A MITEL
PRODUCT
GUIDE

Unify OpenScape Voice Trace Manager

OpenScape Voice Trace Manager V8, Service Manual

Service Documentation
07/2024

A31003-H8080-S105-25-7620

Mitel

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Europe Limited. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos, and graphics (collectively “Trademarks”) appearing on Mitel’s Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively “Mitel), Unify Software and Solutions GmbH & Co. KG or its affiliates (collectively “Unify”) or others. Use of the Trademarks is prohibited without the express consent from Mitel and/or Unify. Please contact our legal department at iplegal@mitel.com for additional information. For a list of the worldwide Mitel and Unify registered trademarks, please refer to the website: http://www.mitel.com/trademarks.

© Copyright 2024, Mitel Networks Corporation

All rights reserved

Contents

1 History of Changes **8**

2 About This Guide **10**

3 Trace Manager Portal Benefits **11**

4 OSV-TM Tool Architecture **12**
4.1 OSV-TM Operating Sequence 12
4.2 Data Collection 13
4.3 Data Storage 13
4.4 Data Mapping in OSV-TM 14
4.5 Data Display, Selection, Analysis and Export 14

5 Trace Information Flow **16**

6 Trace Security **18**
6.1 Trace Configuration - Privacy Concerns 19
6.2 Safety - Password Concerns 19

7 OpenScape Voice Trace Manager End User Functionality **21**
7.1 Logon Related Tasks 21
7.1.1 How to Log into the Trace Manager Portal 21
7.1.2 How to Request Access 22
7.1.3 How to obtain a Temporary Password 22
7.1.4 How to Reset a Password 23
7.1.4.1 Password Policy for OSV-TM Accounts 24
7.1.5 How to Select an OSV System 24
7.2 OSV-TM System Views tabs 25
7.2.1 Home View 26
7.2.2 OpenScape Voice (OSV) System Views (main tabs) 26
7.2.3 OpenScape SBC View 27
7.2.4 OpenScape Branch (OSB) View 28
7.2.5 OpenScape Session Border Controller (SBC) View 29
7.2.6 Phone View 30
7.2.7 OpenScape UC (OSUC) View 31
7.2.8 HiPath Media Server (HMS) View 32
7.2.9 Xpressions (XPR) View 32
7.2.10 Contact Center Extensions (OSCCE) View 33
7.2.11 Administration View 34
7.3 Displaying OSV-TM Data 34
7.3.1 How to Change the Number of Rows per Page 35
7.3.2 How to Display Detail View 36
7.4 Filtering Trace Data 37
7.4.1 Restrictions on Setting Filter Dates 38
7.4.2 Default Filters 39
7.4.3 How to Set Filters for OSV-TM Data 39
7.4.4 How to Save Current Query for OSV-TM Data 42
7.4.5 How to Clear Filters 42
7.4.6 Advanced Queries 42
7.4.7 How to Filter an Existing Query 43
7.4.8 How to Create a New Query 43
7.4.9 How to Edit Existing Queries 45
7.4.10 How to Delete Queries 47

7.5 File Handling Option....47
7.5.1 How to Open CAP Files with Wireshark....48
7.5.2 How to Open Multiple Downloaded Cap Files....48
7.5.3 How to Analyze an Event File....50
7.5.4 How to Send Files via FTP....51
7.5.5 How to Zip and Download Files....52
7.5.6 Capture Query Results in a CSV Formatted File....53
7.5.6.1 How to Capture Query Results in a CSV Formatted File....53
7.5.7 Trace Manager (TM) Explorer....54
7.5.7.1 TM_Explorer Explorer Functionality....55
7.5.7.2 Overview....56
7.5.7.3 Trace Files....57
7.5.7.4 Job Status....58
7.6 Working with Graphs....59
7.6.1 Restrictions on Displaying Graphed Data....60
7.6.2 Graphs Navigation Frame....61
7.6.3 How to Zoom on a Graph's Time Interval....63
7.6.4 Hovering on a Graph's Point....63
7.6.5 Types of Graphs....64
7.6.6 Calls....65
7.6.7 Calls Effectiveness....66
7.6.8 Registration....67
7.6.9 Media Packet Traffic....68
7.6.10 Media Traffic Quality....69
7.6.11 New and Stable Calls....70
7.6.12 SIP Messaging....71
7.7 Performance Monitoring from/to a Branch....71
7.7.1 How to Access Branch Status Report....72
7.7.2 How to Set Filter for Branch Status Report....72
7.7.3 How to use the Branch Graphs....74
7.7.4 OpenScape Branch Graph Types....76
7.7.4.1 OpenScape Branch Graph: All Calls....76
7.7.4.2 OpenScape Branch Graph: Originating On Net Calls....77
7.7.4.3 OpenScape Branch Graph: Originating Off-Net Calls....77
7.7.4.4 OpenScape Branch Graph: Terminating On-Net Calls....78
7.7.4.5 OpenScape Branch Graph: Terminating Off Net Calls....78
7.8 OpenScape Voice Resource Graphs....78
7.8.1 How to Use Resource Graphs....79
7.8.2 Resource Graph: CPU Usage....84
7.8.3 Resource Graph: CPU Core Usage....84
7.8.4 Resource Graph: Performance....85
7.8.5 Resource Graph: Memory Usage....86
7.8.6 Resource Graph: Swap Memory Used....86
7.8.7 Resource Graph: Swap Frequency....87
7.8.8 Resource Graph: Logging....87
7.8.9 Resource Graph: Process Queues....89
7.8.10 Resource Graph: Ethernet I/O....90
7.8.11 Resource Graph: Disk I/O....90
7.8.12 Resource Graph: Registration and Call Statistics....91
7.8.13 Resource Graph: Database....92
7.8.14 Resource Graph: Disk Partition Fill Level Percentage....94
7.9 Call Analyzer....94
7.9.1 Call Analyzer Analysis Screen....95
7.9.2 Call Analyzer Call Data Screen....96
7.9.3 Call Analyzer Call Data Screen Working with Mouse....100
7.9.4 Call Analyzer List Data Screen....100

7.9.5 Call Analyzer Sequences Screen..... 102
7.9.6 Call Analyzer Statistics Screen..... 103
7.10 OpenScape Voice Obfuscation tool..... 104

8 Administration Tasks for Trace Manager..... 107
8.1 Where to Find the OSV-TM Application..... 107
8.2 Hardware Requirements..... 107
8.3 3rd Party Software Product Requirements..... 109
8.4 Pre-Installation Requirements: What is needed before OSV-TM Installation..... 113
8.4.1 How to Enable .NET Framework on Windows 2008 R2..... 113
8.4.2 Trace Data Storage Planning..... 114
8.5 Migration from an Earlier OSV-TM Version..... 115
8.6 Migrating an OSV-TM Server on Windows 2003 to Windows 2008 R2..... 116
8.6.1 OS Upgrade Preparation: OSV-TM Backup..... 117
8.6.2 Upgrade Server to Windows 2008 R2..... 118
8.6.3 Installing OSV-TM and Migrating Data..... 118
8.7 Installation of OSV-TM..... 119
8.7.1 How to install OSV-TM on Windows 2008 R2 or newer..... 120
8.8 Fresh Installations: Required Post Installation Configuration..... 123
8.8.1 How to Generate a Digital HTTPS Certificate for the OSV-TM Server..... 123
8.8.2 Enabling/Disabling OSV-TM Communication Ports with the OSV-TM Firewall Security Manager..... 125
8.8.3 How to Run the "OSV-TM" Firewall Security Manager..... 126
8.8.4 How to Enable\Disable Remote Internet Browser Access to The OSV-TM Web Portal (FADE)..... 126
8.8.5 Setting up the FTP Windows Server and SFTP Support..... 128
8.8.5.1 How to Create the OSV-TM FTP/SFTP Server Account..... 128
8.8.5.2 FTP Server Functionality..... 129
8.8.5.3 How to Modify Windows Firewall Rules..... 130
8.8.5.4 Secure FTP (SFTP) Support..... 131
8.8.5.5 Configuring Multiple SFTP Accounts for Trace Data Transfer..... 132
8.8.5.6 How to Create Additional SFTP User Accounts..... 132
8.8.5.7 Additional 3rd Party Software Required Configuration..... 133
8.8.5.8 How to Configure OSV-TM as a Trusted Site..... 133
8.8.5.9 How to Disable IE Enhanced Security Configuration..... 135
8.8.5.10 Additional Configuration Required in OSV-TM to Display OpenScape Branch and Session Border Controller Performance Monitoring Graphs..... 136
8.9 Upgrading from an Earlier OSV-TM Version..... 137
8.9.1 Upgrading Strategies - Systems Upgrading from OSV-TM V1R3 and Earlier..... 139
8.9.1.1 Clean Upgrade..... 139
8.9.1.2 How to Start a Clean Upgrade..... 140
8.9.1.3 Re-process all Traced Data Files..... 140
8.9.1.4 How to Upgrade with Re-process All Traced Data Files..... 140
8.9.1.5 Partial Trace Data Re-processing..... 141
8.9.1.6 How to Upgrade with Partial Trace Data Re-processing..... 142
8.9.1.7 How to Perform an Upgrade Installation..... 143
8.9.1.8 Manual Upgrade of Additional 3rd Party Software..... 147
8.10 Uninstallation of OSV-TM..... 148
8.10.1 How to Stop FTP Transfer Configuration from OpenScape Voice Server V3.x..... 148
8.10.2 How to Stop OpenScape Voice Trace File Transferring for OSV Server V4 and Later..... 149
8.10.3 How to Stop Further Trace Processes..... 150
8.10.4 Removing OSV-TM Base and 3rd Party Software..... 150
8.10.5 How to Run the Uninstall OSV-TM Server Utility..... 150
8.10.6 Additional Manual Removal Procedures..... 153
8.11 Configuring OSV-TM through FADE..... 154
8.11.1 Adding/Removing OSV-TM Systems..... 156
8.11.2 How to Add a System..... 156
8.11.3 How to Remove an OSV-TM (OpenScape Voice) System..... 158

8.11.4 Manual Post-System Removal Cleanup..... 159
8.11.5 Configuration OSV-TM Systems..... 159
8.11.6 How to Set Database Parameters - SQLite Configuration.....160
8.11.7 How to Set Email Parameters.....161
8.11.8 How to Set DIPAZ Configuration..... 161
8.11.9 How to Read the Trace Folder tab..... 162
8.11.10 How to Set Other Configuration Fields..... 163
8.12 Configuring the OpenScape SBC Listener, and Phone Listener for an OSV-TM System.....165
8.12.1 How to Add, Remove and Configure OpenScape SBC Tracing to an OSV-TM System..... 165
8.12.2 How to Manage Phones in an OSV-TM System.....168
8.13 Configuring Tracing on Devices to Integrate with the OSV-TM Server.....170
8.13.1 Pre-Setup for Trace File Exporting (FTPing) to OSV-TM Server.....171
8.13.1.1 How to Set Up Packet Filtering Role for FTP Connection..... 171
8.13.1.2 How to Configure Denial-of-Service Prevention.....172
8.13.2 Configuring OpenScape Voice Server V3.1R2 and V3.1R3.....172
8.13.2.1 Transfer Tracing Scripts to the OpenScape Voice Server.....172
8.13.2.2 How to Transfer Tracing and Configuration Scripts to OSV Server V3.1 PS0035 and Prior Releases.....173
8.13.2.3 How to Transfer Tracing and Configuration Scripts to OSV Server V3.1 PS0036 and Above..... 174
8.13.2.4 Set Up Tracing and Configure FTP Transfer to OSV-TM Server..... 174
8.13.2.5 Configuration Script "setup_tracing.ksh".....175
8.13.2.6 Transfer Script "setup_trace_transfer.ksh".....175
8.13.2.7 How to Set Script Permissions and Modes.....175
8.13.3 Configuration of Tracing and File Transferring for OpenScape Voice Server V7R1 and Later Releases..... 177
8.14 Setting up Tracing for OpenScape SBC..... 177
8.14.1 How to Enable OpenScape SBC Tracing from the OSV Assistant CMP.....178
8.14.2 How to Disable OpenScape SBC Tracing from the OSV Assistant CMP.....178
8.14.3 How to Enable OpenScape SBC Tracing from the SIP Object CLI Interface..... 179
8.14.4 How to Disable OpenScape SBC Tracing from the SIP Object CLI Interface..... 181
8.15 Configuring Phone Devices to Send QoS Data and Tracing to OSV-TM..... 181
8.16 How to Configure Phone Devices to Send QoS Data to OSV-TM Listener.....182
8.16.1 How to Configure OptiPoint Phone Devices to Send QoS Data to OSV-TM.....183
8.16.2 How to Configure OpenStage Devices.....183
8.16.3 How to Configure OpenStage Phone Devices..... 184
8.17 Setting up Tracing for OpenScape Branch..... 185
8.18 Setting up Tracing for OpenScape Session Border Controller..... 186
8.19 Setting up Tracing for OpenScape UC..... 186
8.20 Setting up Tracing for the HiPath Media Server..... 186
8.21 Setting up Tracing for Xpressions.....187
8.22 Setting up Tracing for Contact Center Extensions (OSCCE).....187
8.23 Stopping or Re-starting OSV-TM Services..... 187
8.23.1 How to Restart DIPAZ Monitor..... 188
8.24 User Accounts Administration..... 188
8.24.1 How to Create a User Account.....188
8.24.2 How to Delete a User Account..... 189
8.24.3 How to Reset Password..... 190
8.24.4 How to Change Access Level..... 190
8.24.5 How to Manage User Account Request..... 191
8.24.6 Password Security Rules..... 191
8.24.7 How to Disable Password Security Rules..... 192
8.25 OSV-TM Database Optimization Schemes.....193
8.25.1 Types of OSV-TM Database Partitioning Schemes.....193
8.25.2 DB Partitioning Screen for New Systems.....194
8.25.3 Database Partitioning Scheme for Existing Systems.....194
8.25.4 How to Change the DB Partition Scheme..... 195

8.26 Using a RAM Drive Storage for Performance Solutions....196
8.26.1 How to Enable RAM Drive on New OSV-TM Installations....197
8.26.2 How to Enable RAM Drive Feature during an OSV-TM Upgrade....198
8.26.3 How to Enable the RAM Drive on an Existing OSV-TM Installation....199
8.26.4 How to Migrate or Move an Existing OSV-TM System to A RAM Drive....200
8.26.5 How to Create a New OSV-TM System on a RAM Drive....201
8.26.6 How to Increase the Size of the RAM Drive....203
8.26.7 Troubleshooting RAM Drive Issues....204
8.27 OSV-TM Performance Guidelines....204
8.28 OSV-TM Automated Maintenance Processes and Backup....205
8.29 Monitoring OSV-TM Status and Processes Logs....206
8.29.1 How to Access OSV-TM Administraton Logs....206
8.30 Configuring OSV-TM through configuration file....207
8.30.1 How to Store SIP Notify Messages....207

9 Reconfiguration Procedure after Restoring An OSV-TM Server from Windows Backup....209

10 How to Report Problems/Bugs....210

Index....211

1 History of Changes

Issue	Date	Change Description
24	09/2023	Document to OSV Git Duplicates changed to Duration under Performance in "OpenScape Voice (OSV) System Views (main tabs)" chapter.

Issue	Description
23	-
22	-
21	-
20	Added support statement for Windows Server 2019 - 64 bit Standard Edition
19	Two new sections, Configuring OSV-TM through configuration file and How to Store SIP Notify messages have been added.
18	Section Configuring Phone Devices to Send QoS Data and Tracing to OSV-TM has been updated with a new note regarding phone devices.
17	Section Hardware Requirements has been updated.
16	Sections Cipher configuration to also support aes-cbc mode and Fix OpenSSH log file permissions and reduce log level of chapter 3rd Party Software Product Requirements have been updated.
15	Section SFTP/SSH Server of chapter 3rd Party Software Product Requirements has been updated.
14	Chapter Administration Tasks for Trace Manager has been updated with a new note. The Note in section Installing SSH software of chapter 3rd Party Software Product Requirements has been updated. Chapter SFTP Installations on Unify Servers has been removed. Updated step 6.b in chapter Additional Manual Removal Procedures The image in step 2.c in chapter How to Run the Uninstall OSV-TM Server Utility has been updated, the section Security Settings removed and the section Important Uninstall Notes updated.
13	Section Registration Failures in chapter Registration has been updated.
12	Support of Windows 2016 server has been added across the document.
11	Updated the link in chapter How to Enable RAM Drive on New OSV-TM Installations
10	Chapter 3rd Party Software Product Requirements has been updated with two new sections Cipher configuration to also support aes-cbc mode and Fix OpenSSH log file permissions and reduce log level and chapter Additional Manual Removal Procedures has been updated with a new Step 1.
9	Chapters How to Install an FTP Server on Windows 2008 R2 Server and How to Configure an FTP Server on Windows 2008 R2 have been removed. Chapter How to install OSV-TM on Windows 2008 R2 has been renamed to How to install OSV-TM on Windows 2008 R2 or Windows 2012 R2. Step 4 in chapter How to Generate a Digital HTTPS Certificate for the OSV-TM Server has been updated.
8	A new chapter OpenScape Voice Obfuscation tool has been added.
7	A new chapter OSV-TM Performance Guidelines has been added.

Issue	Description
6	Changed product name to OpenScape Voice Trace Manager and the version to V8. Added section SFTP/SSH Server in chapter 3rd Party Software Product Requirements. Updated chapters Secure FTP (SFTP) Support, SFTP Installations on Unify Servers, How to Run the Uninstall OSV-TM Server Utility and How to Perform an Upgrade Installation. Deleted chapter How to Configure SFTP User Account.
5	Updated Section Secure FTP (SFTP) Support
4	Updated Section Resource Graph: Registration and Call Statistics
3	Updated Section How to Configure Denial-of-Service Prevention
2	Updated Section Resource Graph: Registration and Call Statistics
1	First issue

2 About This Guide

This book provides an overview of the OpenScape Voice Trace Manager software application and provides step-by-step procedures for both the basic user and the system administrator.

Intended Audience

This guide is intended for OpenScape Voice support personnel.

3 Trace Manager Portal Benefits

The benefit of the OSV-TM is the capability to correlate the data collected from all the OpenScape Voice Solution components and provide the means to analyze the data and identify the corresponding trace files that contain detailed information to aid in a faster correction of the problem.

Benefits Overview

The benefits of the OSV-TM include:

- Long-term storage of OSV trace files to support error debugging by OSV development
- Fast identification of trace files containing data associated with a particular call, error condition, or time frame
- Export of trace files to a remote server (e.g., customer service or development server)
- Database queries to find and display calls and SIP registrations filtered by directory number, time, and error condition
- Graphical display of OSV signaling and registration traffic supporting easy recognition of network failures and/or abnormalities
- Improved diagnosis capability assisting in the identification of the root cause of an error condition thereby expediting the resolution

This continual capture of trace data and the ability to filter trace data significantly reduces the amount of time required to resolve error conditions, especially for large customer networks.

The data collected by the OSV-TM is primarily used for error resolution purposes. Once the proper corrective action is taken and the error correction resolved, the trace data is no longer needed and it can be deleted by the user. A data aging function of the application aids with this task.

4 OSV-TM Tool Architecture

OpenScape Trace Manager provides the ability to collect and correlate OpenScape Voice Solution trace files 24 hours a day, seven days a week.

For the diagnosis of complex, non-reproducible or sporadic voice communication problems in the OpenScape Voice Solution, trace data is collected and stored for longer periods of time. Trace data is comprised of signaling messages (e.g., SIP, CSTA, and MGCP) sent and received by the OpenScape Voice Server.

Manual trace data can be collected and stored via 3rd party tools (e.g., NetScout Sniffer Portable Analyzer, Wireshark / Ethereal, 3Cdaemon) or by using the onboard integrated tools, such as:

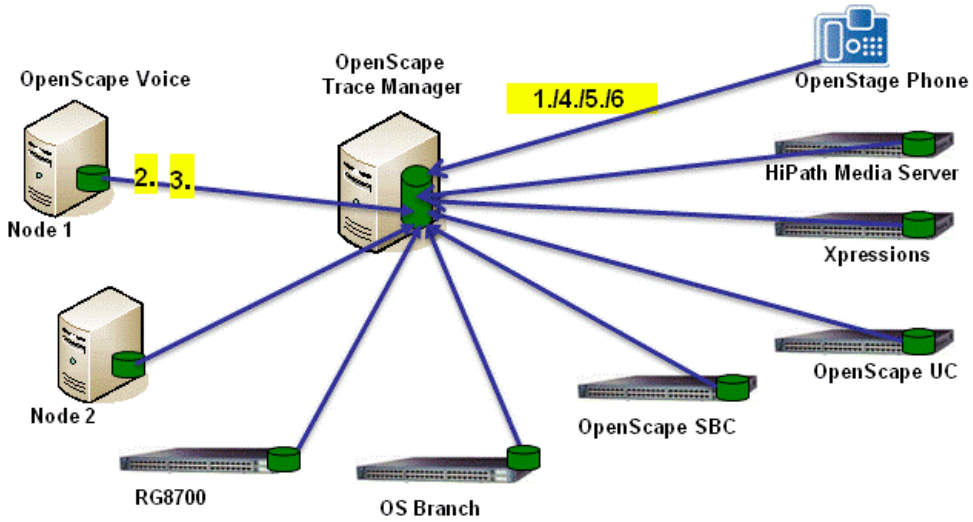
- OpenScape Voice: Real Time Tracing (RTT)
- OpenScape SBC: Real Time Tracing (RTT)

However, these methods have the following limitations:

- The onboard tools where designed to capture trace data for a limited time period and only for individual components.
- Third party tools must be routinely checked to ensure that the data collection is still active.

OSV-TM, on the other hand, can collect trace files 24x7 and store them for longer periods of time.

4.1 OSV-TM Operating Sequence



The example in this figure depicts the tracing and data files collection sequence.

The numbered items below correspond to the numbers within the figure.

1) Configure tracing on the OSV
2) Trace data is collected on the OSV node and stored in files
3) The trace data files are pushed to the OSV-TM server
4) Trace data files are stored, parsed and indexed
5) Data can be filtered, analyzed and displayed (by directory number, IP address, time, data) from OSV-TM

6) Export trace data files

An OSV trace data record consists of the following entries:

- Calling or called DN (Directory Number)
- Data
- Time stamp
- Call IDs
- Message Type

The OpenScape SBC Gateway is configured for continuous tracing and it streams data to the OpenScape SBC Listener component on the OSV-TM server. The data collected is parsed and stored in cap and event files.

The OpenScape Branch, Session Border Controller, OpenScape UC (UC), Xpressions (XPR), HiPath Media Server (HMS) and OpenStage Phone (PH) are configured for tracing and generate trace files. These files are sent to the OSV-TM server where they are stored and processed.

OSV-TM also collects trace files from the Contact Center Extension (Concierge).

NOTICE:

The necessary configuration steps for Contact Center Extensions (Concierge) can be found in the latest issue of the "OpenScape Contact Center Extensions V3, Configuration Concierge, Administrator Documentation".

4.2 Data Collection

Data collection entails the starting/stopping of continuous tracing and enabling/disabling trace file copying to the OSV-TM server.

For the OpenScape Voice, the Real Time Trace GUI is run from the OSV-TM server to start/stop and configure tracing and to set up the files transfer to the OSV-TM server.

Tracing on the OpenScape SBC is enabled via the Common Management Platform (CMP) OpenScape SBC Assistant interface or from the OpenScape SBC’s Command Line Interface (CLI).

Tracing and transferring of the trace files for the OS Branch and Session Border Controller are configured through the CMP OpenScape Branch Assistant interface.

4.3 Data Storage

Data collected in OSV-TM is stored in two formats: files and database records.

The trace files received from the OpenScape Voice Solution components and from the cap and event files generated during the parsing process are stored in a local directory called “Tracedata.”

Trace files are parsed and the processed data is stored in an internal database.

Storage Size and Use

The size required for trace data storage depends on whether the trace files are gzipped or not. The unzipped trace file size is generally configured to 20 MB. The zipped file size is about 3 MB. A 1 TByte drive is recommended for the OSV-TM server.

NOTICE:

One SIP call may produce about 1 MByte of trace data.

Trace files stored on the OSV server are deleted once sent to the OSV-TM. Trace files stored on the OSV-TM server are deleted automatically after a configurable number of days (the default is 10 days on the OSV-TM) or when space is needed for newer trace files.

4.4 Data Mapping in OSV-TM

The interface of an OSV node with the OSV-TM server is identified by an OSV-TM "system" name. This OSV-TM system name is used to access the trace data processed for the related OpenScape Voice Server node, OpenScape SBC, OpenScape Branch, OpenScape Session Border Controller, OpenStage Phone, OpenScape UC, HiPath Media Server and Xpressions.

OpenScape Voice Servers configured in a cluster or dual node (duplex) system are identified by the same "OSV-TM system name"; therefore, both nodes are configured with the same SFTP target system.

All trace files from both nodes are transferred to the same OSV-TM "system" folder under the "\Tracedata" storage directory, i.e., \tracedata\<system-name>.

4.5 Data Display, Selection, Analysis and Export

End users and system administrators use the FADE (Filtering, Analysis and Data Export) tool for displaying, selecting, analyzing and exporting data. A graphical plotting for some data can also be displayed.

The FADE tool can be used by end users and administrators when attempting to locate and analyze trace data for a specific issue, problem or error condition. Specific information about the fault, such as time of occurrence, directory numbers involved, errors observed, etc., can be used as filtering criteria.

Functional Sequence

FADE provides a GUI interface to the following functionalities:

1) Data Filtering: The user can enter any combination of search criteria and the tool will search the stored index data to locate and identify the trace files associated with the requested data.
2) Data Analysis: The user can access basic analysis tools against the selected data, i.e., opening PCAP files with Ethereal (if installed).
3) Data Exporting: The user can request that the related trace data files be exported using SFTP or HTTPS download.

Data Export Information

The FADE tool can be instructed to transport selected trace files to another server using SFTP. SFTP transfer rates range from 2 Mbit/sec to 400 Mbit/sec.

5 Trace Information Flow

The Trace Information Flow describes the interactions between the OpenScape Voice System (OSV), the OpenScape Voice-Trace Manager Interface (OSV-TM), users and external servers.

OpenScape Voice

- Trace statements are collected in a trace buffer
- The trace buffer content is stored in trace files
- Trace files are transferred via SFTP to the OSV-TM server

OpenScape Voice <-> OpenScape Voice-Trace Manager

- The push method is protected by SFTP user id and password
- It is only possible to pre-configure on the OSV the IP address of the OSV-TM server, not on its name. This is enforced by OSV packet filter rules.
- Files are deleted from the OSV node after they have been successfully sent to the OSV-TM server or when space is needed to accommodate newer files

OpenScape Voice-Trace Manager

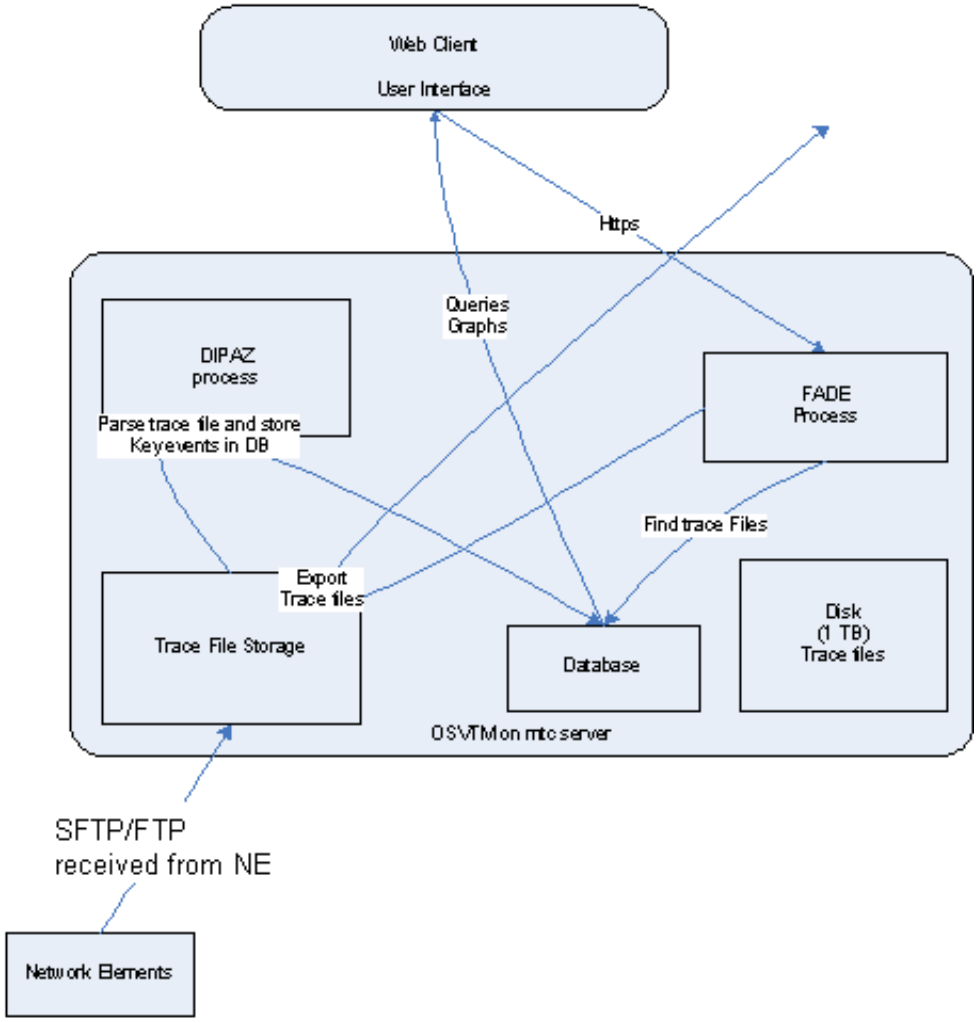
- Trace files are stored in a trace file directory
- Trace files are deleted after a specified time
- Trace files are parsed for external signaling messages and main signaling information is stored in a database (e.g., time, type of message, directory number, Call ID, error code)
- Data records are deleted based on an aging parameter configured on the OSV-TM server

OpenScape Voice-Trace Manager <-> User

- Data queries and traffic graphs are visible via a Web client

OpenScape Voice-Trace Manager <-> External Server

- The trace files identified by time, directory number, error code, etc., can be exported to the user’s client machine via SFTP.



Limitations

Statically the number of supported network elements is:

- 20 OSV servers
- 50 OpenBranches
- 50 OpenScape SBCs
- The number of OpenStage phones is not limited

Related tasks

How to Set DIPAZ Configuration on page 161
How to install OSV-TM on Windows 2008 R2
How to install OSV-TM on Windows 2003 Server

6 Trace Security

The collected trace data can contain system and user sensitive data.

The OpenScape Voice Trace Manager (OSV-TM) application allows for the collection and parsing of trace data information from different OpenScape (OSC).

This data can be used for analysis and troubleshooting of problems in an OpenScape Solution. It is assumed that the environment where the OSV-TM server runs is secured; on instances where security is a concern, a stricter configuration is advised for the server.

FADE, the OSV-TM web client interface uses SSL to connect to the OSV-TM server. Transactions are sent via https. A default certificate is included in the OSV-TM server installation package; a personalized certificate for the server can be generated by the OSV-TM administrator.

The data collected on the trace files by each device has only the minimal information about the flow of a call required to analyze a problem in the path.

The origination and destination DN or telephone numbers, the IP addresses of the devices involved in the processing of the call flow, and the acknowledgement statements are captured on the traces.The actual content of the call is not included in these trace files.

Presumably, the OSV-TM server and integrated OSC devices are hosted on a secured network based on the safety measures of your company.

The following security measures are provided:

- Access to the data and safeguards for the data
  - Trace data files stored on OSV are only accessible with the ‘srx’ and ‘root’ administrative accounts
  - Trace data files stored on the OSV-TM server are only accessible to the MS Windows user logged on as “tracedata” or “administrator”
  - OSV-TM Database:

    Local Read only is allowed for the MS Windows user logged on as “administrator” and for the SQLite account user.

    The Web interface accesses data in read-only mode; a FADE account protected with user-id and password is required to login. Two access roles are available: administrator or user role.
  - Remote Trace Analysis:

    Remote access to the data is only possible via remote desktop into the OSV-TM server (MS Windows administrator) and through a Web client which is disabled by default.
- Data Storage

  The OSV-TM database stores trace data taken from external SIP, CSTA and MGCP messages, as well as OSV platform resource usage data (such as CPU memory, etc.) and QOS data retrieved from the phone reporting the quality of the voice connection. Non-message data is limited to statistics derived from the messages and links to the associated trace files. The trace files contain additional data useful for debugging. There is no difference

between the trace files stored on the OSV-TM server and the files stored on the OSV disk.

Trace files stored on the OSV node and on the OSV-TM server are deleted automatically after a configurable number of days.

6.1 Trace Configuration - Privacy Concerns

Information stored in trace files can be used to find out who called whom, how often a call was placed, when a call was placed, for how long a call was up before cleared/disconnected, and what features were used on a call. Due to the sensitivity of this information, the end user should follow appropriate sensitive data protocol.

6.2 Safety - Password Concerns

User-ids and passwords for the OSV to OSV-TM trace file copy process are stored on the OSV disk and only readable by its administrator.

The SFTP password required to connect to the OpenScape Voice node from the RTT Trace Management Tool on the OSV-TM server is not displayed by default; it has to be entered/typed by the administrator. The SFTP server password stored on the OSV is encrypted.

Functional Sequence

OSV-TM Server

- The OSV-TM trace analyzer and filter software runs locally as a service and is secured by the Windows Administrator user-id and password.
- Remote access is possible via remote desktop.

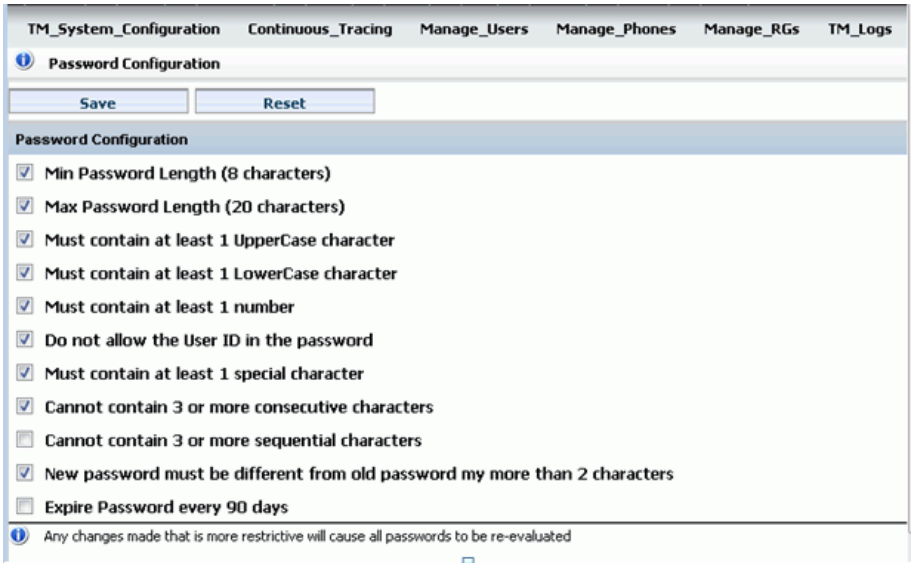
OSV-TM Client

- Remote web access to the OSV-TM is controlled by the OSV-TM client user-id and password.
- Password complexity is enforced for the OSV-TM web client.
- OSV-TM Web interface login attempts are logged (i.e., user name, IP address, and time).

Password and PIN Policy

The severity of a password/PIN vulnerability is dependent on the use case (client access, administration access) as well as the location (local access only or remote access).

The figure below summarizes the password configuration:


TM_System_Configuration
Continuous_Tracing
Manage_Users
Manage_Phones
Manage_RGs
TM_Logs
Password Configuration
Save
Reset
Password Configuration
Min Password Length (8 characters)
Max Password Length (20 characters)
Must contain at least 1 UpperCase character
Must contain at least 1 LowerCase character
Must contain at least 1 number
Do not allow the User ID in the password
Must contain at least 1 special character
Cannot contain 3 or more consecutive characters
Cannot contain 3 or more sequential characters
New password must be different from old password my more than 2 characters
Expire Password every 90 days
Any changes made that is more restrictive will cause all passwords to be re-evaluated

7 OpenScape Voice Trace Manager End User Functionality

The following functionality is available to the OSV-TM user: logon related tasks, how to access to a target system, how to display data, accessing the OSV-TM FADE Portal "views", how to filter data, trace filing handling procedures and the steps to follow when reporting a trouble condition.

7.1 Logon Related Tasks

This section includes procedures for logging into the OSV-TM system, and addresses the most basic access related procedures, i.e, requesting a password, password reset, etc.

7.1.1 How to Log into the Trace Manager Portal

The OSV-TM data is accessed via the Trace Manager Portal (FADE). End users connect remotely through a Web browser using FADE's remote access URL which is provided by the administrator. OSV-TM administrators can connect to the Web interface locally on the OSV-TM server by clicking on the FADE icon on the server's desktop.

Prerequisites

Only the following web browsers are supported: Internet Explorer V8 and V11, Mozilla Firefox.

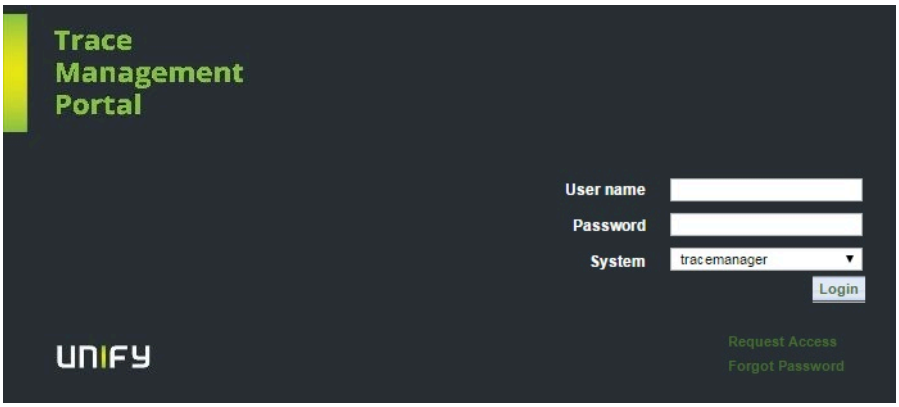
"Cookies" and "Pop-up Windows" requests from the OSV-TM server must be authorized on the web browser for FADE to function properly.)

Step by Step

1) Access locally from the OSV-TM server by clicking on the **FADE** icon on the server's desktop or, if remote, by typing the FADE URL provided by the administrator on the Internet Browser.

   The security certificate from the OSV-TM server must be accepted to access the portal.

   The remote access URL is structured as: https://<server-name>:28081/FADE/public/index.php/login



2) Enter *<username>* (case sensitive)
3) Enter *<password>* (case sensitive)
4) Click on the **System** drop down menu.
5) Select your system.
6) Click **Login**

7.1.2 How to Request Access

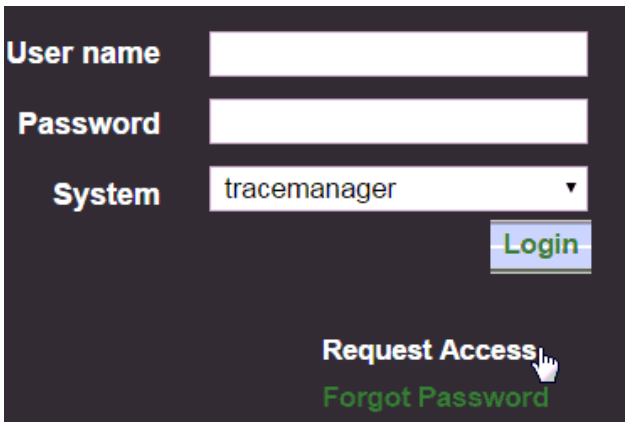
User accounts can be requested via the FADE login screen by clicking on the "Request Access" link.

Prerequisites

Access to the Open Trace Manager Portal (FADE) logon screen.

Step by Step

1) Open the Trace Manager Portal (FADE) web interface logon screen.



2) Click **Request Access**
3) Enter: *<first name> <last name> <e-mail address>* in the appropriate fields.
4) Click **Submit**
5) Contact the administrator to complete the registration process.

7.1.3 How to obtain a Temporary Password

The "Forgot Password" feature is used to obtain a temporary password; with a temporary password, the user can access the system and reset their password.

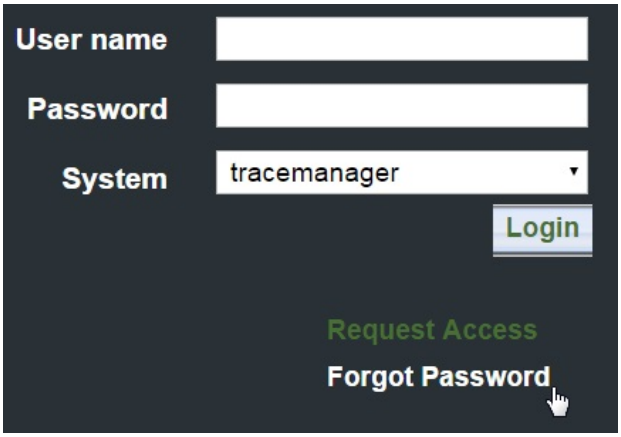
Prerequisites

An existing user id and password.

Access to the Trace Manager PortalTrace Manager Portal (FADE) web interface login screen.

Step by Step

1) Open the Trace Manager Portal (FADE).



2) Click **Forgot Password** (in the login screen)
3) Enter: *<user id>*
4) Click **Submit**

   A temporary password is emailed to the user. You will be prompted to change your password when logging in.

7.1.4 How to Reset a Password

The Reset Password feature allows the user to update their password as needed.

Prerequisites

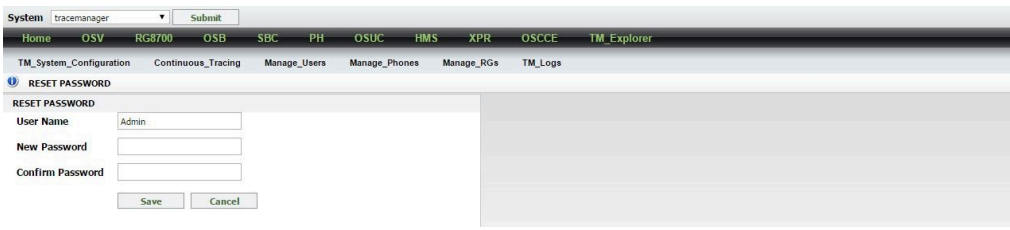
An existing user id and password.

Access to the Trace Manager Portal (FADE) web interface login screen.

Step by Step

1) Login to Trace Manager Portal (FADE).
2) Click on **Reset Password**

   The Password Policy is described in the next section below.



3) Enter the new *<password>*
4) Re-type the *<password>*
5) Click **Save**

7.1.4.1 Password Policy for OSV-TM Accounts

OSV-TM enforces the following account password rules to ensure better security on user accounts. You will need to adhere to these rules when resetting your password.

- Minimum password length = 8 characters
- Maximum password length = 20 characters
- Password should contain at least 1 uppercase character
- Password should contain at least 1 lowercase character
- Password should contain at least 1 number
- User account name should not be part of the password
- Password should contain at least 1 special character
- Password should not contain more than 3 sequential characters in a row
- Password should not contain more than 3 identical characters in a row
- A changed password should have at least 2 characters difference from the original password
- User account name in reverse should not be part of the password
- User password is reset every 90 days

These additional rules may be enabled by your administrator:

- Password should not contain more than 3 sequential characters in a row
- Password should not contain more than 3 identical characters in a row

7.1.5 How to Select an OSV System

:A "system" is the name given to identify an instance of an OpenScape Solution component that interfaces with the OSV-TM server. The system name gives access to the trace data processed for its related OpenScape Voice Server node, OpenScape SBC, Phone QoS data, OpenScape Branch, Session Border Controller, OpenScape Unified Communications, and/or HiPath Media Server, and Xpressions server. FADE, the Trace Manager Portal, provides access to all the systems that have been configured in the OSV-TM server. The procedure below describes how to switch to a different system after log in.

Prerequisites

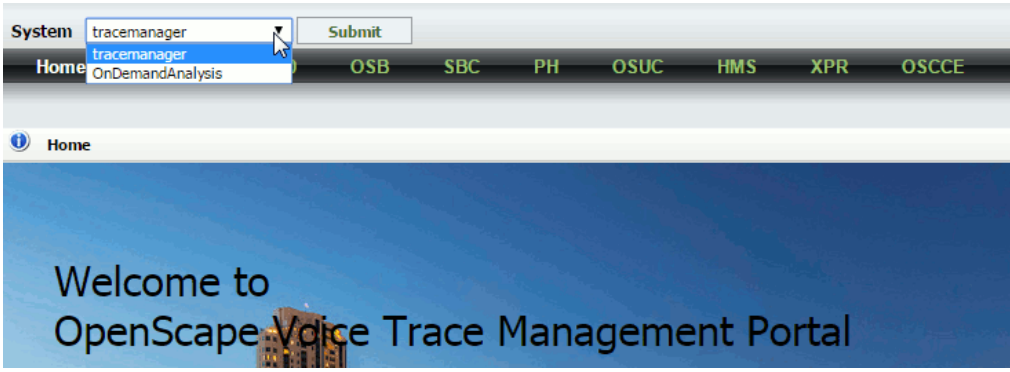
The user is logged into Trace Manager Portal (FADE).

Step by Step

1) Click on the **System** drop down menu in the upper left hand corner of the screen.

The drop down list displays the system names for all of the systems that have been configured in the OSV-TM server.

