and online. • Check if all network connections are up. • Verify the firewall configuration according to the requirements of the specific integrations. For more information, see Firewall configuration. • Check if the anti-virus scanner is not interfering with the recording functionality. For more information, see Antivirus software considerations. • Check if there is any error in the Windows Event Log which could affect the recording and import functionality. • Check if there is enough disk capacity for recording. The lack of disk space can have an adverse effect on the services or the operating system. • Check if there is any system alert raised on the server. The services are designed to automatically raise alerts if errors occur affecting the normal operation.
Check if the recorder and import services are up and running and if there are no errors in the log	Follow the checks below to verify if the recorder and import services are up and running properly: • Check if the recorder and import services are running. To verify which services have to be enabled for specific, integrations, refer to the configuration guide of the integration. • Check the logs of the respected services and search for error messages. Also, try to find any related entries for the affected calls, try to search for the conversation/call IDs available in the recorded platform (e.g. SIP call ID)
Check if the SQL database server is reachable for the recorder and import services	Verify if the SQL Server connection is up and there are no SQL errors in the related service logs.
Check if the calls are on the Recording Servers waiting to be inserted and uploaded	Verify if there are recorded or imported files on the local disk of the Recording Server waiting to be inserted or uploaded. This would indicate that the recorder or import service cannot connect to the database and/or to the storage infrastructure.

Check with the network team if there are any issues with the network connections	It is important to understand if there was any change in the network configuration or any issues detected for the time period under investigation. Even intermittent network connection errors could cause recording failure.
Check with the telephony team if there is any error related to the calls missing	There could be many issues on the communication platform which could cause recording issues. Verify if there were any errors or configuration changes in the time period under investigation.

Troubleshooting playback issues

Internet Explorer

Symptom

When you try to open Verba player to listen to a conversation, an error message is shown:

> TypeError: Unable to get property 'duration' of undefined or null reference

Root cause

This error is shown by the Verba JavaScript player when it is not able to identify the length of the call and the ActiveX controller is not able to load.

The ActiveX controller is not able to load when the PC/Server doesn't have an audio device assigned or the media player can't open the call's media file because it is stored in Verba Media Format.

Resolution

- If the workstation where you are trying to listen to the call doesn't have an audio device attached, please try the playback on another machine where at least one audio device is configured.
- If you have an audio device connected but the playback still has not started, please check the format of the media files. If the calls are recorded in the Verba Media Format, then you have to install the Verba Media Codec. Please refer to the following article: Installing Verba Unified Media Codec
- Make sure that the Windows edition you are using contains the Windows Media Player, and Internet Explorer has the Windows Media Player plugin.
- If you are trying to playback a video, desktop or screen share recording, but the Verba Media Codec installation is not possible, then it has to be converted to MPEG4 (.mp4) format first. Use the File Format Selection Pane on the left side of the player.

Chrome and Firefox

> Make sure that the **Verba Media Stream and Content Server** service is activated and started on the **Media Repository** server. Please refer to the following article to verify the service state: Service control and activation

> Please refer to the following article for playback support: Web-based media player and viewer

Symptom

When you try to open Verba player to listen to a conversation, an error message is shown, that contains a link to this article.

Root cause

This error is shown by the Verba JavaScript player when it is not able to retrieve the media file of the conversation.

In this case, the player is not able to find or connect to the Media Repository server.

A potential cause is that the media file is not uploaded to the storage.

Resolution

- Make sure that the Firewall on the Media Repository server is turned off or an allow rule is defined for ports 10105 and 10106. (These are the ports where the Media Streamer is listening for player connections)
- If your company is using an HTTP load balancer or HTTP proxy, make sure that these nodes are configured for session stickiness for ports 10105 and 10106 and these ports are not blocked on the components.
- If you are trying to playback a video, desktop or screen share recording, then it has to be converted to MPEG4 (.mp4) format first. Use the File Format Selection Pane on the left side of the player.
- Make sure that the call is covered by an upload policy.

Log files

All system components produce one or more text-based log files. All Verba components create their log files under the standard Verba log directory (your application path might be different):

```
C:\Program Files\Verba\log
```

Changing the logging settings

Most system components allow you to modify the logging parameters using Verba Web Application under **System / Servers / Hostname of your server** and select the **Change Configuration Settings** tab.

Drill down to **Service Logging** to access the logging specific configuration.

Changing the logging configuration for a service

In order to change the logging settings for a service, drill down to the service under Service Logging and change the following settings according to your needs:

Configuration	Description	Default
Log Level	Log level setting of the application. Only change this parameter temporarily (e.g. when you are doing troubleshooting or customer support asking you), because it can affect the performance of the system greatly.	Info
Maximum Log File Size	Maximum size of a log file in bytes. If a file is full, the next message is written into the next file. The maximum number of log files is limited.	20000000
Maximum Number of Log Files	Maximum number of log files. If all of the files are full, the oldest is overwritten.	10

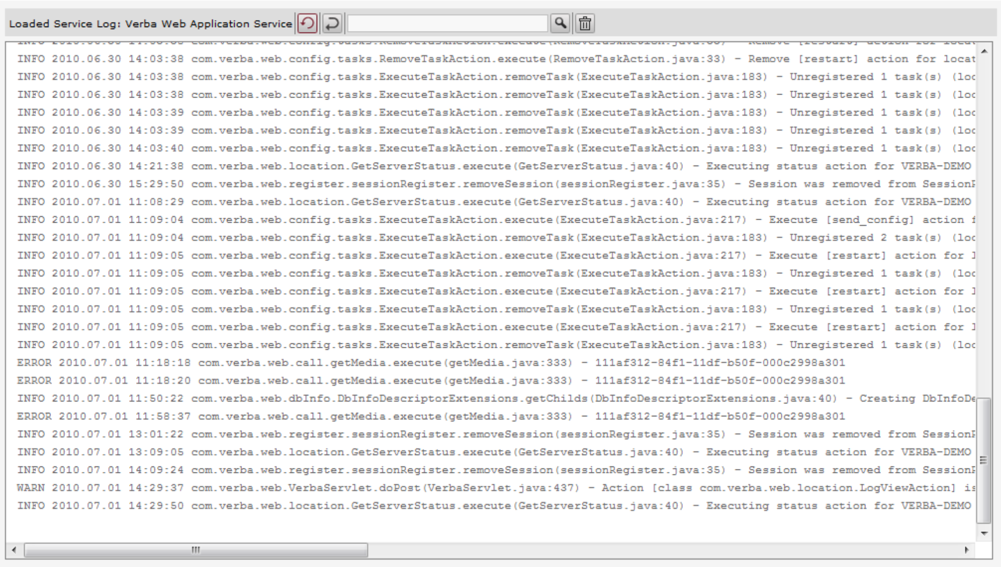
Configuring log masking

Log masking allows masking certain parts of the log files to prevent the system from logging sensitive information. For more information, refer to Customer Identification Data Masking.

Viewing the logs

The administrator and the system administrators can also access the log files using the Web Application under **System / Servers / Hostname of your server** and select the **Service Control** tab.

After selecting the **View Service Log** button for a service, the system loads the most recent lines from the service log.



```
INFO 2010.06.30 14:03:38 com.verba.web.config.tasks.RemoveTaskAction.execute(RemoveTaskAction.java:33) - Remove [restart] action for locat
INFO 2010.06.30 14:03:38 com.verba.web.config.tasks.ExecuteTaskAction.removeTask(ExecuteTaskAction.java:183) - Unregistered 1 task(s) (loc
INFO 2010.06.30 14:03:38 com.verba.web.config.tasks.ExecuteTaskAction.removeTask(ExecuteTaskAction.java:183) - Unregistered 1 task(s) (loc
INFO 2010.06.30 14:03:39 com.verba.web.config.tasks.ExecuteTaskAction.removeTask(ExecuteTaskAction.java:183) - Unregistered 1 task(s) (loc
INFO 2010.06.30 14:03:39 com.verba.web.config.tasks.ExecuteTaskAction.removeTask(ExecuteTaskAction.java:183) - Unregistered 1 task(s) (loc
INFO 2010.06.30 14:03:40 com.verba.web.config.tasks.ExecuteTaskAction.removeTask(ExecuteTaskAction.java:183) - Unregistered 1 task(s) (loc
INFO 2010.06.30 14:21:38 com.verba.web.location.GetServerStatus.execute(GetServerStatus.java:40) - Executing status action for VERBA-DEMO
INFO 2010.06.30 15:29:50 com.verba.web.register.sessionRegister.removeSession(sessionRegister.java:35) - Session was removed from SessionR
INFO 2010.07.01 11:08:29 com.verba.web.location.GetServerStatus.execute(GetServerStatus.java:40) - Executing status action for VERBA-DEMO
INFO 2010.07.01 11:09:04 com.verba.web.config.tasks.ExecuteTaskAction.execute(ExecuteTaskAction.java:217) - Execute [send_config] action f
INFO 2010.07.01 11:09:04 com.verba.web.config.tasks.ExecuteTaskAction.removeTask(ExecuteTaskAction.java:183) - Unregistered 2 task(s) (loc
INFO 2010.07.01 11:09:05 com.verba.web.config.tasks.ExecuteTaskAction.execute(ExecuteTaskAction.java:217) - Execute [restart] action for I
INFO 2010.07.01 11:09:05 com.verba.web.config.tasks.ExecuteTaskAction.removeTask(ExecuteTaskAction.java:183) - Unregistered 1 task(s) (loc
INFO 2010.07.01 11:09:05 com.verba.web.config.tasks.ExecuteTaskAction.execute(ExecuteTaskAction.java:217) - Execute [restart] action for I
INFO 2010.07.01 11:09:05 com.verba.web.config.tasks.ExecuteTaskAction.removeTask(ExecuteTaskAction.java:183) - Unregistered 1 task(s) (loc
INFO 2010.07.01 11:09:05 com.verba.web.config.tasks.ExecuteTaskAction.execute(ExecuteTaskAction.java:217) - Execute [restart] action for I
INFO 2010.07.01 11:09:05 com.verba.web.config.tasks.ExecuteTaskAction.removeTask(ExecuteTaskAction.java:183) - Unregistered 1 task(s) (loc
ERROR 2010.07.01 11:18:18 com.verba.web.call.getMedia.execute(getMedia.java:333) - 111af312-84f1-11df-b50f-000c2998a301
ERROR 2010.07.01 11:18:20 com.verba.web.call.getMedia.execute(getMedia.java:333) - 111af312-84f1-11df-b50f-000c2998a301
INFO 2010.07.01 11:50:22 com.verba.web.dbInfo.DbInfoDescriptorExtensions.getChilds(DbInfoDescriptorExtensions.java:40) - Creating DbInfoDe
ERROR 2010.07.01 11:58:37 com.verba.web.call.getMedia.execute(getMedia.java:333) - 111af312-84f1-11df-b50f-000c2998a301
INFO 2010.07.01 13:01:22 com.verba.web.register.sessionRegister.removeSession(sessionRegister.java:35) - Session was removed from SessionR
INFO 2010.07.01 13:09:05 com.verba.web.location.GetServerStatus.execute(GetServerStatus.java:40) - Executing status action for VERBA-DEMO
INFO 2010.07.01 14:09:24 com.verba.web.register.sessionRegister.removeSession(sessionRegister.java:35) - Session was removed from SessionR
WARN 2010.07.01 14:29:37 com.verba.web.VerbaServlet.doPost(VerbaServlet.java:437) - Action [class com.verba.web.location.LogViewAction] is
INFO 2010.07.01 14:29:50 com.verba.web.location.GetServerStatus.execute(GetServerStatus.java:40) - Executing status action for VERBA-DEMO
```

The following table describes the available features:

Icon	Feature	Description
↺	Toggle log tail follow	If this option is enabled, the system automatically refreshes the log panel with the latest service log file content and scrolls the panel to the end.
↩	Toggle line wrapping	If this option is enabled the log lines are wrapped to fit into the log window.
🔍	Toggle log filter	Enables log filtering using the expression entered into the input box.
🗑	Clear log buffer	Clears the log buffer on the screen.

Collecting and downloading the logs

The system has a built-in tool to collect log files from multiple servers at once. For more information, see Log and Configuration Collector.

Alternatively, the log files can be manually collected in the file systtem.

Debug log and command line output

Debug and verbose log levels

Troubleshooting often requires additional, more detailed information about a specific service. You can change the log level of a specific service to enable more detailed logging. For more information, refer to Log files.

> Only increase the log level temporarily when you are doing troubleshooting or you were asked by support. Leaving the log level on Debug/Verbose level can have an adverse effect on system performance which could lead to data loss in critical situations.

Debug command line output

Debug output shows messages about the operation of the internal activities and algorithms of the services. It could be especially useful when troubleshooting service startup issues, e.g. when a service cannot be started. In order to run a component in debug mode, first, you have to stop the desired service through the Web Application under **System / Servers / Service Control and Activation** or through Windows Service Control application (**Start Menu / Settings / Control Panel / Administrative Tools / Services**).

> If Verba System Monitor is enabled for a given service, make sure that you stop the Verba System Monitor service too, unless it will automatically restart the given service.

The following table lists the supported services and their command line debug options:

Verba service	Binary folder	Command line
Verba Passive Recorder Service	c:\Program Files\Verba\bin	verbaengine.exe -d
Verba Unified Call Recorder Service	c:\Program Files\Verba\bin	unifiedrec.exe -d
Verba Import Service	c:\Program Files\Verba\bin	cdrimport.exe -d
Verba Unified IM Recorder Service	c:\Program Files\Verba\bin	unifiedimrec.exe -d
Verba Dial-in Recorder Service	c:\Program Files\Verba\bin	activerecorder.exe -d
Verba Media Streamer and Content Server Service	c:\Program Files\Verba\bin	mediastreamer.exe -d

Verba Storage Management Service	c:\Program Files\Verba\bin	verbastorage.exe -d
Verba Media Utility Service	c:\Program Files\Verba\bin	waveform.exe -d
Verba System Monitor Service	c:\Program Files\Verba\bin	verbasysmon.exe -d
Verba Node Manager Agent	c:\Program Files\Verba\bin	verbaagent.exe -d

Capturing network traffic for troubleshooting

There are certain situations when a problem can only be resolved if the support team can take a closer look at the actual network traffic seen by the applications. This can help identify network issues and bottlenecks, and analyze network and application level protocols.

We recommend using the following network capture tools:

- Wireshark
- Tshark
- Verba Packet Capture

Installing Wireshark and Tshark on Verba servers

You can download and install Wireshark (and the Tshark command line tool with it) on the Verba servers. To learn more about Wireshark and download the installer, visit https://www.wireshark.org/.

> **Do not remove the Winpcap driver when installing Wireshark.** Otherwise, the system components relying on the Wincap drive will not work anymore

> Capturing on Recording Servers causes extra load on CPU and disk utilization and can interfere with the recording process which can lead to data loss under critical circumstances. The load of the packet capture on the Recording Servers should be always considered and if possible should only be used during non-busy hours.

Tshark

Tshark is a high performance packet capture application that is part of the Wireshark installation package. It is a command line tool for high performance continuous capturing. It is useful when network traffic is high and/or capturing with Wireshark becomes unstable, and when we need to leave tracing on for a longer period of time (many hours or days).Examples

Get help:

```
tshark -h
```

List interfaces:

```
tshark -D
```

Start capturing with capture file rotation:

```
tshark -i 3 -B 96 -b filesize:250000 -b files:100 -w c:\tmp\test.pcap -F pcap
```

Where:

- -i specifies the interface with the ID retrieved by tshark –D
- -B sets capture buffer size in Mbyte. Default is 2 Mbyte, if there is a large traffic, you should go up to 96 Mbyte

- -b specifies the capture rotation: filesize:xxx max size of a single capture file in Kbytes, files:xxx the number of files after which the oldest one is overwritten. Using file rotation set based on available disk space we can make sure there will be enough space left for the other applications when we leave tracing on for a longer time.
- -w output file
- -F output format (could be pcap or pcapng. We prefer pcap, that can be directly processed by the passive recorder)
- **-f can specify capture filter in BPF syntax, see below. Using an appropriate capture filter highly reduces the load on CPU and Disk**

BPF filter syntax

For the full syntax, see https://biot.com/capstats/bpf.html or https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.3/com.ibm.qradar.doc/c_forensics_bpf.html.

Important filter examples:

Filtering all (src/dst) IP traffic of given host:

```
host 10.110.77.200
```

Filtering inbound/outbound IP traffic of given host:

```
src host 10.110.77.200 / dst host 10.110.77.200
```

Filtering for specific subnet:

```
(src/dst) net 10.110.77.0/24
```

Filtering for specific TCP or UDP port:

```
tcp/udp src/dst 443
```

Logical combination: or/and and grouping with () supported

Filtering for SIP (non secure, 5060 default port):

```
traffic of 10.110.77.200 CUCM: (udp port 5060 or tcp port 5060) and host 10.110.77.200
```

Filtering for proxy-filter communication:

```
tcp port 10201
```

Filtering for proxy-recorder communication:

```
tcp port 11112
```

Filtering for recording director – media recorder communication:

```
tcp port 10500
```

Wireshark

Wireshark is a GUI based packet trace analyzer. It can parse the real-time traffic capture or read a network packet capture file. The application can identify encapsulations and interpret and visualizes protocol data at all layers. It uses a different syntax than the BPF capture filter (used by Tshark). Filtering can only be applied to displaying the packets (and not capture filtering). For more information on display filters, see https://wiki.wireshark.org/DisplayFilters.

Display filter examples

Searching for string "xxxx" in the whole packet:

```
frame contains "xxxx"
```

Filtering for SIP or Skinny or H.323 call control packets:

```
sip or sccp or h323
```

Filtering for HTTP messages:

```
http
```

Filtering for IP traffic of 10.110.77.200:

```
ip.dst=="10.110.77.200" or ip.src=="10.110.77.200"
```

Filtering for TCP traffic on 5060 port (works with udp as well):

```
tcp.dstport==5060 or tcp.srcport==5060
```

Verba packet capture

The system comes with a built-in packet capture tool called **Verba Packet Capture**. This tool collects and stores network traffic without analyzing it or interfering with the recording progress, similar to Tshark. Verba Packet Capture creates **standard PCAP** files that can be opened by WireShark.

The tool is especially useful when troubleshooting proxy based recording issues because the tool can take into account the recorder settings and connect to the same proxies as a redundant/2N recorder pair of the recorder. That way it receives exactly the same traffic as the recorder service. The tool should be run on the servers where the Passive Recorder service runs.

Gathering support information

When contacting support, it is important to collect all relevant information about the issue you are experiencing. The information can help the support engineer to determine the root cause of your issue faster and provide you guidance on correcting the issue.

The support engineer would need as much of the following information as possible:

Data	Description
Customer Name	The name of the customer. This helps to identify any known issues or past information about the deployment.
Site location	Location information about the deployment. This can help to identify the deployment if the customer has multiple installations.
Issue	A clear and concise description of the issue.
Reproduction	A detailed description of the steps to reproduce the issue.
Desired outcome	A clear and concise description of the desired outcome.
Integrations	List of the associated integrations (Phone System / Trading platform) to make the scenarios and the architecture more understandable. The version numbers of the integrations can be crucial for bug detection.
System software version	The version of the system. We usually need service version numbers up to build numbers (e.g. 9.7.5.5275), not just the main version of the system such as 9.6.
Recent changes	The description of any recent environmental changes: • firewall configuration changes • network configuration changes • server configuration changes • integration related configuration changes • Windows operating system changes on Verba servers (e.g. patched applied)
Troubleshooting	Troubleshooting actions and log analysis results. Dates/times of relevant alarms, and tests to replicate the issue etc.
Logs and Configuration	Collection of relevant log files and current server configuration. For more information on collecting logs and configuration data, see Log files and Log and Configuration Collector. Server information for the attached logs: list the related Verba servers from the architecture, to make the logs more understandable (server hostname/IP and server role).
Other relevant information	Anything you believe is important to understand the issue better and help find the resolution.

Manage MP4 transcoding profiles

There can be a case, where the provided MPEG-4 encoder profiles are not sufficient. There are ways to add or edit profiles depending on where these are used.

Profiles for server configuration - Store Management / Video Transcoding / Video Encoder Profile

The list of selectable profiles is in *<verba installation path>\resources\nodemanager\dropdowns.xml*

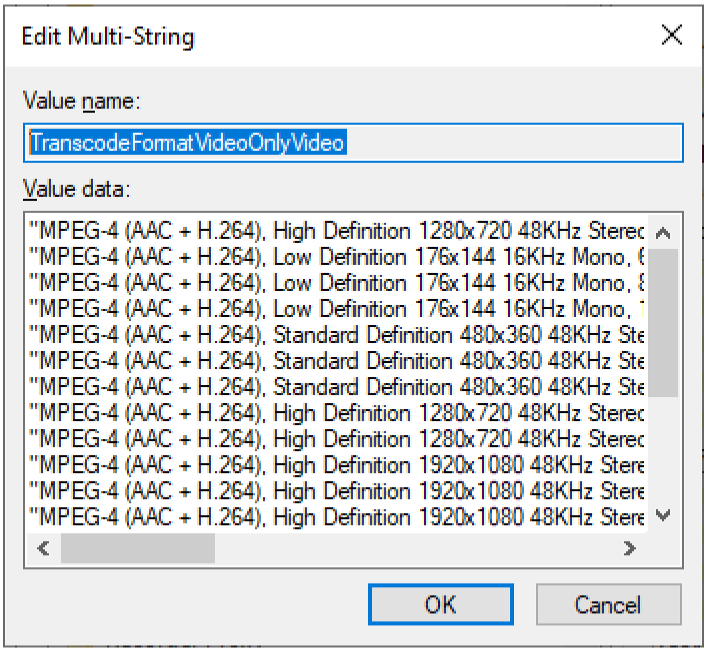
```
<dropdowns>
    <category name="transcodingvideo">
        <dropdown name="Profile">
            <item displayname="MPEG-4 (AAC + H.264), Low Definition 176x144 16KHz Mono, 60 kbit/s

            ...
```

An item can be added here using similar format, removed or rearranged if needed. The *Verba Web Application Service* needs to be restarted after editing the file.

Profiles for the Web-base media player

The profiles are stored in the Windows Registry under the following path:

> Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Verba\Web\TranscodeFormatVideoOnlyVideo



Value name:

TranscodeFormatVideoOnlyVideo

Value data:

```
"MPEG-4 (AAC + H.264), High Definition 1280x720 48KHz Stereo
"MPEG-4 (AAC + H.264), Low Definition 176x144 16KHz Mono, 6
"MPEG-4 (AAC + H.264), Low Definition 176x144 16KHz Mono, 8
"MPEG-4 (AAC + H.264), Low Definition 176x144 16KHz Mono, 1
"MPEG-4 (AAC + H.264), Standard Definition 480x360 48KHz Ste
"MPEG-4 (AAC + H.264), Standard Definition 480x360 48KHz Ste
"MPEG-4 (AAC + H.264), Standard Definition 480x360 48KHz Ste
"MPEG-4 (AAC + H.264), High Definition 1280x720 48KHz Stereo
"MPEG-4 (AAC + H.264), High Definition 1280x720 48KHz Stereo
"MPEG-4 (AAC + H.264), High Definition 1920x1080 48KHz Stere
"MPEG-4 (AAC + H.264), High Definition 1920x1080 48KHz Stere
"MPEG-4 (AAC + H.264), High Definition 1920x1080 48KHz Stere
```

An example:

> "MPEG-4 (AAC + H.264), High Definition 1920x1080 48KHz Stereo, 3128 kbit/sec" - mp4;videoWidth=1920;videoHeight=1080; videoQuality=3;videoBitrate=3000000;audioSampleRate=48000;audioChannels=2;audioBitrate=128000

An item can be added here using similar format, removed or rearranged if needed.

System backup

Having an extensive backup procedure in place for a recording solution is of utmost importance. In case of a hardware failure or other serious disruptive events, this will allow for recovering all recorded conversations and configuration into a newly reinstalled system.

> ⓘ Without extensive backup procedures, recordings are at risk. **It is the responsibility of the customer to employ proper backup tools and procedures.**

What data needs to be backed up?

The backup is complete and the system could be **completely restored** from the backup including all recordings and configuration if it contains the following two components:

- **media files** - media path, archiving path, storage targets, all disk folders where recorded conversation media is stored
- **database backup file** - a SQL database backup file created by the SQL server during a backup job
- **customized files** - in rare cases, the deployment might contain customized configuration files (e.g. recording announcement prompts, MoH files, etc.) on the servers or special build of executables, these files should be backed up as well

No other component needs to be backed up.

When to back up data?

Depending on the business requirements, daily, weekly, or other regular backups need to be done. Most users choose daily backups.

We recommend to run the file backup:

- during the lowest traffic period of the operation (in most cases between 1:00-3:00 AM during the night)
- after the database backup is completed and the local database backup file is available for file backup (in case of a local SQL Server installation)

> ✓ If the recording system is recording during the backup, make sure that the backup is executed in a time period, when recorded traffic is lower and when other servers are not using the backup system. This approach significantly decreases the time demand of the backup process.

How to find media files?

All the media files are stored in the following locations:

- **Media Folder** - with administrative rights, under **Administration menu / Verba Servers / (select your Media Repository) / Change Configuration Settings / Directories / Media Folder**
- **Storage Targets** - with administrative rights, under **Administration / Storage Targets**

All these folders and solutions must be included in the file backup for complete coverage of all the recordings.

How to backup the database?

The goal of the database backup is to create a .bak backup file that can be used with the standard file backup methods.

For more information refer to these topics:

- Creating a one-off full database backup
- Scheduling database backups (not available on Express Edition)

ⓘ **Do not make a file backup of the SQL Server database and index files**, since those are not suitable to restore operations. Run a backup in the SQL Server to create a .bak file and include that file in the backup.

How to restore the system?

The Verba system can be completely restored if a **backup for the media files** and a **database backup is available**. No other information is required.

Follow the steps below to restore the database, conversation media, and installation of the Verba Media Repository

Step 1 - Restore the database into a Microsoft SQL Server.

Step 2 - Copy the media files to a folder on the Media Repository server or NAS.

Step 3 - Install the Verba Media Repository (during the installation point to the restored SQL Server and the restored Media folder).

Step 4 - In the Verba menu, navigate to **Administration / Verba Servers**. Select **Media Repository** and click on **Change Configuration**. Follow the instructions that appear.

Follow the steps below to restore a Verba Component (Recording, Proxy, Announcement, Speech server, Lync /SfB Filter, Media Collector)

Step 1 - Install the Verba Component.

Step 2 - In the Verba menu, navigate to **Administration / Verba Servers.** Select the Verba component that needs to be restored and click on **Change Configuration**. Follow the instructions that appear.

SQL Server administration and maintenance

For the smooth and reliable operation of the Verba system, it is imperative to have a properly sized and well managed database system.

Verba system administrators have the following common tasks with the SQL Server:

- Configuring backup and database maintenance plans
- Restoring the database after a (hardware) failure
- Helping support team with direct database access

There are two types of tools, which can be used to maintain and administer SQL Server:

- Command line tools
- Graphical management tools (recommended)

This chapter contains the following information:

- Database backup and restore
- Database maintenance
- Database table partitioning
- Database purging
- SQL Server GUI tools
- SQL Server command line tools

Database backup and restore

Overview

The main purpose of backing up the Verba database is to provide increased reliability and system recovery (fault tolerance) of the system. In case of a media or database failure, data can be restored from earlier database backups.

It is important to note, that the Verba media files (recordings) are stored in the file system, and backing up the database does not provide fault tolerance for the media files. Verba administrators have to choose another method to backup media files regularly to provide the reliability of the system. The Verba media file backup procedures have to be synchronized with the Verba database backup in order to provide the ability to restore a consistent Verba system in case of a failure.

Microsoft SQL Server provides high-performance backup and restore capabilities. The SQL Server backup and restore component provides an essential safeguard for protecting critical data stored in SQL Server databases. Implementing a well-planned backup and restore strategy helps protect databases against data loss because of damage caused by a variety of failures. Testing your strategy by restoring a set of backups and recovering your database prepares you to respond effectively to a disaster.

The following topics provide a brief explanation of the most important backup topics.

For detailed information about SQL Server backup and restore features, refer to https://docs.microsoft.com/en-us/sql/relational-databases/backup-restore/back-up-and-restore-of-sql-server-databases.

This page has the following content:

For further information:

- Creating a one-off full database backup
- Scheduling database backups
- Restoring a full database backup
- Changing the database recovery model

Selecting a recovery model

SQL Server provides three recovery models to:

- Simplify recovery planning.
- Simplify backup and recovery procedures.
- Clarify tradeoffs between system operational requirements.

Each of these models addresses different needs for performance, disk and tape space, and protection against data loss. For example, when you choose a recovery model, you must consider the tradeoffs between the following business requirements:

- Performance of large-scale operation (for example, index creation or bulk loads).
- Data loss exposure (for example, the loss of committed transactions).
- Transaction log space consumption.
- The simplicity of backup and recovery procedures.

Depending on what operations you are performing, more than one model may be appropriate. After you have chosen a recovery model or models, plan the required backup and recovery procedures.

This table provides an overview of the benefits and implications of the three recovery models.

Recovery models comparison table

Recovery model	Benefits	Work loss exposure	Recover to point in time?
Simple	Permits high-performance bulk copy operations. Reclaims log space to keep space requirements small.	Changes since the most recent database or differential backup must be redone.	Can recover to the end of any backup. Then changes must be redone.
Full	No work is lost due to a lost or damaged data file. Can recover to an arbitrary point in time (for example, prior to application or user error).	Normally none. If the log is damaged, changes since the most recent log backup must be redone.	Can recover to any point in time.
Bulk-Logged	Permits high-performance bulk copy operations. Minimal log space is used by bulk operations.	If the log is damaged, or bulk operations occurred since the most recent log backup, changes since that last backup must be redone. Otherwise, no work is lost.	Can recover to the end of any backup. Then changes must be redone.

Simple Recovery

Simple Recovery requires the least administration. In the Simple Recovery model, data is recoverable only to the most recent full database or differential backup. Transaction log backups are not used and minimal transaction log space is used. After the log space is no longer needed for recovery from server failure, it is reused.

The Simple Recovery model is easier to manage than the Full or Bulk-Logged models, but at the expense of higher data loss exposure if a data file is damaged.

Simple Recovery is not an appropriate choice for production systems where the loss of recent changes is unacceptable.

When using Simple Recovery, the backup interval should be long enough to keep the backup overhead from affecting production work, yet short enough to prevent the loss of significant amount of data.

The backup strategy for simple recovery consists of:

- Database backups.
- Differential backups (optional).

To recover in the event of media failure:

- Restore the most recent full database backup.
- If differential backups exist, restore the most recent one. Changes since the last database or differential backup are lost.

Full and Bulk-Logged Recovery

Full Recovery and Bulk-Logged Recovery models provide the greatest protection for data. These models rely on the transaction log to provide full recoverability and to prevent work loss in the broadest range of failure scenarios. The Full Recovery model provides the most flexibility for recovering databases to an earlier point in time.

The Bulk-Logged model provides higher performance and lower log space consumption for certain large-scale operations (for example, create index or bulk copy). It does this at the expense of some flexibility of point-in-time recovery.

The backup strategy for full recovery consists of:

- Database backups.
- Differential backups (optional).
- Transaction log backups.

Full and bulk-logged recovery are similar and many users of the Full Recovery model will use the Bulk-Logged model on occasion.

You can restore a database to the state it was in at the point of failure if the current transaction log file for the database is available and undamaged.

To restore the database to the point of failure:

- Back up the currently active transaction log.
- Restore the most recent database backup without recovering the database.
- If differential backups exist, restore the most recent one.
- Restore each transaction log backup created since the database or differential backup in the same sequence in which they were created without recovering the database.
- Apply the most recent log backup (created in), and recover the database.

The backup strategy for bulk-logged recovery consists of:

- Database backups.
- Differential backups (optional).
- Log backups.

Backing up a log that contains bulk-logged operations requires access to all data files in the database. If the data files are not accessible, the final transaction log cannot be backed up and all committed operations in that log will be lost.

To recover in the event of media failure:

- Back up the currently active transaction log.
- Restore the most recent full database backup.
- If differential backups exist, restore the most recent one.
- Apply in sequence all transaction log backups created since the most recent differential or full database backup.
- Manually redo all changes since the most recent log backup

Database backups

Full database backups

A database backup creates a duplicate of the data that is in the database when the backup completes. This is a single operation, usually scheduled at regular intervals. Database backups are self-contained.

You can re-create the entire database from a database backup in one step by restoring the database. The restore process overwrites the existing database or creates the database if it does not exist. The restored database will match the state of the database at the time the backup completed, minus any uncommitted transactions. Uncommitted transactions are rolled back when the database is recovered.

A database backup uses more storage space per backup than transaction log and differential database backups. Consequently, database backups need more time to complete the backup operation and so are typically created less frequently than a differential database or transaction log backups.

Differential database backups

A differential database backup records only the data that has changed since the last database backup. You can make more frequent backups because differential database backups are smaller and faster than database backups. Making frequent backups decreases your risk of losing data.

If you have created any file backups since the last full database backup, those files will be scanned by SQL Server at the beginning of a differential database backup. This may cause some degradation of performance in the differential database backup.

You use differential database backups to restore the database to the point at which the differential database backup was completed. To recover to the exact point of failure, you must use transaction log backups.

Consider using differential database backups when:

- Only a relatively small portion of the data in the database has changed since the last database backup. Differential database backups are particularly effective if the same data is modified many times.
- You are using the Simple Recovery model and want more frequent backups, but don't want to do frequent full database backups.
- You are using the Full or Bulk-Logged Recovery model and want to minimize the time it takes to roll forward transaction log backups when restoring a database.

A recommended process for implementing differential database backups is:

- Create regular database backups.
- Create a differential database backup periodically between database backups, such as every four hours or more for highly active systems.
- If using Full or Bulk-Logged Recovery, create transaction log backups more frequently than differential database backups, such as every 30 minutes.

The sequence for restoring differential database backups is:

- Restore the most recent database backup.
- Restore the last differential database backup.
- Apply all transaction log backups created after the last differential database backup was created if you use Full or Bulk-Logged Recovery.