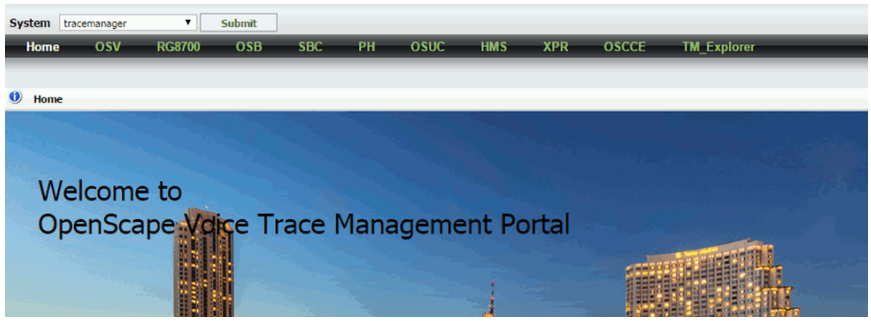
2) Select the appropriate **System** from the drop down list.



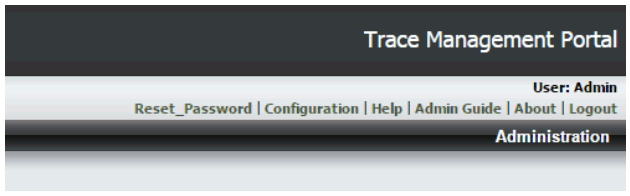
3) Click **Submit**

7.2 OSV-TM System Views tabs

A "view" is the main tab in FADE that gives access to the trace data processed in an OSV-TM system. The following user views are currently active in the OSV-TM FADE Portal: Home, OSV, OpenScape SBC, OSB, SBC, PH, OSUC, HMS, XPR, OSCC-E and TM_Explorer.



In addition, a user with administrator privileges has access to the "Administration" view which gives access to the system Configuration screens; this view is restricted.



To access a view, click on the corresponding tab on the top of the screen.

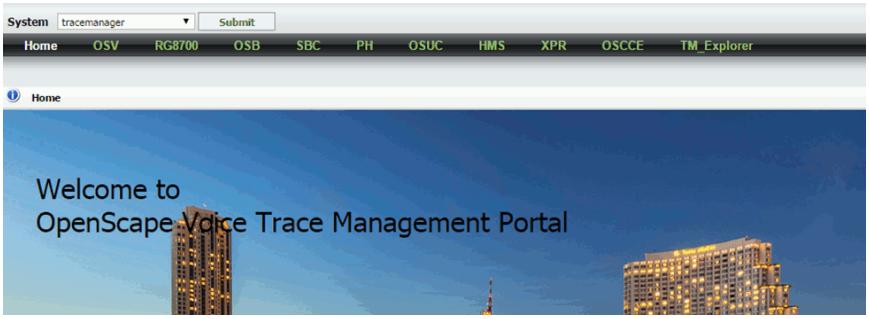
Through all these views, you have the ability to filter data, view call details, open related trace files directly and transfer files to your local site for further analysis.

7.2.1 Home View

The home view displays the OSV-TM Welcome screen.

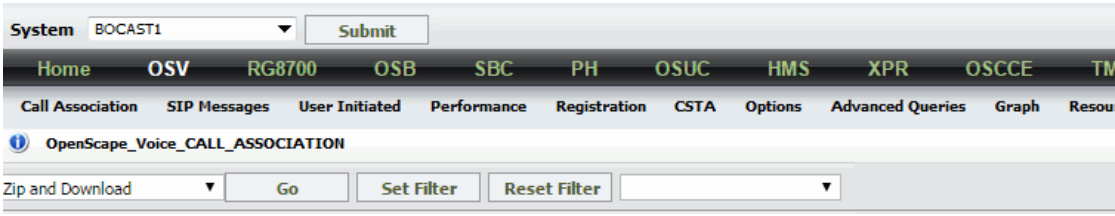
Functional Sequence

This screen appears after the user successfully logs on.



7.2.2 OpenScape Voice (OSV) System Views (main tabs)

This view displays trace data for the current OSV integrated to the system. If no trace data is being generated and/or transferred to the OSV-TM system, the message "No Data available" is displayed.



The tabs are defined as follows:

- Call Association - Shows A-side and B-side of all calls
- SIP Messages - Detailed information about each leg of a call
- User_Initiated - Lists the calls that have been traced from a "user initiated" action; these traces are identified by a unique "Trace ID" that maps to the "CallID". See description on the "PH" view below.
- Performance - Measures the Quality of Service for a call as provided from the OSV traces. The following data is displayed:
  - Date: Date and time when the call was started
  - CallID: Unique identification number for the call
  - DNA: Telephone number of the call originator
  - DNB: Telephone number of the call terminator
  - Sent: number of packets sent during the call
  - Recv: number of packets received during the call
  - Loss: Indicates the number of "Voice Packet Loss" experienced for the call. It occurs during a surge on network traffic causing a network router to drop data packets. The performance of an IP call suffers greatly if a

packet loss reaches more than 5 percent. This is detected on the call as dropped conversations or small sounds.
  - Jitter: Indicates the network delay experienced during a call calculated as the difference between when the RTP packet is expected and when it is actually received. Jitter leads to poor audio quality.
  - Latency: Is the time an RTP voice packet takes to be transmitted to the moment it reaches its destination. Latency is caused by a slow network and leads to delay and echo problems.
  - Duration: Shows the call duration in seconds
  - Version: Version of the device that handled the call
- Registration - Data for OpenScape Voice
- CSTA - Detailed information about CSTA calls
- Options - Displays processed calls with "Disposition = Options" condition
- Advanced Queries - Allows user to create custom queries for the OpenScape Voice system
- Graph - Displays quasi-real-time charts of the processed OSV trace data for the current system.

  Restriction on Displaying Graphed Data: If multiple systems are configured in the OSV-TM server, only the graphs for one system can be displayed and refreshed at a time. This is a restriction of the web browser.
- Resources - Displays Resource usage and Performance counters graphs for the OSV server integrated with the current system.

  The same restriction for displaying graphed data above applies to Resources graphs.
- Branch_Status: This tab provides information on Branch performance.

  The OpenScape Voice reports information about all integrated OpenScape Branches via its traces; the performance monitoring counters for these OpenScape Branches are accessible through this tab.

  A status summary is presented per Branch in the default table and detailed data is graphed when a "Device IP" is clicked.

  The following counters are tracked for Originating and Terminating on-net and off-net calls:

  - Answered
  - Not-answered
  - Error calls

    See the "OpenScape Branch Performance Monitor Counter Graphs" section for detailed information about the graphed data.

7.2.3 OpenScape SBC View

The OpenScape SBC view displays trace data for the OpenScape SBC devices configured in the system. If there are no OpenScape SBCs configured, the message "No Data available" is displayed.

This tab views are summarized below:

- Call_Association

  This tab shows the A-side and B-side of all calls.

- SIP_Signaling

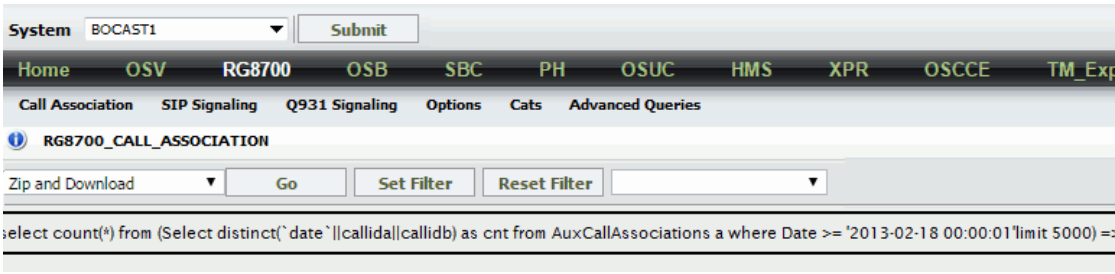
  This tab shows SIP call information.
- Q931 Signaling

  This tab shows Q931call information.
- Options

  Displays processed calls with "Disposition = Options" condition
- Cats

  This tab displays the log files for the "CATONs" configured on the OpenScape SBC listener.
- Advance_Queries

  This tab displays the system queries pre-defined for OpenScape SBC data filtering. It also allows end users to create custom queries to filter OpenScape SBC data from devices configured in the system.



Functional Sequence

The user clicks on the appropriate tab to open the view.

7.2.4 OpenScape Branch (OSB) View

The OSB view displays trace data for the OpenScape Branch devices configured in the current system. If no trace data is being generated and/or transferred to the OSV-TM system, the message "No Data available" is displayed.

The following tabs are defined for the OpenScape Branch View:

- Call_Association

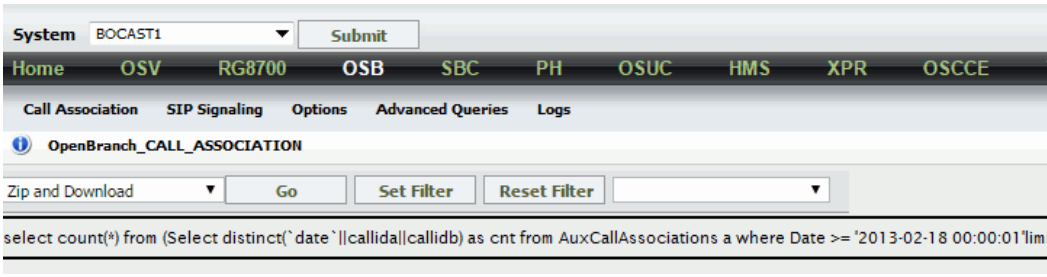
  This tab shows A-side and B-side of all branch calls reported by the OSB if configured in stand-alone mode.
- SIP_Signaling

  This tab provides detailed information about SIP Signaling calls.
- Options

  Displays processed calls with the "Disposition = Options" condition.
- Advance Queries

  This tab allows the user to create custom queries for the OSB data and displays pre-defined system queries for the same data.
- Logs

  This tab shows OpenScape Branch debug logs.



Functional Sequence

The user clicks on the appropriate tab to open the view.

NOTICE:

The Call Association tab under the OpenScape Branch view only shows data if the calls were made when the network was down and the calls had to be routed through the PSTN. Otherwise, during normal operation of the OpenScape Branch, only data in the SIP Signaling tab will display. This behavior is accepted as normal and is not longer considered an exception.

7.2.5 OpenScape Session Border Controller (SBC) View

This view displays trace data for the OpenScape SBC devices configured in the current system. If no trace data is being generated and/or transferred to the OSV-TM system, the message "No Data available" is displayed.

NOTICE:

The Call Association tab will only show data if the calls originate and terminate on the Session Border Controller; otherwise, the OpenScape Session Border Controller calls will be displayed on the SIP Signaling tab.

The following tabs are defined for the OpenScape Session Border Controller View:

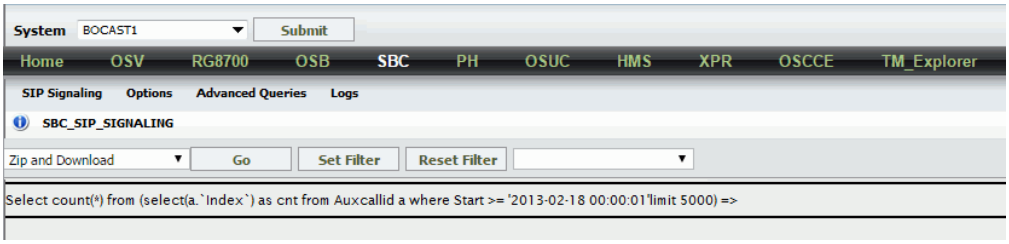
- SIP_Signaling

  This tab provides detailed information about SIP Signaling calls.
- Options

  Displays processed calls with "Disposition = Options" condition.
- Advance Queries

  This tab allows users to create custom queries for the SBC data and provides pre-defined system queries for the same data.
- Logs

  This tab shows SBC debug logs.



Functional Sequence

The user clicks on the appropriate tab to open the view.

7.2.6 Phone View

Phone data is accessible via the Phones (PH) view. Traces are received from configured Phone devices via the OSV-TM Phone TrapCollector (Listener) and the processed data is displayed on the Phone view.

Phone traces can also be initiated by the user from the OpenStage phones.

The user dials a pre-defined prefix before the destination phone number (DN) which is recognized by the OpenStage phone and converted to an internal "traceID". This traceID is added to the SIP signaling and triggers the start of tracing on the originating phone and terminating phone -if also an OpenStage phone. Trace files are generated for a limited time and sent to the OSV-TM server via DSL.

If continuous tracing is also active on the OSV server before initiating the test call, the related call is also captured in the OSV trace files and sent to the OSV-TM server. The traces are processed and made available in the User_Initiated tab for analysis.

If no Phone devices are configured to send traces to the OSV-TM system or no User Initiated tracing started, the message "No Data found that matches your search filter" is displayed.

The following tabs are defined for the Phone View:

- SIP_Signaling

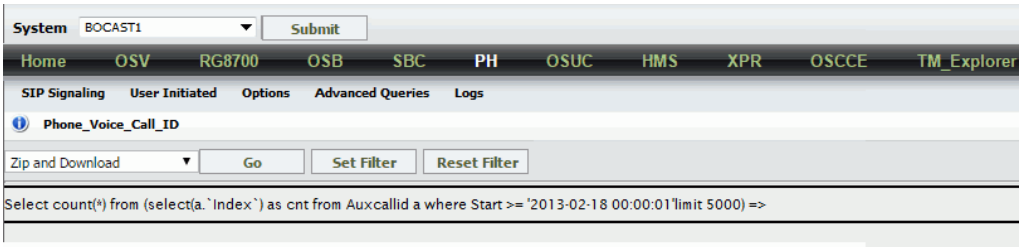
  Display the SIP Messages filtered from Phone traces.
- User Initiated

  Displays trace data sent from a user initiated action. These traces are identified by a unique "Trace ID" that maps to the "CallID" and are also tracked in the OpenScape Voice traces. Clicking on the record will display the detailed data for the call.
- Options

  Displays processed calls with "Disposition = Options" condition.
- Advance Queries

  Allows user to create custom queries for the Phones traces and provides pre-defined system queries for the same data.
- Logs

  Other phone data that is process by OSV-TM displayed for information only.



Functional Sequence

The user clicks on the appropriate tab to open the view.

7.2.7 OpenScape UC (OSUC) View

This view displays trace data received from the OSUC device and provisionally from the HMS device. If no trace data is being generated and/or transferred to the OSV-TM system, the message "No Data available" is displayed. If the OSUC and HMS devices are collocated in the same server, they send their traces in a single file and parsed data will be displayed in FADE only through the OSUC view. The information from the HMS messages is displayed on the "SIP_Signaling" tab. No data is displayed in the HMS view.

The following tabs are defined for the OpenScape UC View:

- SIP_Signaling

  Sip messages from the HMS traces. Empty if HMS is not collocated with the OSUC.
- CSTA_Events

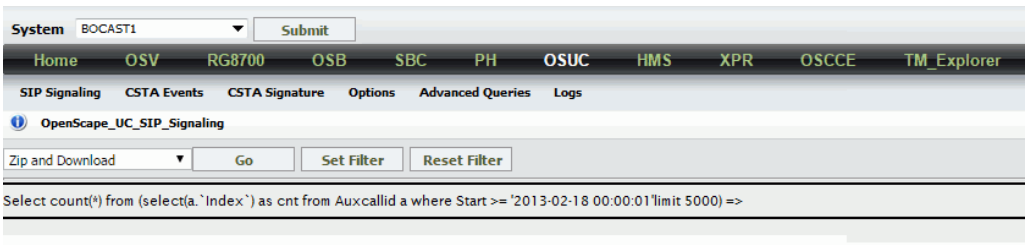
  Detailed information about CSTA calls from the OSUC
- CSTA_Signature

  CSTA events filtered by signature
- Options

  Displays processed calls with "Disposition = Options" condition.
- Advance Queries

  Allows user to create custom queries for the OSUC messages and provides pre-defined system queries for the same data.
- Logs

  Other OSUC data received that is not process by OSV-TM; displayed for information only.



Functional Sequence

The user clicks on the appropriate tab to open the view.

7.2.8 HiPath Media Server (HMS) View

The view displays trace data received from the HMS device. If no trace data is being generated and/or transferred to the OSV-TM system, the message "No Data available" is displayed. If the HMS is located on an external server, it sends separate trace files to OSV-TM. Parsed data from the HMS traces will display in FADE on the HMS view in the "SIP_Signaling" tab. The OSUC -> "SIP_Signaling" will be empty since the HMS messages are not integrated with the OSUC traces. If the HMS device is collocated in the same server with the OSUC, both devices send their traces in a single file and parsed data is displayed in FADE only through the OSUC view. The information from the HMS messages is displayed on the "SIP_Signaling" tab. No data is displayed in the HMS view.

The following tabs are defined for the HiPath Media Server View:

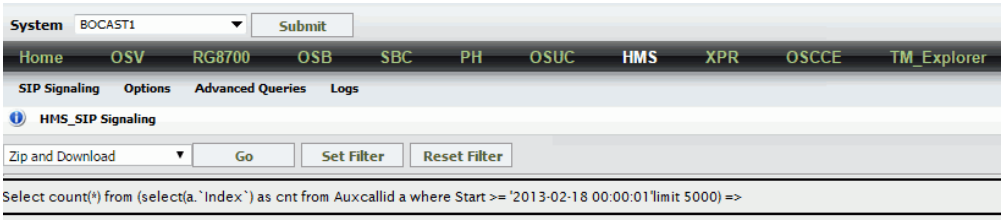
- SIP_Signaling

  Sip messages from the HMS traces.
- Options

  Displays processed calls with "Disposition = Options" condition.
- Advance Queries

  Allows user to create custom queries for the HMS traces.
- Logs

  Other data from the HMS that is not process by OSV-TM; displayed for information only.



Functional Sequence

The user clicks on the appropriate tab to open the view.

7.2.9 Xpressions (XPR) View

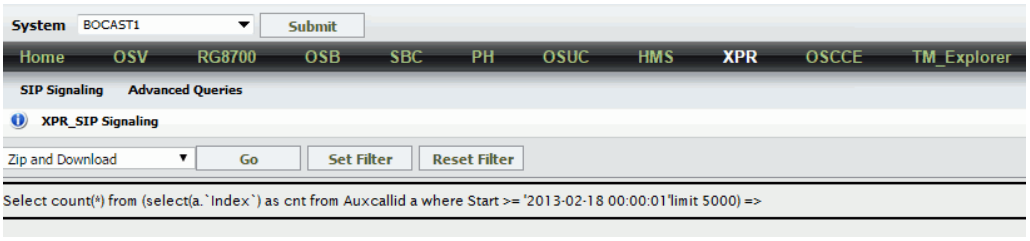
The XPR view displays trace data for the Xpressions device configured in the current System.

The following tabs are defined for the Xpressions View:

- SIP_Signaling

  Sip messages identified in the Xpressions traces.
- Advance Queries

  Allows user to create custom queries for the XPR traces.



Functional Sequence

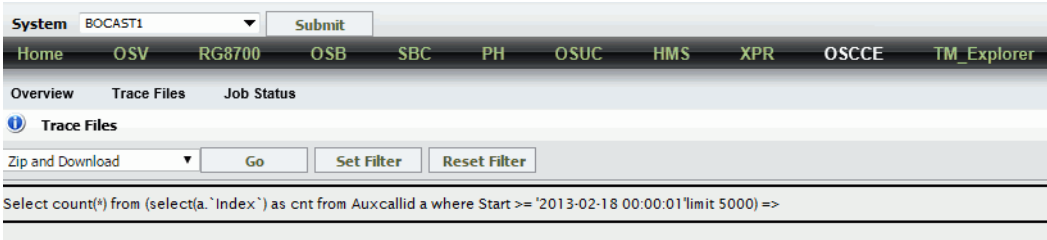
The user clicks on the appropriate tab to open the view.

7.2.10 Contact Center Extensions (OSCCE) View

The OSCCE view displays trace data for the Contact Center Extensions device configured in the Contact Center Extensions System. OSV-TM collects and stores OpenScape Contact Center Extensions (OSCCE) trace files to support only trace file filtering and access. The trace data is not processed by OSV-TM. No further configuration is required in OSV-TM for OSCCE trace collection.The instructions on how to configure Contact Center Extensions to send traces to the OSV-TM server can be found in the latest issue of the "OpenScape Contact Center Extensions V3, Configuration Concierge, Administrator Documentation".

The following are defined for the Contact Center Extensions View:

- File name
- File Date
- Processed Date
- Size
- Device Type
- Component ID
- Status

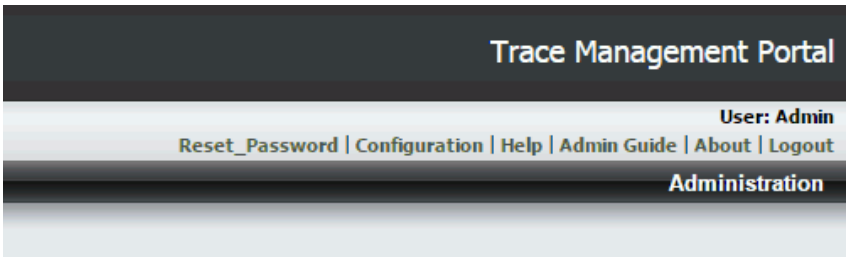


The trace files can be found in the OSCCE Data Directory:

`C:\tracedata\<system-name>\OSCCE`

7.2.11 Administration View

The Administration view is only visible to users who have administrative level permission, i.e., administrator rights. Refer to the section of this manual titled, "Administrator's Guide for Trace Management".



Functional Sequence

For Advanced users, the "Configuration" link on the top of the Trace Manager Portal screen displays the overall configuration of the OSV-TM server and the current system in a separate window.

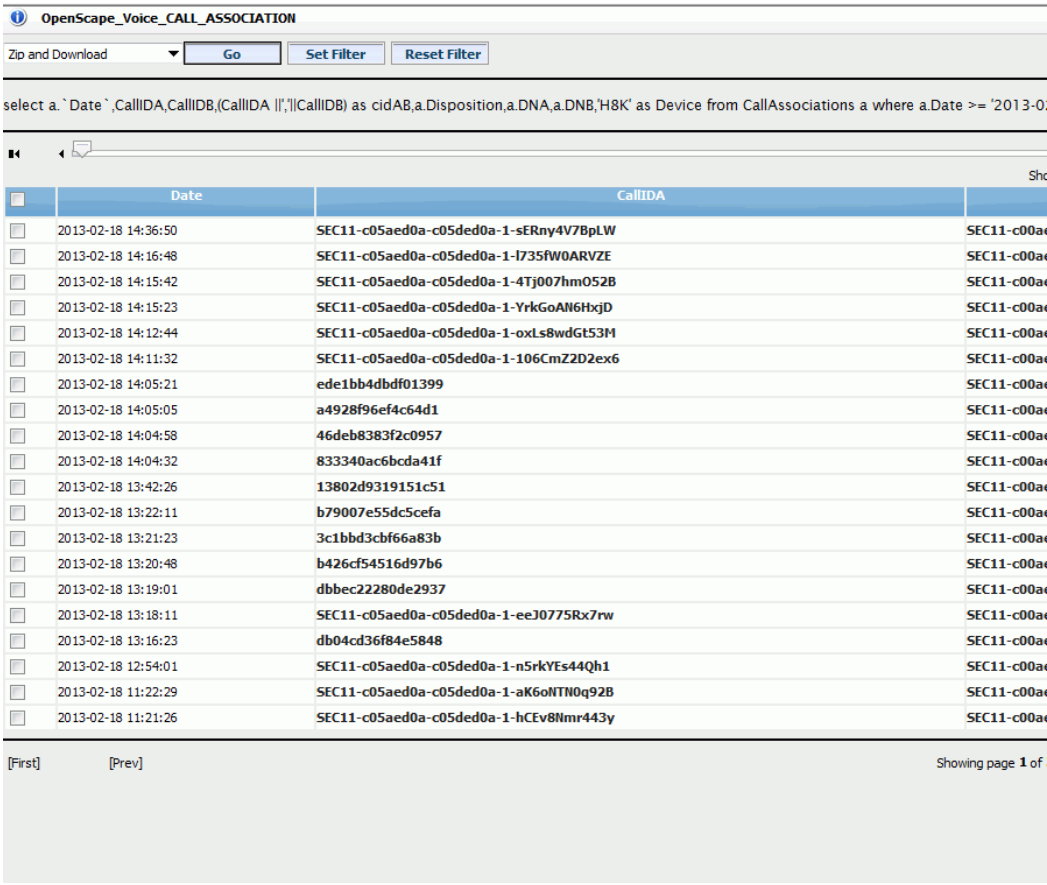
Related concepts

Administration Tasks for Trace Manager on page 107

7.3 Displaying OSV-TM Data

The default number of rows of data displayed per page when you access a device View in FADE (i.e.: OSV, OpenScape SBC, SBC, etc) is set by default to

20 rows. The OSV-TM Administrator can increase or lower this value globally or you can temporarily change it for your browsing session.



7.3.1 How to Change the Number of Rows per Page

The user is able to modify the number of rows displayed per page.

Prerequisites

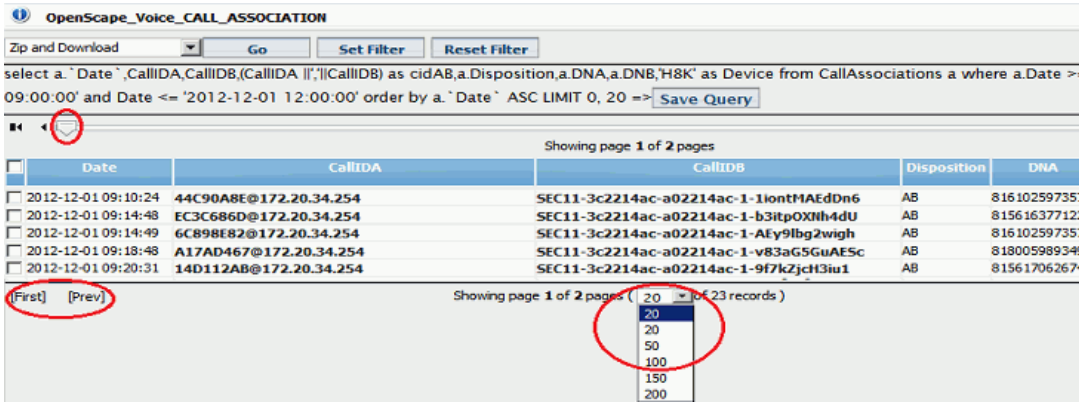
Adequate administrative permissions.

Step by Step

1) Login to Trace Manager Portal (FADE).
2) Click on the **Rows per Page** drop down menu located in the right corner of the screen.
3) Select the number of rows to view.

   The browser will automatically refresh the view and display the number of data rows selected.

4) Browse the pages, as needed, using the slider bar at the top or the **[Next]** / **[Last]** links at the bottom of the screen.



7.3.2 How to Display Detail View

FADE provides a detailed view of a call if the information is available from all the devices that traced that call.

Prerequisites

Adequate administrative permissions.

Step by Step

1) Login to Trace Manager Portal (FADE).
2) Filter the data to find the call you want to analyze.

   The browser will automatically refresh the view and display the number of data rows selected.
3) From the displayed results click on the call to display its details.

The "Details" view displays all the related information that has been received from the devices that traced the call:

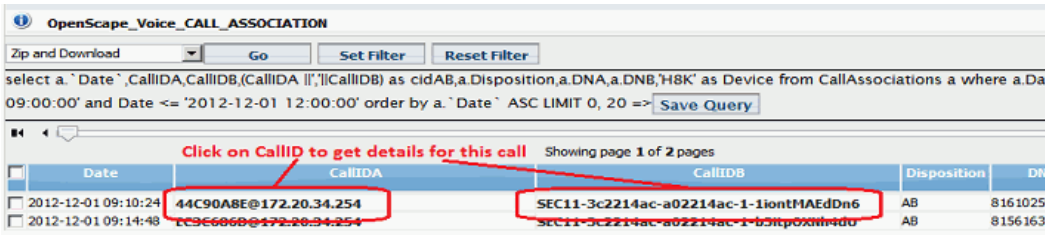
- SIP Information
- CSTA Information
- UC_CSTA Information
- Performance Data

NOTICE:

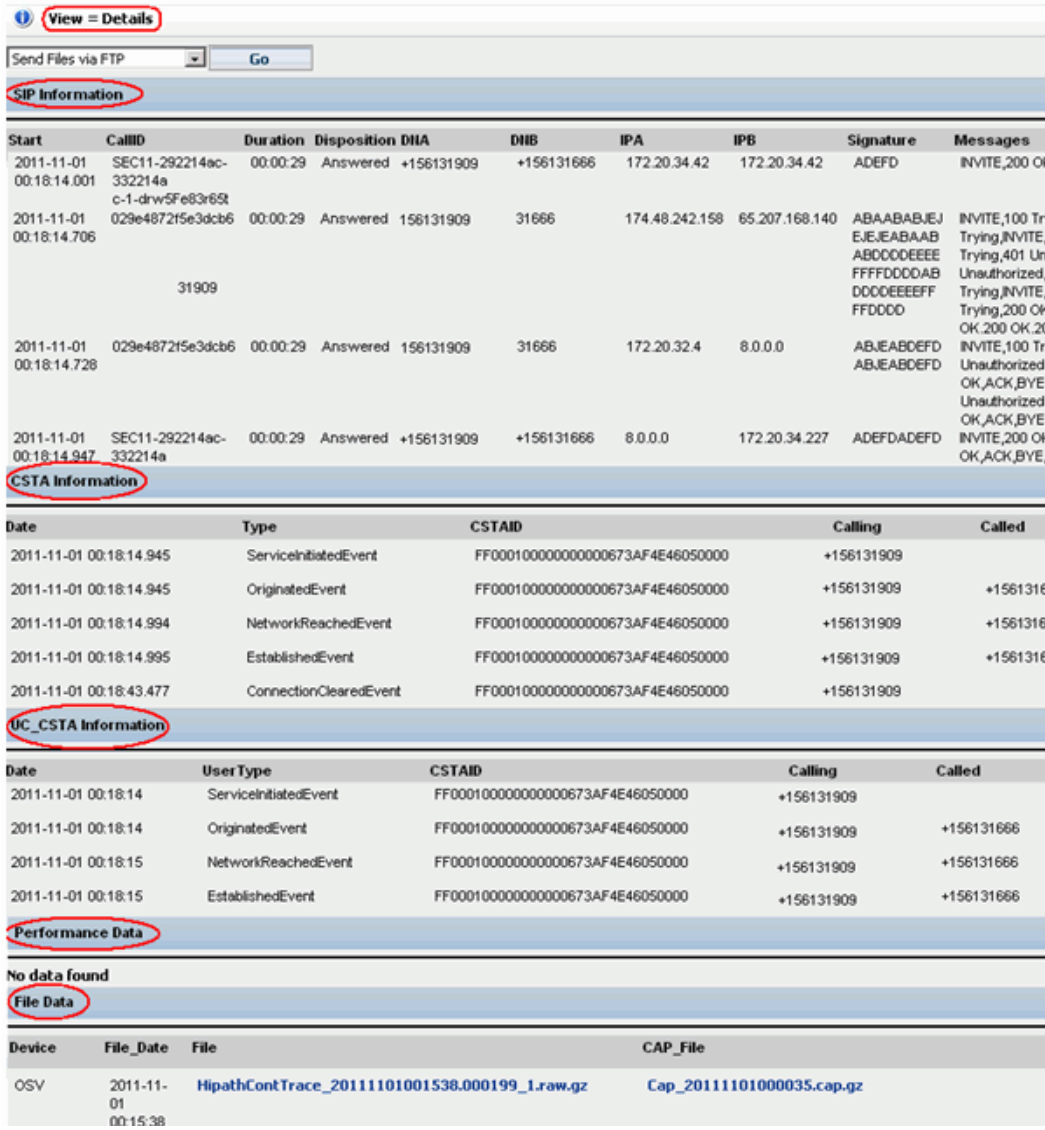
If the call did not pass through a device or the device is not sending traces to the OSV-TM server, the information is not displayed.

Example

Clicking on CallIDA, sorts the display based on CallIDA.



Clicking on the actual ID will generate the details for the call:



7.4 Filtering Trace Data

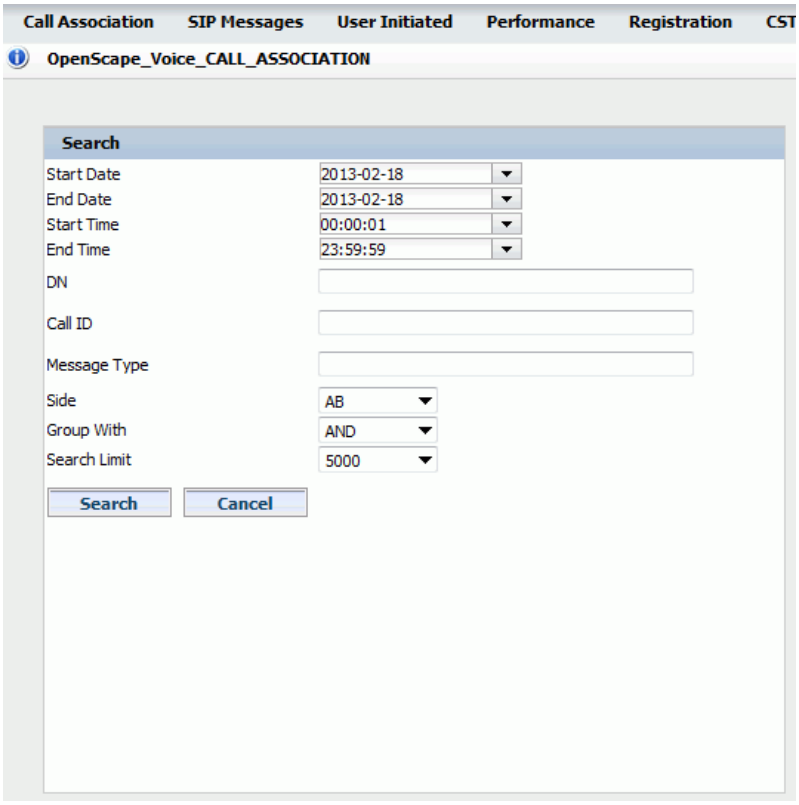
The trace data collected in the OSV-TM server can be filtered by attribute, i.e., by date, time, directory number, call id, message type, etc. (see below).

System Specific Information

NOTICE:

The trace information displayed in FADE is based on the time zone in which the data has been collected not on the time zone of the client browser.

For example, clicking on set Set Filter displays the following:



7.4.1 Restrictions on Setting Filter Dates

The Start and End dates in the filters will be restricted according to the OSV-TM system data storage configuration.

Functional Sequence

For OSV-TM systems running the default database configuration, no date restrictions are applied; systems running a weekly or daily database configuration will have the filter dates restricted to a single week or to a single day accordingly.

- OSV-TM systems configured with a weekly storage scheme:

  Filtering data is restricted on a per week basis; it is not possible to query the system for days across multiple weeks. Users will be required to change the filter to a "weekly" period: Sunday through Saturday.

  For example: if the system is configured to parse data for 10 consecutive days, and you want to query the system for the whole 10 day period, you will have to run two separate queries: one for each week period.
- OSV-TM systems configured with a daily storage scheme:

  Filtering data is restricted on a per day basis; it is not possible to query the system for multiple days on a single filter. The "Start Date" and "End Date" parameters will be limited to the same calendar day.To query for multiple days, the filter needs to be reset for each day.

  For example, if you want to query data for two consecutive days, you will have to run the filter for day 1 then change the filter date for day 2.

Please check with your OSV-TM Administrator if you need to verify the database configuration scheme used for the system.

7.4.2 Default Filters

When accessing any of the system views, a default filter is set to display traced data for the current day starting at 12:01AM to 11:59PM.

If there is any data in the database that matched the above criteria then that data will be shown. Otherwise you will have to modify your filters.

The number of records retrieved from the database by the filter is defaulted to 5,000. You can increase this number by changing the value in the "Search Limit" field. The maximum number of records to return by a query is restricted one million.

NOTICE: Important performance notice: Increasing the number of records returned by a query will affect FADE performance. The larger the "Search Limit" parameter, the longer you will have to wait to see the records displayed in the browser. Delays could increase to over 10 minutes.

7.4.3 How to Set Filters for OSV-TM Data

Prerequisites

Adequate administrative permissions.

The user is logged into the Trace Manager Portal.

Step by Step

1) Navigate to **OpenScape Voice** > **Advance Queries** > **Set Filter**

This function allows you to filter the data based on Date, time, DN's, CallID's or error codes. CSTA IDs can also be filtered from the OSV > CSTA view > Set Filter.

2) Enter or modify the search criteria:

- **Start Date (See the Section titled, "Restrictions on Setting Filters".)**

  The default is the current date.
- **End Date (See the Section titled, "Restrictions on Setting Filters".)**

  The default is the end of the current date.
- **Start Time**

  The default is 12:01 AM of the current day.
- **End Time**

  The default is 11:59 PM of the current day.
- **DN**

  DN represents directory number. Multiple directory numbers can be entered; separate the directory numbers with a comma(,). See wildcard usage below.
- **Call ID**

  Multiple Call IDs can be entered; separate the Call IDs with a comma (,).
- **Message Type**

  Multiple message types can be entered. Separate with a comma (,).
- **Side**

  View either A, B or AB side of the call.
- **Group With**

  AND/OR - Used to group the above parameters into one filter.
- **Sort**

  ASC/DESC - The order in which the search results will be sorted: Ascending or Descending. The default is "DESC". The chosen sort option will be preserved throughout the login session, and can be changed on a results page by clicking on a columns header.
- **Search Limit**

  The number of records to be retrieved from the database by the current filter (default: 5,000 records). This value can be increased to 10,000, 20,000, 50,000, 100,000, 200,000, 500,000, or 1,000,000 (2,000,000, 5,000,000). See notice above for performance warnings.
- **CSTA ID**

  The CSTA view also provides filtering for CSTA ID. Separate multiple CSTA IDs with a comma (,).

You can enter multiple directory numbers, Call IDs or message types (i.e., Response codes). Use a comma as the separator.

3) Wildcards usage in "DN" and "Call ID" fields:

The percentage character (%) can be used as a wildcard parameter when searching for "DN" and "Call ID" data:

- Entering a parameter with no wildcards will default to the "equal" or exact match operation, i.e.: entering DN: 9231337 - will return the records with this exact "9231337" parameters.
- When using a wildcard, the resulting operation will be "startwith, endwith, contains" based on the location of the wildcard within the search parameter: i.e.:

  entering DN: %1337 finds all records with a DN ending with 1337

  entering DN: 923% finds all records with a DN starting with 923

  entering DN: %1337% finds all records with a DN containing 1337

4) Click **Search**

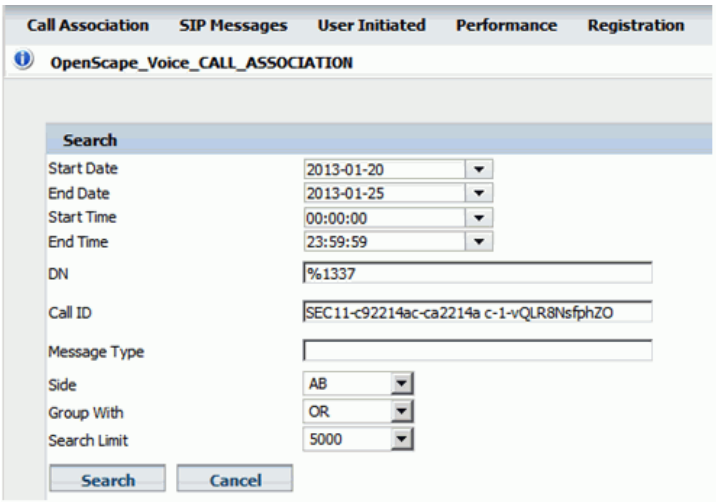
NOTICE:

You can enter multiple DN's, Call IDs, CSTA IDs or Response code by separating the search values with a comma (,). Wildcards can be included in the parameters. i.e.:

DN: 3139231337,3139234327 returns all records that match DN 3139231337and DN 3139234327

DN: 3139231337,%4327 returns all records that match DN 3139231337and records with DNs ending with 4327

Example



NOTICE:

See the Section "Restrictions on Setting Filter Dates", if additional information is needed.

7.4.4 How to Save Current Query for OSV-TM Data

Although queries can be created from scratch, the recommended method to create a new query is to modify an existing Advanced Query and save the modification as a personal query.

Prerequisites

The user is logged into the Trace Manager Portal (FADE).

Adequate administrative permissions.

The user possesses SQL Syntax knowledge.

Step by Step

1) Navigate to **OSV** > **Advanced Queries** > **Set Filter**

   The default or modified query syntax is displayed.
2) Click **Save Query** located below **Set Filter**
3) Fill in all the blanks in order to save it as a Personal Query:
   - *<Query Name>*
   - *<Query Type>*
4) Click **Save**

7.4.5 How to Clear Filters

OSV-TM allows the user to reset filter data to the default values.

Prerequisites

The user is logged into the Trace Manager Portal (FADE).

Adequate administrative permissions.

Step by Step

Click **Reset Filter**

Default values are restored.

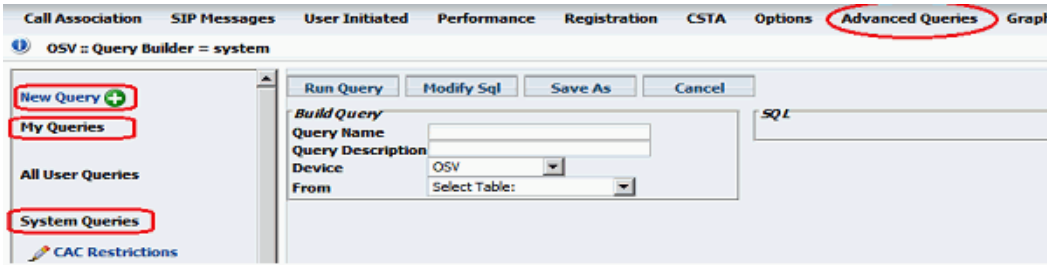
7.4.6 Advanced Queries

A set of preconfigured advanced queries are provided in FADE and user private advanced queries can be created with the Query Builder tool.

Functional Sequence

Advanced queries are accessible from the "Advanced Queries" tab on the systems views: OSV, OpenScape SBC, OSB, SBC, PH, OSUC, HMS, and XPR.

Predefined queries are listed under the "System Queries" section; queries manually created are private and listed under the "My Queries" section.



7.4.7 How to Filter an Existing Query

Queries run from the Advanced Queries tab can be further sifted by using the additional filter parameters available from the results pane.

Prerequisites

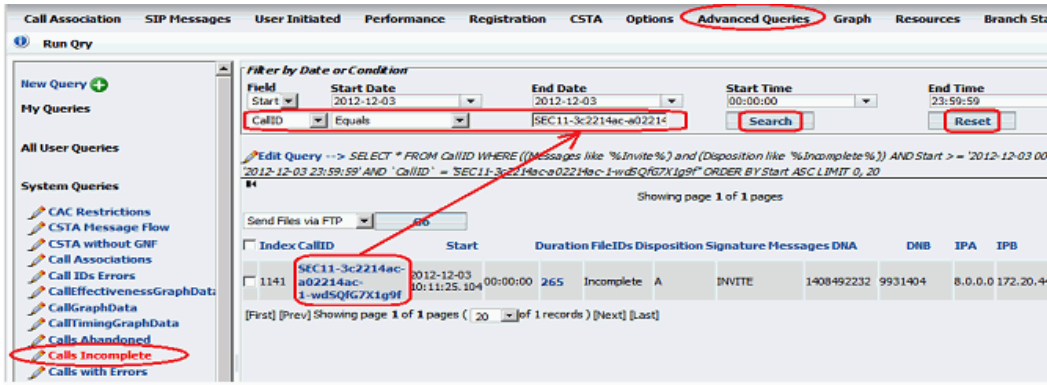
The user is logged into the Trace Manager Portal (FADE).

Adequate administrative permissions.

In the example below, the "Calls Incomplete" system query was run and the results filtered only for the CallID that equaled the value "SEC11-3c2214ac-a02214ac-1-wdSQfG7X1g9f". This feature allows for displaying only the records that matches a specific value.

NOTICE:

The filters can be cleared by clicking the "Reset" button.



Step by Step

Click **Reset**

Filters are now cleared.

7.4.8 How to Create a New Query

Prerequisites

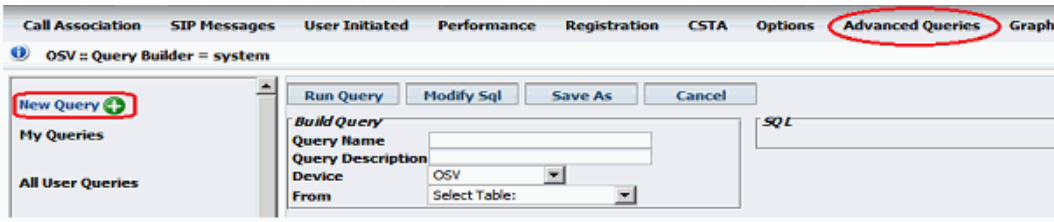
Adequate administrative permissions.

The user is logged into the Trace Manager Portal (FADE).

Step by Step

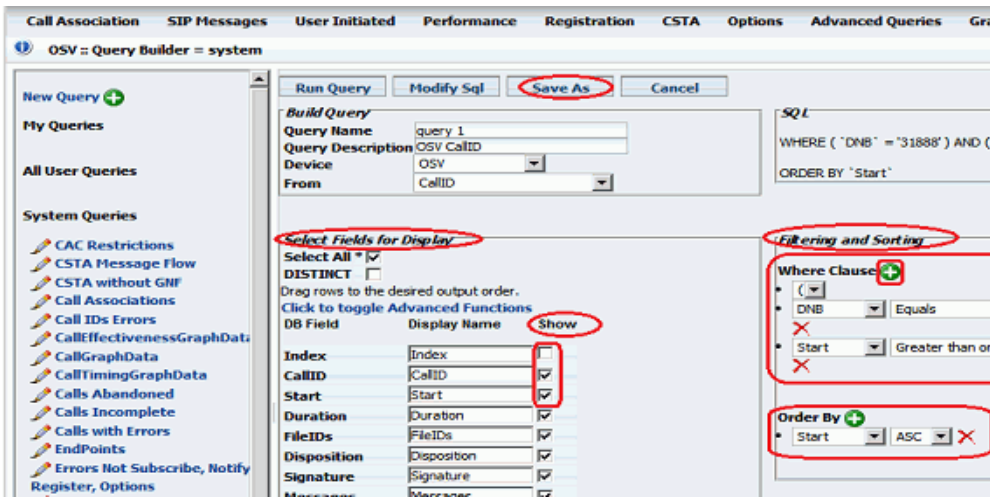
1) Click on Advanced Queries
2) Click **New Query**

   The query builder tool is displayed.
3) Enter a name for the query in the "Query Name" field.
4) Type a "Query Description" to identify the query.
5) The "Device" field displays the current device the query will filter data for (i.e.: OSV).
6) The "From" field provides the list of tables to query information from. Select a table to start building your query.

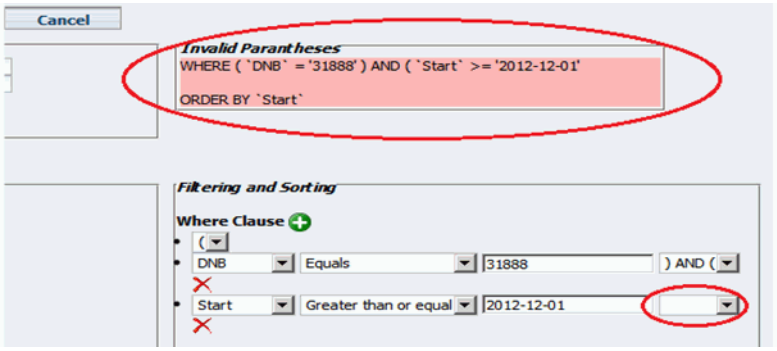


   The SQL building modules are displayed.
7) Select the fields to display in your results by setting a checkmark under the "Show" column for each field. You can change the "Display Name" for each field if necessary.
8) Set a filter for the data by using the "Where Clause" parameters. Clicking on the "Plus" icon adds fields to build a compound (AND/OR) filter.

9) Use the "Order By" element to select how your query results should be sorted.



The "SQL" box shows the syntax built by the "Where Clause" and "Order By" modules. If there is an error with the Where Clause syntax, the text is shaded in red and a hint of the cause for the problem indicated.



10) Click "Run Query" to run the query without saving it. You results are displayed in a new window.

11) Click "Save As" to save the query with the name given in the "Query Name".

12) The new query is listed under "My Queries" list section.

7.4.9 How to Edit Existing Queries

Prerequisites

Access to the Open Trace Manager Portal (FADE) logon screen.

Step by Step

1) Edit using Query Builder

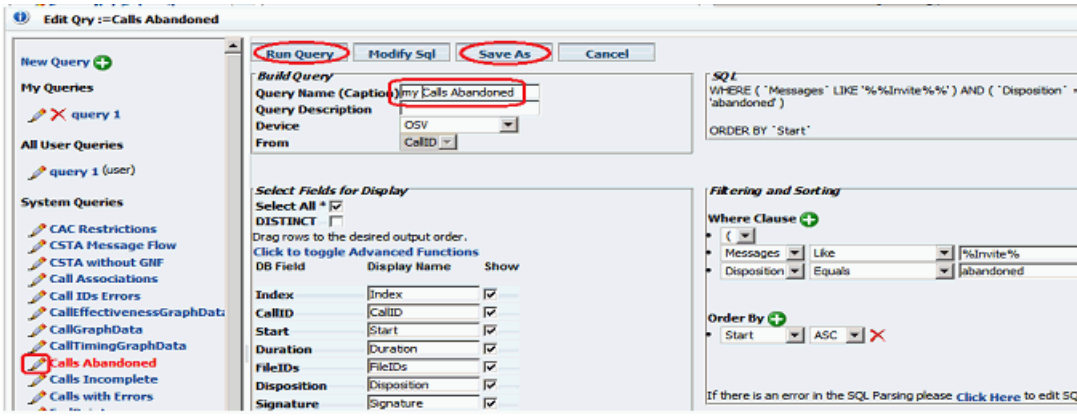
2) Click on the pencil icon next to the query's name.

   You can modify most parameters for the query, except the **From** table that it queries from.

   For advanced queries, toggling the **Advanced Functions** under the **Select Fields for Display** section, will allow you to format the output of the query using SQL functions such as substr() and date().

3) After completing all changes, **Run Query** allows you to see the results without saving them.

4) Change the "Query Name" and click **Save As** to save the query as a private query.



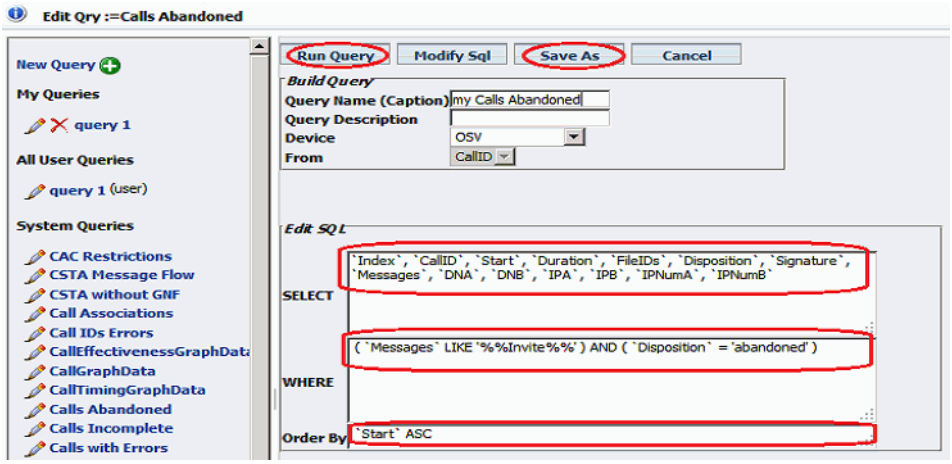
Using the Manual SQL Editor:

You can also modify directly the SQL statements in a query instead of using the Query Builder. Just click on the **Modify Sql** button to open the SQL editor.

NOTICE:

SQL knowledge is necessary when using this manual feature.

Some of the existing **System Queries** cannot be modified with the Query Builder since they include complex SQL statements. Those queries can only be customized or edited by modifying the SQL parameters by hand.



5) Type in a new name for the query and click **Save As** to save changes under a new saved query.

7.4.10 How to Delete Queries

FADE allows deletion only of personal or private Queries. System queries are managed by the OSV-TM Administrator

Prerequisites

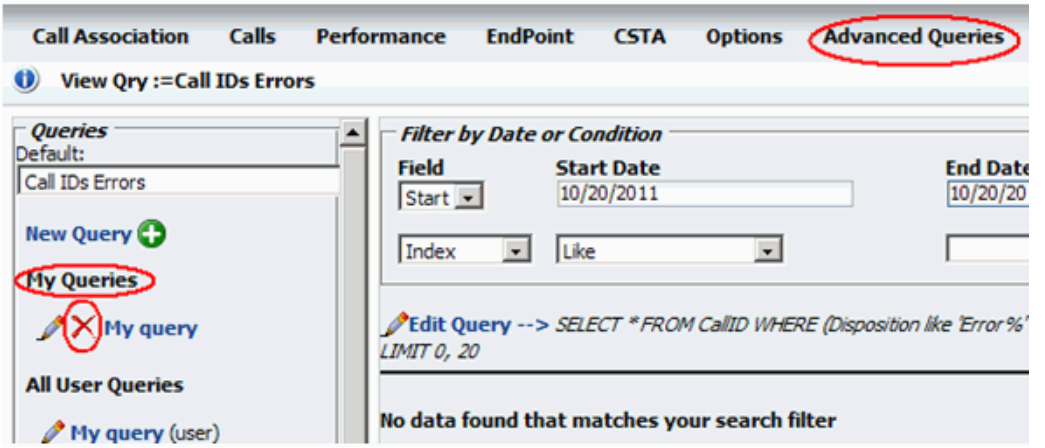
Adequate administrative permissions.

The user is logged into the Trace Manager Portal (FADE).

Step by Step

1) Navigate to **OSV** > **Advanced Queries**
2) Select **My Query**
3) Click on the X next to your query's name.
4) Click OK to continue with the deletion.

Example



7.5 File Handling Option

The file handling option procedures provide instructions on how to open or transfer trace files for further analysis. These trace files are accessed from the system views.

The additional 3rd Party client applications needed to open these files must be downloaded and manually installed by the user on the client machine.

In addition to handling trace files, the Export to CSV feature allows the user to capture the results of the currently viewed query and export the captured results to a CSV file.

7.5.1 How to Open CAP Files with Wireshark

Ethereal Wireshark, the network protocol analyzer used for capturing and browsing network traffic, is used to analyze the CAP Files generated by DIPAZ for OpenScape Voice, or generated directly by the OpenScape SBC or OpenScape Branch.

Prerequisites

Adequate administrative permissions.

NOTICE:

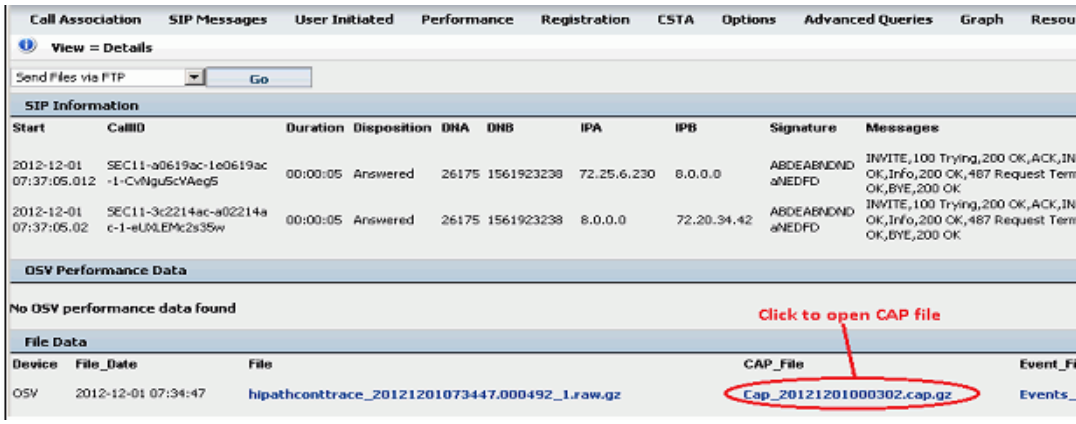
Wireshark should be downloaded from the Internet and installed locally in your computer to be able to open trace files.

Wireshark is installed locally on the computer.

The user is logged into the Trace Manager Portal (FADE).

Step by Step

1) Click on the Index for the record to be analyzed, or any of its links.
2) Scroll down to the **File Data** section.
3) Click on the link under **CAP_File**



The system prompts with: "File download"

4) Click **Open**

The file downloads and unzips.

5) Double click on the CAP file to open it.

7.5.2 How to Open Multiple Downloaded Cap Files

Some calls can have multiple CAP files related to their traces. You can follow this procedure to combine all cap files of a particular trace and open them at once with Wireshark using the "mergecap" utility.

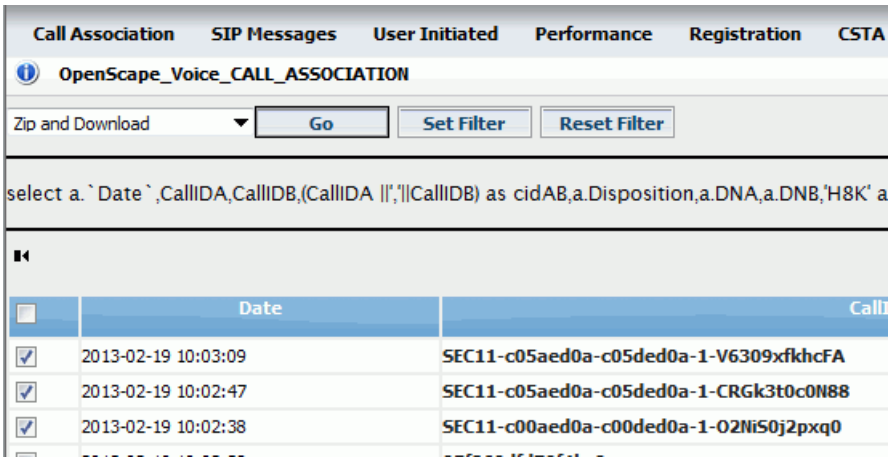
Prerequisites

Wireshark must be already installed on your client machine to use this utility.

Step by Step

1) Check mark the Index for the Calls you want to analyze.

2) Select the "Zip and Download" option from the actions menu and click "Go"



3) Save the zip file to a temp folder (Ex.: c:\temp\osvtm_files); un-zip the downloaded file to the same directory, and extract the ".cap.gz" files to the same location.

4) Open a CMD shell:

a) From the "Start" menu click "Run

b) On the "Open:" field type: cmd

A CMD window opens

5) Type the following commands on that shell;

a) Change directory to the temp folder

cd c:\temp\osvtm_files

b) Run the following command:

"C:\Program Files\Wireshark\mergecap" -a -w <destination-folder>\mergedfile.cap <specify-input-cap-file-path>*.cap.gz

---

NOTICE:

We use assumes that Wireshark's installation path is: C:\Program Files\Wireshark; change the path if it is installed on a different location.

Use the double quotes (") around the command; otherwise the path will not be found.

<destination-folder >\mergedfile.cap is the target path and output file for the merged files; If you do not specify a

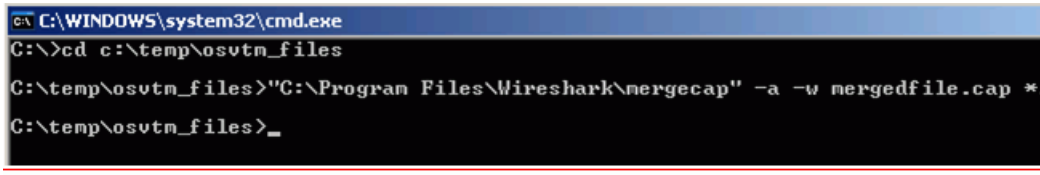
path to the output file, the file will be created in the current folder where the command was run from.

"specify-input-cap-file-path" is the path to the source folder where the individual cap files are stored.

You can use a wild card "*" to merge all ".cap" files in that source folder or you can specify the individual cap file names.

Example: "C:\Program Files\Wireshark\mergecap" -a -w mergedfile.cap *.cap.gz

In the example, the input cap file path and the destination storage folder for the output "mergedfile.cap" are the same: c:\temp\osvtm_files:



6) Open the mergedfile.cap with Wireshark.

7.5.3 How to Analyze an Event File

The Event File contains all the events for the protocols used in a call. The file opens in an Excel Worksheet.

Prerequisites

Adequate administrative permissions.

Excel is installed on the client machine containing the file.

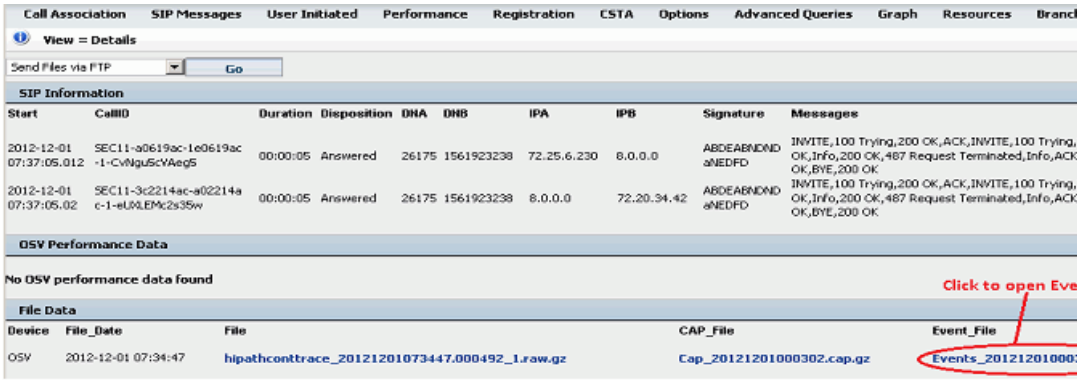
The user is logged into the Trace Manager Portal (FADE).

Step by Step

1) Click on the Index for the Record you want to open the Event file for.

2) In the detail page, scroll to the **File Data** section.

3) Click on the file link under the "Event_File" column.



The system prompts with: "File download"

4) Click **Open**

   The file downloads and unzips.

5) Double click on the `.csv` file.

   The file opens as an Excel worksheet.

7.5.4 How to Send Files via FTP

The FTP function allows the user to FTP files from the OSV-TM server to a private FTP server.

Prerequisites

NOTICE:

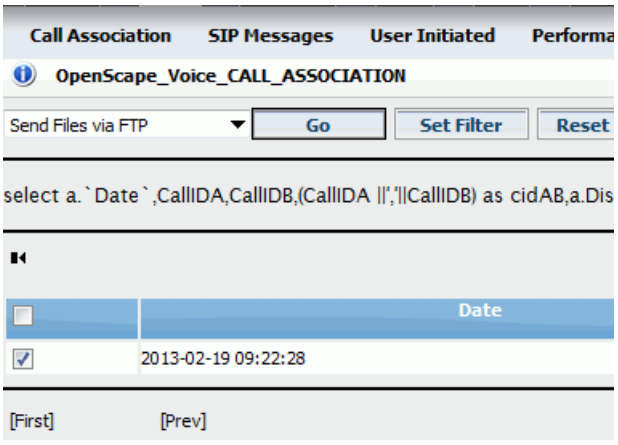
This feature may be not be available in your system for security compliance. If you do not see "Send Files via FTP" displayed in the actions list, the feature has been disabled. Please check with your OSV-TM system administrator.

Adequate administrative permissions.

The user is logged into the Trace Manager Portal (FADE).

Step by Step

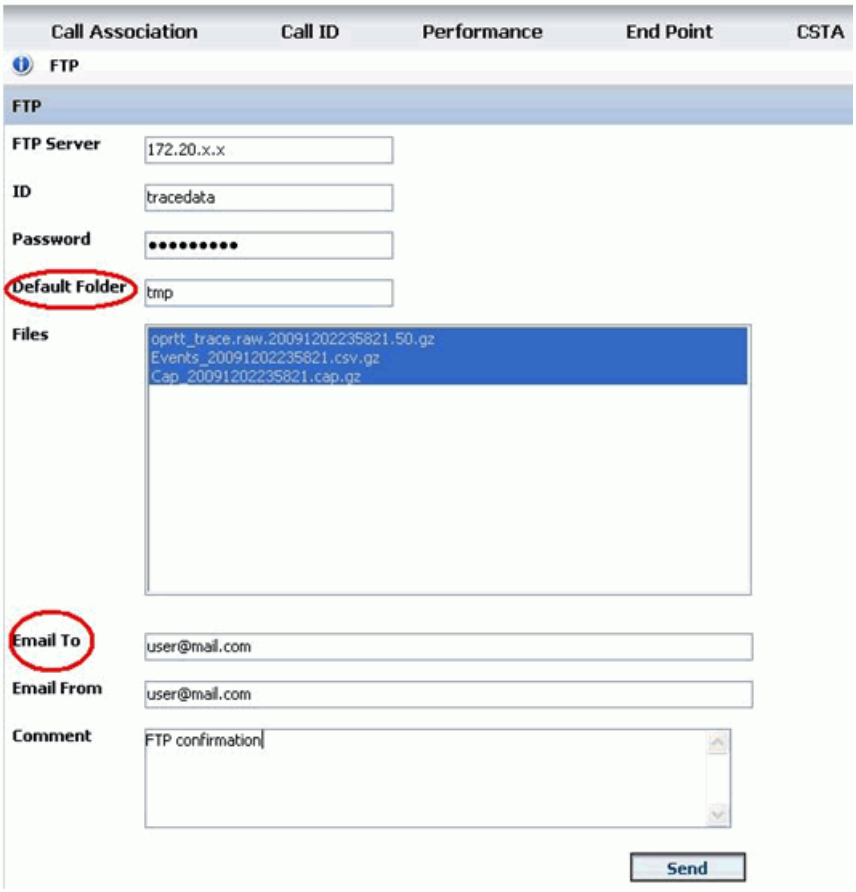
1) Click on the check box to the left of the record to be sent.
2) Select **Send Files via FTP** from the drop down box.



3) Enter *<your private FTP server address>*
4) Enter *<ftp user account>*
5) Enter *<password>*
6) The **Default Folde**r field is set to **temp**; you can change this setting to your own folder name.
7) Enter your email address in the **Email To** field to receive a confirmation notification of the transfer.

8) Click **Send**

The user can send the files to the user's own FTP Server, if an FTP installed on the user's computer.



9) Verify that the file was sent correctly by reading the displayed log.

The link provided in the log provides the full path to the location in the FTP folder where the file is stored:

To view your files please click on this link -> FTP Folder

7.5.5 How to Zip and Download Files

Trace files can be downloaded directly via http.

Prerequisites

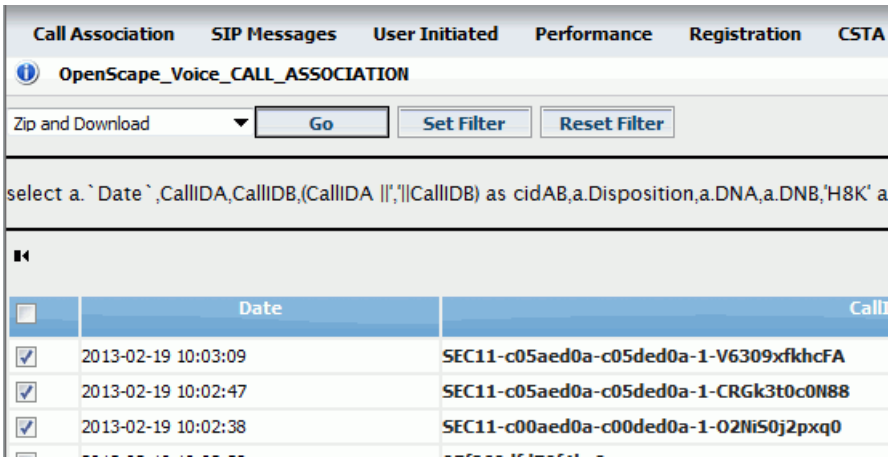
Adequate administrative permissions.

The user is logged into the Trace Manager Portal (FADE).

Step by Step

1) Select the check box to the left of the record to be downloaded.

2) Select **Zip and Download** from the dropdown box.



3) Click **Go**

   The system will prompt with: Do you want to open or save this file?

4) Click **Save**

5) Browse your local disk to the location where the file is to be stored.

   The files can be accessed and unzipped at a later time.

7.5.6 Capture Query Results in a CSV Formatted File

The **Export to CSV** feature allows the user to capture the entries displayed in the current view and save them to a CSV file or open them directly.

Functional Sequence

This function is primarily designed to save the results obtained from running a query, so that they can be viewed later in a table format.

All the entries included in the result pages are enclosed in the export, so if there are, for example, 270 result pages, they are all saved in the file.

NOTICE:

Only the high level result pages are captured via the **Export to CSV** feature. The detailed Call ID information page viewed when clicking on a call record is not exportable.

7.5.6.1 How to Capture Query Results in a CSV Formatted File

The Export to CSV feature allows the user to capture the entries displayed in the current view (i.e., any view) and save them to a CSV file or open them directly. This procedure provides the steps to run the query and to save the results.

Prerequisites

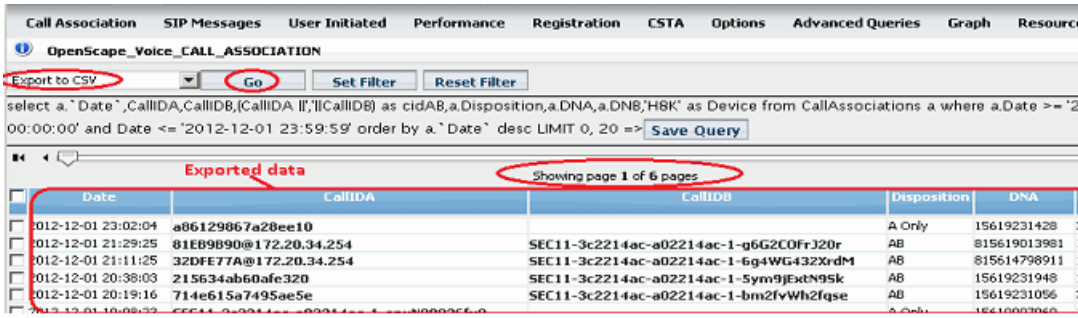
Adequate administrative permissions.

The user is logged into the Trace Manager Portal.

The user is on the view to be queried.

Step by Step

1) From any View of the system (i.e.: OSV, SBC, etc) run the query you want to capture results for.
2) From the drop down menu, select **Export to CSV** and click **Go**



3) Save the file to a local drive; Click **save**

   The data is saved with **tab** delimiters. To see it as column formatted output, import the file into an external application such as MS Excel and select **tab** as the delimiter.

7.5.7 Trace Manager (TM) Explorer

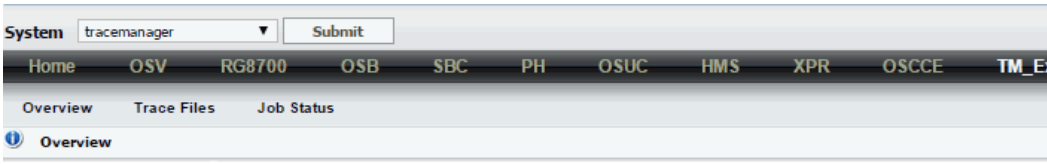
The TM_Explorer feature in FADE provides two functionalities: display status information on the trace files received on the OSV-TM server that are currently in the "Tracedata" archive storage for the different devices integrated with an OSV-TM system, and allow the user to setup background jobs on these files to speed up access to trace information.

Statuses of the Trace Files processing can be viewed on the "Overview" or the "Trace Files" panes. To transfer selected trace files off the OSV-TM server to a local storage, you can set compress and download or FTP jobs. To request a quicker processing of trace files already in the "Tracedata" storage queue, an "On Demand Processing" job can be used; this feature expedites parsing of the traces you select by copying the trace files to the "OnDemandAnalysis"internal OSV-TM System and displaying the FADE information through this system.

The "On Demand Processing" job will not work on trace files dated older than seven (7) days. The "OnDemandAnalysis" internal OSV-TM System is configured with a "daily" partition mode and has a default processing and aging period of seven (7) days. Submitting a job for older files will copy the files, but they will never be processed.

If you need to parse older traces, ask the OSV-TM Administrator to create a separate OSV-TM system and set the DIPAZ processing parameters to a larger number of days. You will then need to manually copy the files into that system's Tracedata storage for processing.

To access the Explorer for the current OSV-TM system click on the "TM_Explorer" view:



7.5.7.1 TM_Explorer Explorer Functionality

Information displayed by the TM_Explorer is for the OSV-TM system currently indicated by the "System" field (i.e.: tracemanager). To get information about other OSV-TM systems configured in the server, select it on the "System" field and click the "Submit" button.

Three navigation tabs are available in the TM_Explorer: Overview, Trace Files, and Job Status.

The Global Filtering pane sets the parameters to filter data by:

- Date and Time - "Start Date", "End Date", "Start Time", and "End Time"

  Default: today, 24 hours
- Device - Sets the specific device to search for: OSV (Default), OpenScape SBC, OSB, OSS, PH, OSUC, XPR, HMS

  "All" option only available in the "Overview" pane and displays a summary of the trace files being processed for the set period selected by the filter.
- File Status - Filter by processing status of the trace files: All (Default - List all files in any status, including Missing files), Pending, Processed, OnHold (files not to be parsed by OSV-TM), NA (logs and miscellaneous files, not parsed by OSV-TM), Unknown (unidentified files that are not process by DIPAZ), and Missing (files received by OSV-TM that were manually deleted by an Admin before being processed; they no longer exist on the TM server).
- Reset (button) - Resets all filters to the defaults

Use the selection boxes to mark the data or files to perform an action on.

NOTICE:

File entries with a "Missing" File Status are displayed for information only. No Actions can be perform on these files; an error message will be generated if an action is attempted.

The Action pull-down list allows you to select which action to take with the selected data. Each action spawns a job that is processed in the background. The results are viewable from the "Job Status" tab (see the "Job Status" section for details).

- Zip And Download: Selected Traces Files are zipped together and downloaded via http as an archive file.

  Depending on the number of files selected in the filter, multiple zip files could be created for downloading.
- Open with OSVTM Archive: Traces Files are packaged in an ".osvtm" archived file that can be opened with the OSV-TM client add-on.
- On Demand Processing: see section "Processing Trace Files On Demand" below for a complete description of this feature.

- Send files via FTP: The selected files are FTP'ed to the remote server you indicate.

  Enter the IP address of the FTP server where the files will be sent to, the FTP user account and password.

  NOTICE:

  If the Output Folder does not exist in the FTP server, the folder will be created in the remote location and the jobID appended to the folder name. If no "Output Folder" is entered, a default folder name will be created.

7.5.7.2 Overview

The Overview tab shows the overall trace processing status for all the devices integrated with the current OSV-TM system for the period set by the date and time filters.

If a device is not integrated or configured to send traces to the OSV-TM system, it will not show in the list.

Summary information for a specific device can be filtered by selecting that device on the "Device" filter.

Overview Definitions

Date - Date when the trace files were generated

Device - Identifies the integrated device the trace file belongs to: All (default), OSV, OpenScape SBC, OSB, OSS, PH, OSUC, XPR, HMS

Status - Indicates the status of the filtered trace files: Processed, Pending, OnHold, NA, and Unknown

Count - Number of trace files included in the filter that has the same status

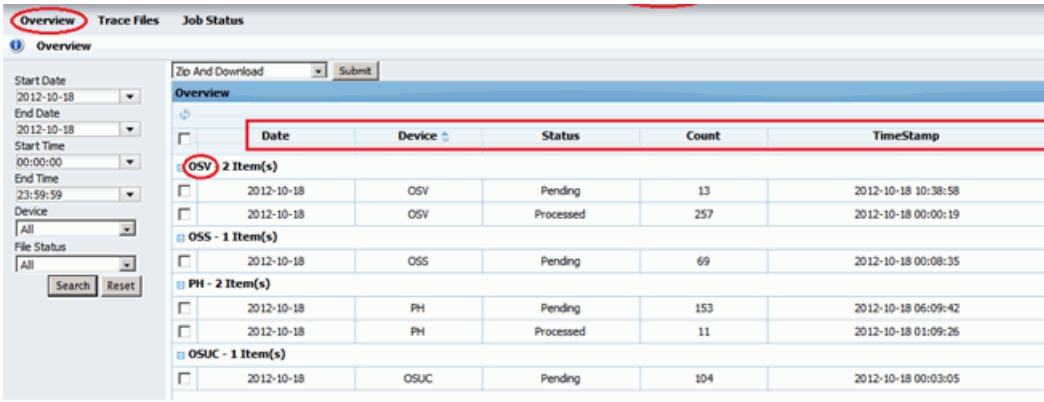
TimeStamp - Date and time from the trace file name

Total Size - Sum of all the trace files sizes that have the same status for a device

NOTICE:

If the status field is "Pending", the "TimeStamp" indicates the last file that arrived at the Tracedata storage that has not been processed yet.

The gap between the TimeStamp for the "Processed" status and the TimeStamp for the "Pending" status is the 'delay' window the OSV-TM system is behind processing trace files.



7.5.7.3 Trace Files

The Trace Files tab lists the individual trace files information for a specific device, date, and time set by the filters on the left pane. The default date period is set to the 24 hours of "today"; the default Device is set to "OSV", and the default File Status is "All".

To see trace file information for another device select it from the "Device" filter pull-down list. If a device is not integrated or configured to send traces to the selected OSV-TM system, it will not list any files.

TM Trace Files View Definitions

File - Trace file name

File Date - Date and time when the trace file was generated; derived from the actual name of the file.

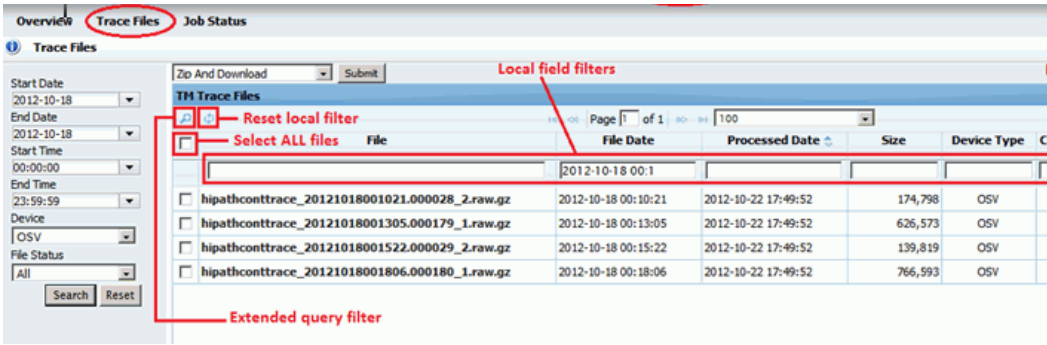
Processed Date - Date and time when the trace file was parsed in OSV-TM.

Size - Individual trace file size

Device Type - Identifies the device where the trace file was received from: OSV, OpenScape SBC, OSB, OSS, PH, OSUC, XPR, HMS

Component ID - The internal ID within the trace file that identifies the device where the information comes from

Status - Indicates the processing status of the trace file: Pending, Processed, OnHold (files not to be parsed by OSV-TM), NA (logs and miscellaneous files, not parsed by OSV-TM), Unknown (unidentified files that are not process by DIPAZ), and Missing (files received by OSV-TM that were manually deleted by an Admin before being processed; they no longer exist on the TM server).



Two additional filtering methods are available in the "Trace Files" pane:

- Local field filter: allows you to type a parameter to filter on a specific field.

  Just type the data to filter by and press the [Enter] key
- Extended query filter: use to build a filter using compound query statements.

  Click on the "Magnifier" icon above the column headers
- The "Refresh" (reset local filter) icon above the column headers resets the data to the global filter

7.5.7.4 Job Status

The Job Status tab lists the jobs submitted via a TM Explorer action on the current OSV-TM system.

Jobs can be found or filtered by using the Global filter pane or the local field filters.

Job Status Information

Start - Date and time when Job was submitted

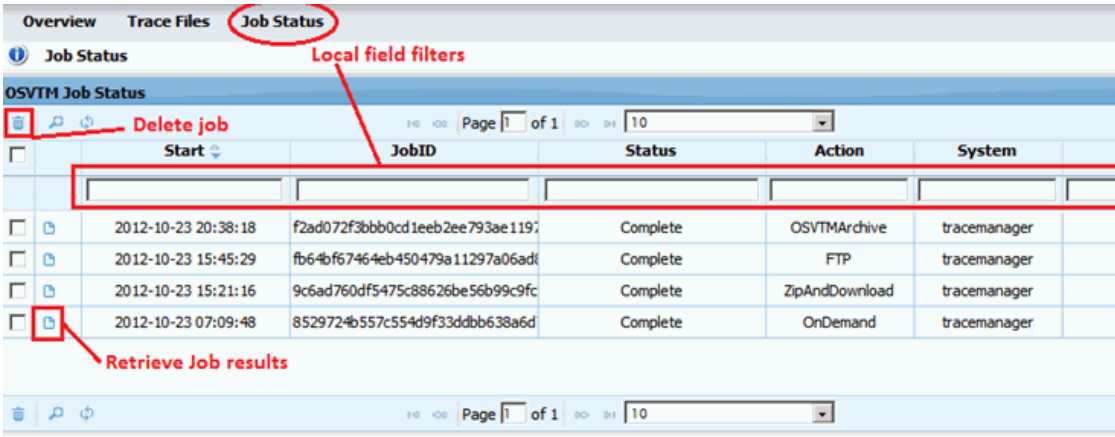
JobID - Unique identification for a Job

Status - Status of a Job: Pending (job in progress) or Complete

Action - Action requested with this Job: ZipAndDownload, OSVTMArchive, OnDemand, FTP

System - Indicated the OSV-TM system where this Job was run on

User - Login ID of the user who requested the Job



Job Results

The output or results of a job can be retrieved by clinking on the "Details" icon on the second cell.

- FTP job results will access the remote FTP server and location where the files were copied to. You need to provide the FTP user ID and password.

  A "Complete" status indicates the files were transferred to the remote FTP server.

- The results for an OnDemand job are accessed by switching the "System" name to the OnDemandAnalysis.

  A "Complete" status indicates the trace files were moved to the "OnDemandAnalysis" system Tracedata folder to be processed. To verify the status of the files being processed, switch the System to the "OnDemandAnalysis" and navigate to the "TM Explorer" view; when all the files are finished the status will indicate "Processed".

Deleting Jobs

Jobs are kept in the "Job Status" indefinitely until manually removed.

NOTICE:

Deleting a job does not remove any trace files, nor does it clear the traces from the "OnDemandAnalysis" system. Trace files are aged by the OSV-TM internal processes according to the default aging period set for the system; the default for the "OnDemandAnalysis" is three (3) days.

To delete a job:

- Check Mark the job to be deleted.
- Click on the Trash Can or "Delete Selected row" icon located on the top-left area in the OSVTM Job Status pane.
- Click "Delete" in the confirmation window.

7.6 Working with Graphs

The system graphs display quasi-real-time charts of Key Performance Indicators (KPI) for the integrated Open Scape Voice node.

The following KPIs are used to generate graphs:

- Stable (Active) Calls
- New Call Attempts
- Answer Seizure Ration (ASR)
- Ineffective Call Attempts
- Ineffective Machine Attempts
- Active Registrations
- New Registration Attempts
- Registration Change Ratio
- Ineffective Registration Attempts
- Voice, i.e., Real Time Protocol (RTP) Transmit Packets
- RTP Received/Loss/Jitter/Duplicate packets
- Post dial delay
- Subscribe
- Notify
- Option

Each line on the graph represents a Key Performance Indicator and has a unique color. The x-axis, always represents the date and time that the event occurred. The y-axis, varies from graph to graph. Refer to each graph’s description for detailed information. The navigation frame to the left, on the

Graph screen, allows the user to change the filtering parameters for the data to plot.

NOTICE:

The OSV-TM Graphs will only display data that has been parsed from OSV traces. If no trace data files have been received for a system or the parsing of the traces is delayed, the graphs will be blank. The "TM Explorer" view can give you an indication of the most current data that has been processed for a system.

7.6.1 Restrictions on Displaying Graphed Data

Displaying Graphs for Multiple OSV-TM Systems

If multiple systems are configured in the OSV-TM server, only the graphs for one system can be displayed and refreshed at a time. Displaying the graphs of a second system on a separate window is not supported,

This is a restriction of the web browser.

Displaying Graphs for Systems with Special Database configuration

The graphed data for an OSV-TM system is restricted according to its data storage configuration.

For OSV-TM systems running the default database configuration, no restrictions on the graph filters are applied; systems running a weekly or daily database configuration will be limited to graph data for a single week or for a single day accordingly.

- OSV-TM systems configured with a weekly storage scheme:

  Graphed data is restricted on a per week basis; it is not possible to display graph data across multiple weeks.

  You will be required to change the graph filter to the week you are interested on: Sunday through Saturday

  For example: if the system is configured to parse data for 10 consecutive days, and you want to see the graph for that 10 day period, you will have to run two separate queries: one for each week period.
- OSV-TM systems configured with a daily storage scheme:

  Graphed data is restricted on a per day basis; it is not possible to display graph data for multiple. The "Start Date" and "End Date" parameters will be limited to the same calendar day.

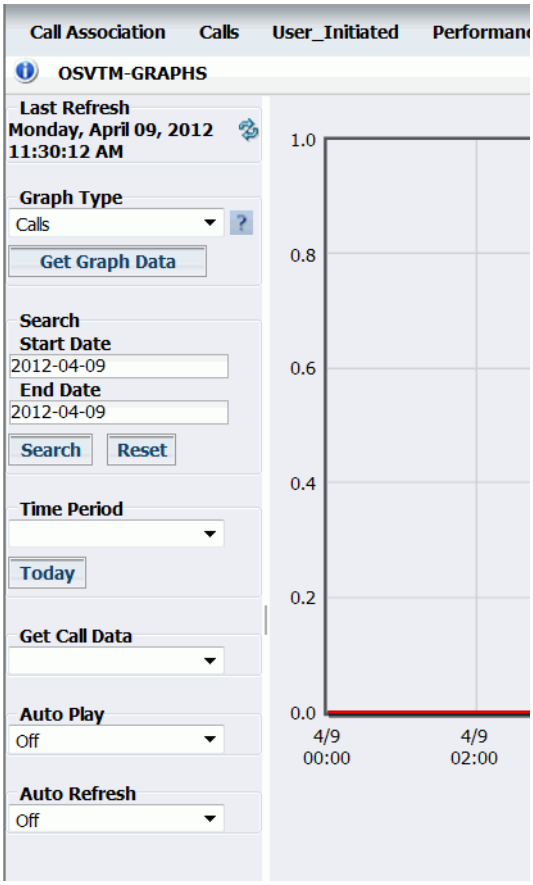
  To display a graph for multiple days, the filter needs to be reset to each day's date.

  For example, if you want to graph data for two consecutive days, you will have to display the graph for day 1 then change the filter date for day 2 to display its graph.

Please check with your OSV-TM Administrator if you need to verify the database configuration scheme used for the system.

7.6.2 Graphs Navigation Frame

The Navigation frame is used to change the parameters for displaying graphed data.



These parameters include:

- **Last Refresh**

  This parameter indicates the date and time of the last refresh. Clicking the icon in this box forces the graph to refresh.

  The small "Icon" inside this box, gives you the option to force a graph refresh.

- **Graph Type**

  Use the drop down list to change the graph type to view.

  The question mark **?** icon opens the help page which contains detailed information for the graph.

  The **Get Graph Data** button brings up the actual data from the database used to plot the points in the graph.

- **Search**

  The search function allows the user to plot data between the selected date range in the current graph type.

  – Start Date
  – End Date
  – Search (button)
  – Reset (button)

- **Time Period**

  Ths drop down box is used to select a "pre-defined" time interval and to plot it in the current graph.

  – Today
  – 24 Hours
  – 1 Week
  – 1 Month
  – 6 months
  – YTD

  Using **Today** button displays the data for the current day. This is the same function as the Today option in the drop down box.

- **Get Call Data**

  Allows graphs of different types of call data based on the following selections:

  – CallAssociation
  – CallIDs
  – Performance
  – Call IDs Errors
  – Calls Abandoned
  – Calls Incomplete

  When a user makes a selection, another window pops up displaying the calls for the selected call data type corresponding to the same time period.

- **Auto Play**

  Provides the user with the option of cycling through all of the available graphs based on the selected time interval:

  – Off (default): the browser stays in the same graph.
  – 30 Seconds: The FADE browser cycles through to the next available graph every 30 seconds.
  – 1 Minute: The FADE browser cycles through to the next available graph every minute.
  – 2.5 Minutes: The FADE browser cycles through to the next available graph every 2.5 minutes.
  – 5 Minutes: The FADE browser cycles through to the next available graph every 5 minutes.
  – 10 Minutes: The FADE browser cycles through to the next available graph every 10 minutes.
  – 15 Minutes: The FADE browser cycles through to the next available graph every 15 minutes.

  The user must manually stop this feature by selecting the **Off** option.

- **Auto Refresh**

  This parameter is used to select how often the current graph is refreshed based on the following time intervals:

  – Off (default): The browser stays in the same graph.
  – 30 Seconds: The browser refreshes the current graph every 30 seconds.
  – 1 Minute: The browser refreshes the current graph every minute.
  – 2.5 Minutes: The browser refreshes the current graph every 2.5 minutes.
  – 5 Minutes: The browser refreshes the current graph every 5 minutes.
  – 10 Minutes: The browser refreshes the current graph every 10 minutes.
  – 15 Minutes: The browser refreshes the current graph every 15 minutes.

  The user must manually stop this feature by selecting the **Off** option.

  NOTICE:

  The **Auto Play** and **Auto Refresh** functions are mutually exclusive. Running these two features simultaneously on the local OSV-TM server may affect the server's performance.

7.6.3 How to Zoom on a Graph's Time Interval

The system allows the user to zoom-in on the graph, narrowing the time range for a more granular view.

Prerequisites

Adequate administrative permissions

The user is logged into the Trace Manager Portal (FADE).

Step by Step

Use the mouse to zoom in and out.

- To zoom in:

  Click on a **<start time>** any where on the graph, then drag your cursor to the **<end time>** to zoom into that period.

  The graph will auto adjust and display only the selected time frame.
- To zoom out:

  In the Navigation frame, press **Reset** in the Search section.

7.6.4 Hovering on a Graph's Point

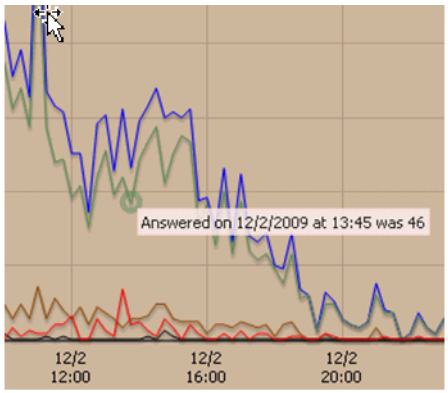
Detailed information about a point on the graph can be displayed by hovering over any of the plotted lines.