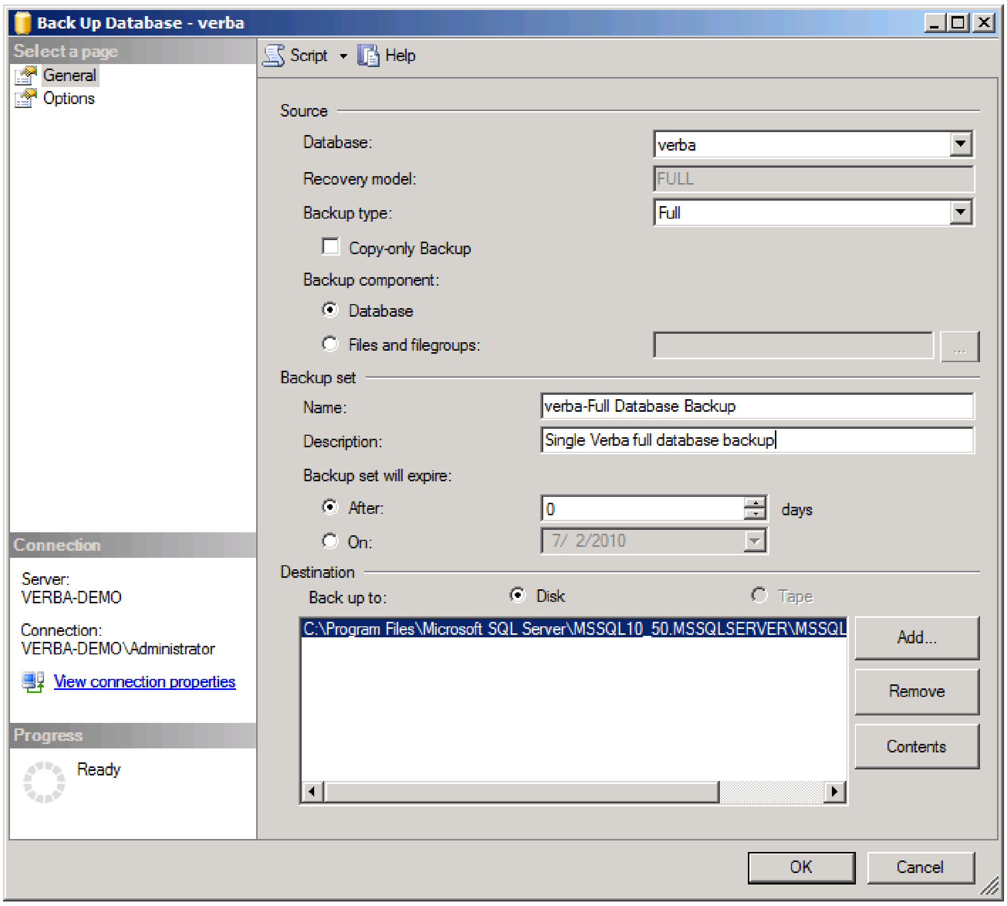
Creating a one-off full database backup

This section explains how to create a full Verba database backup.

If you would like to schedule a recurring full database backup, please see the appropriate sections below. Alternatively, you can use the Maintenance Plan Wizard to create database backups.

For further information about creating a full database backup using SQL Server Management Studio, refer to https://docs.microsoft.com/en-us/sql/relational-databases/backup-restore/create-a-full-database-backup-sql-server

> ⓘ When you specify a backup task by using SQL Server Management Studio, you can generate the corresponding Transact-SQL BACKUP script by clicking the Script button and selecting a script destination.



Back Up Database - verba

Select a page: General, Options

Source

Database: verba

Recovery model: FULL

Backup type: Full

□ Copy-only Backup

Backup component:
● Database
○ Files and filegroups:

Backup set

Name: verba-Full Database Backup

Description: Single Verba full database backup

Backup set will expire:
● After: 0 days
○ On: 7/ 2/2010

Destination

Back up to: ● Disk ○ Tape

C:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL

Connection

Server:
VERBA-DEMO

Connection:
VERBA-DEMO\Administrator

View connection properties

Progress

Ready

Step 1 - After connecting to the appropriate instance of the Microsoft SQL Server Database Engine on the Verba Media Repository component, in Object Explorer, click the server name to expand the server tree.

Step 2 - Expand Databases, and select the **Verba** database.

Step 3 - Right-click the Verba database, point to **Tasks**, and then click **Back Up**. The **Back Up Database** dialog box appears.

Step 4 - In the **Database** list box, verify the database name.

Step 5 - You can perform a database backup for any recovery model (FULL, BULK_LOGGED, or SIMPLE).

Step 6 - In the **Backup type** list box, select **Full**.

Step 7 - Note that after creating a full database backup.

Step 8 - For **Backup component**, click **Database**.

Step 9 - Optionally, in the **Description** text box, enter a description of the backup set.

Step 10 - Either accept the default backup set name suggested in the **Name** text box, or enter a different name for the backup set.

Step 11 - Specify when the backup set will expire and can be overwritten without explicitly skipping verification of the expiration date:

- To have the backup set expire after a specific number of days, click **After** (the default option), and enter the number of days after set creation that the set will expire. This value can be from 0 to 99999 days; a value of 0 days means that the backup set will never expire.
- The default value is set in the **Default backup media retention (in days)** option of the **Server Properties** dialog box (Database Settings Page). To access this, right-click the server name in Object Explorer and select properties; then select the **Database Settings** page.
- To have the backup set expire on a specific date, click **On**, and enter the date on which the set will expire.

Step 12- Choose the type of backup destination by clicking **Disk** or **Tape**. To select the paths of up to 64 disk or tape drives containing a single media set, click **Add**. The selected paths are displayed in the **Backup to** list box. To remove a backup destination, select it and click **Remove**. To view the contents of a backup destination, select it and click **Contents**.

Step 13 - To view or select the advanced options, click **Options** in the **Select a page** pane.

Step 14 - Select an Overwrite Media option, by clicking one of the following:

- **Back up to the existing media set**
  For this option, click either **Append to the existing backup set** or **Overwrite all existing backup sets**.
  Optionally, select **Check media set name and backup set** expiration to cause the backup operation to verify the date and time at which the media set and backup set expire.
  Optionally, enter a name in the **Media set name** text box. If no name is specified, a media set with a blank name is created. If you specify a media set name, the media (tape or disk) is checked to see whether the actual name matches the name you enter here.

- **Back up to a new media set, and erase all existing backup sets**
  For this option, enter a name in the New media set name text box, and, optionally, describe the media set in the New media set description text box.

Step 15 - In the **Reliability** section, optionally check:

- **Verify backup when finished**.

- **Perform checksum before writing to media**, and, optionally, **Continue on checksum error**.

Step 16 - If you are backing up to a tape drive (as specified in the **Destination** section of the **General** page), the **Unload the tape after backup** option is active. Clicking this option activates the **Rewind the tape before unloading** option.

Scheduling database backups

You can backup your data at regular hourly, daily and weekly intervals, using three different backup methods - full, differential and incremental (transaction log) backups. With a backup strategy that enables these three backup types, you can restore databases to any hour of any specific day of the week. This suggested backup strategy is based on rigorous lab tests. You may choose any backup strategy which is acceptable to your organization:

- Do not create overlapping schedules for backups since only one backup at a time can be executed.
- Start with a full backup of the database.
- Create a full backup for weekend nights.
- Create a differential backup for every night of a working day.
- Create a transaction log backup for every hour (exclude hours when full and differential backups are running).
- Backup to a remote machine or use a local drive and copy the backup files to a remote server.
- Save four full database backup generations. That is, save four weeks of full database backups.
- If you save the last two full, six differential, and 24 incremental database backups so that they are stored on the network, you can restore any database to any hour of any day during the last week, or to the last full backup for the previous week.

Creating a backup job using the maintenance plan wizard

Before you begin:

- Decide on your database backup strategies. For more information, see Database backup and restore.
- Decide on backup job names that follow System Monitor naming conventions.
- Ensure the user running the SQL Server Management Studio has sysadmin privileges.

To configure a recurring backup, follow the steps below:

Step 1 - Open the **SQL Server Management Studio** (SSMS), and click Object Explorer.

Step 2 - Connect to the relevant server.

Step 4 - Right-click the Management folder and select the **Maintenance Plan Wizard**.

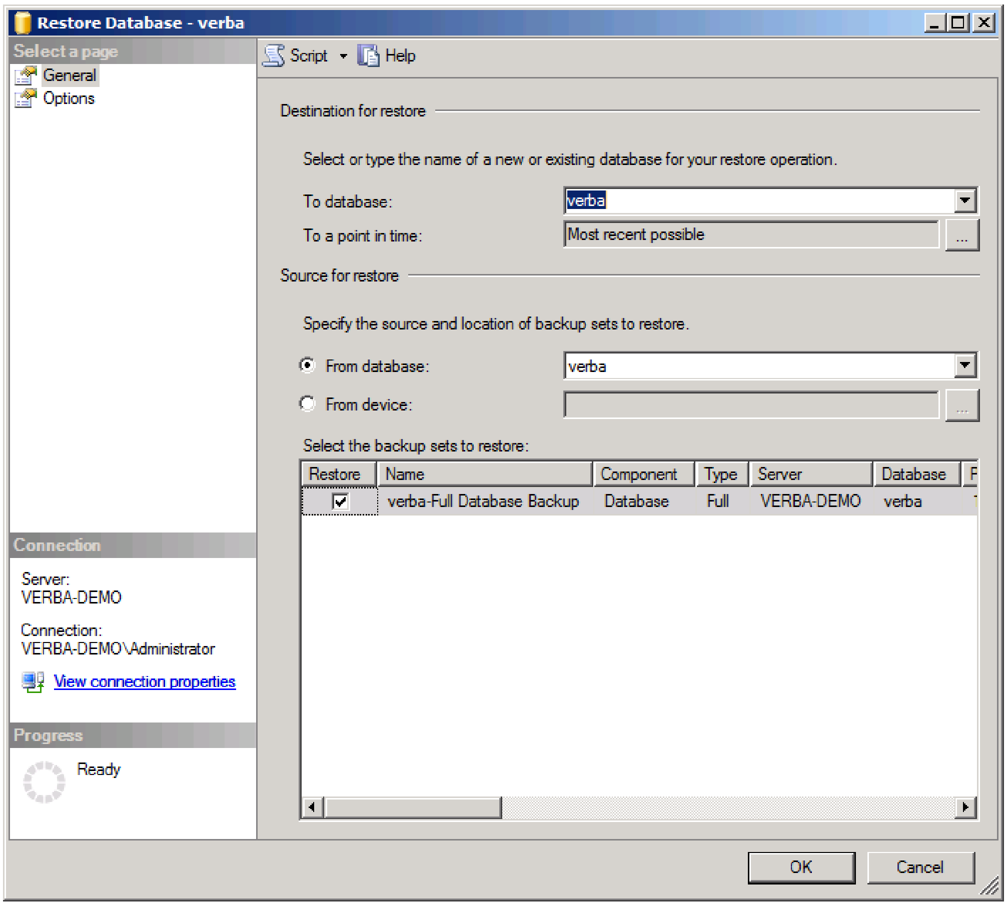
Step 5 - Select the **Backup** task. Follow the steps of the wizard to create a maintenance plan, according to your database backup strategies.

For more information on using the wizard, see https://docs.microsoft.com/en-us/sql/relational-databases/maintenance-plans/use-the-maintenance-plan-wizard

Restoring a full database backup

This section explains how to restore a full Verba database backup.

For further information about restoring a full database backup using SQL Server Management Studio, refer to https://docs.microsoft.com/en-us/sql/relational-databases/backup-restore/restore-a-database-backup-using-ssm



Destination for restore

Select or type the name of a new or existing database for your restore operation.

To database: verba

To a point in time: Most recent possible

Source for restore

Specify the source and location of backup sets to restore.

● From database: verba

○ From device:

Select the backup sets to restore:

Restore	Name	Component	Type	Server	Database	F
☑	verba-Full Database Backup	Database	Full	VERBA-DEMO	verba	

Server:
VERBA-DEMO

Connection:
VERBA-DEMO\Administrator

Ready

Step 1 - After you connect to the appropriate instance of the Microsoft SQL Server Database Engine, in Object Explorer, click the server name to expand the server tree.

Step 2 - Expand Databases. Select **verba** database.

Step 3 - Right-click the database, point to **Tasks**, and then click **Restore**.

Step 4 - Click **Database**, which opens the **Restore Database** dialog box.

Step 5 - On the **General** page, the name of the restoring database appears in the **To database** list box.

Step 6 - In the **To a point in time** text box, either retain the default (**Most recent possible**) or select a specific date and time by clicking the browse button, which opens the **Point in Time Restore** dialog box.

Step 7 - To specify the source and location of the backup sets to restore, click one of the following options:

- **From database**
  Enter a database name in the list box.

- **From device**

Click the browse button, which opens the **Specify Backup** dialog box. In the **Backup media** list box, select one of the listed device types. To select one or more devices for the **Backup location** list box, click **Add**.

After you add the devices you want to the **Backup location** list box, click **OK** to return to the **General** page.

Step 8 - In the **Select the backup sets to restore** grid, select the backups to restore. This grid displays the backups available for the specified location. By default, a recovery plan is suggested. To override the suggested recovery plan, you can change the selections in the grid. Any backups that depend on a deselected backup are deselected automatically.

Step 9 - To view or select the advanced options, click **Options** in the **Select a page** pane.

Step 10 - In the **Restore options** panel, you can choose the following option: **Overwrite the existing database**

Changing the database recovery model

If you would like to set transactional log backups, you have to set the Verba database recovery model to full.

To change the recovery model to full:

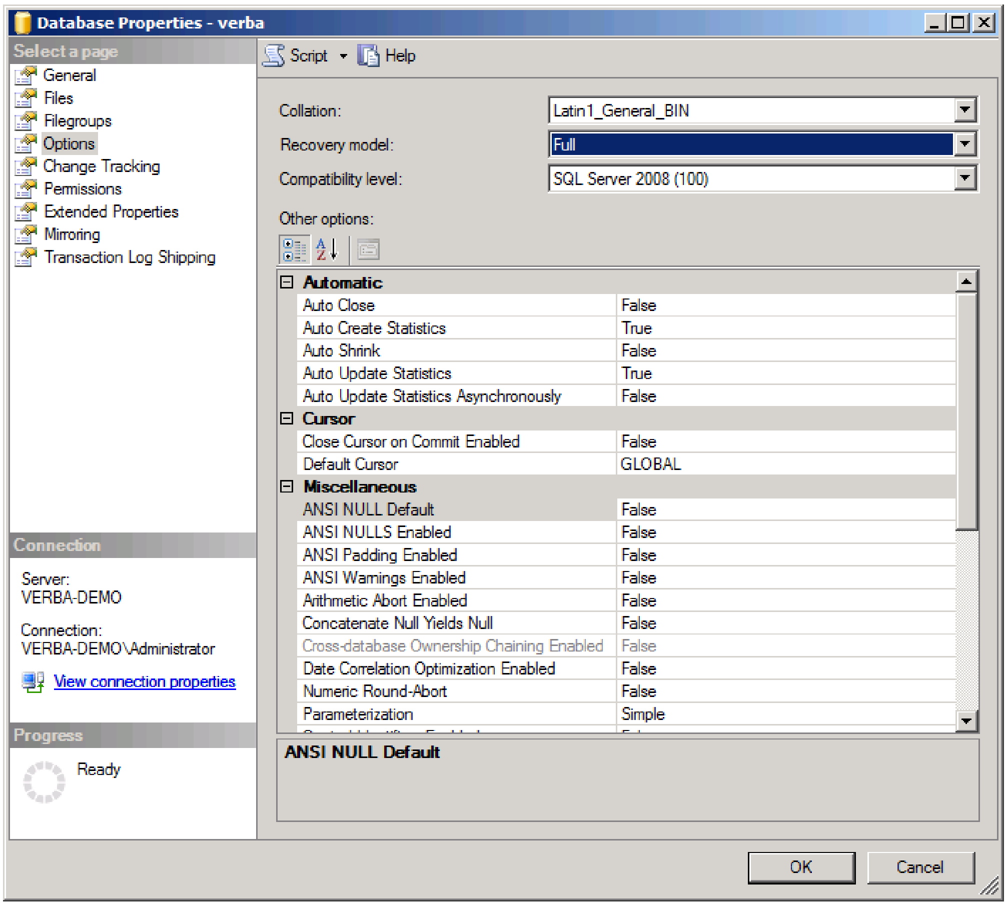
Step 1 - Start SQL Server Management Studio or SQL Server Management Studio Express.

Step 2 - After you connect to the appropriate instance of the Microsoft SQL Server Database Engine, in Object Explorer, click the server name to expand the server tree.

Step 3 - Expand **Databases**. Select **Verba** database.

Step 4 - Right-click the database, and then select **Properties**.

Step 5 - On the left pane select the **Options** page and set the **Recovery model** to **Full**.



Collation: Latin1_General_BIN

Recovery model: Full

Compatibility level: SQL Server 2008 (100)

Other options:

Automatic	
Auto Close	False
Auto Create Statistics	True
Auto Shrink	False
Auto Update Statistics	True
Auto Update Statistics Asynchronously	False
Cursor	
Close Cursor on Commit Enabled	False
Default Cursor	GLOBAL
Miscellaneous	
ANSI NULL Default	False
ANSI NULLS Enabled	False
ANSI Padding Enabled	False
ANSI Warnings Enabled	False
Arithmetic Abort Enabled	False
Concatenate Null Yields Null	False
Cross-database Ownership Chaining Enabled	False
Date Correlation Optimization Enabled	False
Numeric Round-Abort	False
Parameterization	Simple

ANSI NULL Default

Server:
VERBA-DEMO

Connection:
VERBA-DEMO\Administrator

Ready

Step 6 - Click **OK**.

Database maintenance

The system runs database maintenance jobs automatically on a daily basis and moves records every 15 minutes from the small temporary tables to the final tables. The maintenance jobs help to optimize large-scale deployments by running bulk operations during off-hours and periodically reorganizing indexes on the database tables. The database maintenance runs as standard SQL Server jobs on SQL Server Standard and Enterprise Editions and is executed by the Verba Web Application service in the case of SQL Server Express Edition (where jobs are not supported). The SQL Server jobs are created during install time by the installer running specific SQL scripts. To run these scripts, the installer requires specific permissions on the SQL Server. For more information see SQL Server requirements.