As the cursor hovers over the graph, a disk along with help text pops up providing information about the data on the x-y coordinate selected at that point.

The color of the disk changes according to the line you are hovering over.

The help text indicates:

- The name of the line plotted that the cursor in on
- The date and time at that point
- The value at the targeted point



7.6.5 Types of Graphs

The goal of the OpenScape Voice Trace Manager (OSV_TM) Visuals is to enable a level 1 technician to identify service affecting network conditions, and localize them to repairable network elements. The following graph types are provided:

- Calls
- Call Effectiveness
- Registration
- Media Packet Traffic
- Media Traffic Quality
- New and Stable Calls
- SIP Messaging

Each line on the graph represents a Key Performance Indicator and has a unique color.

In all graphs the X-Axis represents time of day.

The data points on the graph represent a cumulative total for the last 15 minutes.

The data points on the graph represent a cumulative total for the last 15 minutes.= Value at time t minus value at time t-1, where t = 15 Minutes

The y-axis, varies from graph to graph. See each graph's description for detailed information.

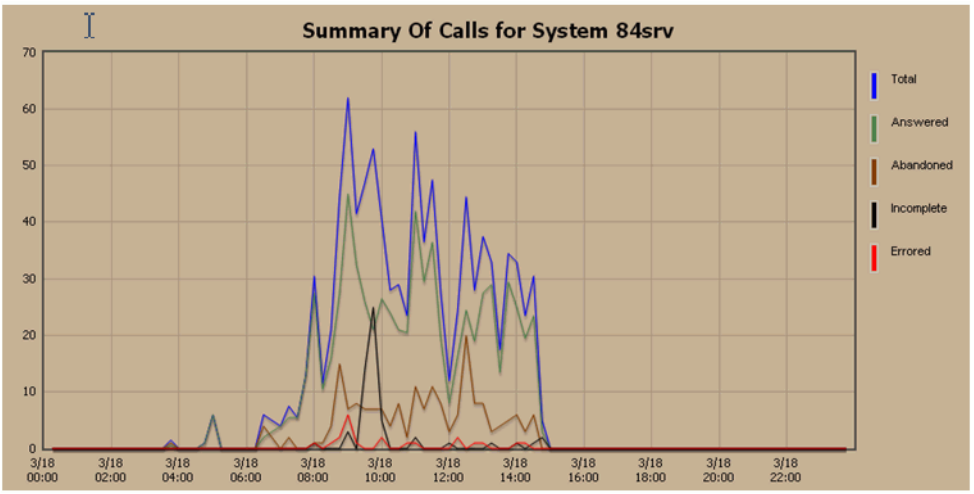
NOTICE:

Please note that due to the complexity of SIP managed calls the graphs cannot show exact call numbers, but only display trends over time.

The call results and numbers are derived from all involved half calls divided by two. This includes additional call legs triggered by service (serial ringing, simultaneous ringing, …) or by forking (multiple contacts or keyset line appearances).

Calls can be abandoned by the call originator or by the OSV itself when cancelling half calls on the terminating side of the call.

7.6.6 Calls



This graph displays the total number of calls received during a 15 minutes time interval. It shows lines for:

- Answered

  Calls that were answered by the B-party or the party forwarded to or by voicemail (connected calls), in general calls that resulted in a stable voice connection.
- Abandoned

  Calls that did not reach a voice connection, mainly calls that were cancelled by the originating party because the terminating party did not answer. In most cases these calls reach the ringing state.
- Errored

  Message flows that resulted in error (the request was not completed correctly). For non-call cases (register, subscribe and notify) it usually indicates a configuration error.

  For these call cases it is not necessarily an indication of a failed call. The error may have happened during the termination of the call (the call was answered correctly, but failed to disconnect correctly).
- Incomplete

  Calls that have just started and they are in the initial phases of call establishment. This is usually a temporary status. The status will be updated to one of the above (answered, error, abandoned, etc.) once more messages for the call are received and processed.
- Total

  This is sum of all calls in the systems during a 15 minutes time interval. It is the sum of all processed half calls (call legs) divided by 2. Due to the used calculating algorithms the 'Total' number is not necessarily the sum of the other numbers.

- What to look for

  Any Errored line above zero

  Answered unusually less than Total

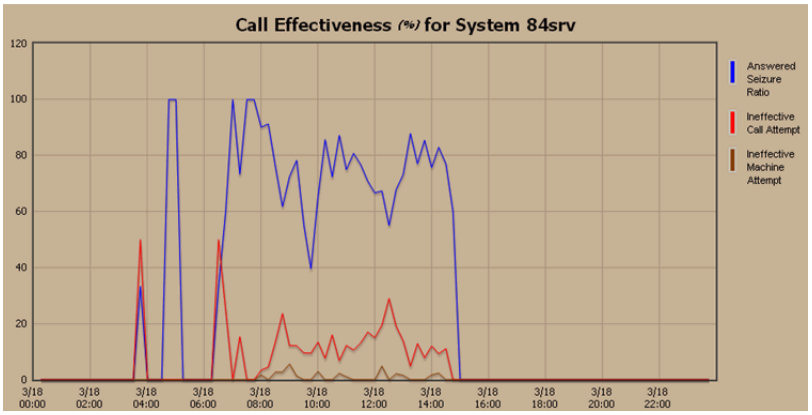
7.6.7 Calls Effectiveness

Answered Seizure Ratio

Ineffective Call Attempt

Ineffective Machine Attempt

What to look for



The y-axis, represents the percentage (%) and summed over a predefine time interval (default = 15 minutes).

This is the number of answered calls divided by the total number of calls attempted multiplied by 100. A total of zero calls is also shown as an Answered Seizure Ration of zero.

A Lower Answered Seizure Ratio number could be due to:

- Switch congestion
- Busy number
- Not answered by the called party

Answered Seizure Ratio = 100 * Σ SIP_Answered / Σ SIP_Invites

This is the sum of Abandoned and Errored calls divided by the total number of calls attempted multiplied by 100.

Ineffective Call Attempt = 100 * Σ (SIP_Abandoned+SIP_ErroredCalls) / Σ SIP_Invites

This is total of number of Errored calls divided by total number of calls attempted

Ineffective Machine Attempt = 100 * Σ SIP_ErroredCalls / Σ SIP_Invites

---

NOTICE:

SIP Invites = a dialed call

Calls Abandoned = A called abandoned by party "A" before ringing

Errored Calles = Calls refused for "any" reason

- Low Answer Seizure Ratio that can't be explained by no calls at all in the shown 15 minutes or by B-Party not answering
- Ineffective Call Attempts unusually high
- Non zero Ineffective Machine Attempts

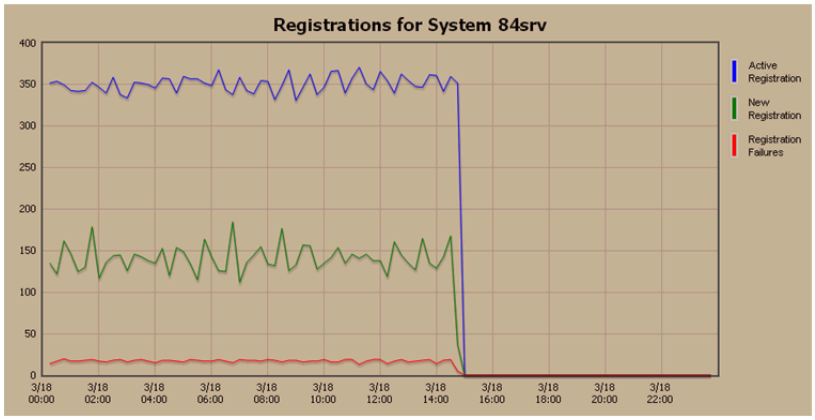
7.6.8 Registration

Active Registration

New Registration

Registration Failures

What to look for



The y-axis shows counts of Active and New Registrations. The count is an absolute value and summed over a predefined time interval (default = 15 minutes).

Sum of all endpoints that are currently registered.

It is the sum of all endpoints whose current time is between endpoint's last_register_time and next_register_time_due

Sum of SIP_Register messages received. It includes new registrations and re-registrations

Sum all registration requests that failed.

NOTICE:

"401 Unauthorized" error messages, as part of the registration process with Digest authentication active, are not considered as registration failures, thus they will not be displayed as such.

A drop in active registrations or new registrations.

- This may indicate a network or gateway failure that prevents endpoints from registering

A peak of new registrations:

- This may indicate a gateway returning from standalone where all endpoints register at the same time

---

NOTICE:

Increasing or decreasing registrations are not necessarily a failure indication. It could be that a majority of phones de-register or register during lunch time, night or weekend.

Registration Failures and/or increase of registration failures:

- During registration flooding it is ok that registration attempts are rejected

---

NOTICE:

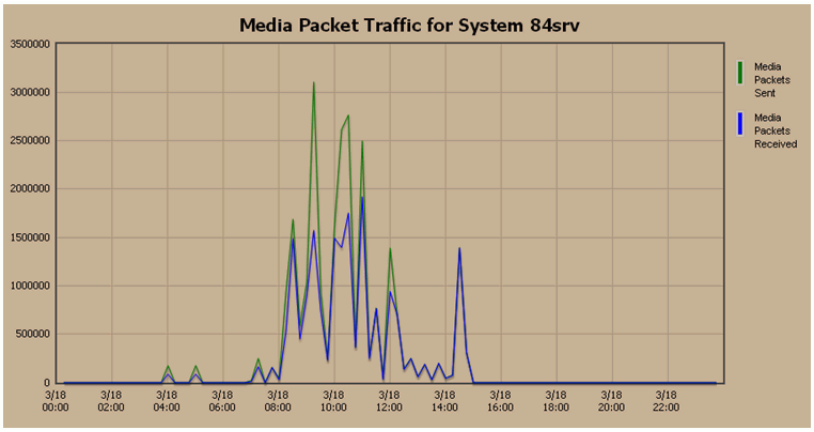
In an established system and when endpoints are configured to re-register after one hour, the active registrations are usually 4 times higher than the new registrations (60 minutes / 15 minutes).

7.6.9 Media Packet Traffic

Media Packets Sent

Media Packets Received

What to look for



The y-axis is a count of the sent and received media packets. The count is an absolute value and summed over a predefined time interval (default = 15 minutes).
Transmit_Packets, as reported by OpenScape SBC, phone on a per call basis.

Received_Packets, as reported by OpenScape SBC, phone on a per call basis.

- Unusual difference between sent and received packets
- Unusual drop in packets indicating no phone traffic

7.6.10 Media Traffic Quality

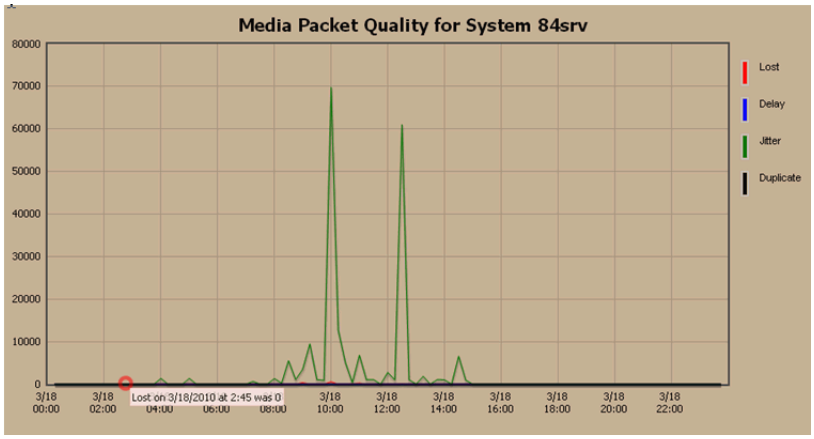
Lost

Delay

Jitter

Duplicate

What to look for



The y-axis is a count of the Lost, Delay, Jitter and Duplicate packets. The count is an absolute value and summed over a predefined time interval (default = 15 minutes).

Packets_Lost, as reported by OpenScape SBC, phone on per call basis. [Wikipedia Info on packet loss]

Packets_Delay, as reported by OpenScape SBC, phone on per call basis. [Wikipedia Info on packet transfer delay]

Packets_Jitter, as reported by OpenScape SBC, phone on per call basis. [Wikipedia Info on packet delay variation]

Duplicate_ Packets, as reported by OpenScape SBC, phone on per call basis.

packet loss > 1 or 2%

delay > 100 msec on WAN, > 10 msec on LAN

jitter > 50 msec on WAN, > 10 msec on LAN

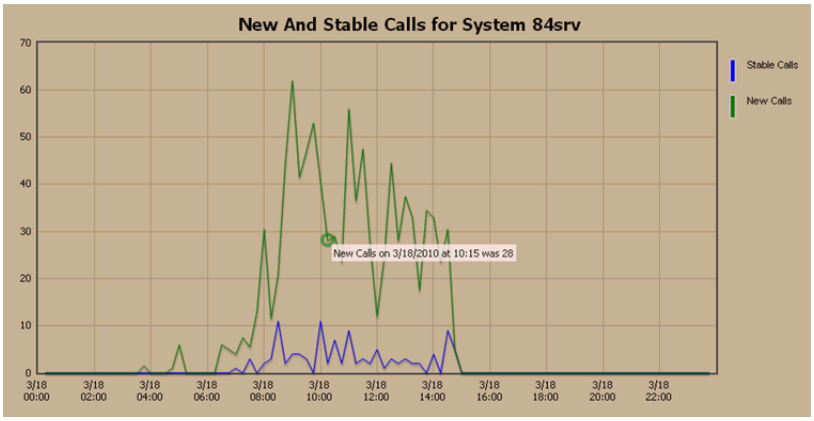
duplicate

7.6.11 New and Stable Calls

Stable Calls

New Calls

What to look for



The y-axis shows counts of Stable and New calls. The count is an absolute value and summed over a predefined time interval (default = 15 minutes).

Sum of all established calls in the system at the end of the monitored interval.

Sum of all in SIP_Invites divided by two.

Unusual Drop in stable calls

Unusual Change in new calls

With an average call duration of 3 minutes, 5 new calls in a 15 minute interval typically results in 1 stable call at the end of the 15 minute interval.

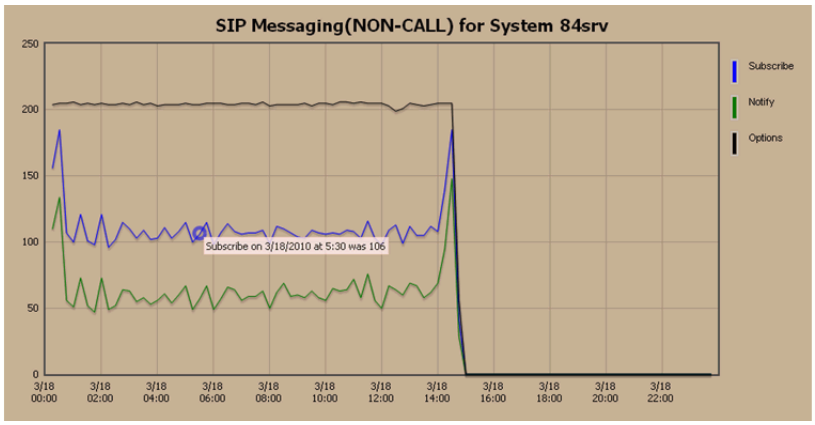
7.6.12 SIP Messaging

Subscribe

Notify

Options

What to look for



This graph describes the Option, Notify and Subscribe load on the system.

Σ SIP_Subscribe

Expressed as an absolute value and summed over a predefined time interval (default = 15 minutes).

Σ SIP_Notify

Expressed as an absolute value and summed over a predefined time interval (default = 15 minutes).

Σ SIP_Options

Expressed as an absolute value and summed over a predefined time interval (default = 15 minutes).

Any unusual drop or peak of one of the lines

7.7 Performance Monitoring from/to a Branch

Performance monitoring counters are counted for answered, not-answered and errored calls for Originating and Terminating on-net and off-net calls. These counters are maintained by the continuous tracing analyzer, i.e., OSV-TM, that documents the VoIP traffic to and from a branch.

Calls to a branch (terminating) are sent from the Openscape Voice switch (OSV) either

- directly to the gateway (for off-net calls) or
- to the OpenBranch (for on-net calls and, optionally, off-net-calls).

Calls from a branch (originating) are sent from the OpenBranch to the OSV.

The OSV-TM database that stores OSV trace information includes the branch name for traces of messages to and from a branch.

In the OSV-TM, a branch consists of an optional branch gateway (to identify offnet calls) and a set of the IP addresses of the branch:

- The gateway is identified by its IP address or FQDN
- The branch is identified either by
  - IP address or FQDN of the branch proxy

    or
  - IP subnet or an IP/FQDN pattern (regular expression) of the branch endpoints.

This information is stored in an OSV-TM configuration file.

7.7.1 How to Access Branch Status Report

The Branch performance graphs are accessed through the Branch Status View.

Prerequisites

Adequate administrative permissions.

The user is logged into the Trace Mangement Portal (FADE).

Step by Step

1) The Branch performance graphs are accessed through the "Branch Status" tab under the "OSV" view in FADE.

The default parameters to filter the branch status are:

- Filter by IP: IP = All
- Start Date = Current day
- End Date = Current day
- Start Time = 00:00:01 AM
- End Time = 23:59:59 PM
- Answer % <= 90%
- Error % > = 1%
- Abandoned % > = 5%
- Group With = OR
- Interval = Last Interval

The initial screen reports all the branches that met a search criteria based on the default filters.

2) Select the branch from list (column **Device_IP**).

3) Continue in the **Navigation Frame**

7.7.2 How to Set Filter for Branch Status Report

By changing filters, the user can generate different branch status reports.

Prerequisites

Adequate administrative permissions.

The user is logged into the Trace Manager Portal (FADE).

Step by Step

1) Navigate to **Branch_Status**

The default parameters to filter the branch status are:

- Filter by IP: IP = All
- Start Date = Current day
- End Date = Current day
- Start Time = 00:00:01 AM
- End Time = 23:59:59 PM
- Answer % <= 90%
- Error % > = 1%
- Abandoned % > = 5%
- Group With = OR
- Interval = Last Interval

2) Enter your settings in the **Filter** window:

- **Filter By**:

  “IP” or “Name”. The radio buttons set filtering by the branch’s IP or its name. Choose the parameter to filter by from the dropdown list.
- **Start Date**:

  Sets the start date to display data from.
- **End Date**:

  Sets the end date to display data for.
- **Start Time**:

  Sets the time to start viewing the data from.
- **End Time**:

  Sets the time to end viewing the data for.
- **Answer%**:

  Percentage of answered calls.
- **Error%**:

  Percentage of error calls.
- **Abandoned%**:

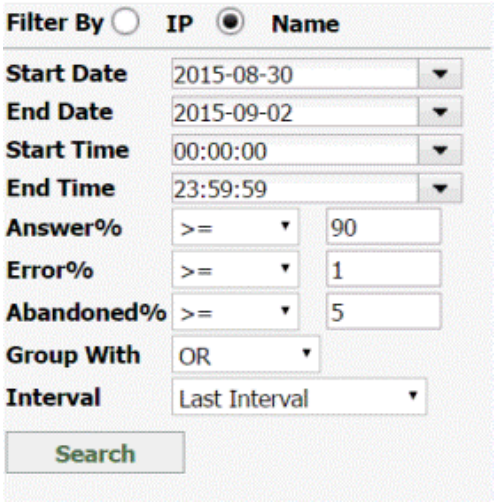
  Percentage of abandoned calls.
- **Group With**:

  AND/OR - Used to group the above parameters into one filter with a Boolean AND or OR.
- **Interval**:

  Interval that matched the search criteria. Possible selections: “All” or “Last Interval”.

3) Click **Search**

Example



7.7.3 How to use the Branch Graphs

The performance monitoring (PM) tables maintain counters for each monitored branch.

The performance monitoring report screen displays a windows with three graphs for answered, abandoned and errored calls. The window scope can be switched between the 5 selections shown in the 5 traffic categories.

Details on how to Use the Branch Graphs

There are 15 counters for each branch, 3 performance monitoring counters for each of the 5 traffic categories:

- All
- Originating on-net (invite from phone)
- Terminating on-net (invite to phone)
- Originating off-net (invite from gateway)
- Terminating off-net (invite to gateway)

The Performance Measure Counters (PM-Counters) are:

- Answered

  The call reached the talking state; (<->200 OK to an invite). (Note that a 3xx (redirection) is not counted as it eventually ends up in one of the 3 other counts.)
- Abandoned

  (Can also be called Not-Answered or Cancelled) The call was cancelled by the calling party (<->487-request-terminated). (Note that Alerting (180 or 183) may or may not have occurred before the cancellation.)
- Errored

  Either the session establishment fails with a 4xx, 5xx,or 6xx error code (except 401(DA) and 486(Busy) and 487 (cancelled)); or the invite did not have any answers (invites with a Call Id that only has Invites as associated messages i.e., Invites without any answers).

Each branch call (which is an OpenScape Voice half call) is grouped into the following classes:

	On-net	Off-net
Originating	OSV receives invite from phone	OSV receives invite from a gateway or SIP trunk
Terminating	OSV sends invite to phone	OSV sends invite to a gateway or SIP trunk

The sum of all branch calls is the sum of 12 counters:

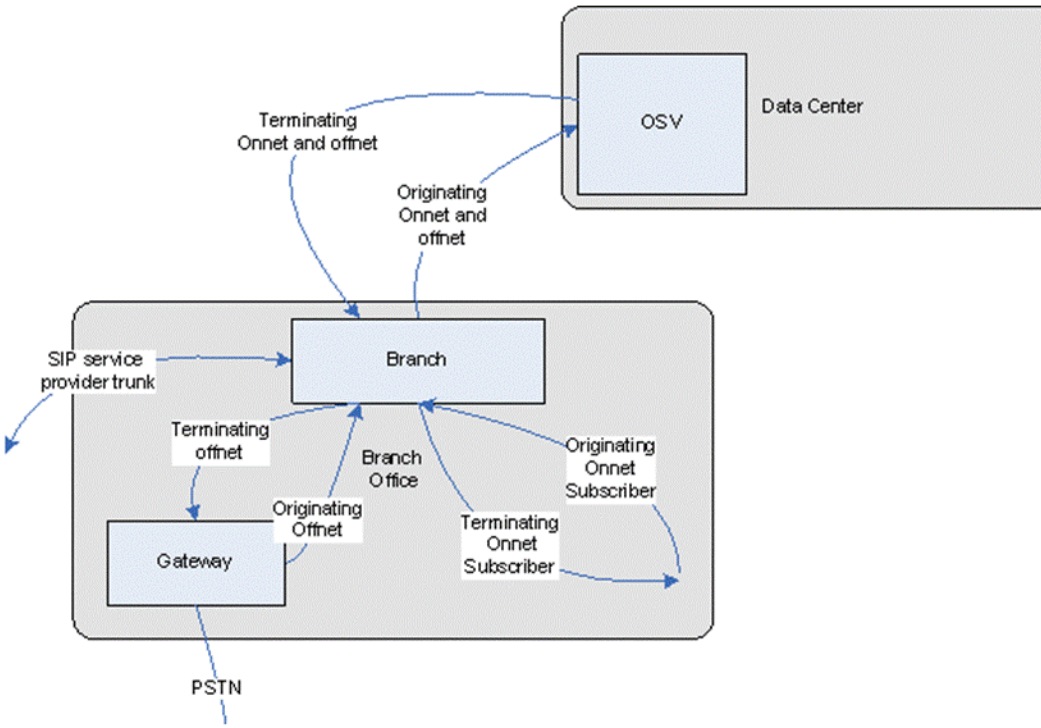
- Originating-on-net: Answered, Abandoned, Error
- Originating-off-net: Answered, Abandoned, Error
- Terminating-on-net: Answered, Abandoned, Error
- Terminating-off-net: Answered, Abandoned, Error

Example:

- Branch A gateway calls phone in Branch B. Phone does ot answer and A gives up:
- Branch A counter Abandoned is incremented for Originating-on-net
- Branch B counter Abandoned is incremented for Terminating-on-net

Example:

- Branch A phone calls phone in Branch B, which is completely outof service. A gives up:
- Branch A counter Abandoned is incremented for Originating-on-net
- Branch B counter Errored is incremented for Terminating-on-net



Other Characteristics

The percentage is zero if the denominator is zero. It is rounded up to the next integer.

The default Percentage thresholds are:

- 90 for Answered Percentage
- 10 for Abandoned Percentage
- 1 for Errored Percentage

7.7.4 OpenScape Branch Graph Types

There are five types of graphs for viewing Branch information: Originating-on-net (invite from phone), Terminating on-net (invite to phone), Originating off-net (invite from gateway), Terminating off-net (invite to gateway), All (showing all types). The default window is “All”.

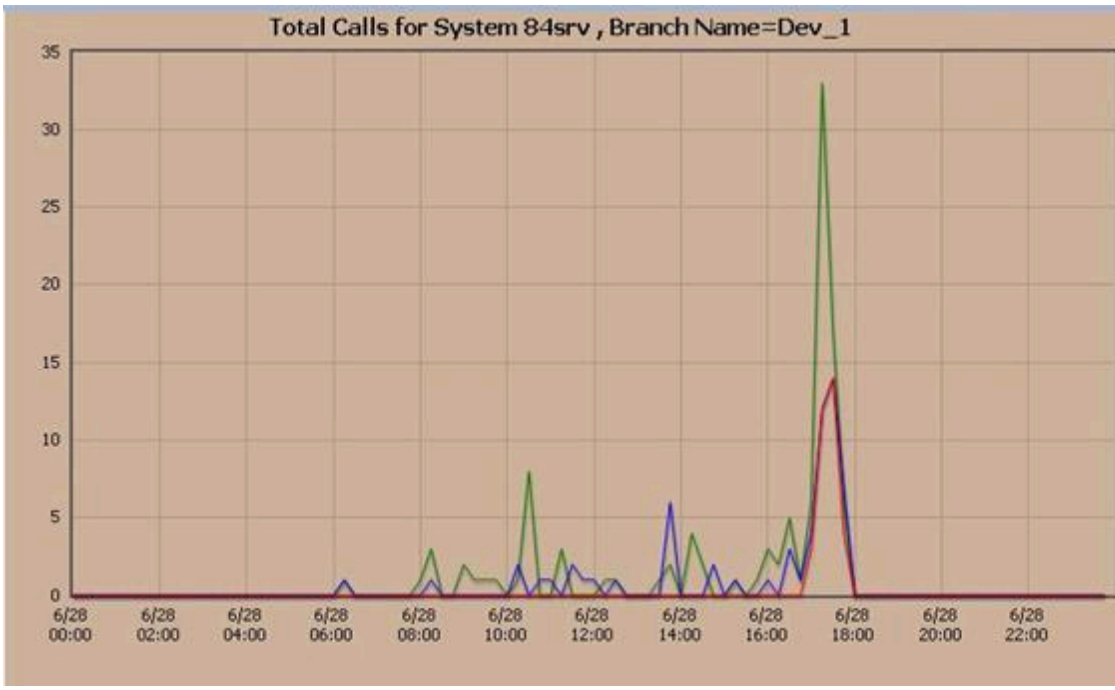
The same restrictions outlined in the section "Restrictions on Displaying Graphed Data" apply to the OpenScape Branch Graphs.

NOTICE:

The same restrictions outlined in the section titled: "Restrictions on Displaying Graphed Data" apply to the OpenScape Branch Graphs.

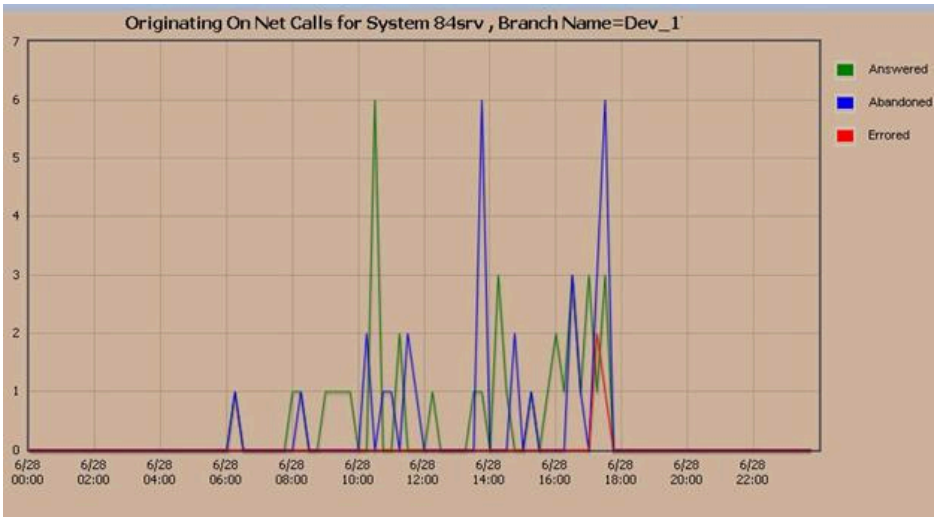
7.7.4.1 OpenScape Branch Graph: All Calls

This is a summary graph of Originating On Net, Originating Off Net, Terminating On Net, Terminating Off Net calls per time interval.



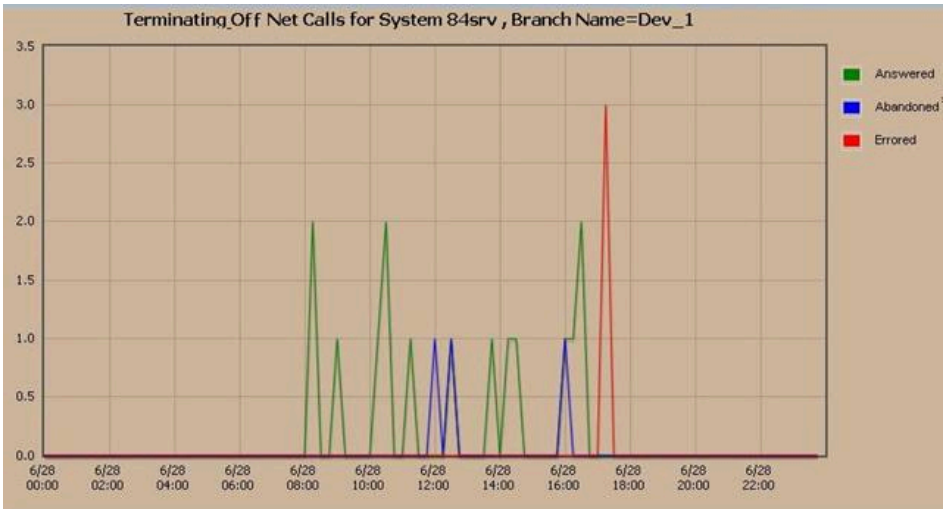
7.7.4.2 OpenScape Branch Graph: Originating On Net Calls

This graphic reflects the OpenScape Voice receives invite from phone.



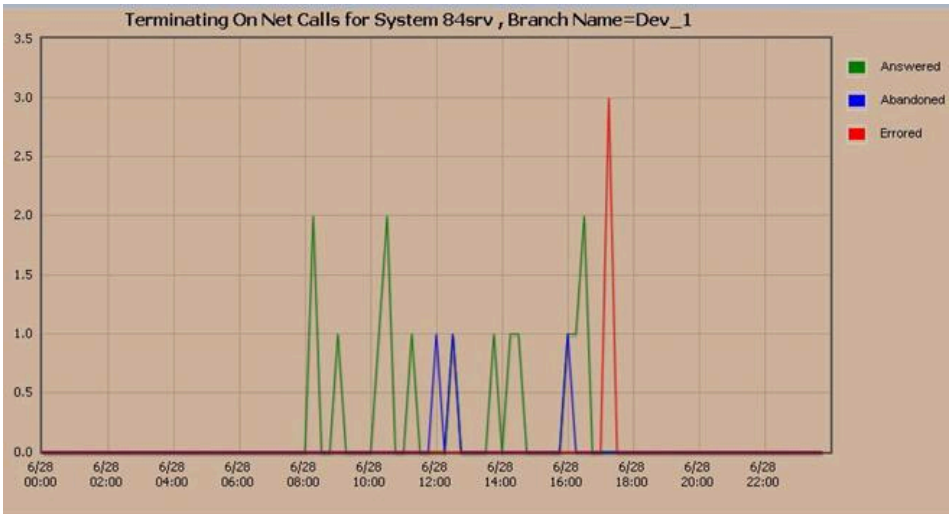
7.7.4.3 OpenScape Branch Graph: Originating Off-Net Calls

This graph reflects the OpenScape Voice OSV receives invite from a gateway.



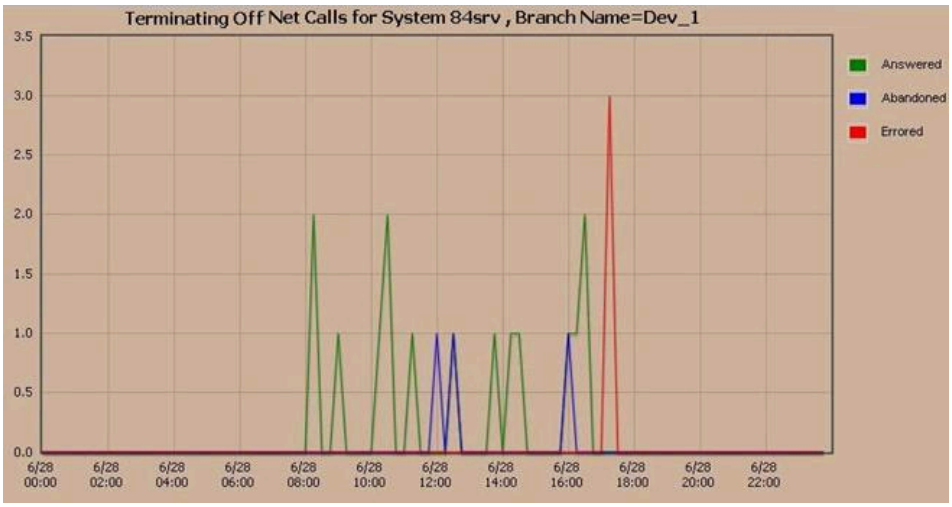
7.7.4.4 OpenScape Branch Graph: Terminating On-Net Calls

OpenScape Voice sends invite to phone.



7.7.4.5 OpenScape Branch Graph: Terminating Off Net Calls

This graph reflects the OpenScape Voice sends invite to Gateway.



7.8 OpenScape Voice Resource Graphs

The Resource graphs display quasi-real-time charts Resource usage and Performance counters for the OpenScape Voice system.

Types of Graphs

The following information is available through the resource graphs:

- **CPU Usage** (CPU usage of node and selected processes)
- **CPU Core Usage** (CPU usage in percentage of each single Core)
- **Performance** (X-channel delay and Internal response times)

- **Memory** (Amount of Free / Used / Cached Memory / Swap memory used)
- **Swap Memory Used** (Percentage of used Swap memory)
- Swapping Frequency
- **Registration and Call Statistics** (Number of currently active registrations stored in the local node (i.e., in memory))
- **Logging** (Number of logging messages per category)
- **Process Queues** (RTP-Message Queue fill level of selected processes)
- **Ethernet IO** (Amount of bytes sent/received per bonding/Ethernet interface)
- **Database** (SolidTech database statistics read from SolidTech PMON tool)
- **Disk Partition Level** (Fill level in percent of all OSV disk partitions)
- **Disk I/O** (Average number of Bytes sent/received from disk)

Restrictions on Displaying Graphed Data

If multiple systems are configured in the OSV-TM server, only the graphs for one system can be displayed and refreshed at a time. This is a restriction of the web browser.

Displaying the performance graphs is a memory intensive feature supported mainly on IE 8 and Firefox 3.5.7 -or later versions.

NOTICE:

The same restrictions outlined in the section titled: "Restrictions on Displaying Graphed Data" apply to the OpenScape Branch Graphs.

General Notes:

Each line on the graph represents a KPI and has a unique color.

In all graphs the X-Axis represents time of day.

The y-axis, on the other hand, varies from graph to graph.

The data points on each graph represent a cumulative total for the last 5 minutes or for some graphs it shows the average, for example, value at time t minus value at time t-1, where t = 15 minutes).

See each graph's description for detailed information.

7.8.1 How to Use Resource Graphs

The Resource graphs are displayed through FADE by selecting the "OSV" view then the "Resources" tab.

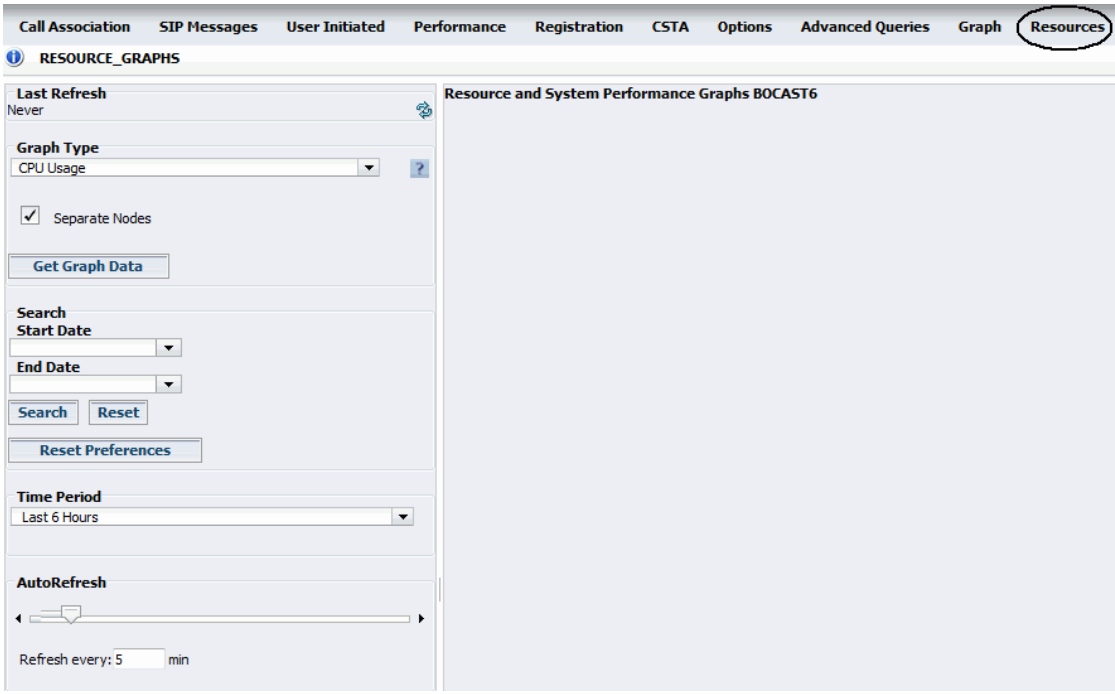
Prerequisites

Adequate administrative permissions.

The user is logged into the Trace Mangement Portal (FADE).

Step by Step

Navigate to **OpenScape_Voice > Resources**



Each line on the graph represents a Key Performance Indicator and it is assigned a unique color at runtime.

The x-axis always represents the date and time that the sample was taken while the y-axis varies from graph to graph. See each graph's description for detailed information.

The data points on each graph represent a cumulative total for the last 5 minutes or for some graphs it shows the average (i.e.: value at time t minus value at time t-1, where t = 15 minutes).

The navigation frame to the left of the graph screen allows the user to change the filtering parameters for the data to plot. The datasets Performance Indicators in each graph can be turned on or off by right-clicking on the graph’s drawing areas.

Example

Resource Graphs Navigation Frame

The Resource graphs Navigation frame is used to change the different parameters for displaying graphed data.

- Last Refresh: Indicates the date and time when the current graph was refreshed

  The small "Icon" inside the "Last Refresh" box, gives you the option to force a graph refresh
- Graph Type: Use the pull down list to select which graph type to display.

  Use the 'Separate Nodes' check box to draw each node of a monitored cluster on its individual graph. If this box is left unchecked, then a single

graph will be drawn for both nodes in the monitored OpenScape Voice system.

The help icon next to the selected graph type, "?", will open a help page with information about the graph.

NOTICE:

The selected graph options are preserved even if you navigate away from OSV-TM. Clear your browser cookies or use the 'Reset Preferences' Button to reset.

- Search: Allows you to plot data satisfying the selected date range in the current graph type
  - Start Date
  - End Date
  - Search (button)
  - Reset (button)
- Time Period: Provides a drop down box that allows you to select a "predefined" time interval and plot it in the current graph.
  - Last Hour
  - Last 6 Hours
  - Last 12 Hours
  - Last 24 Hours
- Auto Refresh: Allows you to choose how often the current graphs are automatically refreshed based on the time intervals selected with the slider.

  The default refresh period is 5 minutes.

  The graphs will not be automatically refreshed when the slider is at the '0' position.

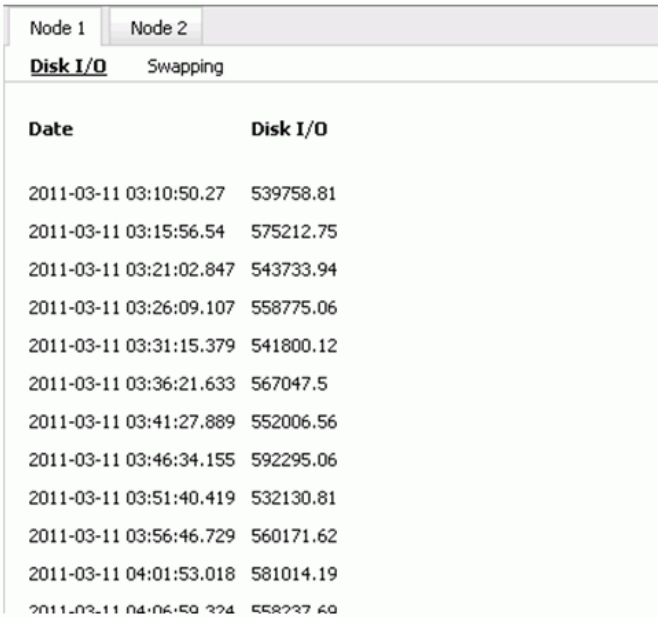
  The maximum time interval than can be selected is 60 minutes.

  NOTICE:

  The slider will automatically reset to the '0' position when the search feature is used.

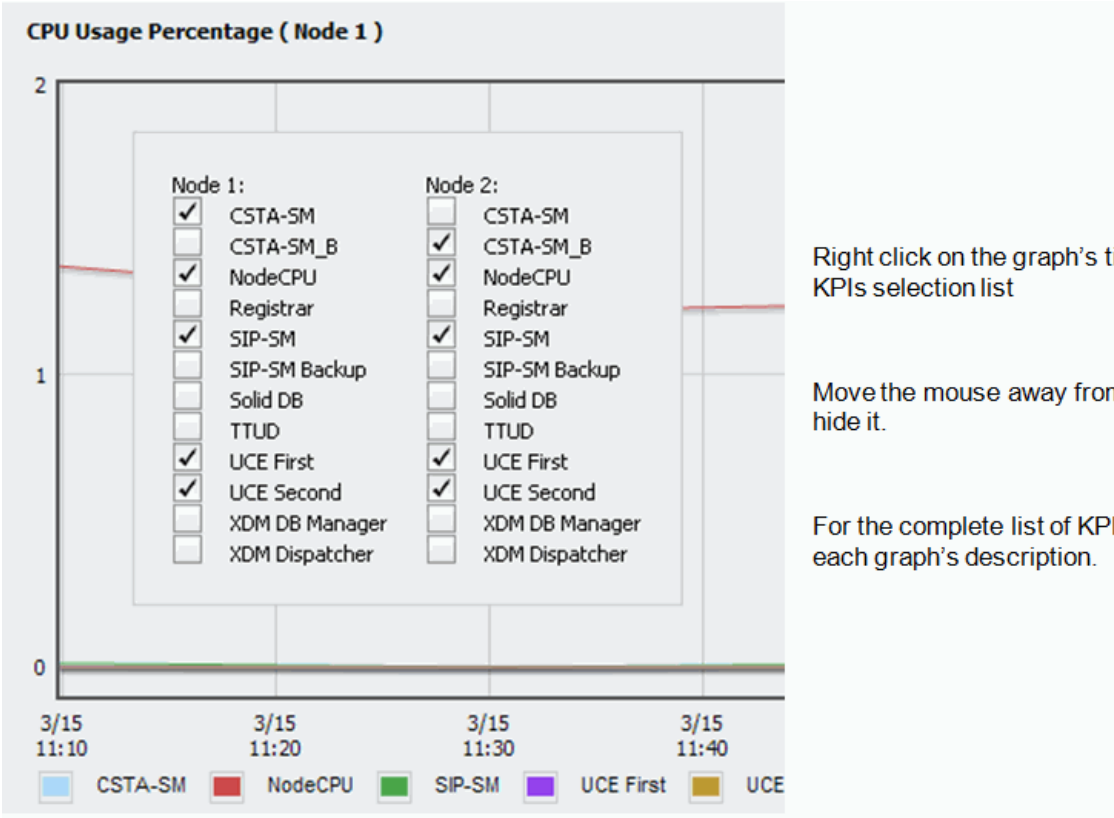
- The "Reset Preferences" button resets the graph displays to the default settings as follows:
  - Last Refresh indicates the date and time when the user performs the last reset operation.
  - Time period = Last Hour
  - Auto Refresh Period = 5 min
  - Search Start Date = Current date
  - Search End Date = Current date
  - The default displayed Graph Type is reset to "CPU Usage"

- Get Graph Data: when this button is pressed, the system will get and display the raw data used to display the currently selected graph for the selected search parameters. Example:



Selecting the Data to Display on each Graph

Each graph has a predefined list of available Key Performance Indicators (KPI) that may be displayed by right clicking on the graph's Title.



Zooming on a Graph's Time Interval

The system allows you to zoom-in on the graph narrowing the time range for a more granular view.