The built-in maintenance jobs provide the following features:

Actions	Description	Schedule
Bulk delete records	The action deletes records in a bulk operation where the retention expired or a matching deletion policy is configured. The data management policy which is executing the deletion only marks the records in the database for deletion and the bulk delete job deletes the records ultimately from the database tables.	Daily
Move data from temporary tables to the final tables	The action moves data from temporary tables which store data for 15 minutes only to the final tables where the data resides for the long term. The move job runs on the following tables: • section1 -> section2 • section_meta1 -> section_meta2 • marker1 -> marker2 • section_participant1 -> section_participant2 • section_cdr_media1 -> section_cdr_media2 • section_file1 -> section_file2 • section_centera1 -> section_centera2 • storage_executed_action1 -> storage_executed_action2 • call_export_log1 -> call_export_log2 • section_message1 -> section_message2	Every 15 minutes
Rebuild indexes	The action rebuilds indexes where the fragmentation is greater than 30% on all tables	Daily
Reorganize indexes	The action reorganizes indexes where the fragmentation is greater than 5% on all tables	Daily
Extend partitions	The action creates new partitions for the next 5 months and merges partitions with a small amount of data for the following tables: • section2 • section_archived • section_message2 • section_meta2	Daily

Reviewing and monitoring job execution

The system automatically sends notification alerts after job completion and error alerts when a job fails.

To review and monitor the execution, the following database tables can be checked:

- maintenance_log: each maintenance job run has a record in this table
- maintenance_log_section: contains a record for each action for the related job
- maintenance_log_section_detail: detailed information for each executed action for the related job

The following SQL query retrieves the most recent 1000 log entries from the tables:

```
SELECT TOP 1000 *
FROM maintenance_log l
INNER JOIN maintenance_log_section s ON s.maintenance_log_id = l.id
INNER JOIN maintenance_log_section_detail d ON d.maintenance_log_section_id = s.id
ORDER BY l.id DESC, s.id DESC, d.id DESC;
```

Always On Availability Groups

The Verba Maintenance SQL Agent Jobs are automatically created in the Primary Replica during the installation. The jobs must be created on the Secondary Replicas manually with the provided update-programs-maintenance-job.sql script. This script must be executed in the Secondary Replicas after an upgrade of the system too because new jobs may be added to the product.

The Jobs will be started on the Secondary Replicas too based on the schedule but will do nothing because the job checks the state of the replica and will immediately stop the execution on the Secondary Replicas. This way the jobs will be running on the new Primary Replica after a failover.

Changing the job schedule

The maintenance job runs at 22:00 by default (SQL Server local time in case of SQL Server jobs or Verba Media Repository / Application Server local time in case of SQL Server Express). The weekly actions run on Saturday by default.

To change the schedule follow the steps below:

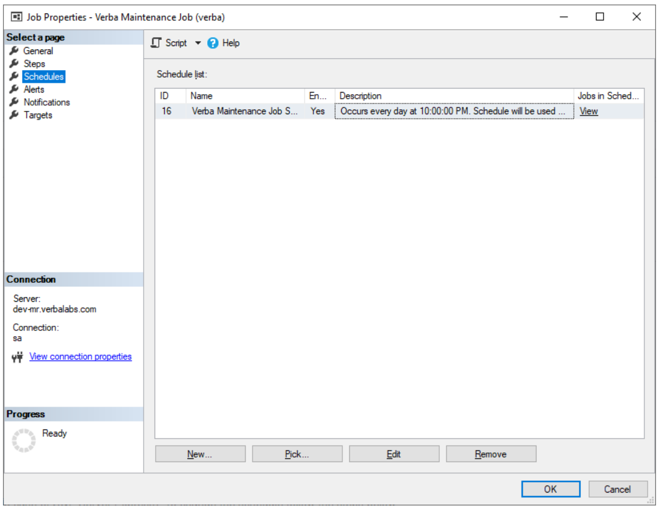
Changing the schedule for SQL Server jobs

Step 1 - Start **SQL Server Management Studio** and connect to the Verba database

Step 2 - Select **SQL Server Agent** from the dropdown and expand Jobs

Step 3 - Right-click on the **Verba Maintenance job (database_name)** and select **Properties**

Step 4 - Select **Schedules** on the top left and click on **Edit**



Job Properties - Verba Maintenance Job (verba)

Schedule list:

ID	Name	En...	Description	Jobs in Sched...
16	Verba Maintenance Job S...	Yes	Occurs every day at 10:00:00 PM. Schedule will be used ...	View

Connection

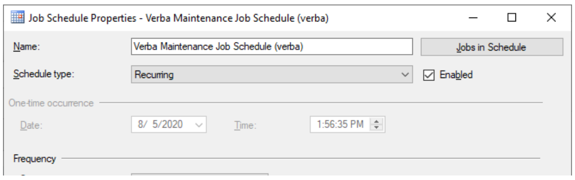
Server:
dev-mr.verbalabs.com

Connection:
sa

Progress

Ready

Step 5 - Change the Daily frequency / Occurs once at parameter to the desired setting



Job Schedule Properties - Verba Maintenance Job Schedule (verba)

Name: Verba Maintenance Job Schedule (verba)

Schedule type: Recurring

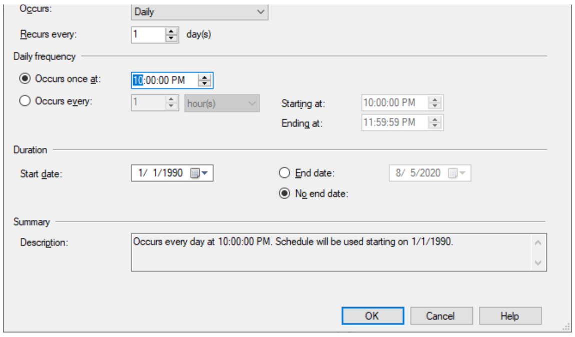
☑ Enabled

One-time occurrence

Date: 8/ 5/2020

Time: 1:56:35 PM

Frequency


Occurs: Daily

Recurs every: 1 day(s)

Daily frequency

● Occurs once at: 10:00:00 PM

○ Occurs every: 1 hour(s) Starting at: 10:00:00 PM Ending at: 11:59:59 PM

Duration

Start date: 1/ 1/1990

○ End date: 8/ 5/2020

● No end date:

Summary

Description: Occurs every day at 10:00:00 PM. Schedule will be used starting on 1/1/1990.

Step 6 - Click **Ok** and **Ok**. The SQL Server saves the changes and the job will run based on the new schedule.

Changing the schedule for jobs executed by the Web Application

Step 1 - Login to the Verba Web Application with system administrator privileges

Step 2 - Navigate to **System / Server** and select the Verba Media Repository / Application Server or navigate to **System / Configuration Profiles** and select the profile for the Media Repository servers.

Step 3 - Click on the **Change Configuration Settings** tab and expand to **Web Application / Miscellaneous**

Step 4 - Under **Daily Job Start At (Server Time Zone)** select the appropriate value from the dropdown list.

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.

Database table partitioning

Overview

SQL Server supports table and index partitioning which has to be enabled for the Verba database in case of storing large amounts of data. The data of partitioned tables and indexes is divided into units that can be spread across more than one filegroup in a database. The data is partitioned horizontally so that groups of rows are mapped into individual partitions. The table or index is treated as a single logical entity when queries or updates are performed on the data. Partitioning large tables or indexes can have the following manageability and performance benefits:

- The search runs faster.
- Data management policies run faster.
- Maintenance jobs run faster.

Prerequisites

Partitioning is only available in specific versions and editions of SQL Server:

- Standard Edition: version 2016 SP1 or later
- Enterprise Edition: all version

When to enable partitioning

We recommend enabling database partitioning when more than 100 million conversations are expected to be stored in the database. It is best to enable partitioning during installation. Partitioning can also be enabled later, retrospectively on existing data. However, this requires careful considerations as partitioning can take a lot of time depending on the size of the database,

Enabling database table partitioning

The following script will install partitioning, and it should be executed in the Verba database: c:\Program Files\Verba\resources\db\manual-partitioning.sql

Use the SQL Server Management Studio to execute the script.

The first partition border will be the first day of the next month by default, so it will not take a long time to execute even on a large database.

```
DECLARE
@first_partition VARCHAR(100) = CONVERT(VARCHAR, DATEADD(m, 1, DATEADD(m, DATEDIFF(m, 0, GETUTCDA
@second_partition VARCHAR(100) = CONVERT(VARCHAR, DATEADD(m, 2, DATEADD(m, DATEDIFF(m, 0, GETUTCD
```

In the following example, the first partition border can be changed manually.

```
DECLARE
@first_partition VARCHAR(100) = '20190101',
@second_partition VARCHAR(100) = '20190201';
```

> Only monthly partitions are supported, so please set up the @first_partition and @second_partition variables to point to the first day of two consecutive months.

Enabling database table partitioning for existing data

If existing data should be split to partitions too, then it is recommended to do it out of business hours, considering it can take several hours to finish. It is recommended to split one month as the first step and measure how long does it take to execute.

On average, a million record in a month takes ~30 minutes to partition.

The following script can be used to split the existing data in the past: c:\Program Files\Verba\resources\db\manual-extend-partitions-past.sql

Use the SQL Server Management Studio to execute the script.

Database purging

Verba database may contain erroneous call records due to various system problems. This Verba function enables the administrator and the system administrators to remove or correct (if possible) these types of call records. You can list erroneous call information by selecting the **System / Database / Database Purging** menu item.

The following scenarios may apply:

- Finished calls without recorded media file
- Ongoing calls started 2 days before without recorded media file
- Ongoing calls started 2 days before with recorded media file

Activating any of the above functions will result in an event log entry. The system does not delete physically the records, they are moved to a table, which contains deleted call records.

Finished calls without recorded media file

Calls without media files are probably very short calls (< 1 sec). The web interface hides these type of calls by default. You can change this setting, refer to Verba user guide for further information in Verba Deployment Guide, article Configuration settings for Verba Web Application.

Calls without media files can appear in the system if something miss-configured on the monitor port (signaling messages are recorded, but the RTP media streams are not)! Contact the system administrator and refer to the manual for detailed information in Verba Deployment Guide, part Configuring monitor port!

Click on the **Delete Record(s)** button to remove these call records.

The system does not physically delete the records, they are moved to a table, that contains deleted call records.

> ⓘ YOU CANNOT UNDO THIS STEP!

Ongoing calls started 2 days before without recorded media file

Ongoing calls started 2 days before without recorded media files are probably erroneous calls. It can be caused by Verba recording engine failure (e.g. stopping the recording engine while a call being recorded can cause this situation)! Contact the system administrator and refer to the manual for detailed information in Verba Deployment Guide, part Configuring monitor port!

Click on the **Delete Record(s)** button to remove these call records.

The system does not physically delete the records, they are moved to a table, that contains deleted call records.

> ⓘ YOU CANNOT UNDO THIS STEP!

Ongoing calls started 2 days before with recorded media file

Ongoing calls started 2 days before with recorded media files are probably erroneous calls. It can be caused by Verba recording engine failure (e.g. stopping the recording engine while a call being recorded can cause this situation)! Contact the system administrator and refer to the manual for detailed information in Verba Deployment Guide, part Configuring monitor port! The update button updates the end time field for these records to an actual date with reason: Manual termination.

Click on the **Update Record(s)** button to take changes effect for these call records.

> ⓘ YOU CANNOT UNDO THIS STEP!

SQL Server GUI tools

The following graphical management tools are recommended to be utilized when working in the Verba environment:

- SQL Server Management Studio
- SQL Server Configuration Manager
- SQL Server Profiler

The following topics provide a brief explanation of these tools. For detailed information about the mentioned applications, follow the provided link to the Microsoft documentation site.

For more information on the available tools, see https://docs.microsoft.com/en-us/sql/tools/overview-sql-tools.

SQL Server Management Studio and SQL Server Management Studio Express

SQL Server Management Studio (SSMS) is an integrated environment for managing any SQL infrastructure. Use SSMS to access, configure, manage, administer, and develop all components of SQL Server, Azure SQL Database, and SQL Data Warehouse. SSMS provides a single comprehensive utility that combines a broad group of graphical tools with a number of rich script editors to provide access to SQL Server for developers and database administrators of all skill levels.

For further information on how to use SQL Server Management Studio, refer to https://docs.microsoft.com/en-us/sql/ssms/sql-server-management-studio-ssms.

You can download SQL Server Management Studio from Microsoft at https://docs.microsoft.com/en-us/sql/ssms/download-sql-server-management-studio-ssms.

SQL Server Configuration Manager

The SQL Server Configuration Manager utility is a tool to manage the services associated with SQL Server, to configure the network protocols used by SQL Server, and to manage the network connectivity configuration from SQL Server client computers. The SQL Server Configuration Manager combines the functionality of the following SQL Server tools: Server Network Utility, Client Network Utility, and Service Manager.

SQL Server Configuration Manager is a Microsoft Management Console snap-in that is available from the Start menu, or can be added to any other Microsoft Management Console display. To invoke the SQL Server Configuration Manager the Microsoft Management Console (mmc.exe) uses the SQLServerManager.msc file located in the Windows System32 folder.

For further information about the SQL Server Configuration Manager, refer to https://docs.microsoft.com/en-us/sql/relational-databases/sql-server-configuration-manager.

SQL Server Profiler

SQL Server Profiler is a tool that captures SQL Server 2008 events from a server. The events are saved in a trace file that can later be analyzed or used to replay a specific series of steps when trying to diagnose a problem. SQL Server Profiler is used for activities such as:

- Finding and diagnosing slow-running queries.
- Capturing the series of Transact-SQL statements that lead to a problem. The saved trace can then be used to replicate the problem on a test server where the problem can be diagnosed.
- Monitoring the performance of SQL Server to determine bottlenecks and identify opportunities to tune database and system workloads. For information about tuning the physical database design for database workloads, see Database Engine Tuning Advisor Reference.
- Correlating performance counters to diagnose problems.

SQL Server Profiler also supports auditing the actions performed on instances of SQL Server. Audits include records on security-related actions for later review by a security administrator.

For further information on SQL Server Profiler, refer to https://docs.microsoft.com/en-us/sql/tools/sql-server-profiler/sql-server-profiler.

SQL Server command line tools

SQL Server ships with many command prompt utilities. Detailed information about the available tools can be found at https://docs.microsoft.com/en-us/sql/tools/command-prompt-utility-reference-database-engine.

We recommend using the **osql** and **sqlcmd** tools.

Alternatively, PowerShell can be used to access the database, for more information, see https://docs.microsoft.com/en-us/sql/powershell/sql-server-powershell

Moving the database to another SQL Server

Moving the database of the Verba system consist of various steps. Before starting the process, make sure you have the followings available:

- Administrator access to the existing SQL Server which is hosting the Verba database
- Administrator access to the new SQL Server which will be hosting the Verba database
- Microsoft SQL Server Management Studio, the application can be downloaded from: https://docs.microsoft.com/en-us/sql/ssms/download-sql-server-management-studio-ssms
- A clear and definite plan for the database move including a rollback plan
- The process includes taking the database offline, which means that certain features will not be available during the procedure, make sure it does not interfere with your business and regulations
- When you have a complex deployment, make sure you have the right engineering resources available knowledgeable of the deployment

The following list briefly outlines the database moving process:

- Reconfiguring the system to use the new SQL Server
- Taking the database offline on the old SQL Server
- Detaching the database on the old SQL Server
- Moving the database files to the new SQL Server
- Attaching the database on the new SQL Server

The following features will be not available while the database is offline:

- Any feature available through the web based user interface including search, playback, configuration changes, etc.
- Storage policies will not run and wait until the database is online again
- Recorders will not insert data into the database, recording will continue to work, database records will be inserted once the connection is restored

Changing the SQL Server connection parameters

Step 1 - Change the database connection parameters to the new server. It has to be done before moving the database because after moving the database, the system configuration cannot be changed until the new database is connected. Login to the web interface and navigate to the **Servers** or **Configuration Profiles** under **System**.

Step 2 - Navigate to **Change Configuration Settings** tab and drill down to **Database Connection.** Change the connection parameters for the new SQL Server. Make sure you enter the right information because once you save the new settings, the system configuration cannot be changed (only manually in the local registry). For more information see [Configuring database connection](#).

Step 3 - Save the changes by clicking on the

💾

icon.

Step 4 - Repeat the steps above on all servers and configuration profiles. It has to be changed on all servers.

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.

> From this point, the system will try to connect to the new SQL Server. Since the Verba database does not exist on the new SQL Server (yet), the system will raise database connection down alerts. See above for restrictions while the database is offline.

Taking the database offline and detaching it

Step 6 - Connect to the SQL Server hosting the Verba database using SQL Server Management Studio.

Step 7 - Expand **Databases**, and select the name of the Verba database you want to move.

Step 8 - Right-click on the database name, select **Tasks**, select **Take Offline.** The database cannot be taken offline if there are active connections blocking the task. In order to close all blocking connections, right-click on the SQL Server instance name and select **Activity Monitor** from the menu. Once Activity Monitor has loaded, expand the **Processes** section. Scroll down to the SPID of the process you would like to kill. Right-click on that line and select **Kill Process**. A popup window will open for you to confirm that you want to kill the process. Once this is done, the process will be terminated and all uncompleted transactions will begin the rollback process.

Step 9 - Lookup the location of the database files on the server and make a note of the information. Right-click on the database name, select **Properties** then select **Files**. You can find the information in the **Path** and **File Name** columns.

Step 10 - Under **Tasks**, click **Detach** to detach the database.

Moving and attaching the database

Step 11 - Copy the database files (both .mdf and .log files) to the new SQL Server.

Step 12 - In SQL Server Management Studio Object Explorer, connect to the new SQL Server and then expand that instance

Step 13 - Right-click **Databases** and click **Attach**.

Step 14 - In the **Attach Databases** dialog box, to specify the database to be attached, click **Add**; and in the **Locate Database Files** dialog box, select the disk drive where the new copy of the database resides and expand the directory tree to find and select the .mdf file of the database. For example C:\Program Files\Microsoft SQL Server\MSSQL13.MSSQLSERVER\MSSQL\DATA\Verba.mdf

Step 15 - The system should be able to reconnect to the database and send database connection up alerts. Verify that all components are able to connect to the database.

Failure scenarios and procedures

- Cisco UCM failure scenarios for passive recording
- How to enable or disable Verba services on Lync servers
- Database failover options and procedures using mirroring
- Cross-datacenter Recording Server failover procedures in a Lync environment
- Storage failover procedures
- Media Repository failover options and procedures
- Isolation procedures for Verba

Cisco UCM failure scenarios for passive recording

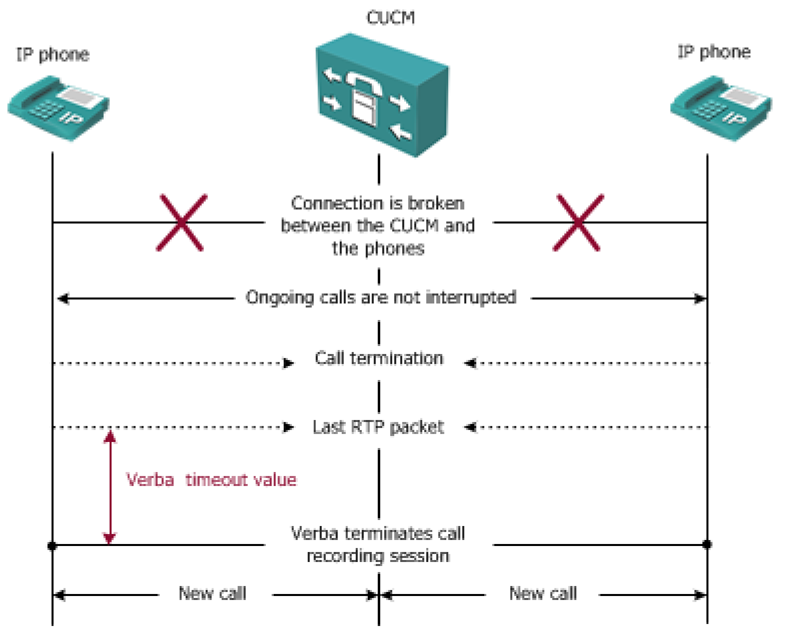
This topic describes the most common Cisco Unified Communications Manager failure scenarios that may impact the passive call recording service. Verba has many built-in features to handle and provide survivability of the system for Cisco Unified Communications Manager failure scenarios.

Timeout

A global parameter defines the timeout value for each Verba system (the default value of this parameter is set to 300 seconds, 5 minutes). If the last received RTP packet of a call/session is older then the timeout value, Verba terminates that recording session. The timeout check is performed in every minute.

When a call has to be terminated, because its last RTP packet is too old, Verba closes the media file at the last received RTP packet and updates the metadata with the proper termination time value (equals to the last RTP packet time). The termination cause value for this call is set to "Timeout" (80).

If the telephony system uses silence suppression then it is possible that none of the calling parties talk for a long period. If the silence takes longer than the timeout value, Verba will terminate this type of call too. In order to avoid this situation; you have to set the timeout value greater in the configuration.

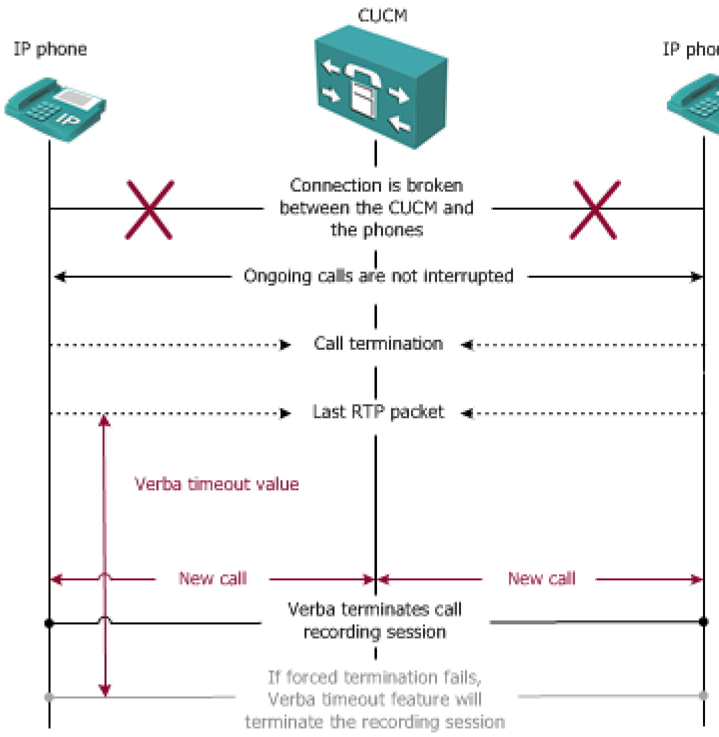

CUCM
IP phone
IP phone
Connection is broken between the CUCM and the phones
Ongoing calls are not interrupted
Call termination
Last RTP packet
Verba timeout value
Verba terminates call recording session
New call
New call

Forced termination

When Verba identifies that a call has started between two IP phones, it terminates all recording sessions forcefully that belong to any of the given IP phones.

This feature enables the system to immediately recognize Unified Communications Manager failure. If an IP phone starts a call, it means that older calls for this station are no longer alive (there was a Unified Communications Manager failure during the previous call).

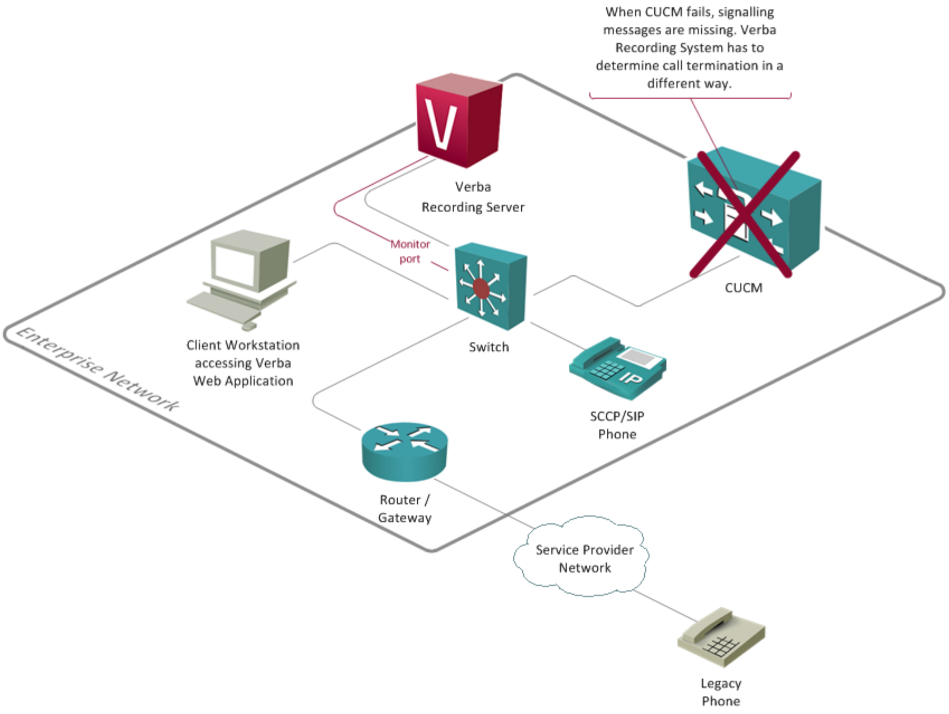
When a call has to be forcefully terminated, because of a new call start, then Verba closes the media file at the last received RTP packet and updates meta data with the proper termination time value (equals to the last RTP packet time) for the given recording session. The termination cause value for this call is set to "Forced termination" (81).


CUCM
IP phone
IP phone
Connection is broken between the CUCM and the phones
Ongoing calls are not interrupted
Call termination
Last RTP packet
Verba timeout value
New call
New call
Verba terminates call recording session
If forced termination fails, Verba timeout feature will terminate the recording session

Single Unified Communications Manager server

This scenario is only applicable, when one Unified Communications Manager is deployed. If the Unified Communications Manager fails, the ongoing calls continue without interruption. Verba is able to record these calls and terminate the recording sessions properly using the following features:

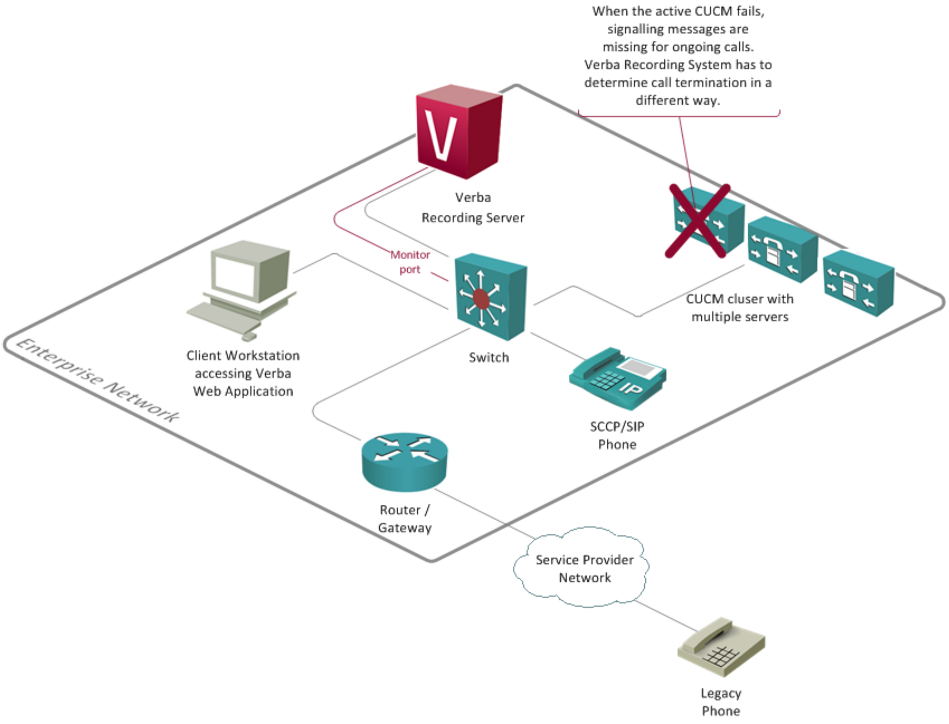
- Initially, calls are terminated by Verba, with reason code 80.
- If the same parties start a new call (after Unified Communications Manager becomes available), previous calls are forcefully terminated by Verba, applying reason code 81.
- When Unified Communications Manager resumes its operation normally, every new call is handled as usual.


When CUCM fails, signalling messages are missing. Verba Recording System has to determine call termination in a different way.
Verba Recording Server
Monitor port
CUCM
Client Workstation accessing Verba Web Application
Switch
Enterprise Network
SCCP/SIP Phone
Router / Gateway
Service Provider Network
Legacy Phone

Multiple Unified Communications Manager servers

This scenario applies, when more than one Unified Communications Manager server is deployed. If the active Unified Communications Manager fails, the ongoing calls continue without interruption. Verba is able to record these calls and terminate the recording sessions properly using the following features:

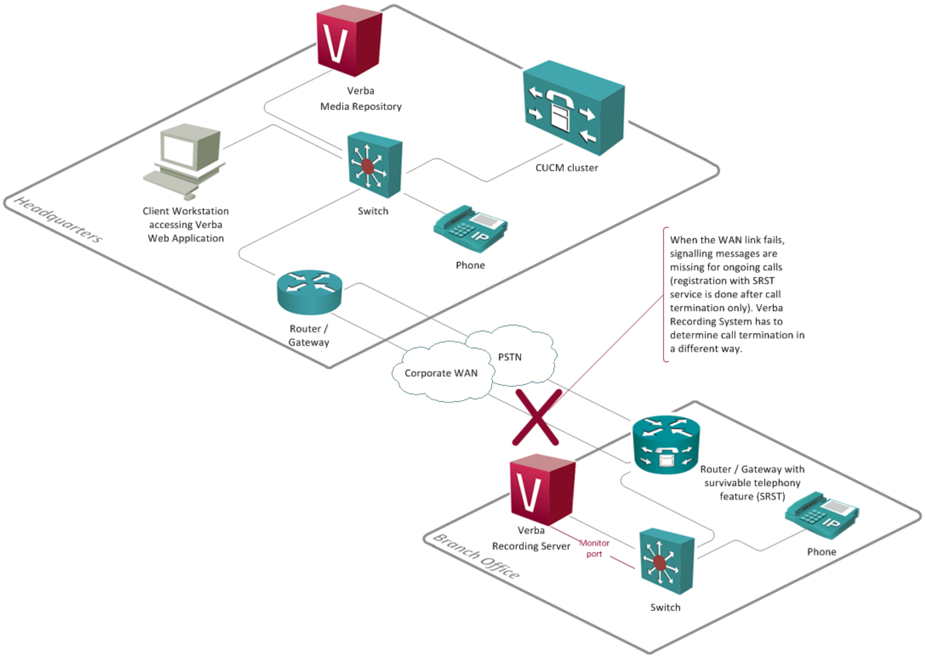
- Initially, calls are terminated by Verba, using reason code 80.
- If the same parties start a new call, previous calls are forcefully terminated by Verba, applying reason code 81.
- When the standby Unified Communications Manager server becomes active and the IP phones register in, all of the new calls are handled as usual.


When the active CUCM fails, signalling messages are missing for ongoing calls. Verba Recording System has to determine call termination in a different way.
Verba Recording Server
Monitor port
Switch
CUCM cluser with multiple servers
Client Workstation accessing Verba Web Application
Enterprise Network
SCCP/SIP Phone
Router / Gateway
Service Provider Network
Legacy Phone

SRST scenario

This scenario applies, when an SRST gateway is deployed at a remote site. If the WAN link fails, the ongoing calls continue without interruption. The Verba Recording Server is able to record these calls and terminate the recording sessions properly using the following features:

- Initially, calls are terminated by Verba applying reason code 80.
- If the same parties start a new call (after registering with the SRST router), previous calls are forcefully terminated by Verba, applying reason code 81.
- When the SRST service becomes active and the IP phones registers with it, all of the new calls are handled as usual.



IP phone failure

When an IP phone fails (e.g. network connection is broken), ongoing calls are interrupted for the given IP phone. Verba is able to terminate the recording sessions properly using the following features:

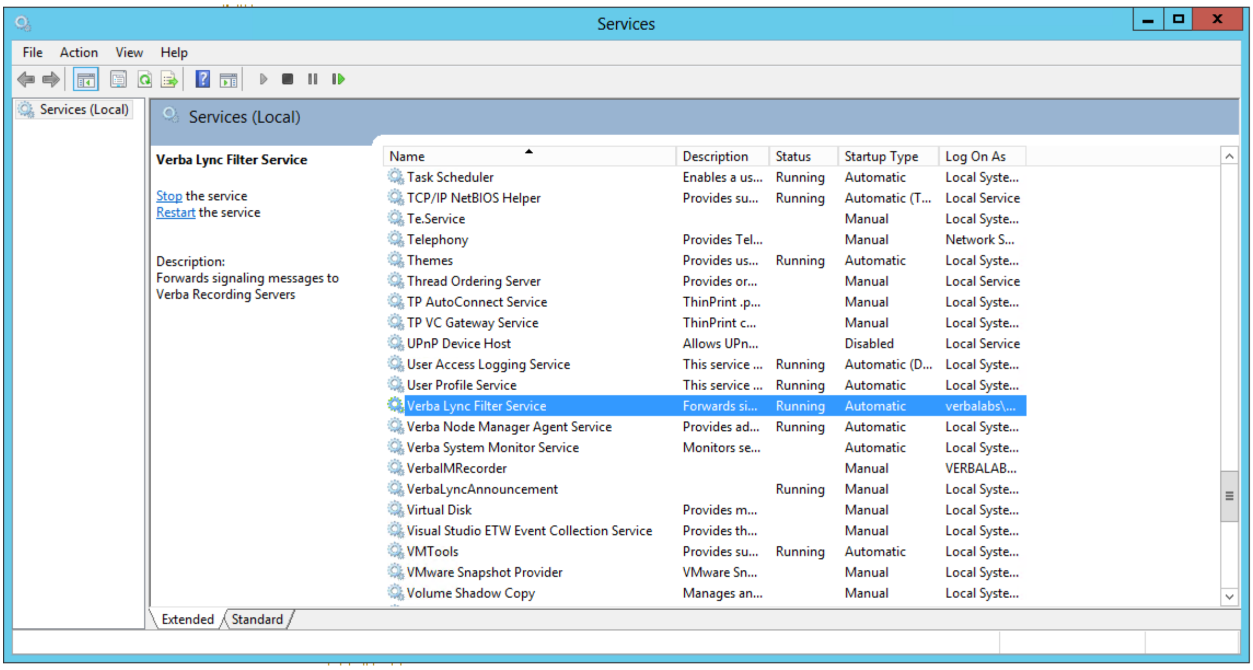
- Initially, calls are terminated by Verba applying reason code 80.
- If the same parties start a new call (after IP phone connection becomes available), previous calls are forcefully terminated by Verba, applying reason code 80.
- When the IP phone becomes active, all of the new calls are handled as usual.

How to enable or disable Verba services on Lync servers

If you are experiencing issues with your Lync environment, you might want to disable Verba services on your Lync servers for troubleshooting and to determine the root cause of the issue in your Lync system.

Enable Verba Service

To enable Verba services on Lync servers navigate to the Windows services by running the 'services.msc' from Start Menu.