Zoom in - To zoom on a particular time interval:

- Using the mouse, click on a start time any where on the graph, then drag your cursor to the end "time" to zoom into that period.
- The graph will auto adjust and display only the selected time frame.

NOTICE:

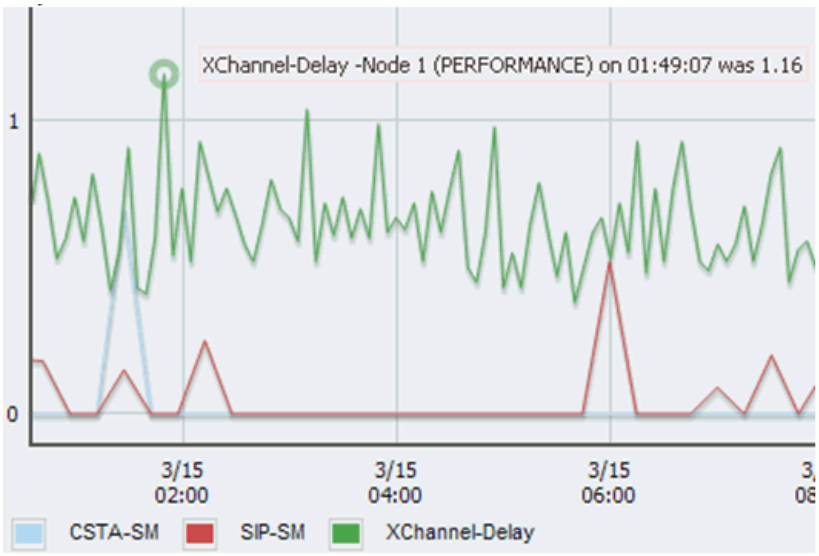
The minimum zoom-in interval is 10 minutes.

Zoom out - To zoom out of the graph:

- In the Navigation frame, press the "Reset" button in the "Search" section

Hovering on a Graph's Point

You can display detailed information about a point on the graph by hovering on any of the plotted lines.



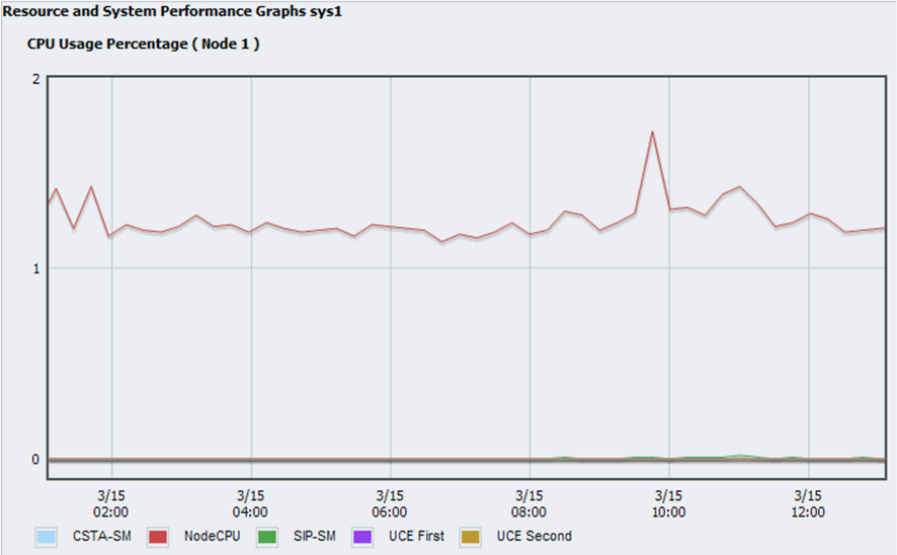
As the cursor hove
disk along with "he
giving information
the x-y coordinate
point.

The color of the di
according to the da
hovering on.

The help text indic
- The name of the
cursor is on.
- The time at that p
- The value at the

7.8.2 Resource Graph: CPU Usage

This graph displays the five minute average of CPU usage over all CPU cores.



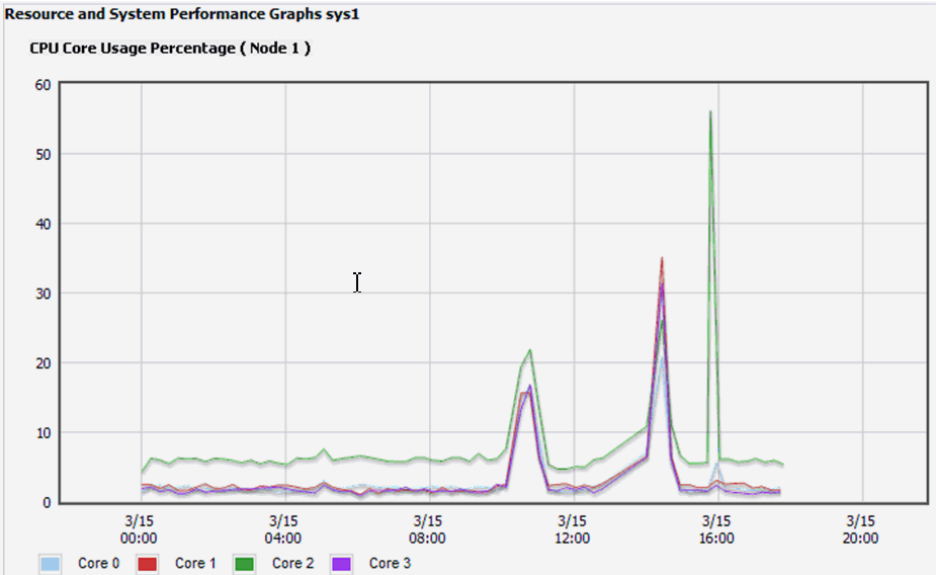
Besides the overall CPU usage of the displayed node, the user can also display the CPU usage of the following selected processes:

- CSTA-SM
- NodeCPU
- Registrar
- SIP-SM
- SIP-SM-Backup
- Solid-DB
- TTUD
- UCE First
- UCE Second
- XDM DB Manager
- XDM Dispatcher

7.8.3 Resource Graph: CPU Core Usage

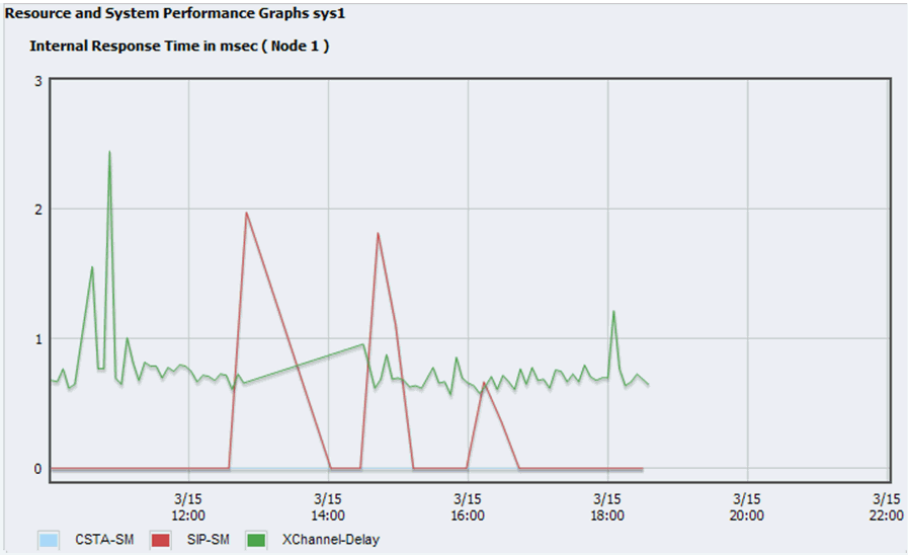
This graph displays five-minute average of CPU usage over all CPU cores.

The number of cores depends on the OSV server hardware type.



7.8.4 Resource Graph: Performance

This graph displays the five minute average of the response times in milliseconds of selected processes as well as the X-Channel roundtrip delay.

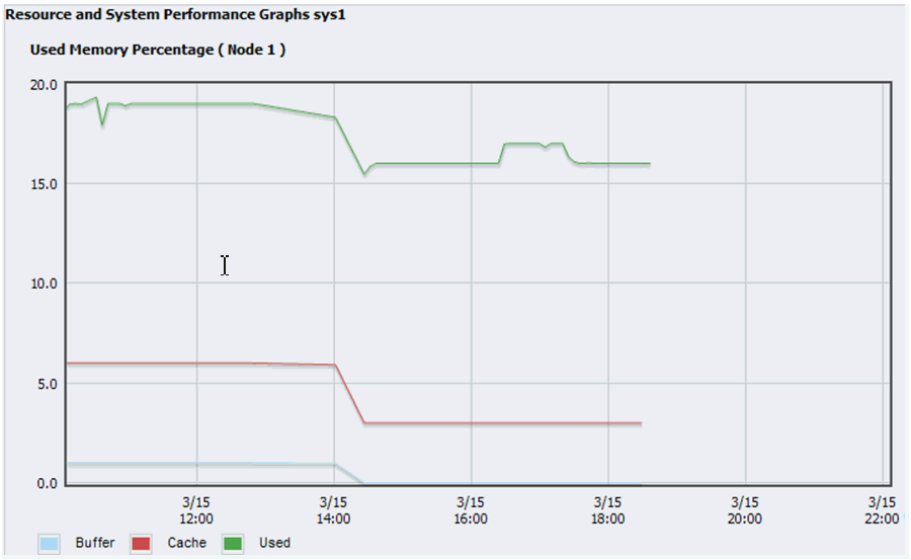


The following processes are monitored:

- CSTA-SM
- SIP-SM
- SIP-SM-Backup
- XChannel-Delay

7.8.5 Resource Graph: Memory Usage

This graph displays the five minute average percentage of buffers, cached and used memory.

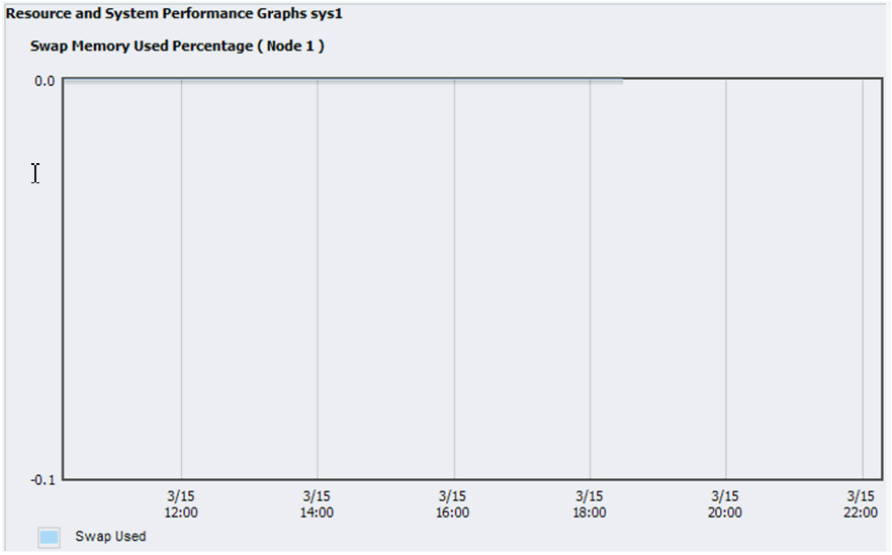


The following KPIs are displayed by default:

- Buffer memory
- Cache memory
- Used memory

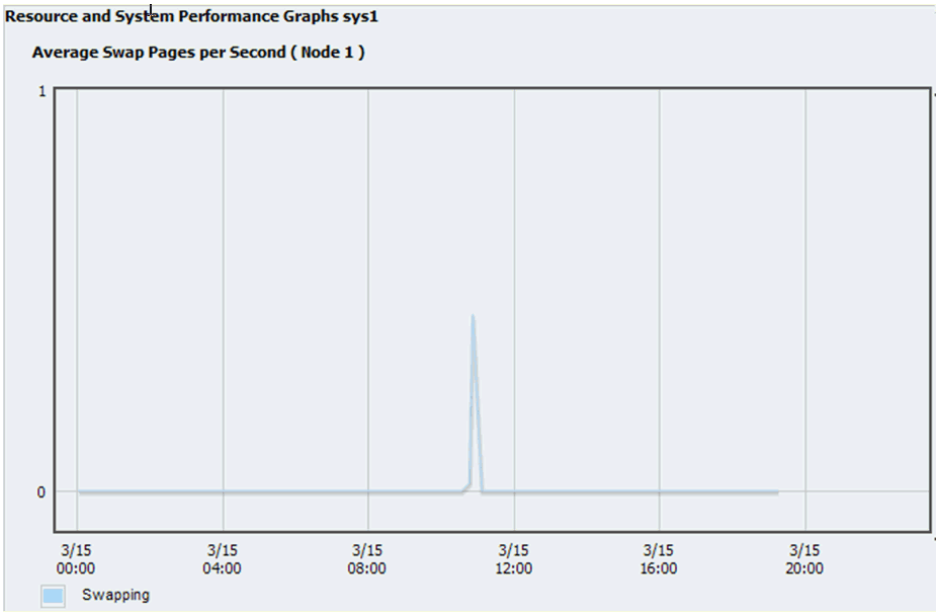
7.8.6 Resource Graph: Swap Memory Used

This graph displays the percentage of used swap space. Used Swap percentage is calculated from /proc/meminfo as 100 * (Swap total - Swap free) / Swap total.



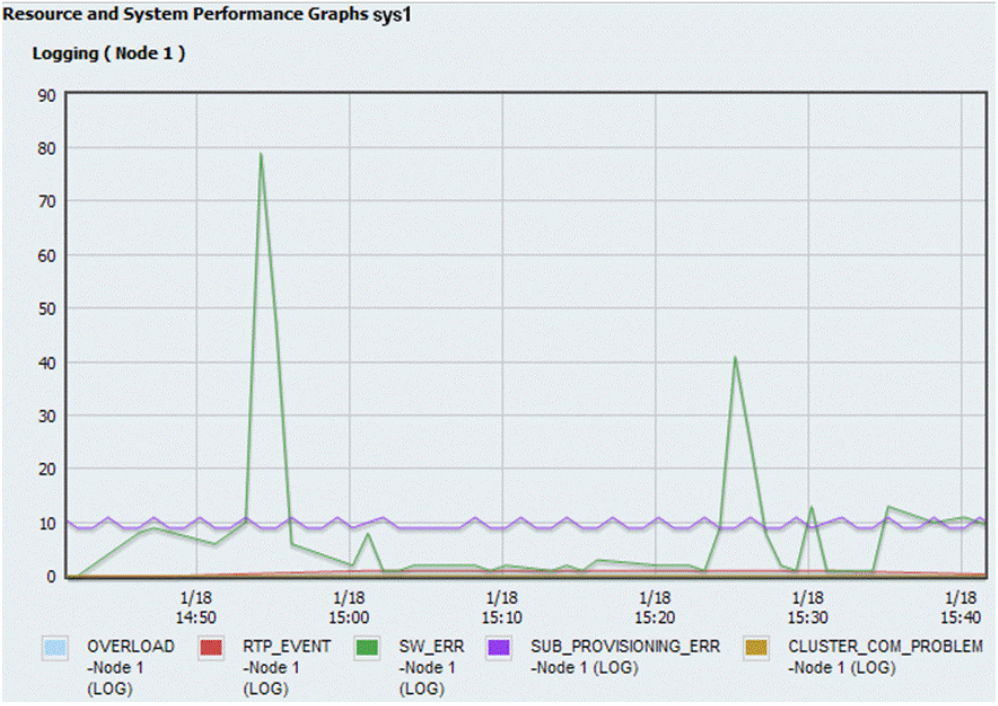
7.8.7 Resource Graph: Swap Frequency

This graph displays the average number of swapped pages per second. It is expected that OSV does not swap pages during normal operation. Constant swapping is an indication for too little memory (RAM) or for a SW error.



7.8.8 Resource Graph: Logging

This graph displays the average number of OP-RTT logging calls per minute.



Only up to six KPIs can be plotted on this graph at the same time. The following parameters are displayed by default:

- Cluster Com Problem
- Overload
- RPT Event
- Sub provisioning Err
- SW Err

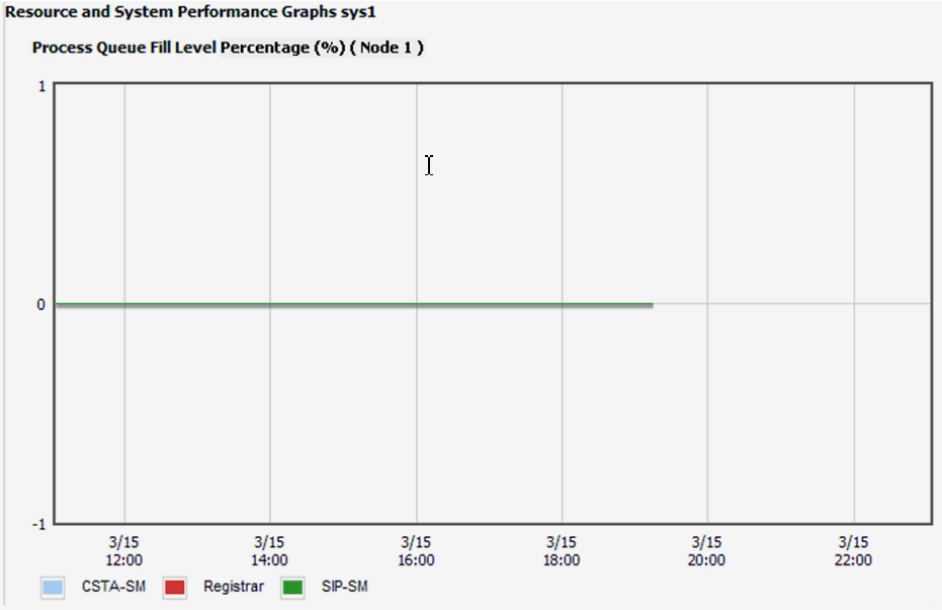
The available logging categories are:

- ALERT_GENERAL
- API_ERR
- AUDIT
- AUDIT_ERR
- CALL_PROC_ERR
- CALL_TRACE
- CLUSTER_COM_PROBLEM
- COM_EXT_BAD_SYNTAX
- COM_EXT_PROTOCOL_ERR
- COM_EXT_RESP_ERR_RX
- COM_EXT_TIME_OUT
- COM_INT_BAD_SYNTAX
- COM_INT_PROTOCOL_ERR
- COM_INT_RESP_ERR_RX
- COM_INT_TIME_OUT
- DATA_ERR
- DATABASE_CON_ERR
- DATABASE_ERR
- DATABASE_SQL_ERR
- DNS_UNAVAILABLE
- END_POINT_EXPIRED
- END_POINT_INS
- END_POINT_INVALID
- END_POINT_OOS
- IPSEC_ERR
- LICENSING
- LINK_ERR
- LOG_FAILURE
- MAINTENANCE
- OVERLOAD
- PROC_EXIT
- PROC_INIT_FAILURE
- PROC_INIT_SUCCESS
- PROVISIONING_ERR
- RES_MGMT_COMM_ERR
- RESOURCE_LIMIT
- RSIP_RX
- RTP_API_ERR
- RTP_EVENT
- SRVR_OR_GW_OVERLOAD
- SRX_LOG_ALERT

- SRX_LOG_ALWAYS
- SRX_LOG_EVENT
- SRX_LOG_INFO
- SRX_LOG_SW_ERR
- SUB_PROVISIONING_ERR
- SW_ERR
- VIP_SUBSCRIBER_PROBLEM

7.8.9 Resource Graph: Process Queues

The Process Queues graph indicates the five-minute average message queue fill level percentage of selected processes plus the number of sent and received messages and the average time spent in the queue.



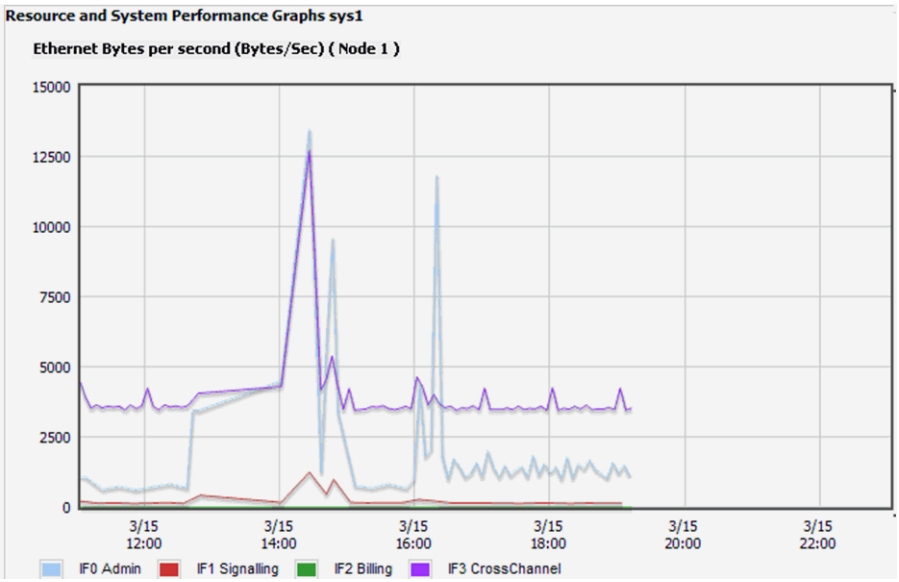
The processes that can be monitored are:

- CSTA-SM
- Registrar
- SIP-SM
- SIP-SM-Backup
- UCE First
- UCE Second
- XDM Dispatcher
- XDM DB Manager

Only up to six KPIs can be displayed concurrently simultaneously on this graph.

7.8.10 Resource Graph: Ethernet I/O

This graph displays the average number of Bytes per second sent and received per Ethernet or bonded Ethernet pair.

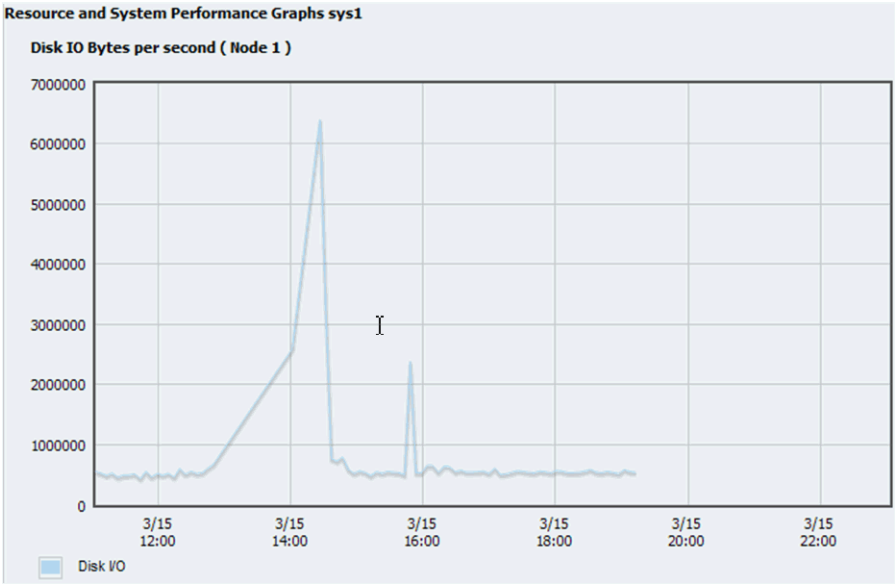


The Interfaces that can be monitored are:

- IF0 Admin
- IF1 Signaling
- IF2 Billing
- IF3 CrossChannel

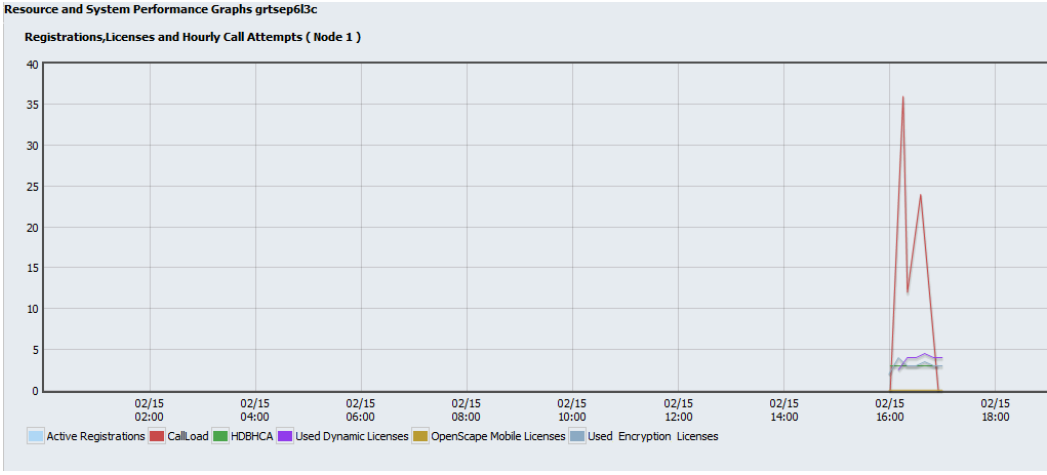
7.8.11 Resource Graph: Disk I/O

This graph shows the average number of Bytes sent to and received from disk.



7.8.12 Resource Graph: Registration and Call Statistics

This graph shows the number of active registrations, the predicted busy hour call attempts value (BHCA) based on the last 5 minutes of call attempts, the highest hour call attempt number over the past week (i.e.: HDBHCA = High Day Busy Hour Call Attempts), and the number of used licenses split into used OpenScape Mobile licenses, Used Dynamic Licenses and Used Encryption Licenses.

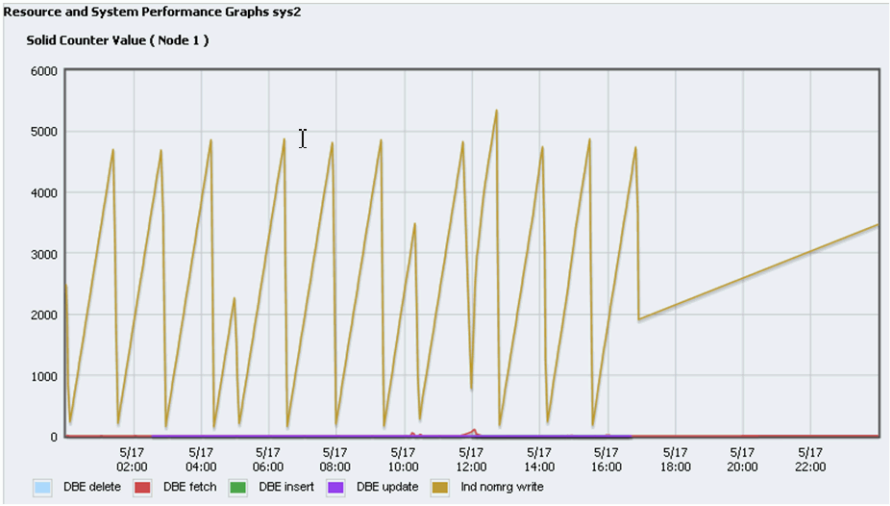


The following KPIs can be monitored:

- Active Registration
- CallLoad
- HDBHCA
- Used OpenScape Mobile Licenses
- Used Dynamic Licenses
- Used Encryption Licenses
- Used Essential Licenses
- Used Basic Licenses

7.8.13 Resource Graph: Database

The Solid Counter Value or Database graph displays for every 5 minutes the per-second average of SolidTech database statistics read from SolidTech PMON tool.



The following statistics values are shown by default:

- DBE delete
- DBE fetch
- DBE insert
- DBE update
- Ind nomrg write

Right click to see a list of all available attributes and to select or remove them from display.

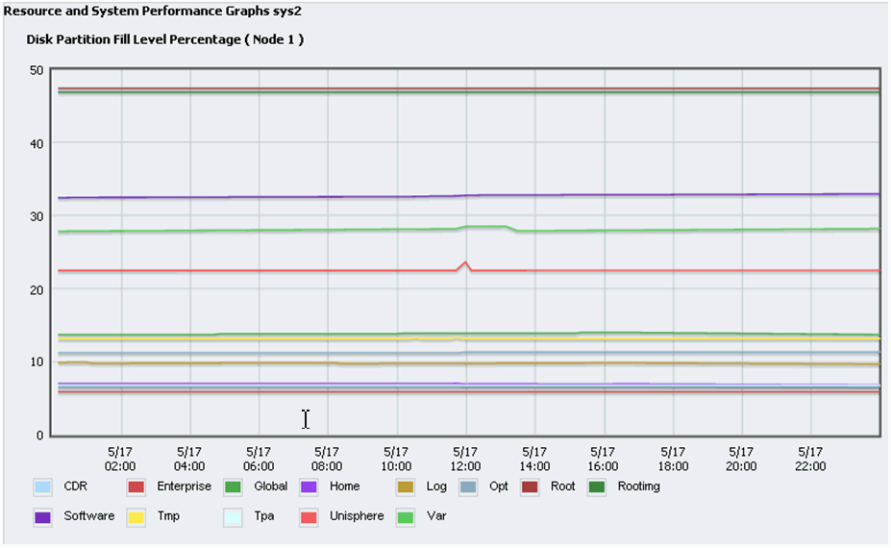
Attribute Description

Counter	Type	Description
Backup active	Backup	Indictes if a Backup is active. Values are 1/0 (Yes/No).
Backup step	Backup	Dababase backup steps/ sec
Cache find	Cache	Cache fetches/sec
Db free size	DB	Free space in the database (page level) in KB
DBE delete	DBE	Table engine row deletes/sec
DBE fetch	DBE	Table engine row fetches/sec
DBE insert	DBE	Table engine row inserts/ sec

Counter	Type	Description
DBE update	DBE	Table engine row updates/sec
File append	File	File append calls/sec
File flush	File	File flush calls/sec
File lock	File	File lock calls/sec
File open	File	File open calls/sec
File read	File	File read calls/sec
File write	File	File write calls/sec
HSB cached bytes	HSB	Primary/Secondary: current size memory based log buffer, in bytes
HSB operation count	HSB	Primary/Secondary: transferred log record/ sec
Ind nomrg write	Ind	Number of non merged rows (committed and uncommitted)
Log file write	Log	Log block writes/sec
Log write	Log	Log record writes/sec
Mem size	Mem	Total size of dynamically allocated memory in KB
Merg oper	Merge	Lower-level merge operations/sec
Merge quickstep	Merge	Quick merge steps/sec
Merge step	Merge	Full merge steps/sec
Proc exec	Proc	Procedure executions/ sec
Search active	Search	Table engine-level active searches
SQL execute	SQL	SQL execute statements/sec
SQL fetch	SQL	SQL fetch statements/ sec
SQL prepare	SQL	SQL perpare statements/ sec
Trans buf	Trans	Current transaction buffer size
Trans commit	Trans	Committed transactions/ sec

7.8.14 Resource Graph: Disk Partition Fill Level Percentage

This graph shows the fill level in percent of all OSV disk partitions with the exception of the swap space, which is shown in a separated graph.



All KPI's are plotted by default:

- CDR
- Global
- Log
- Root
- Software
- Enterprise
- Home
- Opt
- Rooting
- Tmp

7.9 Call Analyzer

The purpose of the RTT Call Analyzer is to correlate call trace records into individual call records and provide a number of display options for analyzing and reporting the data. The Call Analyzer relies on the properly decoded output of the oprtt_msg_filter to perform this analysis.

The Call Analyzer GUI provides the ability to click on a message in the call flow display to see the message details in another window.

Functional Sequence

Trace files are analyzed on startup, but data is not displayed until the user requests it. When analysis is completed, the **Display** button shows the call flow. The Call Analyzer correlates the trace data with the call records and displays the data in conjunction with the call flow. When the graphical interface is used in conjunction with the offline tool installation procedures for offline workstations, the interface also supports the decoding of raw trace data using the RTT reader and message filter.

The Call Analyzer graphical user interface is comprised of five separate screens, for the various analysis functional areas. These screens are accessed via the following tabs:

- Analysis Screen
- Call Data Screen
- List Data Screen
- Sequences Screen
- Statistics Screen

System Specific Information

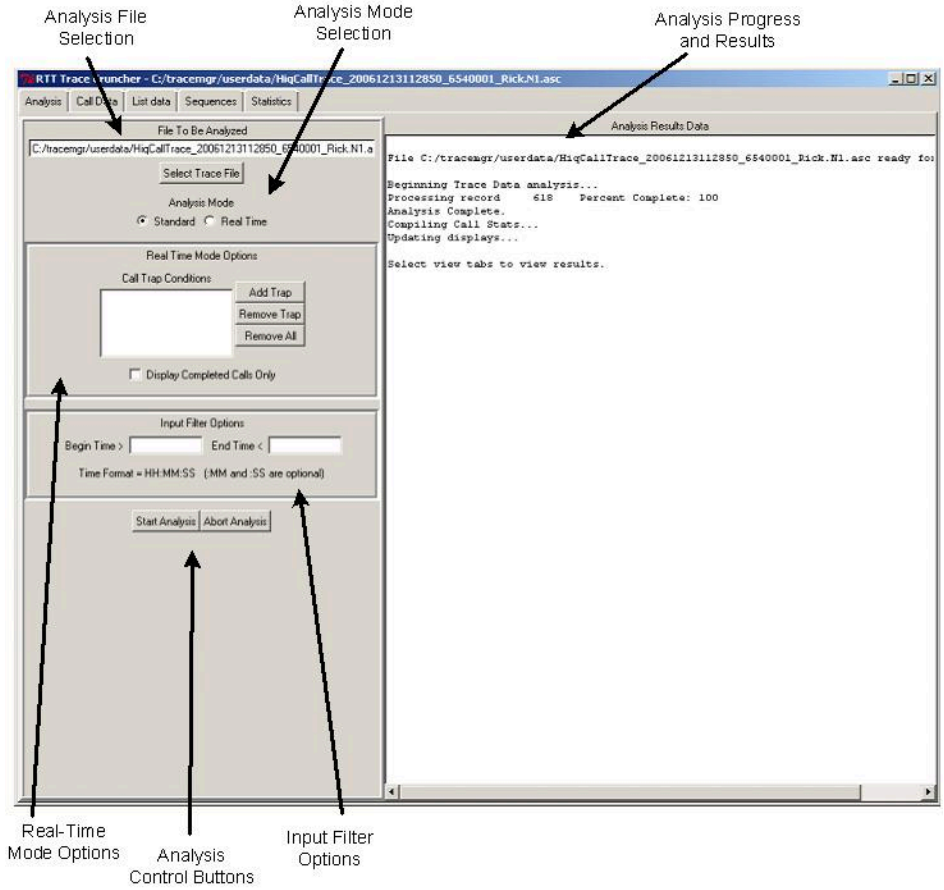
The Call Analyzer GUI is started from the Trace Manager tool using the **Analyze Trace File** button on the Trace Analysis page. The Call Analyzer is invoked as a separate GUI and, once started, is completely independent of the Trace Manager GUI.

Other Characteristics

The Call Analyzer is also referred to as trace analyzer.

7.9.1 Call Analyzer Analysis Screen

The Analysis screen is the initial startup screen. From this screen, the user can select the analysis file and options, start or stop the analysis, and display the progress of the analysis.

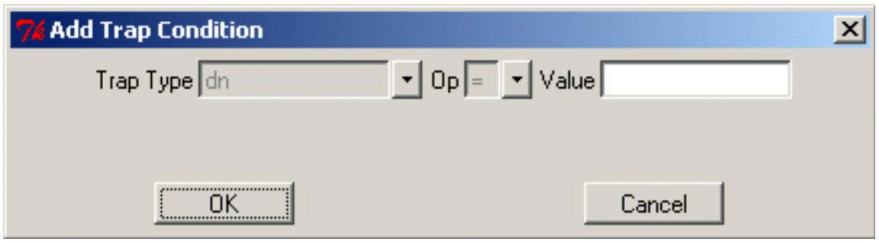


The user selects the file to be analyzed via the fields in the **Analysis File** section. The file name can be selected from a graphical file selection dialog by clicking on the **Select Trace File** button. If a path is not supplied, the current working directory is used. Click the **Start Analysis** button to begin the analysis.

Under **Analysis Mode**, the user can select either **Standard** or **Real Time** mode.

Real Time Mode Options allows the subscriber to set options used during real mode analysis. This includes the setting, modifying, and removal of call trap conditions and the setting of the **Display Completed Calls Only** option. Both of these can also be set via command line parameters. The list of Trap conditions can also be controlled using the three control buttons to the right of the list. An unlimited number of trap conditions can be entered into the list; however, only one trap condition of a given type can be entered.

The **Add Trap** button displays a dialog so the the user can set a new trap condition or modify an existing trap condition. The Trap Type is selected from a drop down list of available trap types populated from the call analysis modules. The **Op** is selected from the list of either "=' (equal to) or "!=" (not equal to). The value must be entered directly into the field and may be either an exact value or a regular expression syntax, if delineated with "/" characters (i.e., /904532\d000/).



Analysis Control buttons provide control over the analysis process. The **Start Analysis** button starts a pending analysis after a file has been selected, while the **Abort Analysis** button stops an analysis in progress.

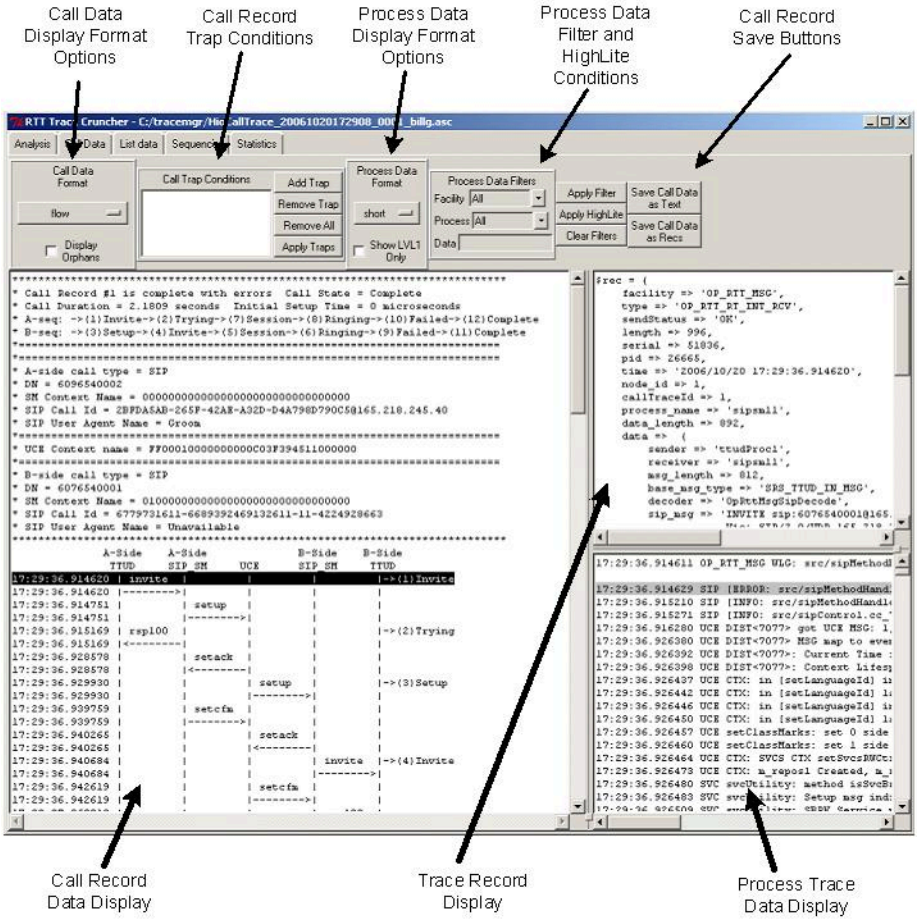
The **Input Filter Options** allows the user to set the input filter options used during analysis. Using these options, the user can restrict the trace analysis to a given subset of the input data by defining a time based "window" to be analyzed. The only records analyzed are those that fall within the window.

The **Analysis Progress and Results** window displays the progress and results of the current analysis. This includes the current record number being processed and a percentage complete indication as well as the completion indications. When running the analyzer in real mode with interval stats, the stats will be displayed here at the selected intervals.

7.9.2 Call Analyzer Call Data Screen

The Call Data Screen displays the analyzed call record data.

Options are provided to choose the call and process data display formats, to selectively trap individual call records, to filter or highlight selected process trace data and to save individual call records in text or Perl record formats. Frame adjusters allow the relative size of the three display panes to be adjusted to suit the users' preferences.



The **Call Record Data Display** window displays the call records created during call analysis, if any. If no call records were created, a message is displayed indicating no call records are available. The format of the data displayed here will vary depending on the chosen call data format and other options, but generally each call record display will consist of the following sections:

- A call record header showing the call record number, the state of the call, the duration and setup time, and the call sequence summary for each leg of the call.
- An A-side call leg header showing the A-side call type, the directory number involved, and a list of call type specific information for the call leg.
- An UCE information header showing the UCE context ID.
- A B-side call leg header for each additional call leg showing the call type and the call type specific data for that leg.
- The message list for the call, displayed in the selected format.

The **Trace Record Display** displays the details of an individual message trace record selected from the call record data display. This window is updated when the user left-clicks on any displayed message in the call record data display window. Records are displayed in their full decoded Perl record format.

The **Process Trace Data Display** window displays a list of all process data analyzed as part of the call analysis. If no process trace data is available, a message is displayed indicating such. The format of the data displayed varies depending on the selected process data format and other options, but generally, each line contains a timestamp, the RTT facility, and the record text. When the user left-clicks on any displayed message in the call record data display

window, this list is updated to scroll to and highlight, the particular process trace data associated with that message (based on timestamps). This data can also be filtered and highlighted using the options described under Process Data Filter and Highlight Conditions.

Call Data Display Format Options allows the user to select the call data display format from a drop-down list of available formats, as well as, choosing whether orphan records will be displayed.

The possible display formats are:

- flow

  Displays a normal flowchart with redundant messages removed.
- detailed_flow

  Displays a complete detailed flowchart including all messages and indicating the send and receive status for each.
- Hi_level_flow

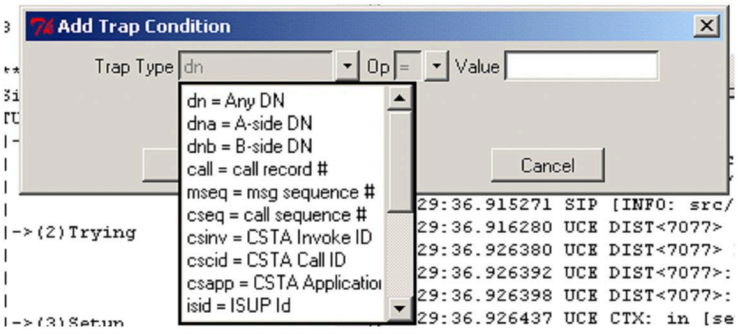
  Displays a high level call sequence flow for the call. Individual message details can not be seen in this display format.
- msg_list

  Displays the call data as a text list of message summaries. Each message is indented to show its associated call leg. Left-clicking on the message summary text shows the message details in the **Trace Record Display** window.
- msg_summary

  Displays the call data as a short summary list of the message sequence for the call. Individual message details can not been seen in this display format.

The selected format is immediately applied to the call trace data.

The **Display Orphans** option allows orphan records (those records unable to be associated with a call) to be displayed in a message list format at the end of the call record display. Left-clicking on any of these orphan records will display the details of the record in the **Trace Record Display** window.



Once a trap condition is added, it is listed in the **Call Trap Conditions** window. Multiple trap conditions can be selected and all listed conditions must be met for a particular call record to be displayed. Only one trap condition of a given type can be active at a time so adding a new trap condition for a type already listed will replace the existing condition.

Individual trap conditions can be removed from the list by selecting them in the **Call Trap Conditions** window, then clicking the **Remove Trap** button. All trap conditions can be removed from the list by using the **Remove All** button.

The displayed trap conditions can be applied to the current analysis by clicking on the **Apply Traps** button. Once selected, only those call records that match all listed trap conditions are displayed in the **Call Record data** window.

Process Data Display Format Options allows the user to select the process data display format from a drop-down list of available formats. The default format is "short", which displays a short summary of each process trace statement and includes the timestamp, the RTT Facility name, and the text of the trace record. The other available formats are "text" which shows only the text from each record or "full" which shows the entire Perl record for each trace statement.

Process Data Filter and HighLite Conditions allow the user to selectively filter or highlight the displayed process trace data based on facility name, process name, and/or selected data in the record text. The facility and process names lists are populated from the actual trace data so only values found in the process trace data can be selected in these fields. The "Data" field uses substring matching so the value entered here matches if the string is found anywhere in the process trace record text. Regular expression syntax can also be used by enclosing the text in "/" characters allowing more complex data matching criteria to be used. Once one or more filter conditions have been selected, they can be applied to the current process trace data by using the **Apply Filter**, or **Apply HighLite** buttons. The **Apply Filter** button filters the displayed process trace data allowing only those records that meet the selected filter conditions to be displayed. The **Apply HighLite** button allows all process trace data to be displayed, but highlights, in green, those trace records that match the selected filter criteria. This allows selected trace data to be easily located within a large list.

The process data filter conditions can be cleared and default values restored using the **Clear Filters** button. Once used, either the **Apply Filter** or **Apply HighLite** button must be used to refresh the process trace data list.

Call Record Save buttons allow the currently displayed call records to be saved to a file in either a text format, or a trace record list format. In both cases, a file dialog is displayed allowing the user to select the output file for the trace data.

When the **Save Call Data As Text** button is used, the currently displayed call records, in the currently selected display format, are written to the selected file in text format exactly as displayed. Only the call record data is saved in this case. Process trace data is not saved in the text format save.

When the **Save Call Data as Recs** button is used, the actual Perl data for each trace record associated with the currently displayed call is written to the selected file. In this case, both message trace records and process trace records that fall within the scope of the currently displayed call are saved. The resulting file contains a list of trace records that can be read by the call analyzer to reproduce the analysis of the selected call. This feature is most useful when a subset of call records has been isolated from a larger list using call trap conditions. This allows only the call record of interest to be saved making a much smaller file which may be easier to distribute and analyze.

7.9.3 Call Analyzer Call Data Screen Working with Mouse

When a call record is displayed in any format except Hi_level_flow or msg_summary, users can left-click the mouse at any point in the message list to see the details of that particular message.

The **Trace Record Display** window in the **Call Data** screen is updated with the details of that particular message, and the **Process Trace Data Display** window will highlight in grey the process trace data statements associated (by timestamp) with that message. This provides an easy method of seeing the details of any given message in a call record.

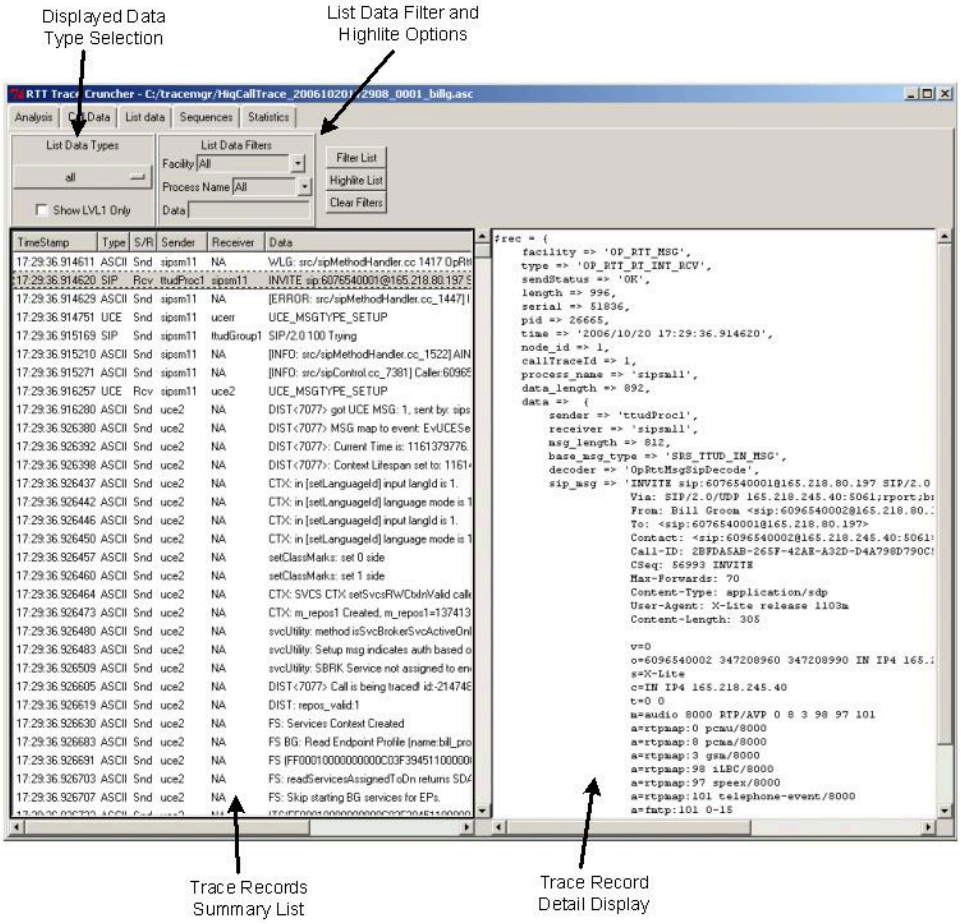
Left-clicking on the record number in the call record header creates a trap condition for that record number allowing individual call records to be easily isolated.

Left-clicking elsewhere in the call data display will have no effect. When a flow display format is selected, middle mouse button clicks can be used to calculate and display time offsets between any two messages. This is done by first left-clicking on some message in the call data display, then clicking and holding the middle button on some other message in the same display. While the button is held down, a small pop-up window displays the time offset between the two messages.

7.9.4 Call Analyzer List Data Screen

The List Data Screen displays the analyzed trace data in a time ordered list format.

This screen displays all analyzed data regardless of whether call records were created. One display pane shows a summarized list of the trace records, and the other shows the details of any selected record. Filtering and highlighting options allow selected data to be isolated and displayed.



The **Trace Records Summary List** window displays a summarized list of all trace records in the currently analyzed trace file. This list includes the record's timestamp, the record type, the snd/rcv indicator, the record sender, the record receiver, and a short summary of the record data itself. Clicking on any displayed record in this list selects that record and display its details in the **Trace Record Detail Display** window.

The **Trace Record Detail Display** window displays the details of any trace record selected in the **Trace Records Summary List** window. The entire Perl trace record is displayed for the selected trace record.

The **Displayed Data Type Selection** options allow the user to select the type of data to be displayed in the list. The drop down list allows the user to select **All** to display all records, **Msgs_only** to display only message data, or **Process_data_only** to display only the ASCII process data.

The **List Data Filter and Highlight Options** allow the user to selectively filter or highlight the displayed trace data list based on facility name, process name, and or selected text in the record data. The facility and process names lists are populated from the actual trace data so only values found in the trace data can be selected in these fields. The **Data** field uses substring matching so the value entered here matches if the string is found anywhere in the trace records data. Regular expression syntax can also be used here by enclosing the text in "/" characters allowing more complex data matching criteria to be used.

Once one or more filter conditions have been selected, they can be applied to the current trace data list by using the **Filter List**, or **Highlight List** buttons. The **Filter List** button filters the displayed trace data list allowing only those

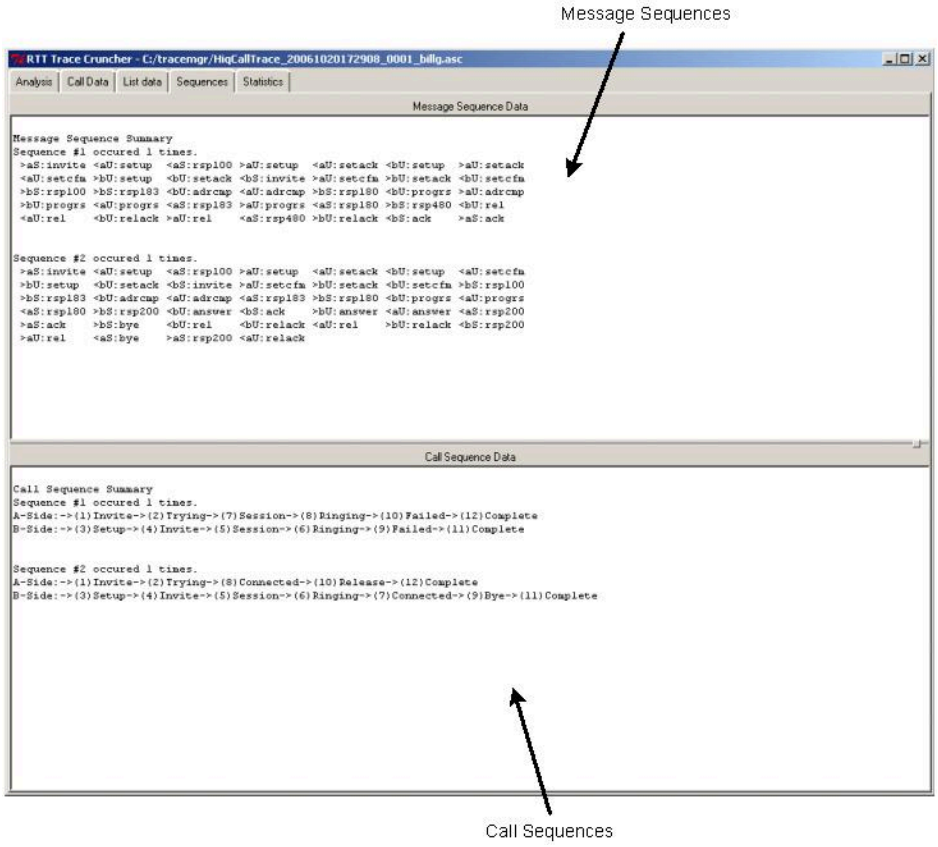
records that meet the selected filter conditions to be displayed. The **Highlight List** button highlights, in green, those trace records in the list that match the selected filter criteria. This allows selected trace data to be easily located within a large list. Highlighting is applied independently from Filters so a list can be filtered first, and then selected records highlighted in the filtered data.

The list data filter conditions can be cleared and default values restored using the **Clear Filters** button. Once used, either the **Filter List** and/or **Highlight List** buttons must be used to refresh the trace data list.

7.9.5 Call Analyzer Sequences Screen

The **Sequence Screen** displays the message and call sequence summaries for the analyzed data.

These summaries are useful when larger numbers of call records are contained in the analyzed data. They can be used to show trends in the way certain call or message sequences are handled by the call processing software.



The **Message Sequence Data** window displays the summarized message sequences for the currently analyzed trace data. For each call record, a summarized sequence of the messages associated with the call is compiled and then grouped with other calls that have identical message sequences. This list of grouped summaries is then displayed.

Each message is summarized as follows:

- A Snd/Rcv indicator (">" means received, "<" means sent)
- A call side/leg indicator (a letter a-z indicating the associated call side)

- Message type abbreviation (S=SIP, U=UCE, M=MGCP, C=CSTA)
- A colon
- A message name abbreviation (SM specific)

The call records associated with any given message sequence can be displayed on the **Call Data** page by using an appropriate message sequence (mseq) trap condition. A message sequence trap can also be created automatically by clicking on one of the Sequence numbers in the message sequence data window. Doing so opens the **Call Data** display page and creates the necessary trap condition to isolate the call records associated with that sequence.

The **Call Sequence Data** window displays the summarized call sequences for the currently analyzed trace data. The call sequences consist of a high level overview of the analyzed call states on a per call side basis. These sequences are then grouped together to show how many calls had identical call sequences. Each call sequence is displayed with a line for each call side, showing the high level state transitions for that call side. The numbers in parentheses show the sequence of the state transitions across the entire call. It should be noted that the call states displayed here are specific to the call analysis process and do not necessarily reflect actual call states as defined in the OpenScape Voice software.

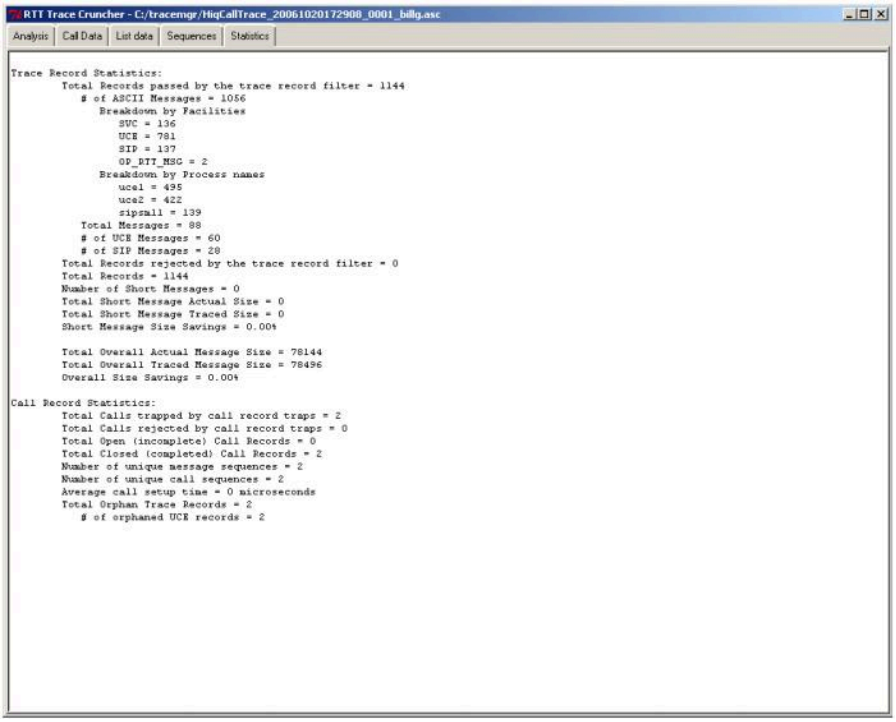
The call records associated with any given call sequence can be displayed on the **Call Data** page by using an appropriate call sequence (cseq) trap condition. A call sequence trap can also be created automatically by clicking on one of the Sequence numbers in the**Call Sequence Data** window. Doing so opens the **Call Data** display page and creates the necessary trap condition to isolate the call records associated with that sequence.

7.9.6 Call Analyzer Statistics Screen

The **Statistics** screen displays the record statistics for the currently analyzed trace data.

These statistics include the following data:

- The Number of ASCII messages (process trace data)
- The number of ASCII messages per RTT facility
- The number of ASCII messages per process
- The number of non-ASCII messages (message trace data)
- The number of messages per message type
- The number of trace records rejected by the input filters.
- The total number of records processed.
- The Message size statistics.
- The number of trapped and rejected call records.
- The number of open (incomplete) call records.
- The number of closed (completed) call records
- The number of unique message sequences.
- The number of unique call sequences.
- The average call setup time
- The number of Orphan Trace Records
- A summary of the number of orphan records per message type.



7.10 OpenScape Voice Obfuscation tool

The obfuscation tool of the OpenScape Voice Trace Manager (OSVTM) is a command line application, that takes as input files with sensitive data, and hides the sensitive data while keeping the rest information and files structure intact.

Prerequisites and Operating systems

The obfuscation tool runs at windows and unix systems. To run, java 1.8.0_241 (64-Bit) needs to be installed beforehand.

Downloading the Obfuscation tool

The obfuscation tool is a windows executable tool that runs on the craft PC. In order to download the tool, click the **Obfuscation Tool Download** button in the main page of the OpenScape Voice Trace Management Portal.

Hardware Requirements

For the obfuscation of 1.5 GB of files the system requirements are set to:

- Processor: Minimum CPU Intel i5/ Xeon 2.10 GHz (Bare-Metal or Virtual Machine).
- Memory (RAM): Minimum 4 GB, Recommended 8 GB or above.
- Hard Drive: Free Space should be three times greater than the total size of files.

To not affect the system performance and disk space the obfuscation tool should not be running in the same machine that produced the logs files.

Using the Obfuscation tool

The obfuscation tool runs on Windows and Unix systems.

The tool takes as input the following flags:

- a: Application name: One of the available applications shown at help menu. Each application has provided a custom list of files, regex, static info, etc. It's recommended to be used when the application that provides the traces is known.
- d (boolean): Disable default regular expressions (IPv4, emails, URIs). By default, they are used at obfuscation process, along with any other provided regular expressions.
- e: Excluded regular expressions file(s). Each file must contain a list of regular expressions to exclude parts of the trace files, one in every new line.
- h: help i (mandatory): Path to the trace file(s). Supports both files, folders and a few types of archive files (e.g. tar.gz, zip,).
- o: Choose path to the output folder. Default location is the "output" folder in the current directory.
- r: Regular expressions file(s). Each file must contain a list of regular expressions, one in every new line. Each regular expression will be used to identify strings in the logs that need to be obfuscated.
- rf: Reference regular expressions file(s). Each file must contain a list of regular expressions, one in every new line. Each regular expression shall be used to generate a list of confidential strings, that will be obfuscated in the trace files.
- rd: Regular expressions file(s) to delete lines. Each file must contain a list of regular expressions, one in every new line. These regular expressions are used to delete lines that are being matched, usually because they contain PII that cannot be obfuscated. s: Static file(s) with Personal Identifiable information. Each file must contain a list of PII strings, one in every new line. These strings will be obfuscated directly whenever found in the trace files. The PII lists should be generated by the UCC Application that generates the log files.
- db (boolean): Enable debugging mode that adds extra information to the report file.
- dbv (boolean): Enable verbose debugging mode that adds extra information to the report file. This option does not need the enabling of simple debug mode. m: Path for loading a pre-generated PII map file from a previous anonymization session. The map reuse feature allows you to run a new anonymization session while maintaining the same encryption key-value pair for existing entries.
- c: Application configuration File. Only on e.yml file can be loaded. Application name should not be defined when this flag is used. To be used when your application is not yet included in our application list, or when you need to test a new .yml file
- ext: Define the length of the extension within a DN. The flag supports the correlation between fully defined directory numbers and their related extension.

Examples of use:

- Obfuscation based on provided static confidential string list and integrated

  regex: java -jar ucc-obfuscation-tool-{version}.jar -i {pathToInput} -s {path to static file}
- Obfuscation based on regex integrated within the tool:

  java -jar ucc-obfuscation-tool-{version}.jar -i {pathToInput}

- Trace obfuscation based on provided static confidential string. Disable default regex:

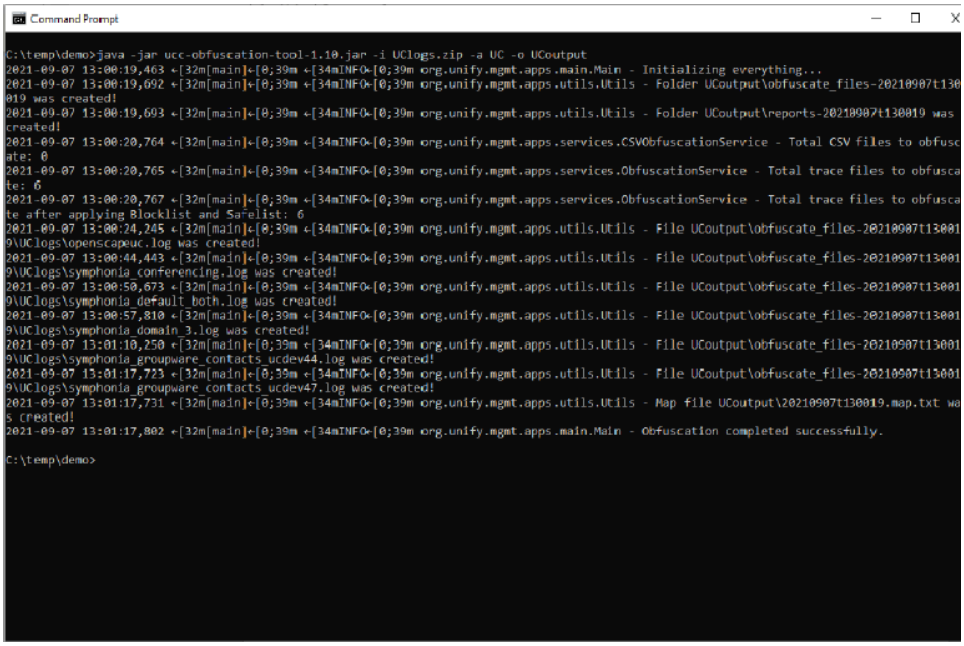
  java -jar ucc-obfuscation-tool-{version}.jar -i {pathToInput} -s {path to static file} -d
- Trace obfuscation with multiple confidential string files, additional regular expressions files as input and application type:

  java -jar ucc-obfuscation-tool-{version}.jar -i {pathToInput} -o {pathToOutput} - s {confidentialStringListFile1} -s {confidentialStringListFile2} -r {RegexFile1} -a {APP}

Important Notes:

- The original files are not modified.
- The *-c* flag cannot be used combined with *-a {application name}*.
- Most development teams have provided extensive regex list per file and folder that are used with each application flag. This means that if the original regex, with the original file and folder names are used, then *-a* flag covers most cases, along with *-i* to provide the files path. If a custom file needs to be obfuscated, or a custom *regex/reference regex/static* file needs to be ran, then the rest of the flags come handy.

Example of the Obfuscation tool



NOTICE: The output folder contains the obfuscated files, a report file, and the map file with the list of the confidential strings and their translations to the obfuscated strings.

8 Administration Tasks for Trace Manager

The administration personnel responsible for the OSV-TM have the permissions and authorization necessary to perform critical tasks.

The administrator performs the following tasks:

- Installation
- Migration
- Upgrades
- Uninstallation
- Configuration
- Starting/stopping continuous tracing
- User account administration
- Problem reporting

NOTICE:

The necessary configuration steps for Contact Center Extensions (Concierge) can be found in the latest issue of the *OpenScape Contact Center Extensions V3, Configuration Concierge, Administrator Documentation*

NOTICE:

OSVTM V8R0.6.0 SFTP service is no longer automatically installed and configured. For more details refer to chapter 3rd Party Software Product Requirements subsection SFTP/SSH Server

Related concepts

Administration View on page 34

8.1 Where to Find the OSV-TM Application

Download the target OSV-TM software version from the SWS Server under:

https://sw-download.unify.com/SWSIntranet/SWSIntra.aspx

- OpenScape Voice Trace Manager Vx Rx.x.x (where x is the current version)
- Save the executable file in a temporary folder in the local file system. (i.e.: C:\temp)

8.2 Hardware Requirements

Please see the OSV_TM V8 Release Notes for the latest hardware requirements.

Windows Server 2019 - 64 bit Standard Edition, Windows 2016, Windows 2012 R2, Windows 2012 and Windows 2008 R2 server Standard Edition - 64 bit (English and German versions) are supported for OSV-TM V8 onwards

Patches: latest OS and security updates must be applied.

It is recommended that OSV-TM is run on a single Windows Server. These hardware recommendations assume that OSV-TM is the only application running on the server. If other applications are deployed on the same machine, the performance impact of those other applications should be considered and factored in the configuration.

Hardware Configuration for Low-End OSV-TM Servers

Low-end integrated OSV-TM environment characteristics: OSV server(s) with less than 2 CPS (Calls Per Second) loads

- Single CPU, Dual Core Processor, 3 GHz Minimum
- 4 GB RAM
- Disk Configuration:
  - C: SAS Drive ~ 150GB minimum for OS & OSV-TM Databases
  - D: SAS Drive ~ 500GB minimum for Trace Files storage

    (Actual Storage required depends on the amount of collected trace files from the integrated devices).
  - SAS Drives are recommended for performance and reliability but SATA drives are acceptable for low load systems.
- Ethernet: 1Gbps Network Connection Recommended

Recommended Configuration

Mid-Range OSV-TM servers' characteristics:

OSV-TM integration with multiple devices: OSV, OSB, SBC, OpenScape SBC, Phones, UC, HMS Performance Profile:

- OSV Call Load with up to 10 CPS, with 10 Busy Hours per day
- Total OSB Load (from all OSBs configured for Continuous Trace): up to 10 CPS
- Total SBC Load (from all SBCs configured for Continuous Trace): up to 10 CPS
- Total OpenScape SBC Load: up to 10 CPS
- Total UC Load (From all UCs configured for Continuous Trace): up to 10 CPS
- Total HMS Load (From all HMSs configured for Continuous Trace): up to 10 CPS
- Total OpenStage Phone Trace: Up to 100 concurrent Phones with average of four CPS each

Recommended Configuration:

- Dedicated OSV-TM Server (non SESAP)
- Windows Server 2019 - 64 bit Standard Edition, Windows 2016, Windows 2012 R2, Windows 2008 R2 64bit Operating System only (Windows-2003 is not supported for this configuration)
- Dual CPUs, four-core processors, 3 GHz Minimum
- 12GB RAM minimum. 32 GB RAM is required if RAM Drive is enabled.

- Preferred Disk Configuration:
  - C: Two 300GB SAS drives, 10K rpm, Configured as RAID-1, to store the OS and databases
  - D: Three Drives (or more) configured as RAID-5, minimum available storage of 1TB

    (More storage might be needed based on actual call model).
  - 7200RPM SATA Drives can be used. SAS drives preferred.
- 1Gbps Ethernet Network Connection minimum

IMPORTANT:

For Performance Profiles that exceed the above scenario, please contact customer service for a custom solution.

8.3 3rd Party Software Product Requirements

The following third party applications are required for OSV-TM server and client functionality. These applications are not included in the OSV-TM installation package and must be downloaded from their providers and manually installed. Follow the instructions that accompany this 3rd party software for installation procedures.

Server Components:

- .NET 3.5 SP1 or later is required for OSV-TM. This software is already installed on server but it needs to be enabled.

  Provider: http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=ab99342f-5d1a-413d-8319-81da479ab0d7
- **OpenScape Voice V7R1 and above** no longer use the RTT Trace Management Tool and do not require Active Perl installation.

For new installations, the OSV-TM administrator is responsible for downloading and installing the indicated software versions from their vendors.

Customers that have any earlier version of an OSV-TM server must verify that the existing versions of the above applications are the same as the required ones and upgrade them, if necessary.

Client Components:

- OSV-TM compresses the files it generates; therefore, a decompression utility is needed on the user client machine to open "cap" and "event" files via the FADE portal. The OSV-TM user will need to install on his local desktop a utility that unzips ".gz" files. (Example: 7-Zip or WinZip)
  - The 7-Zip utility can be downloaded directly from its provider: http://www.7-zip.org/download.html
- As of V2.0, OSV-TM does not deliver trace file analysis tools such as Wireshark. Customers who would like to use Wireshark for detailed trace file analysis should install Wireshark on the user's client PCs. It is recommend not deploying client applications on the OSV-TM server itself in order to not interfere with OSV-TM server operations.
  - The latest Wireshark Windows version is supported.

– Provider: http://wireshark.org/download.html

Users who download and install Wireshark on their PCs are responsible for subsequent Wireshark version updates and security fixes.

IMPORTANT:

It is highly recommended to uninstall Wireshark if it is already installed on the OSV-TM server. If the customer must keep it on the server, then it is the customer's responsibility to upgrade this software on an ongoing basis to the latest stable version that includes the latest security fixes.

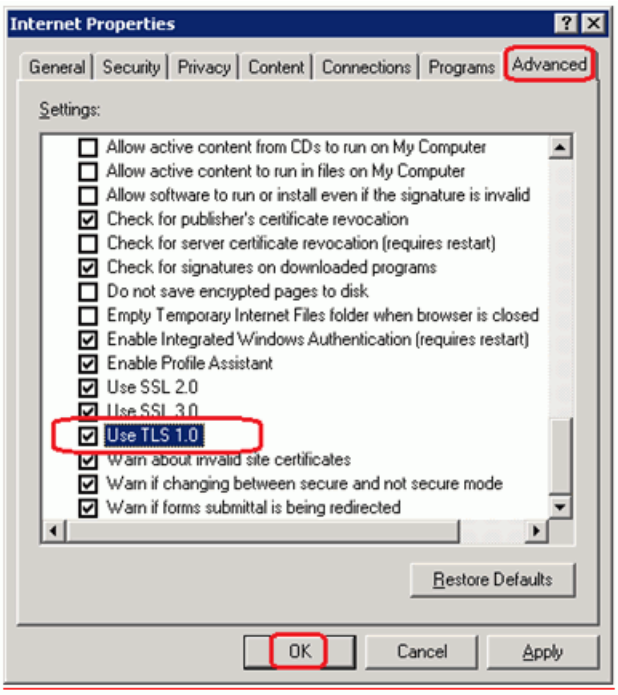
Internet Browsers

- Firefox V3.6 is the officially supported version for OSV-TM; however, the latest versions have worked in our testing laboratory.
- Internet Explorer V11 is the latest version supported for the OSV-TM FADE portal.
- IE V9 is not supported. Windows administrators should not install the update package for IE 9 from Windows Update.
- IE V6 is not recommended for OSV-TM. It only supports querying and fetching data; however, it does not support the OSV-TM graphing features.

  If no upgrade to IE V8 or V11 is possible and IE V6 must be used, the following security configuration changes must be made to make it compatible with the current version of OSV-TM. Access to the FADE portal will not be possible without this configuration; the browser will display a page unavailable error.

  Open IE 6 browser and navigate to the configuration menu:

  – Start menu > Control Panel > Internet Options
  – The "Internet Properties" window opens. Click the "Advanced" tab.
  – Enable the "Use TLS 1.0" entry. Click OK



SFTP/SSH Server

Installing SSH software

- Download the latest OpenSSH for Windows binaries (package OpenSSH-Win64.zip or OpenSSH-Win32.zip)

  NOTICE:

  It is strongly recommended to use this specific OpenSSH version (v7.9.0.0), since this is the latest one tested and verified. Don’t download later versions.

- Extract the package to `C:/Program Files/OpenSSH`
- As the Administrator, install SSHD and ssh-agent services by launching Windows PowerShell. Navigate to `C:\Program Files\OpenSSH` (where OpenSSH contents have been previously extracted) and execute the following command:

  ```
  powershell.exe -ExecutionPolicy Bypass -File install-sshd.ps1
  ```

- Start and Stop the sshd service to create some folders by executing the following commands:

  ```
  net start sshd
  ```

  ```
  net stop sshd
  ```

- As the Administrator, generate server keys and restrict access to them, by running the following commands via Windows PowerShell from `C:\Program Files\OpenSSH`:

  ```
  .\ssh-keygen.exe -A
  ```

  ```
  powershell.exe -ExecutionPolicy Bypass -File .\FixHostFilePermissions.ps1
  ```

  (Select [Y] to all configurations)

- Open a port for the SSH server in Windows Firewall:
  - Navigate to **Control Panel** > **System and Security** > **Windows Firewall** > **Advanced Settings** > **Inbound Rules** and add a new rule for port 22, when there is not one already.
- Start the service and/or configure the automatic start:
  - Navigate to **Control Panel** > **System and Security** > **Administrative Tools**

    and open **Services**. Locate the **SSHD (OpenSSH)** service.
  - For the server to start automatically when you start the machine, navigate to **Action** > **Properties**

    In the Properties dialog, change the *Startup* type to *Automatic* and click **Confirm**.
  - Click **Start the service** to start the SSHD service.

Configuring the SFTP ROOT path

- Under `C:\ProgramData\ssh` edit the "sshd_config file

  NOTICE:

  The ProgramData is a hidden folder.

- Replace line “#PidFile /var/run/sshd.pid” with “PidFile C:\Programdata\ssh \logs\sshd.pid”.

  NOTICE:

  This line should not be commented any more

- On line `Subsystem sftp sftp-server.exe` add

  `-d <desired_sftp_root_path>`

  For example: `Subsystem sftp sftp-server.exe -d C:\Tracedata \`
- Save and close the file
- Restart the SSHD service:
  - Navigate to **Control Panel** > **System and Security** > **Administrative Tools** and open **Services**. Locate the **SSHD (OpenSSH)** service.
  - Restart the **SSHD** service by clicking **Restart the service**.

Configuring SSHD to listen on IPv6 addresses

- Under `C:\ProgramData\ssh` edit the file "sshd_config"
  - uncomment the #ListenAddress lines

    ListenAddress 0.0.0.0

    ListenAddress ::
  - This will bind sshd to every address on your machine
- Restart the SSHD service:
  - Navigate to **Control Panel > System and Security > Administrative Tools** and open **Services**. Locate the **SSHD (OpenSSH)** service.
  - Restart the **SSHD** service by clicking **Restart the service**

Cipher configuration to also support aes-cbc mode

- Under `C:\ProgramData\ssh` edit the file “sshd_config” file by adding the following content above the last entry "Match Group administrators":
  - `Ciphers +aes128-cbc,aes192-cbc,aes256-cbc`

    `KexAlgorithms +diffie-hellman-group-exchange-sha1`
- Restart the SSHD service:
  - Navigate to **Control Panel > System and Security > Administrative Tools** and open **Services**. Locate the **SSHD (OpenSSH)** service.
  - Restart the **SSHD** service by clicking **Restart the service**

Fix OpenSSH log file permissions and reduce log level

- Navigate to `C:\ProgramData\ssh\logs` and modify the Security properties of the folder logs by following the steps below:
  - Right click on the folder *logs* and select **Properties**
  - Switch to tab **Security**
  - Click **Edit** to change permissions
  - On the window **Permissions for logs** click **Add**
  - On the window **Select Users or Groups** under section “Enter the object names to select” type: NT SERVICE\SSHD and click **Check Names** to verify that it resolves to sshd
  - Click **Apply** and/or **OK** to all open Windows to apply the new configuration
- Under `C:\ProgramData\ssh` edit “sshd_config” file by:
  - Replacing the line “#LogLevel INFO” with “LogLevel QUIET" and “#SyslogFacility AUTH” with “SyslogFacility LOCAL0”.

  NOTICE:

  Don't comment on those lines anymore
- Restart the SSHD service:
  - Navigate to **Control Panel > System and Security > Administrative Tools** and open **Services**. Locate the **SSHD (OpenSSH)** service.
  - Restart the **SSHD** service by clicking **Restart the service**

8.4 Pre-Installation Requirements: What is needed before OSV-TM Installation

OpenScape Voice-Trace Manager V8 supports the US English and German versions of Windows Server 2019 - 64 bit Standard Edition, Windows 2016, Windows 2012 R2, Windows 2012 and Windows 2008 R2 64-bit. Additional components need to be set up on the server before OSV-TM is installed.

Windows Server installations do not enable the FTP service by default; if FTP is required in your environment, it should be set up by the administrator. A special storage directory must be configured to store the traces received from the different OpenScape elements. Additionally, the correct .NET Framework needs to be installed for the OSV-TM installation to complete.

Required .NET Framework

For Windows 2003 server, the .NET V3.5 SP1 or higher framework needs to be manually downloaded and installed on the server before installing OSV-TM.

Please see the Requirements section for additional information on how to obtain this software.

8.4.1 How to Enable .NET Framework on Windows 2008 R2

Prerequisites

Adequate administrative permissions.

Step by Step

1) Log into the server as Administrator or with a user account that is a member of the Administrators group.
2) Navigate to the Server Manager window: **Start** > **Control Panel** > **Administrative Tools** > **Server Manager**
3) On the left pane, click **Features**
4) Under the **Features Summary** on the right pane, click **Add Features**

   The Select Features window opens.
5) Select the option **.Net Framework 3.5.1** from the list of features.
6) Click **Next**
7) On the **Confirmation Installation** window, click **Install**

   A confirmation message of the successful installation is displayed.
8) Click **Close**

   Note: You may be prompted to restart the server. NET is now installed and enabled on the server.

8.4.2 Trace Data Storage Planning

The data files generated by the traces from the different artifacts that integrate with OSV-TM will be stored in a central folder called "Tracedata" on the OSV-TM server.

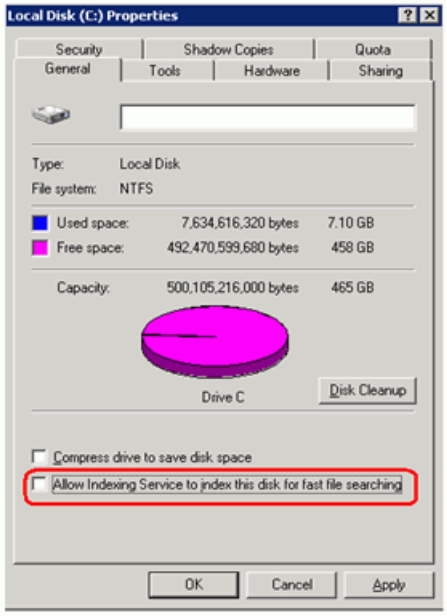
It is highly recommended to have a separate physical hard drive to host this storage folder (see the latest OSV-TM Release Note for the recommended Hardware configuration).

OSV-TM will create the "Tracedata" folder during the software installation. You will be prompted to indicate in which drive it should be created. Choose the drive with the largest storage capacity.

Important Notes:

- The "tracedata" folder name is tightly related to the SFTP/FTP functions. If the folder name is changed, make note to set the FTP account with the same name as the new folder name (see "Setting up the FTP Windows Server and SFTP Support " section for details).
- We have identified performance issues in highly active OSV-TM servers when the hard disk indexing is enabled. Disable indexing on the Tracedata storage hard disks to avoid performance problems by un-checking the "Allow

Indexing Service to index this disk for fast file searching" on the Properties window for the storage drive:



Tracedata Storage Structure

In OSV-TM V6 and above, processed data files are stored in a sub-folder structure by date. As trace files are received, they are moved from the "Tracedata" folder to the corresponding "date" sub-folder to be processed; these data files remain in these folders until they are automatically aged and deleted by the OSV-TM Monitor. When an existing OSV-TM server is upgraded, all trace files that were processed before the upgrade will remain in the Tracedata root folder until they are aged except OSB and SBC trace files which are reprocessed. Only new traces are moved to the date sub-folders.

8.5 Migration from an Earlier OSV-TM Version

The SQL database engine used in older versions of OSV-TM was changed as of OSV-TM V2. SQLite (a free OpenSource application that can be deployed with no restrictions) is used with the current version of OSV-TM. Upgrading from an OSV-TM V1 or an earlier version to V8 requires a database migration from MySQL to SQLite.

- For OSV-TM V1 or earlier versions, only system configuration parameters are migrated:
  - Existing OSV-TM systems are preserved
  - Database tables are modified to the new database schema
  - OpenScape SBC and Quality of Service Configuration parameters are preserved
  - OSV-TM - User accounts
  - User defined Advanced Queries
- Trace data files, including OSV RTT, OpenScape SBC, and OSB, must be re-processed by the DIPAZ utility to populate the database during the upgrade process, or the administrator has the option of performing a Clean

Start. Refer to the Section titled: "Upgrading from an Earlier OSV-TM Version" for detailed information.

- Upgrading from V1 will automatically update third party products and base software.
- **IMPORTANT:**

  Customers running older versions of OSV-TM require careful planning before upgrading since the database engine has been changed in the latest versions of OSV-TM. Review the "Upgrading from an Earlier OSV-TM Version" section before upgrading.
- OpenScape Voice V7 and above no longer uses the RTT Trace Management Tool to configure tracing. Upgraded environments integrating with this and higher versions OSV no longer require Active Perl, and this software can be uninstalled.

Related concepts

Upgrading from an Earlier OSV-TM Version on page 137

8.6 Migrating an OSV-TM Server on Windows 2003 to Windows 2008 R2

OSV-TM is no longer supported on the Windows 2003 operating system. OpenScape Voice Trace Manager V7R0.5.x and above is only supported on servers running the US English or German versions of Windows Server 2019 - 64 bit Standard Edition, Windows 2016, Windows 2012 and Windows 2008 R2 64-bit operating system. Customers running OSV-TM on Windows 2003 who want to upgrade to the latest OSV-TM V7R0.5.x or higher versions should follow the instructions in this section to migrate to the Windows 2008 operating system.

The new OSV-TM server should be installed according to the installation instructions included in this manual. The existing OSV-TM configuration files located under the main OSV-TM directory labeled MTC will be manually migrated from the source OSV-TM server running on Windows 2003 to the target OSV-TM server on Windows 2008. These configuration files contain OSV-TM local accounts credentials and customized settings and will replace the new OSV-TM system configuration files.

NOTICE:

When upgrading the OS on the same OSV-TM server hardware, be aware that until OSV-TM is reinstalled and running, all devices that integrated with the old OSV-TM server will keep sending trace files; these devices might generate an alarm until the migration process is completed.

Requirements for Migrating OSV-TM from Windows 2003 to Windows 2008

- The OSV-TM server must use 64-bit processors. Before you upgrade to Windows 2008, verify if OSV-TM server hardware has the 64-bit architecture:
  - Open a CMD Shell:
  - From the "Start" menu navigate to: All Programs
  - Right click on the "Command Prompt" menu entry and select: "Run as Administrator"
  - On the CMD shell type: wmic cpu get AddressWidth
  - Press "Enter"

  The AddressWidth value should indicate 64.
- Do not proceed with the instructions below, if your hardware does not support 64-bit CPUs. You will need to procure another server that meets this requirement. Please review the hardware requirements in the OSV-TM Release Note.
- If you are running an older version of OSV-TM (V6R0.3.2 and below), upgrade to the latest OSV-TM V7R0.4.1 version supported on Windows 2003 before upgrading the Operating System. This ensures that the configuration files have the required structure.
- Obtain external storage hardware (i.e.: USB or external hard drives) large enough to backup the configuration files and trace files from the existing OSV-TM installation on Windows 2003.
- The Operating System upgrade or installation to Windows 2008 R2 must be performed by your Windows Administrator.
- When configuring the Windows 2008 server, it is required to keep the same storage drive configuration as it was on laid out on Windows 2003 (same drive letters and the same partitioning).

8.6.1 OS Upgrade Preparation: OSV-TM Backup

Before upgrading the server, it is necessary to stop all OSV-TM processes and identify the data that needs to be backed up for migration.

- Stop the Dipaz Monitor service on the Windows 2003 server. See the instructions in the "Stopping or Restarting the OSV-TM Services" section in this manual.
- Stop the File Agent Service (if you are upgrading from V7R0.5.x). See the instructions in the "Stopping or Restarting the OSV-TM Services" section below.
- Make a note of the storage drives configured on the server and identify the drive letters where the OSV-TM configuration files are located. This information will be required when restoring the data to the upgraded server.
- Back up the <system-drive>:\MTC directory (i.e.: C:\MTC) to an external storage.

Optional: Analyze your trace data and decide if any existing records need to be preserved and migrated to the new version. If you also want to migrate trace files, the Tracedata folder: "<system-drive>:\Tracedata" (i.e.: D:\Tracedata), should as well be backed up to the external storage.

8.6.2 Upgrade Server to Windows 2008 R2

Request your Windows Administrator to install Windows 2008 R2 SP1 with the same drive configuration as in the Windows 2003 installation. It is important to keep the same drive settings (drive letters) as before to be able to restore the OSVT-M configuration files from backup to the location they were on the Windows 2003 server.

If possible, use the same IP address and server name as the old Windows 2003 server. This will ease the configuration of the devices that already integrated with the old OSV-TM server.

After Windows 2008 is installed it should be updated with all the latest Windows packages.

8.6.3 Installing OSV-TM and Migrating Data

Before installing OSV-TM it is necessary to configure .NET on the server and restore the configuration files that where backed up during the upgrade preparation. The OSV-TM installation will use this configuration to recreate the systems that were present in the Windows 2003 server.

Manual Procedures before Installing OSV-TM

- Enabling .NET

  For the OSVTM installation to complete, .NET framework needs to be installed. Follow the instructions in the "Pre-Installation Requirements: What is needed before OSV-TM installation" section in this manual to enable .NET.
- Restoring the Configuration Files from Backup

  Restore the MTC directory from the backup storage to the same drive letter where it was stored in the Windows 2003 server.

  Restore the Tracedata directory to the same drive letter where it was stored in the Windows 2003 server if you also want to migrate existing trace files.

Installing OSV-TM on the Migrated Server

- Follow the fresh installation and configuration instructions in the "How to Install OSV-TM" section in this manual.

  NOTICE:

  During the installation, make sure to select the same drive (drive letter) in the "Select Destination Location" window (i.e.: C:\OSV-TM) as the drive where you restored the MTC folder to in the Windows 2008 server.

- Verify that there were no errors reported during the installation.
- After the installation is completed, open the FADE web portal. You should see the same systems that were configured in the pervious Windows 2003 OSV-TM server. The already processed trace data is also displayed; however, if the trace files were not migrated, the OSV-TM functionality that open trace files will not work.

- Verify that the devices that integrate with the OSV-TM server are configured with the correct IP address and that the trace files arrive to the corresponding Tracedata storage.

8.7 Installation of OSV-TM

There are two installation procedures for OSV-TM. A fresh install which installs all components delivered with the OSV-TM software package and sets up the OSV-TM server with the required system default parameters, and the upgrade procedure which updates the OSV-TM software components without resetting system parameters.

Important Notes

An OSV-TM installation configuration file (install.xml) can be built from the CDC. If the administrator wants to use this file to preset the parameters of the OSV-TM installation, the administrator needs to copy the install.xml file into the OSV-TM server.

1) Server administration rights are required to install OSV-TM. Login as the local Administrator or with a user account that has administrator's permission to install the software.

2) Before running the installation, the target system should be set up with .NET framework as indicated in the Pre-Installation section; installing FTP server is only required for environments integrating with OpenScape Voice versions lower than V4.0.

Fresh Installation: Full install of OSV-TM Software Package

During the installation process, system prerequisites and third party software are installed first followed by the OSV-TM software.

Some 3rd party software is not included in the OSV-TM package. This software must be downloaded and manually installed by the administrator.

OSV-TM V7R0.7.x supports RAM drives as storage for the OSV-TM databases. This configuration is only recommended for customers experiencing delays in their trace processing or having performance problems. This feature is not enabled by default when installing OSV-TM; additional hardware requirements are needed to enable it. Please refer to the "Using A RAM Drive Storage for Performance Solutions" section for details.

The OSV-TM installation is mostly silent; however, some default installation windows will display. Minimal user intervention is required and most pop-up windows will close automatically.

3rd Party Software Requiring Manual Installation

Please review the "Requirements" section for details on the 3rd party versions needed by OSV-TM and instructions on how to obtain them.

The "Active Perl" and ".NET" 3rd party applications are not included in the OSV-TM installation package. You must download the software from their provider and manually install it.

"Active Perl" is required by the RTT Trace Management Tool which configures and manages continuous tracing for the OpenScape Voice V4, V5, and V6. OpenScape Voice V7 and later versions do not require Active Perl.

".NET" is essential for the OSV-TM components and must be enabled in Windows.

Related concepts

Installation of OpenScape Voice-TM on Target Server

8.7.1 How to install OSV-TM on Windows 2008 R2 or newer

Prerequisites

Adequate administrative permissions.

Step by Step

1) Download the OSV-TM installation file and store it locally in a temporary folder in the OSV-TM server (i.e.: c:\temp).
2) If you will be using a CDC generated "install.xml" for the OSV-tm installation configuration, copy this file into the same temporary folder (i.e.: C:\temp\install.xml).

   IMPORTANT:

   The "install.xml" configuration file needs to be in the same location where the OSV-TM install ".exe" was downloaded to. Otherwise, the installation program will not be able to read it.