Verba Lync Filter Service

Stop the service
Restart the service

Description:
Forwards signaling messages to Verba Recording Servers

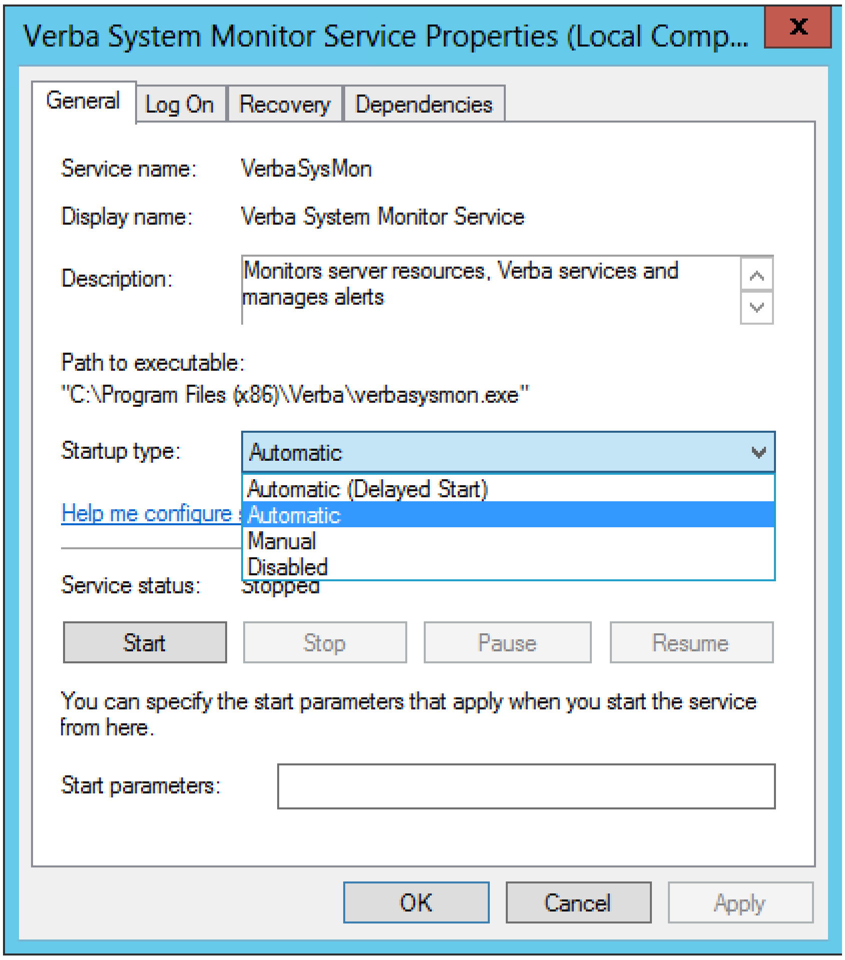
Name	Description	Status	Startup Type	Log On As
Task Scheduler	Enables a us...	Running	Automatic	Local Syste...
TCP/IP NetBIOS Helper	Provides su...	Running	Automatic (T...	Local Service
Te.Service			Manual	Local Syste...
Telephony	Provides Tel...		Manual	Network S...
Themes	Provides us...	Running	Automatic	Local Syste...
Thread Ordering Server	Provides or...		Manual	Local Service
TP AutoConnect Service	ThinPrint .p...		Manual	Local Syste...
TP VC Gateway Service	ThinPrint c...		Manual	Local Syste...
UPnP Device Host	Allows UPn...		Disabled	Local Service
User Access Logging Service	This service ...	Running	Automatic (D...	Local Syste...
User Profile Service	This service ...	Running	Automatic	Local Syste...
Verba Lync Filter Service	Forwards si...	Running	Automatic	verbalabs\...
Verba Node Manager Agent Service	Provides ad...	Running	Automatic	Local Syste...
Verba System Monitor Service	Monitors se...		Automatic	Local Syste...
VerbaIMRecorder			Manual	VERBALAB...
VerbaLyncAnnouncement		Running	Manual	Local Syste...
Virtual Disk	Provides m...		Manual	Local Syste...
Visual Studio ETW Event Collection Service	Provides th...		Manual	Local Syste...
VMTools	Provides su...	Running	Automatic	Local Syste...
VMware Snapshot Provider	VMware Sn...		Manual	Local Syste...
Volume Shadow Copy	Manages an...		Manual	Local Syste...

If the services are stopped follow the instructions bellow on **all required*** Verba services:

Step 1 Right click on **Verba Service** and click on 'Properties'

Step 2 Put the 'Startup type' to '**Automatic**'

Step 3 Hit the '**Start**' button and Apply the changes



Service name: VerbaSysMon

Display name: Verba System Monitor Service

Description: Monitors server resources, Verba services and manages alerts

Path to executable:
"C:\Program Files (x86)\Verba\verbasysmon.exe"

Startup type: Automatic

Service status: Stopped

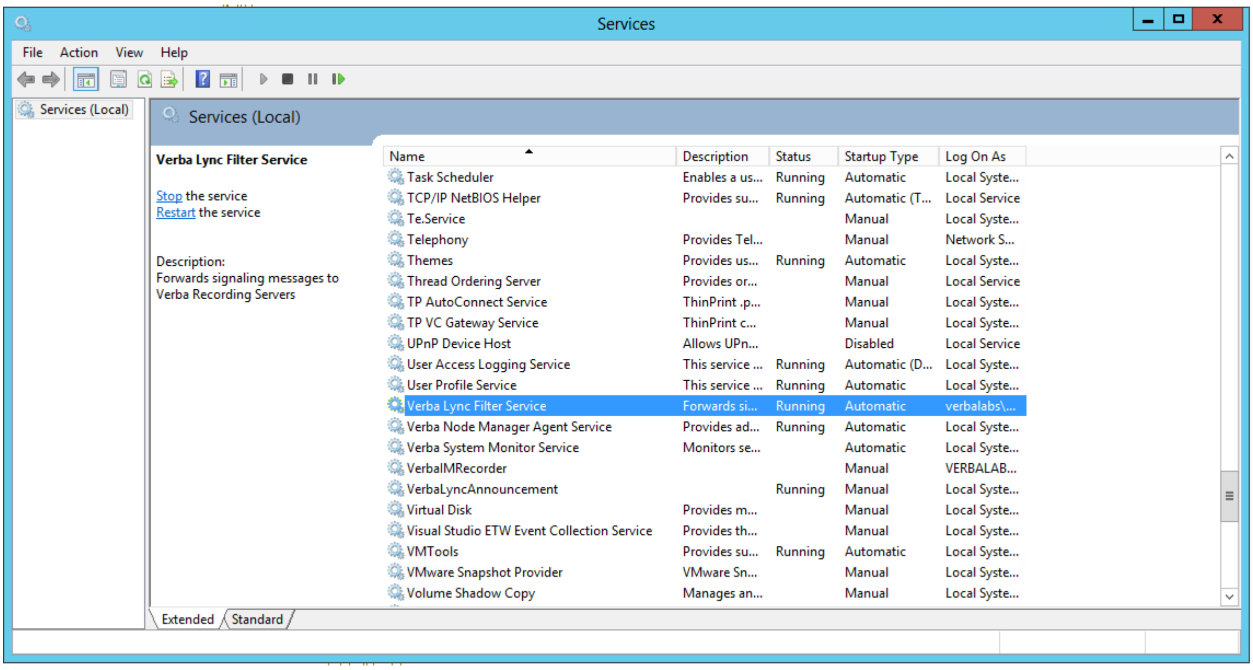
You can specify the start parameters that apply when you start the service from here.

Start parameters:

*Required Verba services on a Lync server can be the followings: Verba System Monitor Service, Verba Lync Filter Service, Verba Node Manager Agent Service or Verba Recorder Proxy Service.

Disable Verba Services

To disable Verba services on Lync servers navigate to the Windows services by running the 'services.msc' from Start Menu.



Verba Lync Filter Service

Stop the service
Restart the service

Description:
Forwards signaling messages to Verba Recording Servers

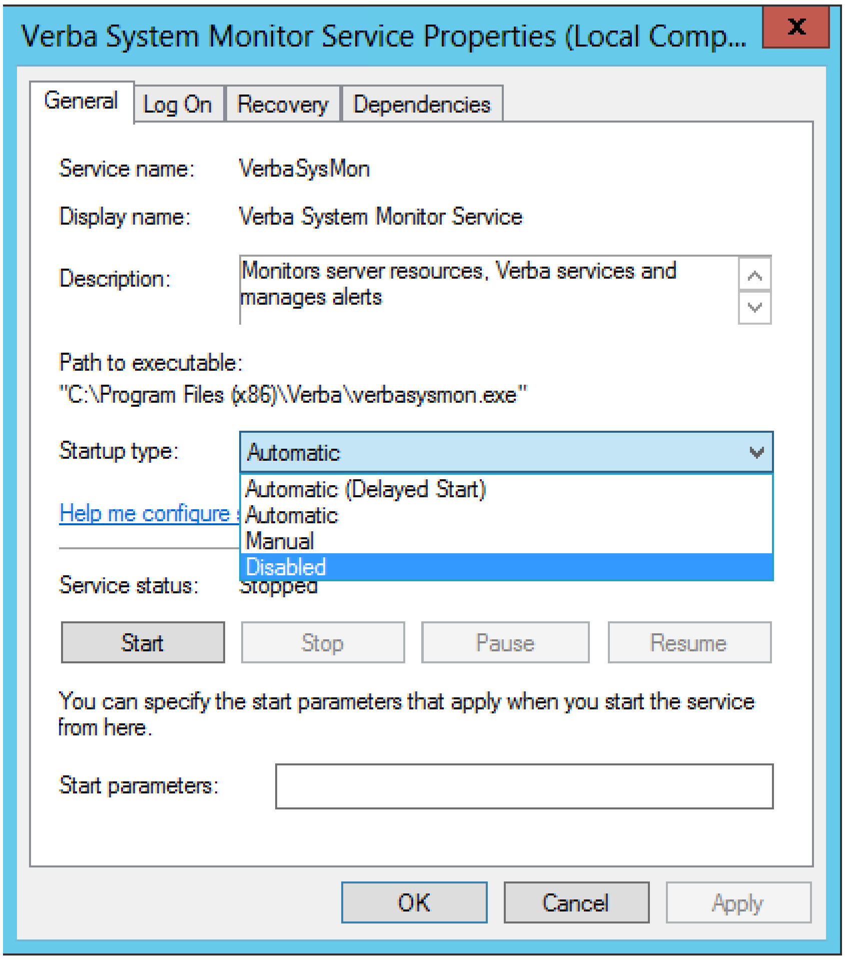
Name	Description	Status	Startup Type	Log On As
Task Scheduler	Enables a us...	Running	Automatic	Local Syste...
TCP/IP NetBIOS Helper	Provides su...	Running	Automatic (T...	Local Service
Te.Service			Manual	Local Syste...
Telephony	Provides Tel...		Manual	Network S...
Themes	Provides us...	Running	Automatic	Local Syste...
Thread Ordering Server	Provides or...		Manual	Local Service
TP AutoConnect Service	ThinPrint .p...		Manual	Local Syste...
TP VC Gateway Service	ThinPrint c...		Manual	Local Syste...
UPnP Device Host	Allows UPn...		Disabled	Local Service
User Access Logging Service	This service ...	Running	Automatic (D...	Local Syste...
User Profile Service	This service ...	Running	Automatic	Local Syste...
Verba Lync Filter Service	Forwards si...	Running	Automatic	verbalabs\...
Verba Node Manager Agent Service	Provides ad...	Running	Automatic	Local Syste...
Verba System Monitor Service	Monitors se...		Automatic	Local Syste...
VerbalMRecorder			Manual	VERBALAB...
VerbaLyncAnnouncement		Running	Manual	Local Syste...
Virtual Disk	Provides m...		Manual	Local Syste...
Visual Studio ETW Event Collection Service	Provides th...		Manual	Local Syste...
VMTools	Provides su...	Running	Automatic	Local Syste...
VMware Snapshot Provider	VMware Sn...		Manual	Local Syste...
Volume Shadow Copy	Manages an...		Manual	Local Syste...

If the services are running follow the instructions bellow on **all running** Verba services:

Step 1 Right click on **Verba Service** and click on 'Properties'

Step 2 Put the 'Startup type' to '**Disable**'

Step 3 If the service is running hit the '**Stop**' button and Apply the changes



Verba System Monitor Service Properties (Local Comp...

Service name: VerbaSysMon

Display name: Verba System Monitor Service

Description: Monitors server resources, Verba services and manages alerts

Path to executable:
"C:\Program Files (x86)\Verba\verbasysmon.exe"

Startup type: Automatic

Service status: Stopped

You can specify the start parameters that apply when you start the service from here.

Start parameters:

After disabling all Verba services on Lync servers, the Verba call recording system does not have any impact on the Lync system. To re-enable the services, please follow the instructions in the first section.

Database failover options and procedures using mirroring

Database mirroring

Database mirroring maintains two copies of a single database that must reside on different server instances of SQL Server Database Engine. Typically, these server instances reside on computers in different locations. Starting database mirroring on a database, initiates a relationship, known as a database mirroring session, between these server instances.

One server instance serves the database to clients (the principal server). The other instance acts as a hot or warm standby server (the mirror server), depending on the configuration and state of the mirroring session. When a database mirroring session is synchronized, database mirroring provides a hot standby server that supports rapid failover without a loss of data from committed transactions. When the session is not synchronized, the mirror server is typically available as a warm standby server (with possible data loss).

More information about SQL Server Database Mirroring can be found here: http://technet.microsoft.com/en-us/library/ms189852.aspx

Role switching

Within the context of a database mirroring session, the principal and mirror roles are typically interchangeable in a process known as role switching. Role switching involves transferring the principal role to the mirror server. In role switching, the mirror server acts as the failover partner for the principal server. When a role switch occurs, the mirror server takes over the principal role and brings its copy of the database online as the new principal database. The former principal server, if available, assumes the mirror role, and its database becomes the new mirror database. Potentially, the roles can switch back and forth repeatedly. The following three forms of role switching exist.

- **Automatic failover**
  This requires high-safety mode and the presence of the mirror server and a witness. The database must already be synchronized, and the witness must be connected to the mirror server.
  The role of the witness is to verify whether a given partner server is up and functioning. If the mirror server loses its connection to the principal server, but the witness is still connected to the principal server, the mirror server does not initiate a failover. For more information, see Database Mirroring Witness.
- **Manual failover**
  This requires high-safety mode. The partners must be connected to each other, and the database must already be synchronized.
- **Forced service (with possible data loss)**
  Under high-performance mode and high-safety mode without automatic failover, forcing service is possible if the principal server has failed and the mirror server is available.

Database failover support in Verba

Verba is compatible with each mirroring mode and will act similarly regardless of the mirroring setup.

In case of a disaster, either the DB administrator switches the roles, or it happens automatically. Until the roles switched, Verba web interface will be unaccessible, but recording will work since when recorder engines cannot connect to the database, they are collecting every information that should had been inserted, and will insert all of the collected data once the connection is up.

Obviously, Verba services have to learn that they need to connect to the new principal DB server. There are three different options to achieve it:

SQL Server built-in "Failover Partner" feature

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 of 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.

Failover Partner can be configured for each Verba server at the database configuration. You also need to install the appropriate native SQL client:

Changing the database server host name's DNS configuration

If the customer thinks that the probability of a Role Switching is very low, then this option might makes sense.

When the original principal server goes down, and the database administrator decides to switch the roles, after the role switching, the DNS server(s) configuration has to be changed such the database host name points to the new principal server's IP address. Verba servers will connect to the new database as soon as the operating system recognizes the DNS change.

The DNS information is cached, and until it is expired, the servers will resolve the database server host name to the old IP address. In order to have the DNS change recognized by the servers as soon as possible, you might consider performing a DNS flush on the Verba servers.

The applications' existing connections will not work, so the system will not be stable until every connection is closed and reopened. This fact does not lead to any data loss in the recorded media, because the recorder services maintain their own cache and will insert the cached data as soon as the database connection gets stable.

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.

Configure Verba to use the new database server

After a Role Switching, instead of changing the DNS configuration, the Verba configuration can be changed as well. The change has to be applied on each Verba server, so depending on the number of Verba servers this approach might take a longer time that the previous ones.

After the database connection configuration changed, almost each of the Verba services have to be restarted as the Verba web application will warn the user.

More information about the database configuration can be found here: http://kb.verba.com/display/docs/Database+connection+settings

Cross-datacenter Recording Server failover procedures in a Lync environment

This section contains configuration changes regarding cross-datacenter recorder server failover procedures required to manually switch between 2 datacenter sites. These procedures can only be applied in the following use case:

- Verba is deployed across 2 data centers.
- We assume Media Repository and Lync services are available in both datacenters
- Recording Servers are connected to local, data center specific Lync environments
- There is no cross-reference between the 2 sites on the Recording Server level.
- If all Recording Servers go down on one site, Verba needs to be manually reconfigured to record in the working datacenter the remote Lync system located in the other data center.

The Recording Server failover procedure contains 2 major steps:

- Reconfigure the **Verba Passive Recorder** service to change announcement target URLs to preferred ones
- Reconfigure the **Verba Passive Recorder** service to connect to recorder proxies running on the other site

Reconfigure the Verba Passive Recorder service to change announcement target URLs to preferred ones

Currently, we support recording announcement for only one Lync pool even so we can record conferences from multiple pools on the same recorder server. If you prefer to use the site's with failed recorders announcement service(s) instead of local one(s), you should change recorder service's recording announcement servers list.

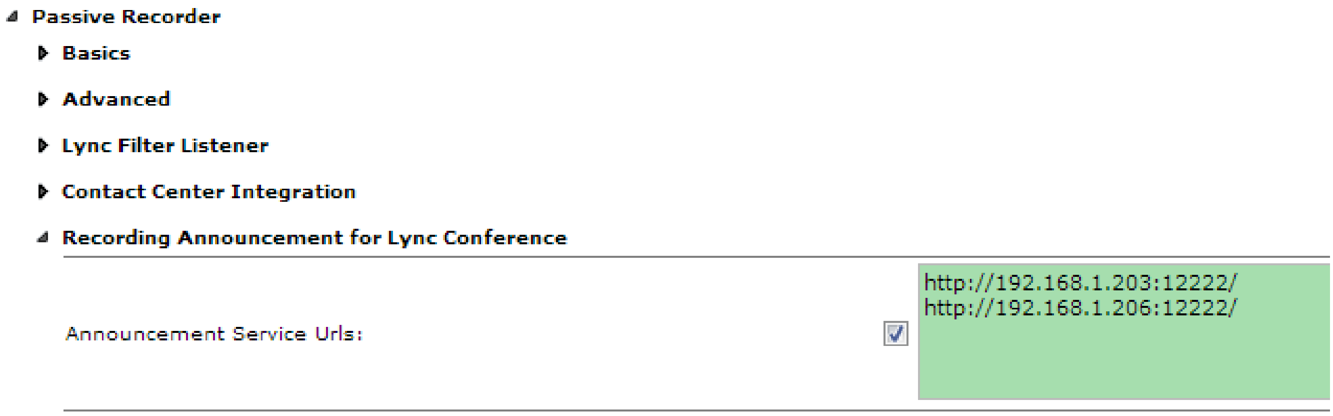
To change the configuration, follow the next steps:

Step 1. Navigate to **Administration/Verba Servers** or **Administration/Configuration Profiles** (in case you want to update the configuration profile used by the recording servers)

Step 2. Select the server which runs the Recording Announcement service or the configuration profile

Step 3. Select the '**Change Configuration Settings**' Tab and open the '**Passive Recorder** node.

Step 4. Change the **Recording Announcement for Lync Conference** to the intended announcement service urls.


Passive Recorder
Basics
Advanced
Lync Filter Listener
Contact Center Integration
Recording Announcement for Lync Conference

Announcement Service Urls: ☑

```
http://192.168.1.203:12222/
http://192.168.1.206:12222/
```

Step 5. After saving the changes, follow the instructions in the upper yellow banner to apply the changes on the affected server(s).

Step 6. Repeat the steps above on all servers or configuration profiles.

Reconfigure the Verba Passive Recorder service to connect to recorder proxies running on the other site

In a failover scenario, the settings of the passive recording service have to be changed in order to connect the recorder service to the other site's Verba Recorder Proxy/Remote Capture services as well. This modification will allow the recording system on the site with working recorder servers to record the calls belonging to the other site and to the local site. Failover feature of remote site's recorder proxies will reassign the to be recorded calls to the local recorder servers.

You need to change the configuration on all related Verba Recording Servers. If you use configuration profiles, you can just update the corresponding profile, instead of updating all servers one by one.

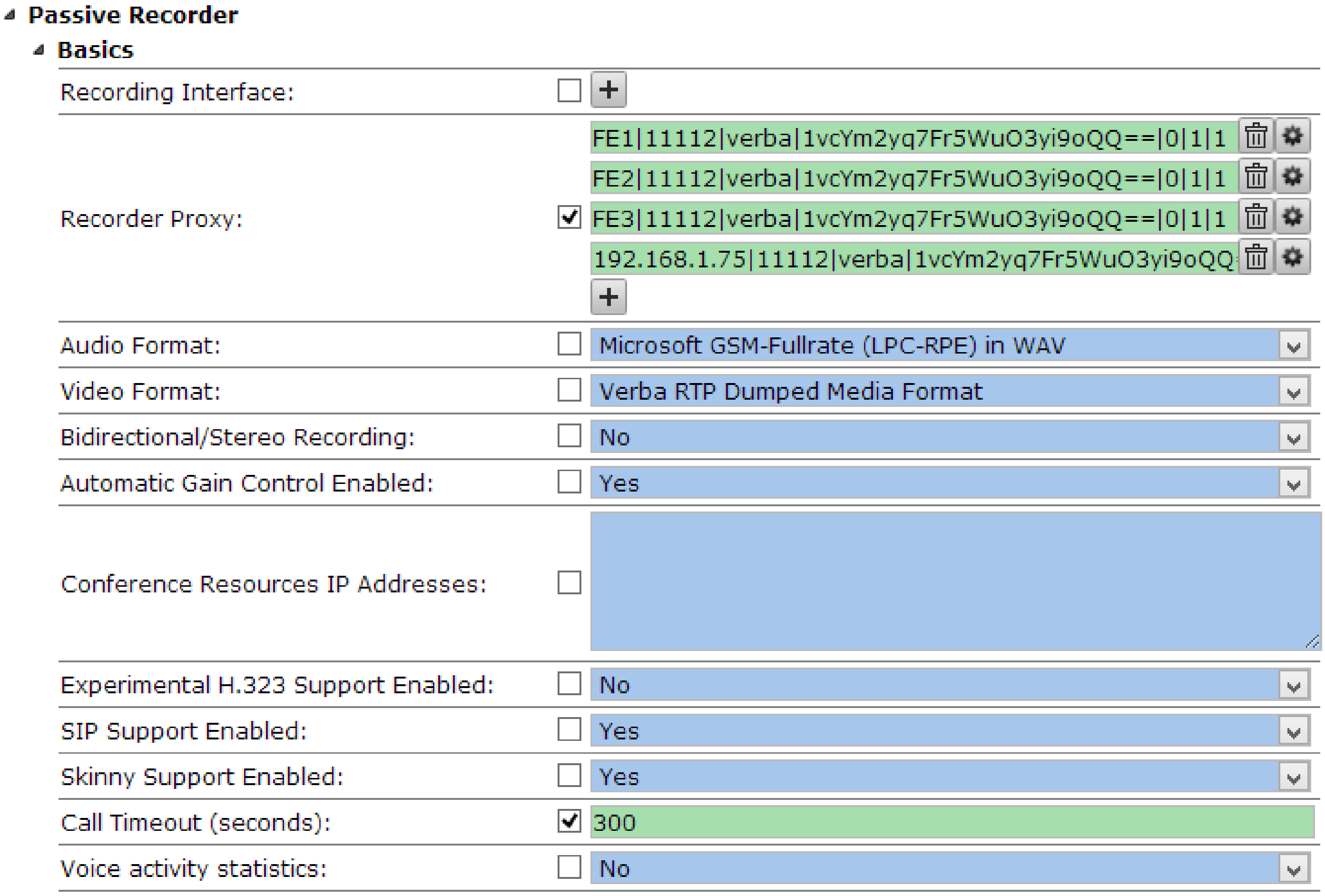
Follow the steps below:

Step 1. Navigate to **Administration/Verba Servers** or **Administration/Configuration Profiles** (in case you want to update the configuration profile used by the recording servers)

Step 2. Select the recording server from the server list or the configuration profile.

Step 3. Select the '**Change Configuration Settings'** tab and open the '**Passive Recorder/Basics'** node

Step 4. Modify the added '**Recorder Proxy'** entries to point at the working sites proxies.



◢ **Passive Recorder**

◢ **Basics**

Recording Interface:	□	+
Recorder Proxy:	☑	FE1|11112|verba|1vcYm2yq7Fr5WuO3yi9oQQ==|0|1|1 FE2|11112|verba|1vcYm2yq7Fr5WuO3yi9oQQ==|0|1|1 FE3|11112|verba|1vcYm2yq7Fr5WuO3yi9oQQ==|0|1|1 192.168.1.75|11112|verba|1vcYm2yq7Fr5WuO3yi9oQQ +
Audio Format:	□	Microsoft GSM-Fullrate (LPC-RPE) in WAV
Video Format:	□	Verba RTP Dumped Media Format
Bidirectional/Stereo Recording:	□	No
Automatic Gain Control Enabled:	□	Yes
Conference Resources IP Addresses:	□	
Experimental H.323 Support Enabled:	□	No
SIP Support Enabled:	□	Yes
Skinny Support Enabled:	□	Yes
Call Timeout (seconds):	☑	300
Voice activity statistics:	□	No

Step 5. After saving the changes, follow the instructions in the upper yellow banner to apply the changes on the affected server(s).

Step 6. Repeat the steps above on all servers or configuration profiles.

Storage failover procedures

This article details the required changes in the Verba configuration to overcome any issues caused by a storage failure.

The failover process requires manual changes in the configuration settings of the Verba Storage Management service.

If your system has multiple redundant storage facilities and Verba uses them for storing the media files of your recorded calls, they are usually referenced in Verba by a UNC path. When a failover occurs between the redundant storages, Verba has to be pointed to the backup storage by changing the configuration at every point where the failed storage location is referenced. These points are in most cases the media folder setting of the media repository server and the upload target of the recording servers. If you have archiving Data Retention Policies, which target the failed storage, the storage target folder of those policies have to be changed as well.

Below you can find step by step guides on how to change each of these settings.

Changing the media folder

The media folder is where the Verba web interface and player looks for the media files for playback and downloading. Please note that on servers with only the 'Recording Sever' role and uploading enabled, the media folder is only used for storing the media files temporarily, until they are uploaded to the configured storage location.

Follow the steps below to change the media folder path:

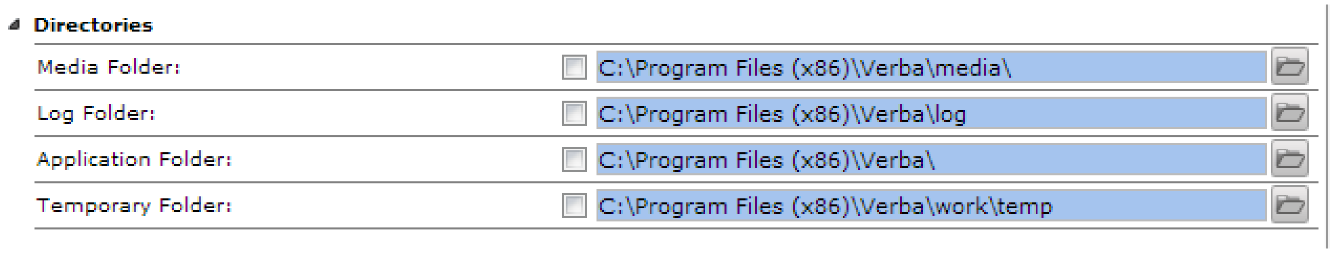
Step 1. In the Verba web interface click on **Administration > Verba Servers** and select your Media Repository server.

Step 2. Click on the **Change Configuration Settings** tab.

Step 3. Expand **Directories** and change the **Media folder** field to the path of the backup storage.

Step 4. Click the **Save** icon to save your settings

Step 5. The system will notify you that the changes need to applied to the server by restarting the involved services. Execute the required tasks. (Note: restarting the Storage Management service will not impact the operation of call recording in any way)



Directories

Media Folder:	□	C:\Program Files (x86)\Verba\media\
Log Folder:	□	C:\Program Files (x86)\Verba\log
Application Folder:	□	C:\Program Files (x86)\Verba\
Temporary Folder:	□	C:\Program Files (x86)\Verba\work\temp

Changing the upload location

The recording servers upload the recorded media files to the media repository or a separate storage location. Follow the steps below to change the path to this location in case you move the recording directly to the storage infrastructure. In case you upload to the Media Repository server, you do not need to change anything in on the Recording Server(s).

Step 1. In the Verba web interface click on **Administration > Verba Servers** and select your Media Repository server.

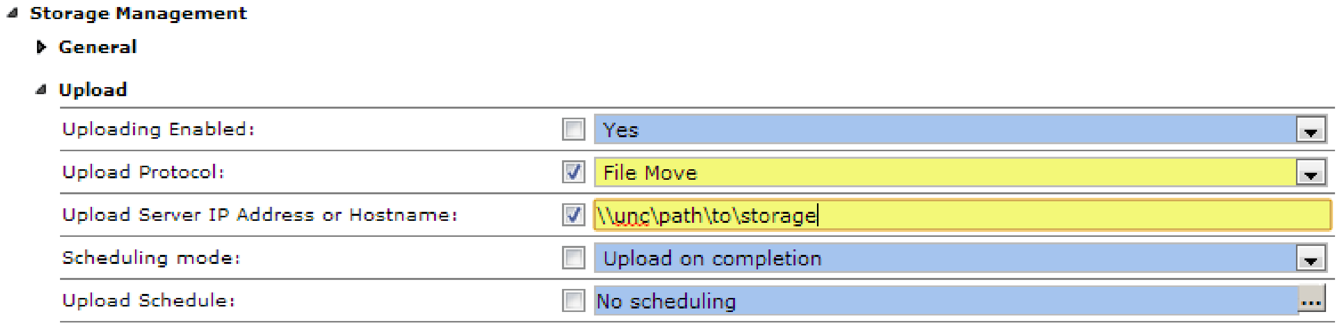
Step 2. Click on the **Change Configuration Settings** tab.

Step 3. Under **Storage Management** expand **Upload**

Step 4. Change the value of the **Upload Server IP Address or Hostname** field to the path of the backup storage.

Step 5. Click the **Save** icon to save your settings

Step 6. The system will notify you that the changes need to applied to the server by restarting the involved services. Execute the required tasks. (Note: restarting the Storage Management service will not impact the operation of call recording in any way)



Storage Management

General

Upload

Uploading Enabled:	□	Yes
Upload Protocol:	☑	File Move
Upload Server IP Address or Hostname:	☑	\\unc\path\to\storage
Scheduling mode:	□	Upload on completion
Upload Schedule:	□	No scheduling

If you have multiple Verba servers of the same role in your architecture, use configuration profiles to change the settings of all the servers of the same role at the same time. To do this, Click on Administration > Configuration profiles, select the server role you want to configure. From this point the steps are the same as the regular server configuration steps above. After making your changes, saving and executing them, all the servers of the same role will be updated to reflect your changes in the configuration.

Changing a storage target folder path

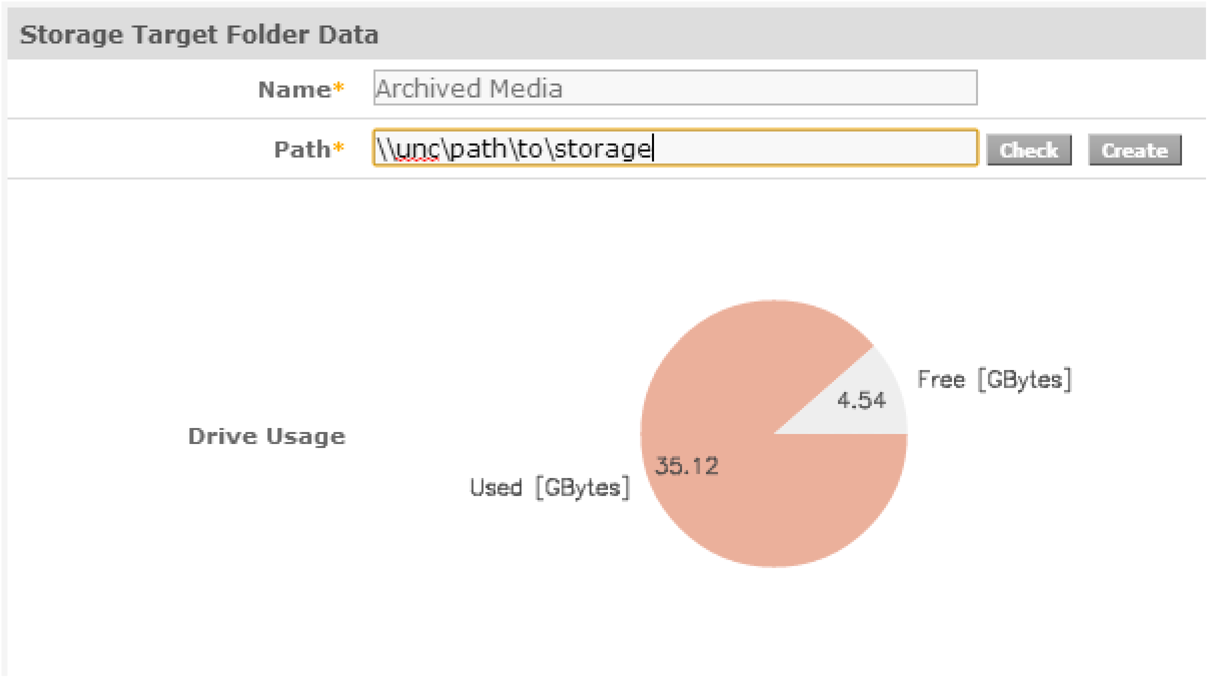
Storage target folders are used by archiving Data retention policies to specify the archive location. If your recording system has one or more archiving policies where the storage target folder is located on the failed storage equipment, you will need to change them to point to the backup storage.

Please follow the steps below to change a Storage target folder.

Step 1. In the Verba web interface click on **Administration > Storage target folders**.

Step 2. Select the storage target folder that has to be changed.

Step 3. Change the value of the **Path** field to the path of the backup storage.



Storage Target Folder Data

Name* Archived Media

Path* \\unc\path\to\storage

Drive Usage

Media Repository failover options and procedures

The Media Repository component provides the central, web based user interface, storage management, administration, etc. features. In smaller deployments, this role can be co-hosted with the Recording Server role, resulting in a simple single server deployment. In larger deployments, the SQL Server is deployed on another server or an existing corporate instance is used. In order to have a reliable, high performance central storage, a SAN/NAS system is connected for recorded media file access.