3) Open Windows Explorer and navigate to the temp folder containing the installation executable file.

   e.g. `<SystemDrive>:\temp`
4) Right click on the executable file `OSV-TM_Vx.x.x.exe (where x is the current version).`
5) Select: **Run as administrator**

   The **Welcome to the OSV-TM Setup Wizard** is launched.
6) Click **Next**
7) Accept the licensing agreement and then click **Next**

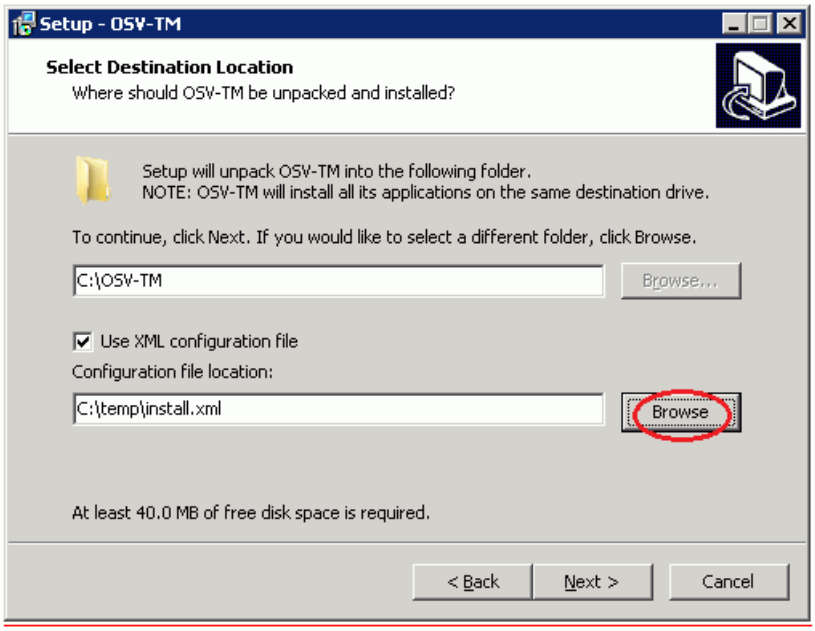
   The **Select Destination Location** window opens.
8) The OSV-TM installation parameters can be changed during the install process, or if a CDC configuration file (install.xml) is available. You

can choose to use this file to preset the default OSV-TM installation parameters.

To install OSV-TM with the preconfigured CDC values:

a) Checkmark the option "Use XML configuration file".

a) Click on the "Browse" button and locate the "install.xml" file.



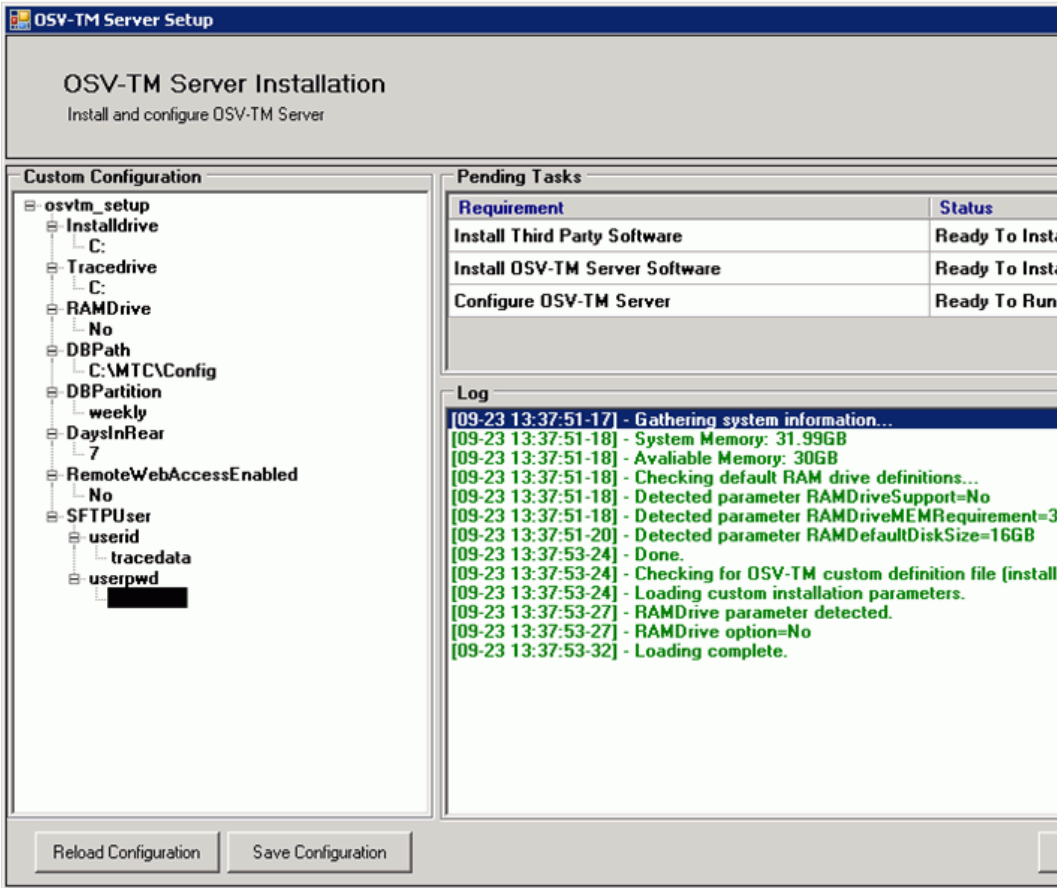
9) In the **Ready to Unpack** window, click **Unpack**

The installation files are extracted to the `<System-Drive>:\OSV-TM` folder and the **Completing the OSV-TM Wizard window displays.**

10) Ensure that the "Setup OSV-TM Server" box is checked.

11) Click **Finish**

The "OSV-TM Server Installation" window opens.

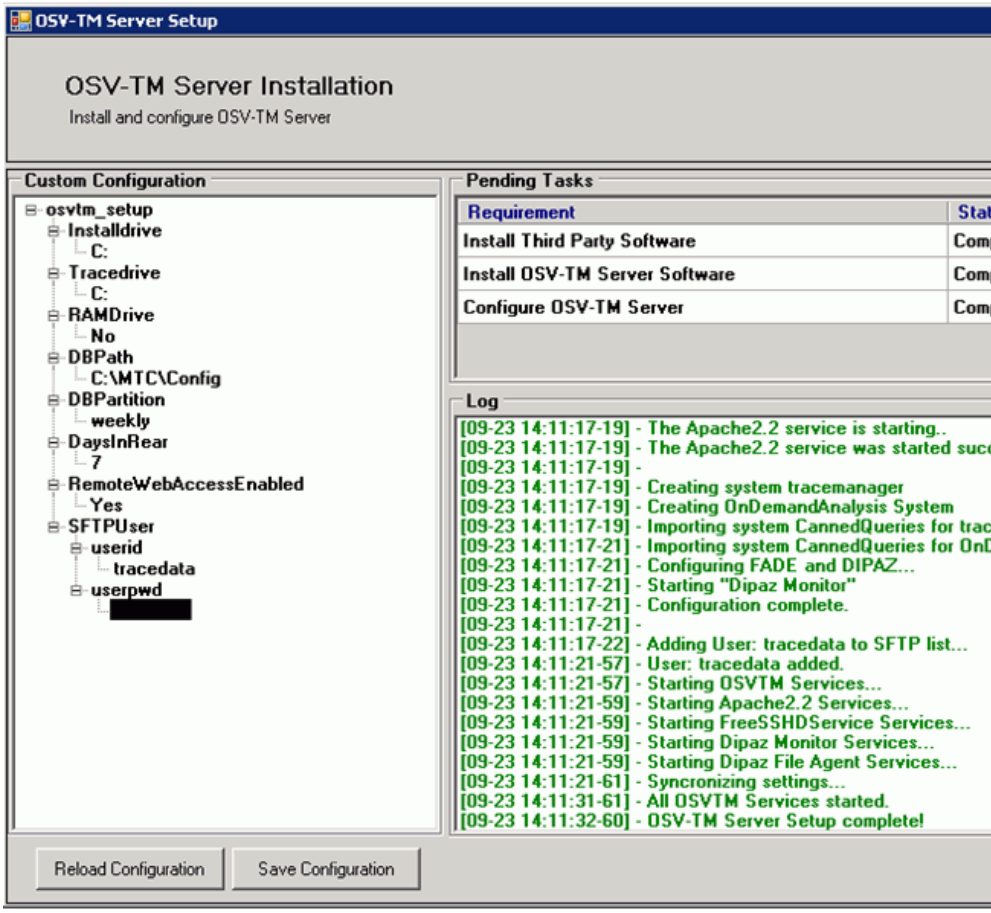


This window displays the OSV-TM installation configuration parameters. To change any of the parameters, double-click on the value and edit it (i.e.: to change the "DaysInRear" value, click on the "7" and change it to the new value). Click on the "**Save Configuration**" button.

12) When you finish your selection, click on the "**Install**" button.

13) During the installation, the "OSV-TM Server Installation" shows the installation status in the "Log" pane.

14) Click "**Finish**" button when the OSV-TM Server setup is complete.



The OSV-TM installation is now complete.

Note: Installation logs are stored in the following location: **<InstallationDrive>:\OSV-TM\Log**

8.8 Fresh Installations: Required Post Installation Configuration

Additional steps are required to complete the installation of 3rd party applications and OSV-TM server configuration.

This section lists all procedures that must be in place before the OSV-TM server is put in service.

8.8.1 How to Generate a Digital HTTPS Certificate for the OSV-TM Server

OSV-TM users connect to the server via the FADE web client or OSV-TM web portal. This client interface uses HTTP via SSL to connect to the OSV-TM server.

Prerequisites

Adequate administrative permissions.

Step by Step

1) All the following procedures need to be run from the command line interface using the Windows Command Prompt (CMD) shell **with a Windows administrator account**..
2) Open the CMD shell:
From the "Start" menu navigate to: **All Programs** > **Accessories**
3) Right Click on the "Command Prompt" menu entry and select: "Run as Administrator"

   Create the Self-Signed Certificate for an OSV-TM server installed on Windows 2008 R2, 2012R2, 2016 OS or 2019 OS:
4) On the CMD shell type:

   cd <system drive>:\Program Files (x86)\Apache Software Foundation \Apache2.4\bin
5) Press the "Enter" key
6) Type the following command: **openssl req -config ../conf/openssl.cnf -newkey rsa:2048 -out server.csr -keyout server.pem**
7) Press the "Enter" key
8) At the "Enter PEM pass phrase:" prompt, type a password to secure the access to the digital key.

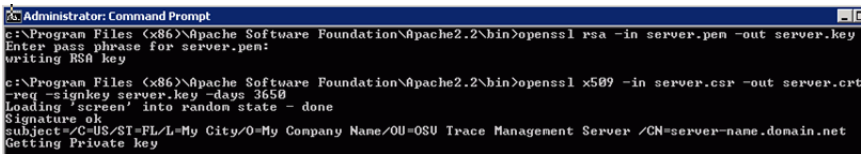
   WARNING: Write down the password phrase since it will be required for administering the SSL certificates.
9) Enter the information that will describe your certificate. Some of these fields can be left blank, but you should provide the following parameters:
   - Country Name (2 letter code) [AU]: <country where the server is located>
   - State or Province Name (full name) [Some-State]: <state or province where server is located>
   - Locality Name (eg, city) []:
   - Organization Name (eg, company) []:<My Company Name>
   - Organizational Unit Name (eg, section) []: OSV Trace Management Server
   - Common Name (eg, YOUR name) []: <server-name> (Note: Use the FQDN is your company enforces it)
   - Email Address []:
10) Type the following command:

    openssl rsa -in server.pem -out server.key
11) Press the "Enter" key
12) At the "Enter pass phrase for server.pem:" prompt, type the password you set in the step above.
13) Type the following command:

    openssl x509 -in server.csr -out server.crt -req -signkey server.key -days 3650

14) Press the "Enter" key

The "-days 3650" parameter sets the certificate aging to 10 years. If you prefer a shorter certificate period, change the days to a shorter period. You will have to create a new certificate after this period expires.



15) The steps above generated a valid certificate. Copy and replace the files: "server.crt" (Security Certificate), "server.csr" (CSR file), and "server.key" (KEY file) into the Apache web server "conf" folder:

%programfiles (x86)%\Apache Software Foundation\Apache2.2\conf

16) Restart the "Apache2.2" service

- From the "Start" menu, go to the Control Panel -> Administrative Tools -> Services
- Select the Apache.2.2 service and click on "Restart"

17) To test the certificate, connect to FADE web client:

- The remote access URL is https://<server-name>:28081/FADE/public/index.php/login
- You should be warned to accept the certificate
- After accepting it, you should be logged in using port 28081.

8.8.2 Enabling/Disabling OSV-TM Communication Ports with the OSV-TM Firewall Security Manager

On OSV-TM V7 and higher installations, the communication ports required for some OSV-TM functionality are not enabled by default. The "OSV-TM Firewall Security Manager" must be run to configure the required Windows Firewall rules and enable remote access.

The following port functionality can be enabled with the "OSV-TM Firewall Security Manager":

- SFTP
- FADE Remote Access
- Phone Listener
- OpenScape SBC Listener

NOTICE:

OSV-TM versions lower than V4 required Windows FTP for trace files transfers. Customers running these versions need to uninstall Windows FTP and ensure that the corresponding FTP ports are closed in the Firewall.

The SFTP feature and its corresponding ports are enabled by default in all OSV-TM V7 and higher installations. You can use the OSV-TM Firewall Security Manager to disable this functionality.

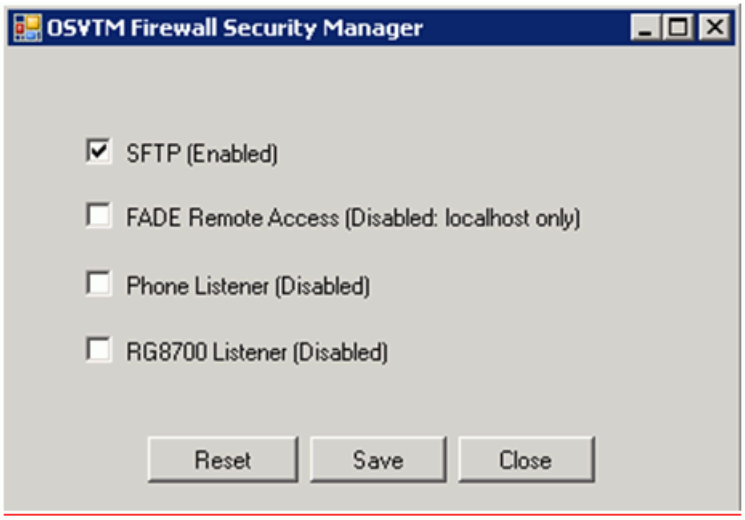
8.8.3 How to Run the "OSV-TM" Firewall Security Manager

Step by Step

1) Login locally to the OSV-TM server with a Windows administrator account.
2) From the "Start" menu navigate to: All Programs -> OSV-TM -> Security
3) Right-Click on the "OSV-TM Firewall Security Manager" utility and select: "Run as Administrator"
4) The "OSV-TM Firewall Security Manager" utility opens.
5) Click on the feature you want to enable or disable the firewall port for.

   The entry will be tagged with (Enable) when the port is open.

   The entry will be tagged with (Disabled) when the port is closed.
6) Click "Save"
7) Click "Close" to exit the utility.



The "Reset" button, restores the options selections to the last saved status.

8.8.4 How to Enable\Disable Remote Internet Browser Access to The OSV-TM Web Portal (FADE)

Access to FADE is restricted to the local OSV-TM server on OSV-TM V7 and higher installations; access from remote Web Client Users is disabled by default. The default server URL is set to "localhost":

https://localhost:28081/FADE/public/index.php/login

To allow access to the FADE Web Portal from remote Web Browsers, the OSV-TM web server and the OS Firewall rules need to be configured via the "OSV-TM Firewall Security Manager".

Step by Step

1) Follow the instructions to run the "OSV-TM Firewall Security Manager" utility in the "Enabling\Disabling OSV-TM Communication Ports with the OSV-TM Firewall Security Manager" section:
   a) Check mark the "FADE Remote Access" entry.

      The (Enabled) label should show up.
   b) Click Save

      The message "Updating Firewall rules" is displayed.
   c) Click on "Close" to exit the utility.

      When the task completes, Internet/Intranet Web remote access is allowed on the web server.

NOTICE:

This step only configures the OSV-TM Web server to allow connections from remote browsers. It is also necessary to configure each OSV-TM system to allow remote access through FADE. The administrator needs in addition to follow the instructions in the "Configuring OSV-TM Systems" section.

When the OSV-TM system is not configured for remote access, FADE displays the following message on the browser:

Remote access to this system from FADE is disabled by the OSVTM administrator.

2) To disable remote Internet Browser Access to FADE:

Follow the instructions to run the "OSV-TM Firewall Security Manager" utility in the "Enabling\Disabling OSV-TM Communication Ports with the OSV-TM Firewall Security Manager" section:

a) Remove the check mark from "FADE Remote Access" entry.

The (Disabled: localhost only) label should show up.

b) Click Save

The message "Updating Firewall rules" is displayed.

c) Click on "Close" to exit the utility.

8.8.5 Setting up the FTP Windows Server and SFTP Support

OSV-TM versions lower than V1R2 required Windows FTP Server to be manually installed to transfer trace files; for later OSV-TM versions, the FTP feature is optional and SFTP is included in the standard OSV-TM installation.

Customers using FTP need to manually install/uninstall Windows FTP to activate or disable FTP.

SFTP is automatically installed and enabled on the latest OSV-TM versions.

The instructions provided below are for OSV-TM servers not hosted in a Windows domain but in a private workgroup network. See the "Configuring Multiple SFTP Accounts for Trace Data Transfer" section below for the recommendations on instances where the OSV-TM server is in a domain.

For new installations of OSV-TM V7 and later, a default local user account called "tracedata" is automatically created and configured for FTP and SFTP transfers:

Default Account: tracedata

Default Password: Asd123!. (note the period "." after the exclamation sign)

NOTICE:

It is highly recommended to reset this password and communicate it to the other administrators of the devices integrating with OSV-TM.

If your security policy requires separate SFTP accounts for the different devices that integrate with OSV-TM, you will need to follow the procedure below to create each account. Please see the instructions: "Configuring Multiple SFTP Accounts for Trace Data Transfer" in the OSV-TM post-install section to complete the SFTP configuration.

8.8.5.1 How to Create the OSV-TM FTP/SFTP Server Account

Follow this procedure to create a new local User Account.

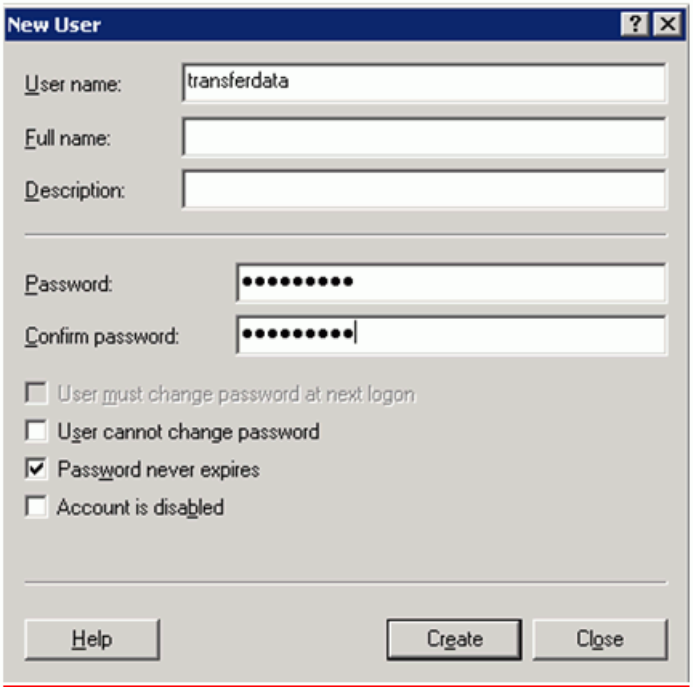
Prerequisites

Adequate administrative permissions

Step by Step

1) From the Start menu, navigate to: Control Panel -> Administrative Tools -> Computer
2) Select **Manage**
3) Expand the "Computer Management" option menu
4) Expand **Local Users and Groups**
5) Click on the folder: **Users**
6) From the **Action** menu, select **New User**

   The **New User** window opens.
7) Create the new user: Ex.: "transferdata"
8) Set the password and confirm it.
   a) Jot the password down. The same password will be required for the OSV-TM configuration.
9) Uncheck **User must change password at next logon**
10) Check **Password never expires**



11) Click **Create**
12) Click **Close**
    The local Windows "transferdata" user should be listed in the users folder.

Related concepts

Pre-Installation for Target OpenScape Voice-TM

8.8.5.2 FTP Server Functionality

FTP Server installation is optional for newer OSV-TM infrastructures. It is required for environments that integrate OSV V3.1 PS0035 and below. SFTP

functionality is installed and configured by default in the newer OSV-TM installation packages to support the later OSV tracing configuration.

The following sections provide the instructions for installing Windows FTP Server.

Enabling/disabling FTP Ports

Installing the FTP application automatically enables the following FTP rules in the Windows Firewall:

- FTP Server Passive (FTP Passive Traffic-In)
- FTP Server Secure (FTP SSL Traffic-In)
- FTP-Server (Incoming FTP Traffic)

To completely disable FTP, remove the FTP Server application and ensure these FTP rules were also deleted or are not active in the Windows Firewall.

8.8.5.3 How to Modify Windows Firewall Rules

The existing firewall rules created by the FTP installation need to be modified for the FTP server to work properly.

Prerequisites

Adequate administrative permissions.

Step by Step

1) Open the Windows Firewall and disable the following FTP rule from the "Inbound Rules"

FTP_Server (FTP Traffic-In) -> Action menu -> Disable Rule

2) Create a new rule firewall for FTP:

a) Select "Inbound Rules" and from the Action menu select "New Rule"

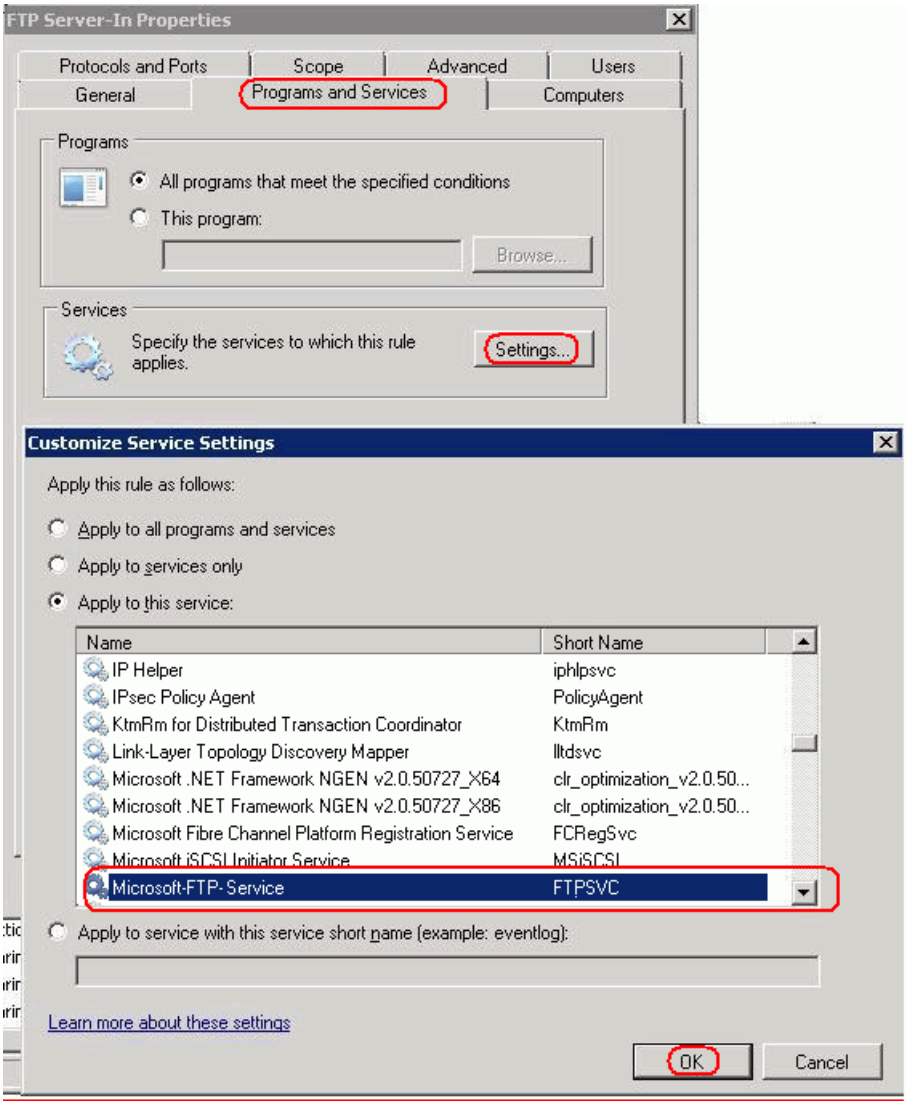
b) On the "New Inbound Rule Wizard" enter the following parameters:

- Rule Type: Select "Port"
- Protocols and Ports: Select "TCP" and Specific local port type "21"
- Action: Select "Allow the connection"
- Profile: Check mark all: Domain, Private, and Public
- Name: type "FTP Server-In"
- Click "Finish"

c) Click on the newly created "FTP Server-In" rule.

From the Action menu select "Properties":

- Click on the "Program and Services" tab
- On the Services section: click the "Settings" button
- The "Customize Service Settings" window opens. Click on "Apply to this service".
- Select "Microsoft FTP Server" from the list -> Click "OK"
- Click "OK" to save the changes to the Properties



The FTP service is now configured.

8.8.5.4 Secure FTP (SFTP) Support

SFTP functionality is configured to support OSV V4 and higher tracing configuration and the other devices that integrate with OSV-TM. OSV-TM V7 and higher releases support secure FTP (SFTP) through the Windows OpenSSH 3rd party software included in this release. This software is automatically installed with OSV-TM. No additional configuration is required by the administrator.

SFTP User Accounts

The same "tracedata" local account configured for FTP is used for the SFTP authentication.

If dedicated SFTP accounts are required for each of the devices that integrate with OSV-TM, they need to be manually created. The sections that follow provide the instructions for creating and configuring these SFTP accounts.

For environments following the MS best practices for Network Security, tracedata accounts must be manually added at "Allow to Log on locally" under "User Rights Assignment".

Please follow the steps below:

1) Open "Local Users and Groups Manager"
   a) Press the **Windows + R** keys to open the Run dialog
   b) Type **lusrmgr.msc**, and press **Enter**
2) On the “Local User and Groups (Local)” on the left side of the window double click on **Groups** folder
3) Select the “Administrators” and press right click
4) Click **Properties**
5) Click **Add**
6) On the **Select Users** pop-up windows, enter the name “tracedata” and click **OK**.
7) Click **Apply** and then click **OK**.
8) Now you can log on locally with the tracedata user

Important Information for OSV-TM Servers Located in a Windows Domain

If the OSV-TM server is located in an Active Directory Windows Domain, a local Windows account or a domain user account can be configured as an SFTP user. However, for these accounts to be authorized to write to the SFTP storage, they need to be added to the "Power Users" Windows local group.

Please consult your Windows Domain Administrator if this is a security restriction for your company. If your policy does not allow the use of the "Power Users" group, the OSV-TM server should not be joined to a Windows domain but placed in a Workgroup.

Domain accounts to be used for the SFTP functionality should be requested from your Domain administrator.

8.8.5.5 Configuring Multiple SFTP Accounts for Trace Data Transfer

To be able to configure multiple SFTP accounts to integrate with other devices, it is required to create those accounts as Windows local user accounts on the OSV-TM server.

NOTICE:

These user accounts will also be added to the "OSVTM" Windows group to be able to write to the "tracedata" storage folder.

8.8.5.6 How to Create Additional SFTP User Accounts

The following procedure should be followed for each Windows local account created for SFTP transfer.

Prerequisites

Adequate administrative permissions.

Step by Step

1) Login locally to the OSV-TM server with a Windows administrator account.
2) From the "Start" menu navigate to "Control Panel"
3) Click on "Administrative Tools" then "Computer Management"
4) Expand "Local Users and Groups" and click on "Users"
5) From the "Action" menu select "New User"
6) Create the new user (i.e.: sftpusersbc)
7) Set a Password and note it down; the same password will be required for the OSV-TM configuration.
8) Uncheck "User must change password at next logon"
9) Check mark the option: "Password never expires"
10) Click the "Create" button then "Close"

    The new user account is created and should be listed under the users folder.

8.8.5.7 Additional 3rd Party Software Required Configuration

Active Perl

IE Enhanced Security

Active Perl is required only for environments running OpenScape Voice V7 and earlier versions which use the RTT Trace Management Tool server component to configure tracing.

"Active Perl" is not included in the OSV-TM package.

IE Enhanced Security requires additional configuration for OSV-TM functionality.

Upon installation, the Windows OS has the Internet Explorer Enhanced Security Configuration feature enabled by default. In order for FADE, the Trace Manager portal, to display correctly in IE, this feature needs to either be disabled or configured to trust the OSV-TM site/links.

8.8.5.8 How to Configure OSV-TM as a Trusted Site

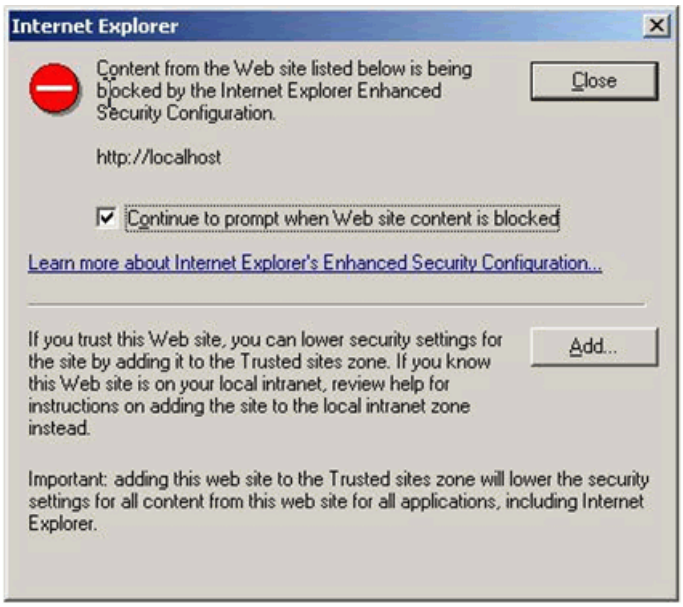
Prerequisites

Adequate administrative permissions

Step by Step

1) From the Desktop, click on the FADE icon.

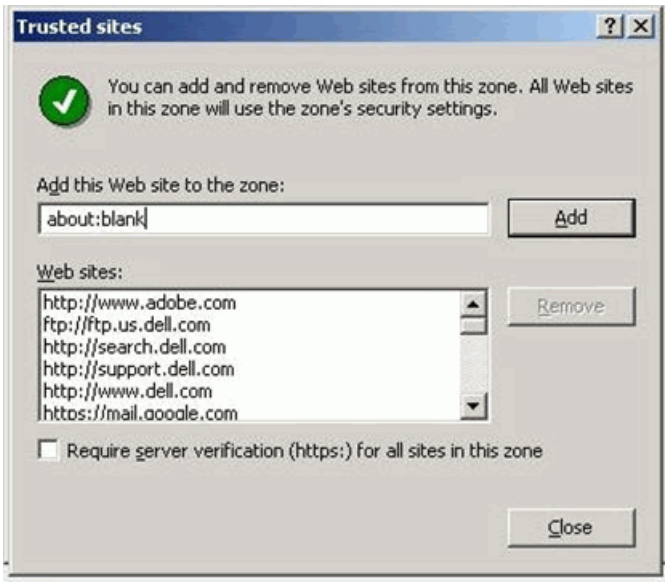
The message box "...content from Web site listed below is being blocked ..." is displayed.



2) Click the "Add" button.

The "Trusted Sites" window opens.

3) On the "Add this Web site to the zone" field, type: about:



4) Click "Close"

The OSV-TM pages and graphs should display correctly. Ignore any Activex warnings; OSV-TM does not utilize this technology.

8.8.5.9 How to Disable IE Enhanced Security Configuration

Prerequisites

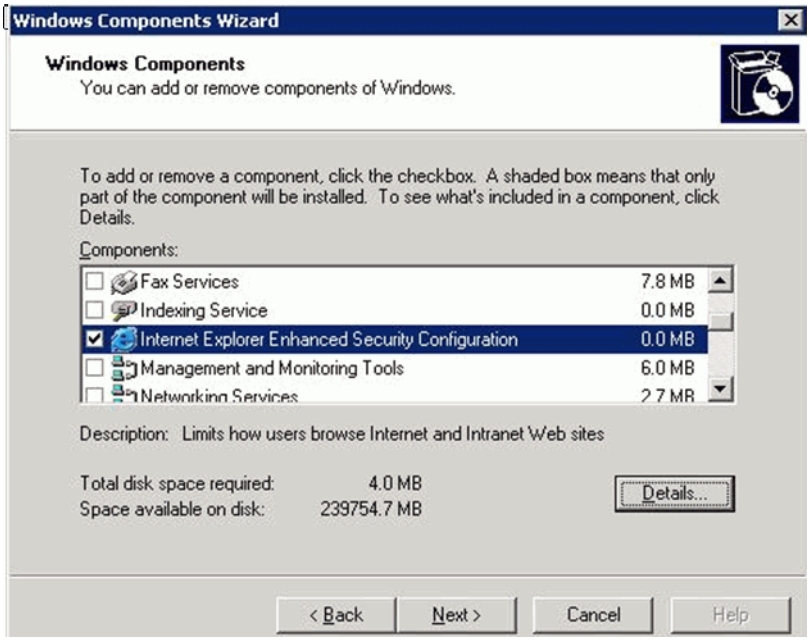
Adequate administrative permissions

NOTICE:

You have the option to disable "IE Enhanced Security"; however, disabling it is not required for OSV-TM functionality and your server may be at risk. Please review IE's security recommendations in Microsoft web site before disabling this feature.

Step by Step

1) Close all IE windows
2) From the "Control Panel" select "Add or Remove Programs"
3) Click on "Add/Remove Windows Components"
4) Check mark the "Internet Explorer Enhanced Security Configuration" option, and click "Next"



5) Click "Finish"

   IE Enhanced Security is no longer enabled.

NOTICE:

The OSV-TM installation is now completed. Proceed to the "Configuring OSV-TM through FADE" section to finalize the configuration of the OSV-TM server.

8.8.5.10 Additional Configuration Required in OSV-TM to Display OpenScape Branch and Session Border Controller Performance Monitoring Graphs

To be able to display OpenScape Branch (OSB) and Session Border Controller (OSS) performance statistics and graphs, the identification information for the branches and gateways to be monitored should be manually added to a specific OSV-TM configuration file.

This performance information is displayed from the OpenScape Voice (OSV) perspective. The OSB and OSS performance data is collected by the OSV server that these devices connect to and stored in the OSV trace data files.

NOTICE:

This configuration must be completed on the OSV-TM server before the OSV starts transferring trace files to the OSV-TM system.

Setting Up the OSB and OSS Performance Monitoring Graphs Configuration File

The OSB and OSS identification information needs to be provided in the "branches.csv" OSV-TM file. This configuration file is located in the corresponding OSV-TM system's folder "<system-drive>:\mtc\config \<sysname>".

You need the IP addresses and names of these devices to complete this configuration.

To setup the branches.csv configuration file:

- Open Windows Explorer and navigate to the OSV-TM system's configuration path <system-drive>:\mtc\config\<sysname> (i.e.: C:\MTC\Config\Sys1)
- Open the file "branches.csv" with Notepad. If the file does not exist, create one with this same name.

NOTICE:

A template file called "branches.tmpl" is provided with the OSV-TM installation. You can open the file to get a sample of the configuration.

This file is a comma delimited file that must have the following format:

```
<Idx,IP,Name,Type,Answer_Threshold,Errored_Threshold,Abandoned_
```

A header line with the title of fields should be
included as the first line in the "branches.csv"
file:Idx,IP,Name,Type,Answer_Threshold,Errored_Threshold,Abandoned_Threshold,Is

These fields define the following values:

- Idx = sequence number
- IP = IP number of the branch
- Name = name of the branch
- Type = type of branch (e.g., branch (Openbranch), Gw (Gateway))
- Answer_Threshold
- Errored_Threshold
- Abandoned_Threshold
- IsActive = 0 or 1 (1= active)

- The parameters for each branch to be monitored should be provided on a separate line.
- Ensure to save the file to the correct path:

  ```
  <system-drive>:\mtc\config\<your OSV-TM systemName>
  \branch.csv
  ```
- Restart the DIPAZ Monitor service after the configuration file is saved.

The performance data will now be parsed from the new OSV trace files received on the OSV-TM server, and the graphs displayed in FADE through the OSV view on the "Branch Status" tab.

8.9 Upgrading from an Earlier OSV-TM Version

3rd Party Software Manual Upgrade Requisite

The "Active Perl" 3rd party application required for environments running OpenScape Voice V7 and earlier is no longer included in the OSV-TM installation package.

Please review the "Requirements" section in this manual for the versions supported by OSV-TM.

NOTICE:

Environments integrating with OpenScape Voice V7R1 and above no longer require Active Perl.

This software can be uninstalled before upgrading OSV-TM.

Upgrade Preparation:

Upgrading from versions higher than OSV-TM V1R3 will automatically migrate existing data; however, some trace files will be reprocessed if necessary. Data may not show in FADE immediately; it will be displayed as the trace files are reprocessed.

OSV-TM changed its database engine from MySQL to SQLite starting with the V2.0 release. If you are upgrading to the latest OSV-TM version from OSV-TM V1R3 or an earlier version, careful planning is necessary.

Important Considerations for Systems Upgrading from OSV-TM V1R3 and Earlier

The processed trace data is stored in the current OSV-TM database engine along with additional configuration data. This data is not automatically migrated by the upgrade process; therefore, before upgrading to the new OSV-TM V7 version, a decision regarding upgrade strategy must be made.

- The OSV-TM systems will be re-created in the new SQLite database engine.
- The trace files collected from the OpenScape Voice server, OpenScape Branch will be preserved in the Tracedata folder during the upgrade or moved to a storage folder called `TRACES.OLD` depending on the upgrade strategy planned by the administrator.
- During the upgrade, the OSV-TM administrator will be prompted to indicate what upgrade strategy will be followed and based upon the answer, either all trace files will be reprocessed again by the DIPAZ service after the upgrade is completed or no data will be re-processed.
- The amount of processing time necessary for the data files to be re-processed depends on the number of trace files in the `Tracedata` storage directory and the `Days in Rear` configuration parameter set for each OSV-TM system.
- After the upgrade is completed, DIPAZ ages the trace data files in the `TRACES.OLD` folder with the same frequency as it is configured for the regular `tracedata` folder based on the `Clean Days in Rear` parameter configured for each OSV-TM system.
- The Quality of Service data for the phones is lost during the upgrade since this data is collected directly into the database by the Phone TrapCollector. This data is not critical as it is also captured by the OpenScape Voice server and can be viewed through the **OpenScape_Voice view** > **Performance** tab in FADE if the option to re-process trace files is selected.
- User accounts are migrated.
- Personal queries are migrated; however, due to syntax differences between MySQL and SQLite, they may not function properly and will probably require either fixing the query definition or re-creating the query by the query owner.
- Any custom reports or applications written by users that interfaced directly with the MySQL database will no longer work. They will have to be redesigned to work with SQLite.

Requirements

- Make sure that there is enough free disk space in `Tracedata` to accommodate the existing trace files and the new files that will be transferred after the upgrade. The DIPAZ monitor ages the preserved files based on how the `Clean Days in Rear` parameter is configured, so calculate disk space based on the selected upgrade strategy.
- The OSV-TM upgrade process does not uninstall the MySQL software and it also does not remove the old MySQL database.

  The administrator must uninstall MySQL and delete the old database from the OSV-TM server after the upgrade has been successfully verified.

Related concepts

Migration from an Earlier OSV-TM Version on page 115

8.9.1 Upgrading Strategies - Systems Upgrading from OSV-TM V1R3 and Earlier

Three upgrading options are available in this release:

1) "Start clean": no data is preserved or re-processed after the upgrade is completed.
2) "Re-process all": all trace data files are re-processed; longer upgrade processing time.
3) "Partial trace data re-processing": only re-process a smaller number of trace data files.

Related tasks

How to Perform an Upgrade Installation on page 143

8.9.1.1 Clean Upgrade

Start Clean Upgrade

IMPORTANT:

With this option, no trace data is re-processed. FADE does not display any pre-existing data after the upgrade.

All processed data stored in the existing MySQL database engine will not be migrated during the upgrade and the trace data files are moved from the "Tracedata\<system-name>" directory to a TRACES.OLD folder. The files in the TRACES.OLD folder are not re-processed; only new trace files transferred after the upgrade to the OSV-TM server will be processed by DIPAZ and displayed in FADE.

The upgrade process will:

- Create of a new SQLite database.
- Re-create the existing OSV-TM system definitions in the database.
- Move the trace data files in the `Tracedata folder` to the `<c:\` or `d:\>tracedata\<system-name>\TRACES.OLD` folder.
- The files in the TRACES.OLD folder will be cleaned/deleted based on the "Clean Days in Rear" value configured for the <system>

To select this upgrade option, the administrator enters **yes** during the upgraded when prompted:

```
Proceed with a Start Clean Upgrade, processing just new
files [y/n]
```

Related tasks

How to Perform an Upgrade Installation on page 143

8.9.1.2 How to Start a Clean Upgrade

Prerequisites

Adequate administrative permissions.

Step by Step

1) During the upgrade, the user is prompted.

```
Proceed with a Start Clean Upgrade, processing just new
files [y/n]
```

2) Type `y(yes)`

8.9.1.3 Re-process all Traced Data Files

With the Re-process all-procedure, all trace data files are re-processed.

Re-process All Traced Data Files

With this choice, an empty database is also re-created -all processed data stored in the existing MySQL database engine will not be migrated; however, all trace data files are preserved in the Tracedata folder to be re-processed after the upgrade is completed.

The upgrade process will:

- Create a new SQLite database.
- Re-create the existing OSV-TM system definitions in the database.
- Preserve all the files in the **Tracedata** folder.
- After the upgrade finishes, DIPAZ re-processes all the pre-existing files in the `Tracedata\<system>` folder.
- FADE displays the pre-existing data after DIPAZ completes re-processing it.

NOTICE:

Selecting this option will increase your upgrade time depending on how many trace data files are stored in the Tracedata folder.

The larger the number of files, the more down time should be allocated to the upgrade.

8.9.1.4 How to Upgrade with Re-process All Traced Data Files

Prerequisites

Adequate administrative permissions.

The "Days in Rear" and the "Clean Days in Rear" parameters must be properly configured for each system; otherwise, this strategy will not work correctly and some trace data files may not be processed. They should be set to a Time Period (in days) that includes all files in the Tracedata folder for each corresponding system.

Step by Step

1) Note the date of the oldest file in the `Tracedata\<system>` directory and calculate the period that includes all the number of days until that date.

   Example:

   OSV-TM system name: sys1

   Today is March 20, 2010

   The "oldest" trace file's date is March 5th (i.e.: \Tracedata \sys1\oprtt_trace.raw.20100305000113.61.gz)

   Time Period (number of days that includes all files) = 15
2) Login into FADE as an administrator and select the system (i.e.,: **sys1**).
3) Configure the `Days in Rear` and `Clean Days in Rear` parameters.
4) Navigate to **Administration** > **TM_System_Configuration** > **DIPAZ**
5) In the fields **Days in Rear** and **Clean Days in Rear** enter the calculated time period.
6) Click **Save**
7) Repeat the steps above for any additional systems configured in the OSV-TM server, i.e., configure the fields **Days in Rear** and **Clean Days in Rear** as required for each system.
8) Proceed with the upgrade installation. The following prompt appears:

   ```
   Proceed with a Start Clean Upgrade, processing just new files [y/n]
   ```
9) Type `n` (no) at the prompt.

8.9.1.5 Partial Trace Data Re-processing

With the Partial trace data re-processing procedure, a smaller number of trace data files are re-processed.

Partial Trace Data Re-processing

This strategy is similar to the "Re-process all" approach but re-processes a smaller number of existing trace data files by pre-selecting the Time Period of files that you consider worth keeping.

The DIPAZ engine will also re-process these reduced set of files after the upgrade based on the "Days in Rear" and the "Clean Days in Rear" parameters.

To select the number of trace files that will be re-processed, the OSV-TM administrator will need to configure the "Days in Rear" parameter for each of the OSV-TM systems. This will tell the DIPAZ engine to only process files for the Time Period defined in this variable.

The unnecessary trace files will be deleted from the corresponding system folder in the Tracedata directory after the re-processing is completed.

The upgrade process will:

- Create a new SQLite database.
- Re-create the existing OSV-TM system definitions in the database.
- Preserve all the files in the **Tracedata** folder.
- The `Days in Rear` and `Clean Days in Rear` settings are preserved in the configuration files.

- After the upgrade completes, DIPAZ reads the `Days in Rear` parameter previously configured and re-processes the trace files in the **Tracedata \<system>** folder for the set time period.
- FADE displays the pre-selected data after DIPAZ completes re-processing it.

NOTICE:

The advantage of this method is a shorter upgrade down time. The lower the number of trace files that need to be re-processed, the less time the upgrade will take to complete.

8.9.1.6 How to Upgrade with Partial Trace Data Re-processing

Analyze your trace data and decide how many of the existing records are necessary to be migrated and preserved to the new version. You will need to identify the trace data files that contain these records and the date when they were created. Then, configure the Time Period for re-processing in the "Clean Days in Rear" variable.

Prerequisites

Adequate administrative permissions.

Step by Step

1) For each system configured in the OSV-TM server, analyze the processed traces and calculate how many days worth of data (i.e., the time period) need to be migrated during the upgrade.