Media Repository servers can be deployed in a redundant fashion if required by placing a load balancing solution in front. In this deployment model, there is a separate, central and redundant SQL Server cluster, and a separate, redundant, central storage system.

The Media Repository servers serve user requests by talking to the same database and the same central storage, so any of them can serve any user. A **(preferably hardware based) load balancer** is necessary in front of the Media Repository. The load balancer has to meet the following requirements:

- **Support for HTTP session stickiness** to make sure authenticated users always go to the same Repository server where their session exists
- Since Verba has components that do not support cookies, the best if the **affinity persistence is based on the client's IP address**
- The Verba Web application's session timeout is 60 minutes, so the **timeout while F5 stores the client's IP address** in its memory should be **greater than 60 minutes**.
- URI path (Might be needed for configuration if the load balancer serves other systems as well): http://<name>/verba
- (This requirement applies only if you use the **Verba phone service for Cisco handsets**) The phones support HTTP only, so even if you would like to restrict HTTP access, port 80 has to be proxied. HTTPS access can be restricted in Verba if needed (it still allows HTTP access for the phone service features).
- (Optional) HTTPS acceleration

In case of Media Repository failure, current user sessions served on the server, will be lost. Users will be logged out automatically and they will need to login back again. The load balancer will route their new login request through the next available Media Repository server. When a specific feature is tied to certain Media Repository (e.g. archiving) and the server fails, ongoing processes are interrupted and when the server is operational again, new tasks will be processed normally

Isolation procedures for Verba

Overview

In some cases it may be necessary to temporarily disable, remove, or disconnect Verba from the network to isolate a problem or to stabilize the network. This topic provides a description of the process and a detailed procedure that will allow a technical support engineer to completely disable and isolate your Verba solution.

In case of mirror port (SPAN) based recording, the Verba Recording Server component is listening on a monitor port of a switch, so it does not generate traffic on the network. The Verba Media Repository component (SQL Server, Apache/Tomcat) behaves like a web server using a database. When users play back recorded calls, the system transfers the media file through the network to the user's computer.

Stopping Verba in a Lync environment

> ⓘ If you are experiencing service degradation in your Lync system, always start by stopping the **Verba filters installed on the Lync Front Ends.** If this does not solve the problem, then follow these steps:

Step 1 Connect to the **Verba Recording server(s) / Verba Media Repository** remotely using Remote Desktop/Terminal Services Client/PcAnywhere or equivalent. If remote connection is not available then perform the following steps locally on the server.

Step 2 Open the Service Control window (services.msc).

Step 3 Select the following services from the list and stop them by clicking on them with the right mouse button and select Stop :

- Verba System Monitor Service (it is important to stop this service first, why? As otherwise, this service will restart other stopped Verba services.)
- Verba Recorder Proxy Service
- Verba Passive Recorder Service
- Verba Storage Management Service
- Verba Node Manager Agent Service
- Verba Web Application Service
- MSSQLSERVER

Stopping all services ensures that Verba is disabled.

Step 4 Connect to the **Lync Front End** server remotely using Remote Desktop/Terminal Services Client/PcAnywhere or equivalent. If remote connection is not available then perform the following steps locally on the server.

Step 5 Open the Service Control window (services.msc).

Step 6 Select the following services from the list and stop them by clicking on them with the right mouse button and select Stop:

- Verba Node Manager Agent Service
- Verba Lync Filter

Stopping all the services ensures that Verba is disabled.

Step 7 Repeat Steps 1-7 on **all Verba servers and Lync Front End** servers.

Step 8 If one of the services does not stop normally then follow the steps outlined in the "Shutting down Verba server" section.

Stopping Verba in a Cisco environment

ⓘ If you are experiencing service degradation in your Cisco UCM system, always start by stopping the **Verba Cisco Central Recorder Database Service** on your recorders.

Step 1 Connect to the **Verba Recording server(s) / Verba Media Repository** remotely using Remote Desktop/Terminal Services Client/PcAnywhere or equivalent. If remote connection is not available then perform the following steps locally on the server.

Step 2 Open the Service Control window (services.msc).

Step 3 Select the following services from the list and stop them by clicking on them with the right mouse button and select Stop:

- Verba System Monitor Service (it is important to stop this service first, why? As otherwise, this service will restart other stopped Verba services)
- Verba Passive Recorder Service
- Verba Cisco Central Recorder Service
- Verba Cisco Central Recorder Database Service,
- Verba Storage Management Service
- Verba Node Manager Agent Service
- Verba Web Application Service
- MSSQLSERVER.

Stopping all the services ensures that Verba is disabled.

Step 4 Repeat Steps 1-7 on **all Verba servers.**

Step 5 If one of the services does not stop normally then follow the steps outlined in the "Shutting down Verba server" section.

Shutting down Verba server

Step 1 Connect to the server remotely using Remote Desktop/Terminal Services Client/PcAnywhere or equivalent. If remote connection is not available log in locally to the server.

Step 2 Initiate a shut down from the Start menu (Start menu/Shut down/Shut down). If the server shuts down normally, Verba is disabled.

Step 3 If the server hangs after initiating the shut down, switch off the server manually.

How to change service log level

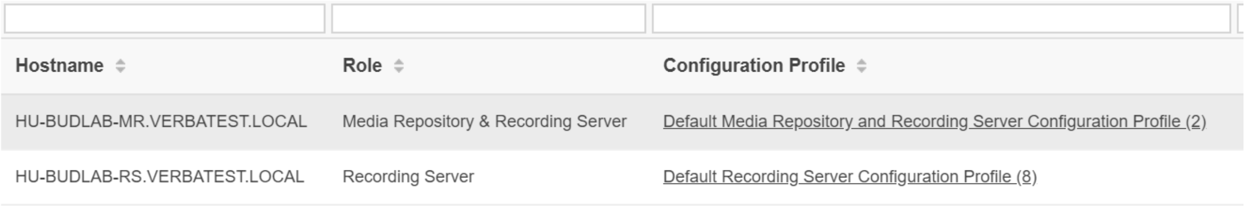
Follow the steps below to change the log level for one ore more services.

> Changing service configuration may require restarting the affected services which can temporarily stop recording. Service restarts should only be done outside of business hours.

Step 1 - Login to the Web Application with a system administrator user

Step 2 - Navigate to **System / Servers**

Step 3 - Select the server by clicking on the **Hostname** column of the server

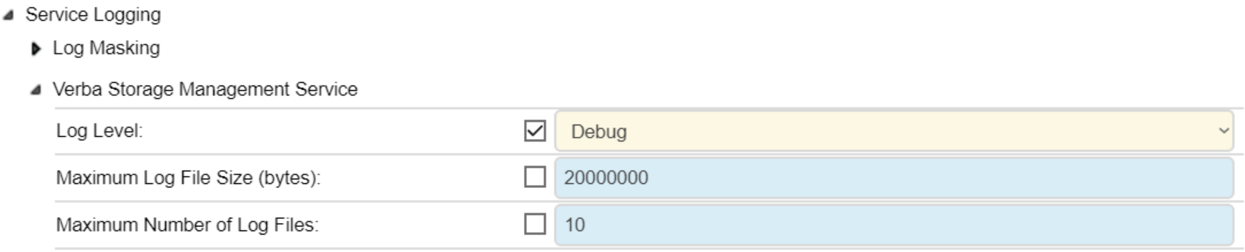


Hostname	Role	Configuration Profile
HU-BUDLAB-MR.VERBATEST.LOCAL	Media Repository & Recording Server	Default Media Repository and Recording Server Configuration Profile (2)
HU-BUDLAB-RS.VERBATEST.LOCAL	Recording Server	Default Recording Server Configuration Profile (8)

Step 4 - Select the **Change Configuration Settings** tab

Step 5 - In the server configuration list open the **Service Logging** node

Step 6 - Open the node for the service, and change the log level to the required level.



- Service Logging
  - Log Masking
  - Verba Storage Management Service

Log Level:	☑	Debug
Maximum Log File Size (bytes):	□	20000000
Maximum Number of Log Files:	□	10

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, and you will be redirected to the **Configuration Tasks** tab. Review the list of affected services and if service restarts are required (or the service is able to reread the new settings without a service restart). Click on the **Execute** button in order to execute the changes.

How to replace a service executable

Upgrading service executable can affect the recording functionality of your environment.
We recommend executing the upgrade during a maintenance window to avoid loss of recording and leave time for testing.

Step 1 - Download the executable provided by the Support Representative.

Step 2 - Open a Remote Desktop Connection to the affected server.

Step 3 - Open the Windows Services application.

Step 4 - Disable the Verba System Monitor Service and the Verba service you are about to update.

Stopping Verba System Monitor will prevent the automatic restart of the Verba services.

Step 5 - Open a File Explorer and navigate to %Verba_Install_Path%\bin folder. (Default install path is C:\Program Files\Verba)

Step 6 - Create a backup of the original executable in case you need to roll back to the original version.

Step 7 - Replace the new executable file in the %Verba_Install_Path%\bin folder.

Step 8 - Go back to Windows Service and start the Verba System Monitor and the updated Verba service.

Step 9 - Repeat the steps above on all affected Verba server.

Step 10 - Verify functionality by making tests.

How to update the Web Application

ⓘ We recommend executing the upgrade during a maintenance window to avoid loss of recording and leave time for testing.

Step 1 - Download the files provided by the Support Representative.

Step 2 - Open a Remote Desktop Connection to the affected server.

Step 3 - Open a File Explorer and navigate to %Verba_Install_Path%\tomcat/webapps/verba/WEB-INF/classes\com\verba\web. (Default install path is C:\Program Files (x86)\Verba)

Step 4 - Create a backup of the folders which will be affected by the upgrade in case you need to roll back to the original version.

Step 5 - Replace the content in the folders with the content in the ZIP file. Make sure that you are replacing the proper files at the right place.

Step 6 - Open Windows Services and restart the **Verba Web Application Service.**

Step 7 - Verify functionality by making tests.

Maintenance mode

Overview

In order to gracefully shut down a Verba server, the server or selected services can be put into maintenance mode. When maintenance mode is activated for a service or for a server, the system will notify all affected services and will gracefully stop the main functionality of the service(s) to prevent data loss or interruption. Maintenance mode is designed to support gracefully draining the resources on a server to be able to move the load to another server in redundant deployment configurations. Once maintenance mode is activated, the user interface shows the actual status of the service and the number of remaining active sessions. Once all active sessions are terminated gracefully, the service enters maintenance mode and can be shut down. The following table summarizes supported Verba services and the effect of activating maintenance mode:

Service Name	Maintenance Mode Description
Verba SfB/Lync Call Filter Service	Once maintenance mode is activated, the service will no longer attempt to start the recording process on new calls and will gracefully wait until all ongoing calls are ended. The service will maintain all active network connections, including the SfB/Lync Server API connection. The call blocking feature is also disabled in maintenance mode.
Verba SfB/Lync IM Filter Service	Once maintenance mode is activated, the service will no longer attempt to start the recording process on new conversations and will gracefully wait until all ongoing conversations are ended. The service will maintain all active network connections, including the SfB/Lync Server API connection. The conversation blocking feature is also disabled in maintenance mode.
Verba SfB/Lync Communication Policy Service	Once maintenance mode is activated, the service will no longer attempt to start controlling (block, filter) new conversations and will gracefully wait until all ongoing conversations are ended. The service will maintain all active network connections, including the SfB/Lync Server API connection.
Verba SfB/Lync Announcement Service	Once maintenance mode is activated, the service will gracefully wait until all ongoing P2P announcements are ended, then it will disconnect from the SfB/Lync Server API and from all Verba Passive Recorder Service. Once the service disconnects from the SfB/Lync Server API, all active conference call connections are terminated. The Verba Passive Recorder Service is able to detect this event and trigger another available Announcement Service to connect to the ongoing conference calls.
Verba Media Collector and Proxy Service	Once maintenance mode is activated, the service will notify all connected Verba SfB/Lync Call Filter Service to stop assigning new calls. The service will gracefully wait until all ongoing calls are finished.
Verba Passive Recorder Service	Once maintenance mode is activated, the service will no longer attempt to start the recording process on new calls and will gracefully wait until all ongoing calls are ended. If the service is connected to Verba Media Collector and Proxy Services, then it will notify them to stop assigning new calls to the recorder.
Verba Unified Call Recorder	Once maintenance mode is activated, the Media Recorder component in the service will no longer attempt to start the recording process on new calls and will gracefully wait until all ongoing calls are ended. The service will notify all connected Verba Recording Director components to stop assigning new calls to the recorder. The Recording Director component of the service will refuse any new connection or call setup attempt from the recorded platforms (for instance sending SIP BUSY), but will gracefully wait until all ongoing calls are terminated.
Verba Cisco Compliance Service	Once maintenance mode is activated, the service will no longer attempt to start controlling (record, block, filter) new conversations and will immediately stop recording/filtering all ongoing conversations. The service will close all EventBroker API connections with the CUPS servers.

Start maintenance mode

To activate maintenance mode, follow the steps below:

Step 1 - Using the web application, navigate to the **Administration / Verba Servers** page.

Step 2 - Select the server where maintenance mode needs to be activated.

Step 3 - Click on the **Service Control** tab.

Step 4 - Click on the
⏻
button to start the maintenance mode for the service or for all services supporting the feature on the server.

Step 5 - Wait until the service enters maintenance mode after gracefully ending its normal operations. Once the service is in maintenance mode, the service can be stopped and/or disabled.

Stop maintenance mode

To stop maintenance mode, follow the steps below:

Step 1 - Using the web application, navigate to the **Administration / Verba Servers** page.

Step 2 - Select the server where maintenance mode needs to be stopped.

Step 3 - Click on the **Service Control** tab.

Step 4 - The service has to be started first if it is not running.

Step 5 - Once the service is running, click on the
⬆
button to stop the maintenance mode for the service or for all services supporting the feature on the server.

Step 6 - Wait until the service enters normal mode.

How to change server IP address and hostname

There are different steps to take when you are changing the IP address and/or the hostname of different Verba components:

Changing Media Repository Address

1. In the menu structure navigate to Administration -> Verba servers -> Select the Media Repository that you want to change the IP address of -> Select the Change Configuration tab
2. Under *Network -> Server IP address* change the IP address
3. Click on the save button (floppy icon) at the top right corner of the frame
4. A yellow strip appears at the top of the page prompting to apply the configuration. Click on apply, then on the page click on the *Execute Selected Tasks* button
5. Open up services.msc on the Media Repository server (after gaining access probably through RDP) and restart the Verba Web Application service
6. Verify that all servers with Verba components can properly resolve the new hostname and IP address (verify eventual /etc/hosts overrides)

If you have Recording Servers, or Desktop Recorders that are uploading media to the Media Repository server's local disk, then also complete the following steps:

1. In the menu structure navigate to Administration -> Verba servers -> Select the Recording Server/Desktop Recorder -> Select the Change Configuration tab
2. Under *Storage Management -> Storage Targets -> Media Repository Local Disk -> Media Repository IP Address or Hostname* change the IP/hostname
3. Click on the save button (floppy icon) at the top right corner of the frame
4. A yellow strip appears at the top of the page prompting to apply the configuration. Click on apply, then on the page click on the *Execute Selected Tasks* button

ⓘ For Single Server deployments only the first 6 steps need to be completed. (And the other 4 if you have Desktop Recorders)

Changing Recording Server Address

1. In the menu structure navigate to Administration -> Verba servers -> Select the Recording Server -> Select the Change Configuration tab
2. Under *Network -> System -> Server IP address* change the IP
3. Click on the save button (floppy icon) at the top right corner of the frame
4. A yellow strip appears at the top of the page prompting to apply the configuration. Click on apply, then on the page click on the *Execute Selected Tasks* button
5. Verify that all servers with Verba components can properly resolve the new hostname and IP address (verify eventual /etc/hosts overrides)

If you are using the Cisco UC platform, then also change the recorder's IP in CUCM, as decribed in the Create and configure a SIP Trunk article.

If you are using SPAN-based recording for Microsoft Skype for Business (Lync), then also complete the following steps:

1. In the menu structure navigate to Administration -> Verba servers -> Select the Recording Server -> Select the Change Configuration tab
2. Under *Lync Filter -> Signaling Information Target Settings -> Recording Server(s)* change the IP/hostname of the Recording Server
3. Click on the save button (floppy icon) at the top right corner of the frame
4. A yellow strip appears at the top of the page prompting to apply the configuration. Click on apply, then on the page click on the *Execute Selected Tasks* button

If you are using other SIP-based telephony platforms, please point the system at the recording server's new IP/hostname.

Changing Desktop Recorder Address

The Desktop Recorder registers itself on the Recording servers with its current IP address. No configuration changes need to be completed on the verba components.
Change the IP/hostname and then verify that all servers with Verba components can properly resolve the new hostname and IP address (verify eventual /etc/hosts overrides)

Changing SQL Server Address

Please use the Microsoft documentation when you change SQL Server address: http://msdn.microsoft.com/en-us/library/ms143799(v=sql.105).aspx

Before changing the IP/hostname of the SQL server, complete the following steps on each Verba server (SfB (Lync) servers with Verba components are also considered to be Verba servers):

1. In the menu structure navigate to Administration -> Verba servers -> Select a server -> Select the Change Configuration tab
2. Under Database Connection -> *Database hostname* change the IP/hostname
3. Click on the save button (floppy icon) at the top right corner of the frame
4. A yellow strip appears at the top of the page prompting to apply the configuration. Click on apply, then on the page click on the *Execute Selected Tasks* button

> ⓘ When changing the database connection parameters on the Media Repository, you will lose the connection (and the ability to access the Web application altogether) until the database server becomes active on the new IP/hostname that you have configured. If you made a mistake in the configuration, then you will need to revert to the previous settings on the server itself in the Windows registry.

For a more detailed description please refer to the Moving the database to another SQL Server article.