Example:

OSV-TM system name: sys1

Today is March 20, 2010

Valuable data to be re-processed from: March 13th

Time Period (number of days of valuable data) = 7

2) Login into FADE as an administrator and select the system (i.e.: **sys1**).

3) Configure the `Days in Rear` and `Clean Days in Rear` parameters.

4) Navigate to **Administration** > **TM_System Configuration** > **DIPAZ**

5) In the **Days in Rear** field, enter the time period calculated above.

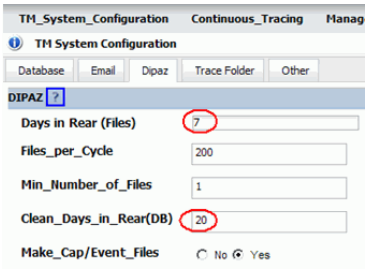
This is the number of "days" in the past time stamp that DIPAZ will consider for re-processing trace files (i.e.: 7 in our example)

6) If the Clean_Days_in_Rear" field is currently less than the Time Period, change it to be the same number as the Time Period or greater (i.e.: 7 in the example above or grater to preserve more files).

   - This parameter is used to "age/delete" the files in the Tracedata \<system> folder. If not set correctly, the DIPAZ monitor could delete the necessary trace files before they are processed.

     Based in our example, if the current date is March 20th and the "Days in the Rear" parameter is set to 7, only trace files containing data from March 13th until today are re-processed.

     – If the "Clean_Days_in_Rear" is set to 5, all trace files dated before March 15th are deleted -we will loose 2 days of valuable data.
     – If the "Clean_Days_in_Rear" is set to 7, all trace files dated before March 13th are deleted -all trace files of valuable data are preserved and processed.
     – If the "Clean_Days_in_Rear" is set to 20, all trace files dated before March 1st are deleted - all trace files of valuable data are preserved and processed, plus you have additional trace data files that you could re-process later on if needed.



7) For any additional systems configured in the OSV-TM server, repeat the previous steps and configure the **Days in Rear** and **Clean Days in Rear** fields appropriately.
8) Proceed with the upgrade installation. To select this upgrade strategy, the administrator must enter "no" during the upgrade process when prompted:

   ```
   Proceed with a Start Clean Upgrade, processing just new files [y/n]
   ```

9) Type `n` (no) at the prompt.

8.9.1.7 How to Perform an Upgrade Installation

Prerequisites

Adequate administrative permissions.

System prerequisites and 3rd party software have been installed and/or upgraded first, and then OSV-TM software will be installed.

OSV-TM V7R0.7.x supports RAM drives as storage for the OSV-TM databases. This configuration is only recommended for customers experiencing delays in their trace processing or performance problems. This feature is not enabled by default when upgrading OSV-TM; additional hardware requirements are needed to enable it. Please refer to the "Using A RAM Drive Storage for Performance Solutions" section for details.

When upgrading from a version older than V1R3.7.0, some of the components are uninstalled first, then reinstalled.

Step by Step

1) Open Windows Explorer and locate the temp folder containing the installation executable.

   Start > **Programs** > **Accessories** > **Windows Explorer**

   Example: `C:\temp`

2) Double click on the file `OSV-TM_Vx.x.exe` (where x represents the current version) to start the installation.
3) If installing on a German Windows OS server, at the prompt, select the language to use during the installation: English or Deutsch.
4) Click **OK**

   The **Welcome to the OSV-TM Setup Wizard** is launched
5) Click **Next**
6) Accept the licensing agreement to continue. Click **Next**
7) On the **Ready to Unpack** window, click **Unpack**
   The installation files are extracted to the `<SystemDrive>:\OSV-TM` folder (i.e.: `C:\OSV-TM`)
8) The **Completing the OSV-TM Setup Wizard** window is displayed.
9) Verify that the "Setup OSV-TM Server" box is checked.
10) Click **Finish** to start the upgrade installation.

    The "OSV-TM Server Installation" window opens. This window displays the status of the installation.
11) Click the "Install" button to initiate the installation.

12) The “Trace Management Server Installation” CMD window opens.

The installation messages are displayed:

a) If upgrading from older OSV-TM versions, some old components will be uninstalled:

Some components are uninstalled first and re-installed.

The following messages are displayed:

```
”Uninstalling HiQ RTT Tool ...”
”Uninstalling WireShark ...”
”Uninstalling 7-Zip...”
”Uninstalling PHP ...”
”Uninstalling Apache HTTP Server ...”
”Uninstalling Perl ...”
Press any key to continue ...
```

Press any key (i.e. **Enter**)

The OSV-TM Base Software and 3rd party is installed: PHP, Apache HTTP Server…

```
Installing Third Party Software . . .
```

The additional OSV-TM applications are installed: DIPAZ Utility, DIPAZ Monitor, FADE Utility, OpenScape Voice Server RTT Utility, OpenScape SBC RTT Utility, Phone Trap Collector ...

Click **Yes** to keep going with the installation.

b) Upgrading from later OSV-TM versions:

The components are upgraded and the following messages are displayed:

```
Check for previous installations ...
Installing Third Party Software...
Installing OSV-TM Applications...
```

The silent installation process continues …

13) The following steps allow you to choose your upgrade strategy and complete the 3rd Party components configuration for OSV-TM.

The command prompt window displays:

```
This script updates Trace Management server
configuration
Stopping DIPAZ services...
Creating necessary folders...
...
```

14) You maybe prompted by the upgrade process to uninstall MySQL after the upgrade completes or keep MySQL.

Additionally, you will need to choose the upgrade strategy you want to follow for the existing trace data.

IMPORTANT:

Please make sure to review the explanation of the different upgrade strategies.

A Warning message related to MySQL support the following will be displayed:

```
WARNING: MySQL is no longer supported by OSV-TM.
OSV-TM will replace MySQL with SQLite from that point
onward.
Please review the Upgrade Instructions in the OSV-
TM Administrators Guide for upgrade preparation and
guidelines.
```

- `The data in the existing database will NOT be preserved.`
- `Selected trace data files will be re-processed after the upgrade completes if you choose not to use the "start clean" upgrade option.`
- `This will increase the upgrade processing time.`

```
You may choose to completely uninstall/remove MySQL
or keep your MySQL database to recover existing data
later.
```

IMPORTANT:

Uninstalling MySQL will destroy existing data.

```
Would you like to uninstall MySQL after upgrade
completes [y/n]? y
```

Enter `y` (yes), if you want to follow the upgrade process to uninstall MySQL.

Enter `n` (no), to proceed with the upgrade. MySQL will remain on the server.

15) Additional configuration messages are displayed and the existing OSV-TM systems are detected:

```
INFO: Found existing setup
Displaying current setup . . .
System: sys1
. . .
Would you like start clean, processing just new files
for system: sys1 [y/n]?
```

Enter `y` or `n` according to your upgrade strategy.

16) Enter `y` for Clean Upgrade.
    The following message is displayed:
    ```
    INFO: Backing up trace files.
    Please wait . . .
    ...
    Configuration complete.
    Press any key to continue ...
    ```
17) Press any key to close the configuration window.
18) "Click "Finish" on the "OSV-TM Server Installation" window.
19) Re-configure the FTP transfer in the OpenScape Voice node.
    It is necessary to update the transfer script on the OpenScape Voice Server node. Follow the configuration steps in the section “Setting up Tracing On the OpenScape Voice server".
20) The OSV-TM upgrade installation is now complete.
    Upgrade installation logs are stored in the following location:
    `<SystemDrive>:\OSV-TM\Log`

Related concepts

Configuring Tracing on Devices to Integrate with the OSV-TM Server on page 170
Upgrading Strategies - Systems Upgrading from OSV-TM V1R3 and Earlier on page 139
Clean Upgrade on page 139

8.9.1.8 Manual Upgrade of Additional 3rd Party Software

Mandatory procedures

If you are upgrading your environments to integrate with OpenScape Voice V7R1 and above, Active Perl is no longer required. This software can be uninstalled from the OSV-TM server.

Java and Wireshark are client components not required for OSV-TM server functionality. If no other application is using Java or Wireshark, then it is recommended that you un-install these components. If the System Administrator of the OSV-TM server chooses to keep these components on the server, then he will need to ensure that at all times the latest secure versions are being deployed.

Follow the provider's instructions to manually install or un-install these components on the OSV-TM server.

Optional Procedures

OSV-TM no longer delivers a file decompressing utility; therefore, to be able to open "cap" and "event" files on the OSV-TM server via the FADE portal. The administrator needs to install an application that unzips ".gz" files. (Example: 7-Zip or WinZip).

Please see the "Requirements" section for more information.

8.10 Uninstallation of OSV-TM

To remove the OpenScape Voice-Trace Management server tracing integration, the following components need to be manually removed from the OpenScape Voice Server node: FTP transfer scripts, crontab jobs, and temporary folders/ files.

8.10.1 How to Stop FTP Transfer Configuration from OpenScape Voice Server V3.x

To remove the OpenScape Voice-TM server tracing integration, the following components must be manually removed from the OpenScape Voice node: FTP transfer scripts, crontab jobs, and temporary folders/files.

Prerequisites

Adequate administrative permissions (root privileges for the OSV Server node).

NOTICE:

The following steps should be run on the OpenScape Voice Server node to stop tracing. You will need "root" privileges.

Step by Step

1) Stop tracing.

Stop all oprtt_read processes on the node before removing the transfer scripts.

a) Enter `ps -ef | grep oprtt_read`
b) Note the process id
c) Enter `kill -9 <process id>`

This stops the process.

2) Remove the transfer Cron job.

a) Enter `crontab -l`

This command lists all the cron jobs and is used to identify the rttftp2.ksh job.

- If the “rttftp2.ksh” job is the only job listed, remove the complete crontab file.

  Continue with step 3.
- Otherwise, edit the cron file and remove the “rttftp2.ksh” job.

  Continue with step 4.

3) Enter `crontab -r root`

It removes the complete crontab file for the "root" subscriber.

IMPORTANT:

This removes all jobs for the “root” account.

Continue with step 8.

4) Enter `crontab -e root`

   This opens the cron file in the ‘’vi’’ editor.

5) Set the cursor on the line that has the “rttftp2.ksh” job.

   Use the “j” key on the keyboard to navigate “down” or use the “k” key to navigate “up”.

6) Delete the line by clicking the **d** key twice.

7) Enter `":", "w", "q" >:wq`.

   This saves the changes to the cron file.

8) Delete all temporary directories, processing and log files:

   - `rm –r /tmp/rttftp2`
   - `rm /var/log/rttftp2.log`
   - `rm /tmp/rttftp2.pid`
   - `rm /root/rttftp2.ksh`

9) Enter `rm setup_trace_transfer.ksh`

10) Enter `cd /software/RTT`

11) Enter `rm *.raw*`

    If this is a cluster/dual node configuration, repeat the removal steps on the second OpenScape Voice node.

8.10.2 How to Stop OpenScape Voice Trace File Transferring for OSV Server V4 and Later

To stop the OpenScape Voice V4 (and later releases) -OSV-TM server tracing integration, the FTP service must be stopped from the RTT Trace Management Tool.

Prerequisites

Adequate administrative permissions.

Step by Step

1) Log into OSV-TM server.
2) Click **RTT Trace Manager** (icon) to open the RTT tool.
3) Login to the expert mode with an expert mode user ID and expert mode password.
4) Click tab **Connection Control**
5) Enter the OpenScape Voice Server IP address for node 1 in the **Node 1 System Name or IP address** field.
6) Enter the OpenScape Voice admin ID (i.e., `srx` or `sysad`) in the **UserName** field.
7) Enter the OpenScape Voice ***<admin password>***
8) From the "RTT Trace Management Tool", go to the tab **Continuous Trace Control**
9) On the "Continuous Trace Data File Export Control" section, click **Stop File Export** on the section **Continuous Trace Data File Export Control**

8.10.3 How to Stop Further Trace Processes

Step by Step

1) Stop OpenScape SBC Tracing

OpenScape SBC tracing is automatically stopped when the OpenScape SBC Listener is uninstalled from the server during the OSV-TM uninstall process.

2) Stop Phone QoS Tracing

All phones programmed to send QoS data to the OSV-TM server must be reconfigured to remove the IP address from the **QCU Home Address** field and to stop the **Send Traps QCU** function.

3) Stop OpenScape Branch Tracing

The OpenScape Branch must be reconfigured through the OpenScape Branch Assistant to stop sending traces to the OSV-TM server.

Any other devices integrating with OSV-TM need to be configured to stop sending traces to the server.

8.10.4 Removing OSV-TM Base and 3rd Party Software

The latest OSV-TM uninstall program allows you to select which components to remove: most 3rd party applications and Trace Manager components, OSV-TM configuration files, and OSV-TM backup files.

However, during the uninstall, not all of the program folders/directories nor any trace data files may get deleted.

Additional manual clean up is required.

8.10.5 How to Run the Uninstall OSV-TM Server Utility

OSV-TM is uninstalled with the "Uninstall OSV-TM Server" Utility and selecting which components to remove.

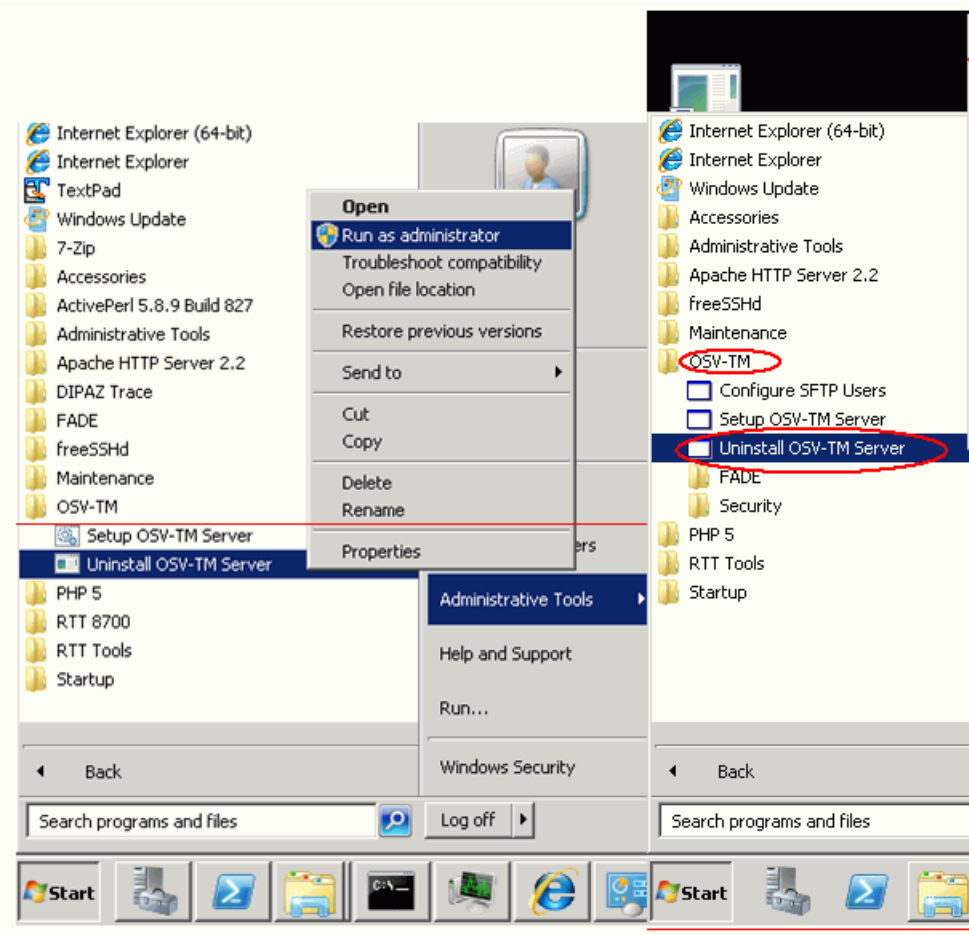
Step by Step

1) Close all applications and OSV-TM related windows before uninstalling OSV-TM. Having open files, folders, and applications will prevent the uninstall process from removing them.

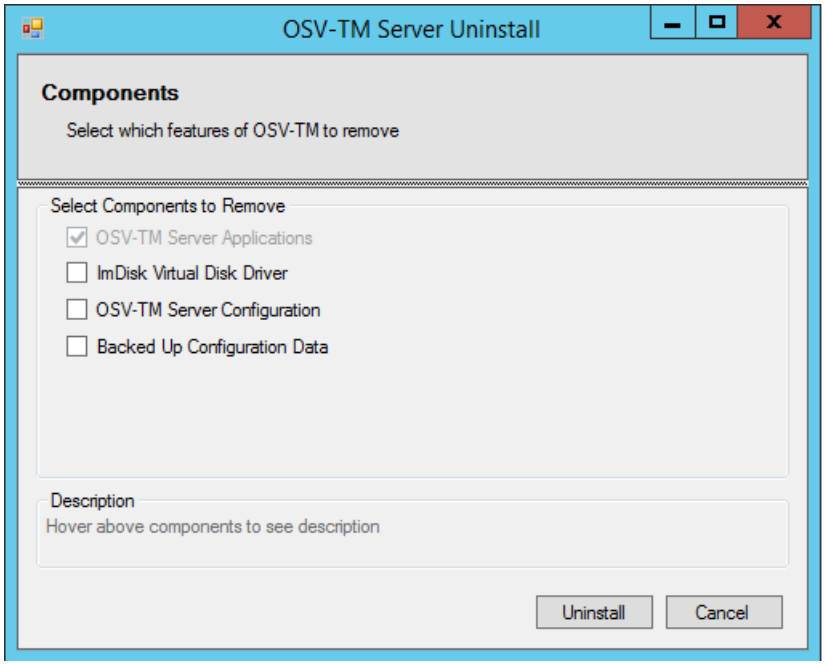
2) Run the "Uninstall OSV-TM Server" Utility as administrator:

a) Navigate to Start->All Programs->OSV-TM

b) Right click on "Uninstall OSV-TM Server" and select "Run as Administrator"



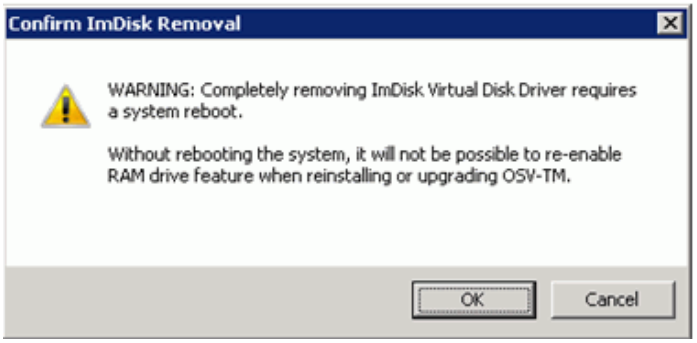
c) On the OSV-TM Server Uninstall window select which Components to uninstall.



- OSV-TM can be partially or completely unistalled.

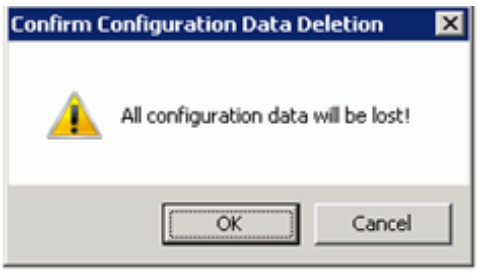
  To completely remove OSV-TM from the server, all components need to be selected for removal and the server restarted after the Uninstall process completes if the RAM Disk feature was enabled in OSV-TM.

  To partially remove OSV-TM components, check mark only the options you want to uninstall:
- OSV-TM Server Applications: This option is enabled by default and will only remove all OSV-TM applications including 3rd party software.
- ImDisk Virtual Disk Driver: This option will only be available if the RAM Disk feature was enabled during the previous OSV-TM installation. The server must be rebooted to completely remove the Virtual Disk Driver.



- OSV-TM Server Configuration: If selected, this option will delete all OSV-TM configuration files. If not selected, the OSV-TM configuration files, the databases and configuration files for the existing OSV-TM systems, and the trace files in the "tracedata" storage are preserved.
- Preserving the configuration is useful if the administrator wants to uninstall the OSV-TM applications but preserve the systems and

tracedata information. A later version of OSV-TM can be installed and re-use the existing configuration.



- Backup Configuration Data: Use this option to delete the storage where the automated backup functionality is dumped to.

The list of applications that were removed is displayed.

d) Click "Next" then "Finish"

Important Uninstall Notes:

- Any local Windows User accounts created manually are preserved in the server.
- The Tracedata storage folder will not be removed when OSV-TM is uninstalled. The folders where the trace files for the existing OSV-TM systems are saved remain in the storage until manually deleted by the administrator.
- If OSV-TM is re-installed and the same Tracedata storage folder is used, traces will be placed in the same folders. They can be reused by the OSV-TM installation.

NOTICE:

If the traces stored in the "Tracedata\tracemanager" folder are older than the default "Days in Rear" parameter (7 days), ensure that you reset the "Days in Rear" and "Clean Days in Rear" accordingly through FADE to be able to see your old traces.

8.10.6 Additional Manual Removal Procedures

Prerequisites

Adequate administrative permissions.

Step by Step

1) Uninstall SFTP/SSH Server

a) Launch Windows PowerShell

b) Navigate to `C:\Program Files\OpenSSH` (or wherever OpenSSH contents have been previously extracted)

c) Execute the following command

```
powershell.exe -ExecutionPolicy Bypass -File
 uninstall-sshd.ps1
```

2) Remove any additional SFTP local Windows User accounts.

3) Delete the Windows User accounts:

a) Navigate to Control Panel -> Administrative Tools -> Computer Manager
b) Expand **Local Users and Groups**
c) Click **Users**
d) Select the account to delete.
e) From the "Action" menu, click "Delete"
f) Click "Yes" on the warning to delete user.
g) Close the "Computer Management" window.

4) Manually remove all tracing files and logs; delete the Tracedata folder.

The Tracedata storage is not deleted when OSV-TM is uninstalled. The files and folders remain in the storage until manually deleted by the administrator.

5) Navigate to the storage drive and delete "Tracedata".

<SystemDrive>:\Tracedata (or drive where it was created)

NOTICE:

This will complete delete your tracing data files. Do not delete this folder if you need to preserve these archives

---

If the Tracedata directory is configured as a Windows File Share, Windows may not remove this; Tracedata needs to be un-shared first. Not removing the share will prevent new versions of OSV-TM to re-install correctly.

6) Some folders and files used by the uninstall feature cannot be automatically removed during the uninstall process; they need to be manually deleted.

a) Reboot the OSV-TM server.
b) Delete the following folders:

- <SystemDrive>\OSV-TM
- <SystemDrive>\Program Files (remove "only" if folder is empty)
- <SystemDrive>\FreeSSHDService (If exists)

7) Empty the "Recycle Bin" on your Desktop

8) If the RAM Disk feature was enabled in OSV-TM, the server must be restarted to completely remove the related components and drivers.

OSV-TM uninstall is complete.

8.11 Configuring OSV-TM through FADE

OSV-TM systems are managed and configured via the Trace Management Portal (FADE), Administration view.

Use the "TM_System_Configuration" tab to change or set the parameters of a system. Use the "Manage_TM_System" tab to create or delete systems. Only users with "administrator" rights have access to these functions.

On new OSV-TM V7 and higher installations, an OSV-TM system/node is created by default; see section below for details.

NOTICE:

Working with an OpenScape Voice Server Cluster Configuration.

If your OpenScape Voice Server (OSV) configuration is a dual node (duplex/ cluster) system, please note that both nodes in the cluster are identified by a single OSV-TM "system name" (i.e.:SYS1); therefore, you will need to use this "system name" to analyze the traces from your cluster.

Both OSV nodes should be configured to transfer their trace files to the same OSV-TM system folder under the <SystemDrive>:\tracedata\<system-name> directory.

Non-Domain Environments

Remote web interface access to OSV-TM for systems located in a non-domain network is only possible by using the IP address of the server in its URL and configuration file.

The administrator must verify that the server name in the OSV-TM is set to its IP address instead of the machine name by opening and logging into FADE locally and then access the **Administration > TM_System_Configuration** tab.

Logging in for the First Time

In the OSV-TM server, login to the Trace Management Portal (FADE) web interface as administrator:

- Open the Trace Management Portal: Click the "FADE" icon on the Desktop.
- The default administrator User Name account is: Admin (case sensitive).
- The default administrator Password is: Admin (case sensitive).
- Change the administrator's password.
- You will be prompted to change the Admin account password the first time you login into FADE.

  The password must be at least 8 characters and must contain a combination of [A-Z], lowercase [a-z], numeric[0-9], and special charters (!@#$%^&*()

Default OSV-TM System: TraceManager

Fresh installations of OSV-TM V7 and above create and configure a new default OSV-TM system on the server. For OSV-TM upgrades, this default system is not created.

Default system name: TraceManager
Default configuration

DBPartition: Weekly

Days in Rear: 7

Clean_Days_in_Rear: 7

Trace storage folder: <sys-drive>:\tracedata\tracemanager

This system is ready for use and automatically setup to start processing traces sent to its tracedata storage folder.

Only the following parameters need to be set up by the administrator:

- Email Parameters
- Enable Remote Access to FADE (OSV-TM web portal)
- Configure FTP for trace files transfers

See the "Configuring OSV-TM Systems" section for instructions.

To create and configure another system, follow the instructions in the following section "Adding/Removing OSV-TM Systems".

8.11.1 Adding/Removing OSV-TM Systems

On new OSV-TM V7 and above installations, an OSV-TM system/node is created by default; see section above for details.

Additional systems can be added, or existing systems be removed, via the "Manage_TM_System" tab in the Administration view.

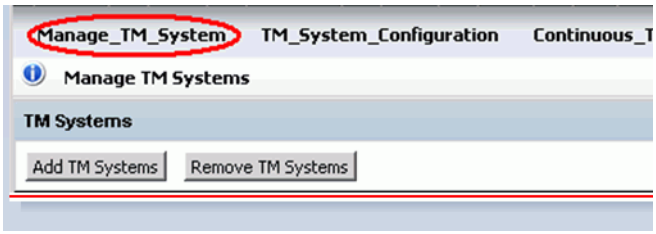
Adding or removing OSV-TM systems can only be done locally from the OSV-TM server via the Trace Management Portal -FADE. You need to have OSV-TM administrator access level.

You must be logged in into the OSV-TM server and open the Trace Management Portal using the FADE icon from the server's Desktop.

The login URL must resolve to the "localhost": https://localhost:28081/FADE/public/index.php/login

NOTICE: The Add/Remove Systems feature is only functional if "localhost" is used in the URL when invoking FADE on the server. Do not use the server's IP address.

After logging into the FADE portal, access the "Manage_TM_System" tab under the "Administration" view.



8.11.2 How to Add a System

Each OSV-TM system integrates with an OpenScape Voice node.

Prerequisites

Adequate administrative permissions.

The administrator is logged on to FADE.

NOTICE: In environments where OSV clusters (duplex) are used, only a single OSV-TM system should be configured. The trace files from both nodes should be transferred and collected in the same Tracedata\ <system> repository

Step by Step

1) Log into the OSV-TM server with an OSV-TM Windows administrative account
2) Login into FADE: Click on the FADE icon located on the server's Desktop
3) Navigate to the Administration view -> Manage_TM_System tab. The Manage_TM_System tab is only active or visible when you are logged locally on the OSV-TM server. Remote FADE sessions do not display this tab. All existing systems are listed.
4) Click on **Add TM Systems**
5) Enter the values required to create the system in the "Add TM System" view:
6) Go to the field: **System(s)**
7) Enter the name associated with the OSV node. This name should be user friendly. Only use numbers and letters as special characters are not allowed.
8) Go to the **Database** drop down box. This field indicates the database engine for this system. The default value is **SQLite**.
9) Go to the **Trace Data Directory** field and enter the trace data storage location: *<drive>:\tracedata*. This is the default location. The drive location must match the trace data storage area location established during pre-installation (e.g., c: or d:) as indicated in the "Trace Data Storage Planning" pre-installation section.
10) Go to **Server Name** and enter the server name: **local host**
11) Go to **Database Path** and enter **<system drive>:\MTC\config**. This is the path where the SQLite database is stored. The default location is: **<system drive>:\MTC\config**. To store the database for the new system in a different storage location, enter the new storage path in this field.
12) Go to **DB Partition**. This indicates the database partitioning scheme used to store the processed trace data. <Weekly> is the default.
    - None: Configures the system with DB Partition scheme 1: One database per device
    - Daily: Configures the system with DB Partition scheme 2: One database per device per day.
    - Weekly: Configures the system with DB Partition scheme 3: One database per device per week.

    NOTICE: Please review the section titled "OSV-TM Database Optimization Schemes" (in this manual) for detailed information on when to use the different storage schemes before selecting a DB Partition for the new system. Changing the default configuration will restrict data filtering and querying.

    ---

13) Use RAM Drive: (default: unchecked). Enable this option to store the system in a RAM Drive. Review the section "Creating a New OSV-TM System on a RAM Drive" for detailed information on how to configure this feature.

14) Click **Save** but do not close the **Add TM system** window. A message indicating not to close the browser is displayed. Any status or errors will be reported to the same window during the creation of the system.

NOTICE: Do not close the browser window.

15) Check the information bar to follow the processing status.
16) Look for the message: **System created**. Please review the log file for more details TM Syslog.
17) Click on **TM Syslog** to review the system creation log.

8.11.3 How to Remove an OSV-TM (OpenScape Voice) System

You can remove a single system, multiple systems, or all systems from the server.

Prerequisites

NOTICE:

Removing a system will delete the entries in the database for that system and all the trace data files in the **Tracedata \<system>** folder.

Adequate administrative permissions.

The user is logged into the Trace Manager Portal (FADE) as an adminstrator.

Step by Step

1) **To remove a Single System:** Navigate to **Administration** > **Manage_TM_System**

   The **Manage_TM_System** tab is only active or visible when the user is logged on to the OSV-TM server locally.

   Remote FADE sessions do not display this tab.

   All existing systems are listed.
2) Mark the checkbox of the system to be deleted.
3) Click **Remove TM Systems**

IMPORTANT:

Removing a system also deletes all the trace data files and database entries related to that system.

A confirmation message is displayed.

4) Click **OK** if you want to proceed or "Cancel" to abandon the removal.
   - If you have more than one system configured, and are logged into is the system that is being removed, FADE will automatically switch the user to another system in the server when the removal is complete.
   - If only a single system is configured in the server, and the system the user is currently logged into the system being removed, FADE automatically logs the user off.
5) Click **OK** to complete the transaction.
6) **To remove All the Systems from the Server:** Click on the **ALL** check box. This will select all the systems in the list.
7) Click **Remove TM Systems**

   IMPORTANT:

   Removing a system also deletes all the trace data files and database entries related to that system.

   A confirmation message is displayed.
8) Click **OK** if you want to proceed or "Cancel" to abandon the removal.

   FADE will automatically log the user off when the removal is finished.
9) Click **OK** to complete the transaction.

   All systems are deleted from the server.

8.11.4 Manual Post-System Removal Cleanup

Stop Trace Data Files FTP Transfer from All Devices

```
All devices that were integrated with the deleted OSV-TM
 system need to be reconfigured to stop the trace data
 transferring to the OSV-TM server.
```

The FTP or SFTP service that transfers the trace files to the removed OSV-TM system needs to be stopped on the corresponding devices.

- For OpenScape Voice Server V3.1, stop the cron job that spawns the FTP session to the OSV-TM server.
- For OpenScape Voice Server V4.0, stop the active mode FTP session that is initiated from the OpenScape Voice system by the PrttReader process.

SFTP transfers from the OSB, OSS, OSUC, and HMS devices need to be stopped if the device is integrated with OSV-TM.

8.11.5 Configuration OSV-TM Systems

The TM_System_Configuration option in the Administration view allows modification to the following components:

- SQLite database
- Systems default E-Mail parameters
- DIPAZ monitor

- Trace Folder location
- Other default system values

It also allows you to enable remote access to a system, disable FTP FADE transfers, and set an OSV-TM system in "stand by mode" or suspended mode.

8.11.6 How to Set Database Parameters - SQLite Configuration

Each OSV-TM system has its own database table. The value in the "Database Name" field indicates the database table name for the system that the user is currently logged in to. The username **tracer** is used internally to execute database transactions.

Prerequisites

Adequate administrative permissions.

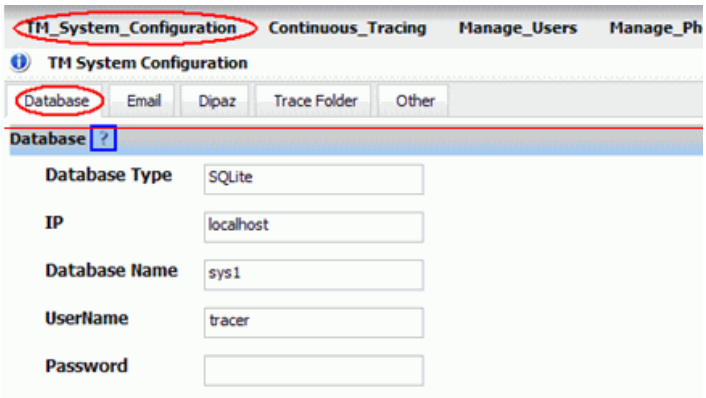
The user is logged into the Trace Manager Portal (FADE).

NOTICE:

The Database Path field indicates the location where the database is stored at.

Step by Step

1) From the **Administration** view, go to **TM_System_Configuration**



2) Select tab **Database**

3) Go to **Database Type**

4) Enter the value **SQLite**

5) Go to **IP**

6) Enter the IP (e.g., localhost).

7) Go to **Database Name** and enter the**<name>** (e.g., sys1)

Each OSV-TM system has its own database table. The value in this field indicates the database table name for the system that the user is logged into.

8) Go to **UserName** and enter **tracer**

The UserName "tracer" is used internally to execute DB transactions.

9) Go to **Password** and specify the password for the database table.

10) Click **Save**

8.11.7 How to Set Email Parameters

The Email tab has the default Email parameters for OSV-TM to send message alerts and notifications. This procedure is used to set the values for the SMTP Server, To, From and Subject fields.

Prerequisites

Adequate administrative permissions.

The user is logged into the Trace Manager Portal (FADE).

NOTICE:

Only a single SMTP server address is supported. If you have multiple OSV-TM systems configured, they all should have the same SMTP server address.

Step by Step

1) From the **Administration** view, go to **TM_System_Configuration**
2) Select tab **Email**
3) Go to **SMTP Server** and enter the name of your SMTP server

   If this field is empty, the email function will not work.
4) Go to **From**
5) Enter the **<email address>** of your SMTP server.

   A default email value is used when sending trace files.

   The "From" and "To" fields set a default email address value when sending messages from the OSV-TM server.
6) Go to **Subject** and enter a subject for the email.
7) Click **Save**

8.11.8 How to Set DIPAZ Configuration

Prerequisites

Adequate administrative permissions.

The user is logged into the Trace Manager Portal.

Step by Step

1) From the **Administration** view go to **TM_System_Configuration**
2) Select tab **Dipaz**
3) Enter a value for **Days in Rear (Files to progress)**

   Default value is 7.

   This value reflects the number of days in the past that trace files are considered for inclusion into the database.

   For example, if the current date is March 20th and the days in the rear is set at 10, all trace files from March 10th to March 20th are checked to determine if they should be incorporated into the database.

4) Enter a value for **Files_per_Cycle**

   Default value is 200.

   This is for the HiPath tracing files. It is the number of files that will be processed in one DIPAZ cycle (3 minutes). For optimal performance, a maximum of 300 is recommended.

5) Enter a value for **Min_Number_of_Files**

   Default value is 1.

   This is for the HiPath tracing files. This is the minimum number of files required for DIPAZ to process data.

6) Enter a value for **Clean_Days_in_Rear**

   Default value is 7.

   This value is used to determine how long records will be stored in the database.

   For example, if the current date is March 20th and the Days in the Rear is set to 10, all data items in the database older than March 10th are deleted. This field is also used by the DIPAZ monitor to age (delete) files older than the selected number of days from the tracedata repository.

7) Make a selection for **Make_Cap/Event_Files**

   Default value is Yes.

   This indicates to DIPAZ if a cap file and an event file should be created for each trace that is processed in the system.

   If "No" is selected, data will only be written to the database for analysis through FADE, but no trace files will be available for FTP or e-mail.

8) Click **Save**

Related concepts

Trace Information Flow on page 16

8.11.9 How to Read the Trace Folder tab

The directories indicated in these parameters represent the storage locations for the traces. These fields are read only.

Prerequisites

Adequate administrative permissions.

The user is logged into the Trace Manager Portal (FADE).

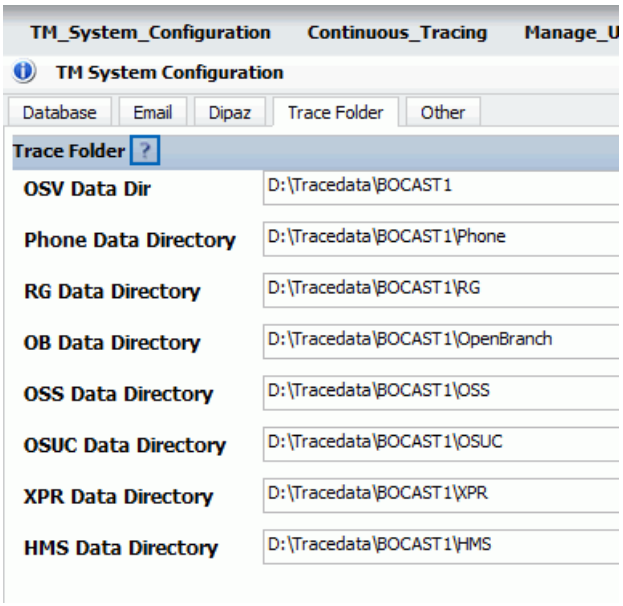
Step by Step

1) From the **Administration** view go to **TM_System_Configuration**

2) Select tab **Trace Folder**

These fields are read-only. These locations are displayed for informational purposes only and cannot be changed through FADE (as they affect the functionality of the system).

"OSV Data Directory" – C:\tracedata\<system-name> (OpenScape Voice trace files
"Phone Data Directory" – C:\tracedata\<system-name>\Phone (Phone trace files cor
"RG Data Directory" – C:\tracedata\<system-name>\RG (RG trace files container
"OB Data Directory" – C:\tracedata\<system-name>\OpenBranch (OpenBrach tra
"OSS Data Directory" – C:\tracedata\<system-name>\OSS (SBC trace files contain
"OSUC Data Directory" – C:\tracedata\<system-name>\OSUC (OSUC trace files cor
"XPR Data Directory" – C:\tracedata\<system-name>\XPR (XPR future trace files
"HMS Data Directory" – C:\tracedata\<system-name>\HMS (HMS trace files contai



Example

8.11.10 How to Set Other Configuration Fields

The values indicated in these fields are read directly by the OSV-TM processes, so when changing a physical path, any back slash "\" must be prefixed with a forward slash "/" (i.e.: `C:/\temp`) or instead of using a back slash, use a forward slash (i.e.: `C:/temp/`).

Prerequisites

Adequate administrative permissions.

The user is logged into the Trace Manager Portal (FADE).

Step by Step

1) From the **Administration** view go to **TM_System_Configuration**
2) Select the tab **Other**

3) Go to **CustomerName** and enter your setting.

   Defaults to the machine's name, but it can be set to the Customer name. This name must be used when FTPing or e-mailing trace files to indicate which customer they originated from.

4) Go to **Temporary Folder** and enter your setting.

   `c:/Temp/` Is the temporary staging area for background processes.

5) Go to **Fade Install Directory** and enter your setting.

   `C:/webdata/fade` Is the directory where FADE is installed.

6) Go to Server Time Zone - (US/Eastern) and enter your setting.

   This field represents the time zone that the server is running on.

7) Go to Search Limit and enter your setting.

   This field sets the default value in the "Search Filter" window for all users. It indicates the number of records that FADE will retrieve from the database when a query is run. Maximum parameter value is 1,000,000.

8) Go to **Allow Remote Access** and enter your setting.

   Yes/No This enables or disables remote access through the FADE Web interface

9) Go to "Allow FTP Access"

   Yes / No - enables or disables FTP download function from the FADE Web Portal interface. Default configuration is enabled (Yes).

10) Go to "DB Partition"

    None / Daily / Weekly - Indicates the partition scheme of the current system.- Weekly is the default value. **The section (in this manual) regarding OSV-TM Database Optimization Schemes, must be reviewed before changing this configuration.**

11) Go to **System Status** and enter your setting.

    Active / Suspended – Indicates the status of the current system.

    - Active: all incoming trace data files in the `Tracedata\<system>` are processed and aging is enabled.
    - Suspended: no traces in the "Tracedata\<system>" storage are processed and aging is disabled for this system. See the "Setting an OSV-TM System in Stand-by or Suspended Mode" section below for instructions on how to use this feature.

12) Go to **Rows per Page** and enter your setting.

    This sets the default value for the number of records to display when a filter or query is run. This parameter only affects the configuration for the system you are currently logged into.

    "Use RAM Drive" - Indicates if the current system is stored in a RAM Drive.

    If the field is checked, the system is using a RAM Drive as storage.

    If the field is not checked, the system storage is on the physical drive. This flag can be use to enable the RAM Drive feature for a system.

    See the section "Migrate or Move an Existing OSV-TM System to a RAM Drive Configuration" (in this manual) for detailed instructions.

13) Click **Save**

8.12 Configuring the OpenScape SBC Listener, and Phone Listener for an OSV-TM System

Integrating OpenScape SBC and Telephone devices with an OSV-TM system requires manual setup of the OpenScape SBC Listener and Phone listener components which is done through the Administration view on the FADE portal.

Related concepts

Initial Configuration of OSV-TM Systems

8.12.1 How to Add, Remove and Configure OpenScape SBC Tracing to an OSV-TM System

OpenScape SBC tracing is a “pull” function. The OpenScape SBC Listener component in the OSV-TM server contacts the OpenScape SBC via IP address requesting trace data; it listens, and puts the data into trace files that are later processed by DIPAZ into the OSV-TM database.

Prerequisites

Adequate administrative permissions.

The user is logged into the Trace Manager Portal (FADE).

Step by Step

1) Enable the OSV-TM Ports for OpenScape SBC communication

The Firewall ports required for OpenScape SBC tracing are not enabled by default in new OSV-TM V7 and later installations.

The Firewall rules for the OSV-TM communication ports with the OpenScape SBC need to be configured via the "OSV-TM Firewall Security Manager".

Follow the instructions to run the "OSV-TM Firewall Security Manager" utility in the "Enabling\Disabling OSV-TM Communication Ports with the OSV-TM Firewall Security Manager" section then enable the ports:

a) Check mark the "OpenScape SBC Listener" option

The (Enabled) label should show up.

b) Click Save. The message "Updating Firewall rules" is displayed.

c) Click "Close" to exit the utility.

The OpenScape SBC Listener ports are now opened.

2) To deactivate OpenScape SBC communication, just uncheck the same "OpenScape SBC Listener" option to disable the ports.

3) Configure the OpenScape SBC Listener.

4) Navigate to **Administration** > **-**

5) There are three possible options to manage OpenScape SBC Tracing: add, delete or modify OpenScape SBC Listeners configuration. Depending on what changes will be made, the corresponding "link" should be clicked.

Please note that the OpenScape SBC device has three IP Addresses:

a) Admin IP Address
b) SIP Signaling IP Address
c) Media IP Address

The "SIP signaling IP address" shall be used when adding or configuring and OpenScape SBC in OSV-TM.

- **Add OpenScape SBC Listener**

  This button located on the top-left of the screen will add a new OpenScape SBC to the system.OpenScape SBC Naming Convention

Restrictions: Only letters and numbers ca be used for the OpenScape SBC name. No special characters are allowed.

Continue with step 3.

- **Delete**

  Continue with step 4.

- **Modify OpenScape SBC**

  Continue with step 5.

6) Go to **Add OpenScape SBC Listener**. This button located on the top-left of the screen will add a new OpenScape SBC to the system. Enter the required information for the OpenScape SBC:

- OpenScape SBC Name
- OpenScape SBC IP address

  The OpenScape SBC device has three IP addresses:

  - Admin IP address

  - SIP signaling IP address

  - Media IP Address

  The SIP signaling IP address is used when adding or configuring an OpenScape SBC in OSV-TM.

- Click **Save**

7) Go to the **Delete** link to the right of an existing OpenScape SBC. This link removes the OpenScape SBC from the system.

The existing trace data for this OpenScape SBC remains in the system until it is aged by the DIPAZ monitor.

8) Go to **Modify** OpenScape SBC. This link to the right of an existing OpenScape SBC allows you to reconfigure the OpenScape SBC behavior. Enter the required information for the OpenScape SBC:

- Enable/disable trace parameters: SIP, Q931, CATS (select or deselect none, one or more)
- Stop or start tracing of this OpenScape SBC via the radio buttons
- Add or delete CATS flags (debugging flags for tracing) by selecting the values on the choice list.
- Click **Save**

  The Save button saves the current configuration. A message will indicate that the changes will take effect in 2 minutes.

- Note: Cancel will discard the current changes.

Related tasks

How to Add an OSV-TM System

8.12.2 How to Manage Phones in an OSV-TM System

The traces and Quality of Service data generated from the phones is collected in the OSV-TM server by the Phone Listener or Phone Trap. The ports used by the phone and by OSV-TM must agree to have successful connectivity.

Prerequisites

Adequate administrative permissions.

NOTICE:

When configuring Phone Listeners for multiple systems on the OSV-TM server, the Trace and Trap port numbers must be unique for each OSV-TM system. Do not use the same port number.

Logged into Trace Manager Portal (FADE) web interface

Step by Step

1) Enable the OSV-TM ports for the Phone Listener

The Phone Listener Firewall ports on the OSV-TM server are not enabled by default in new OSV-TM V7 and later installations. These ports need to be enabled via the "OSV-TM Firewall Security Manager".

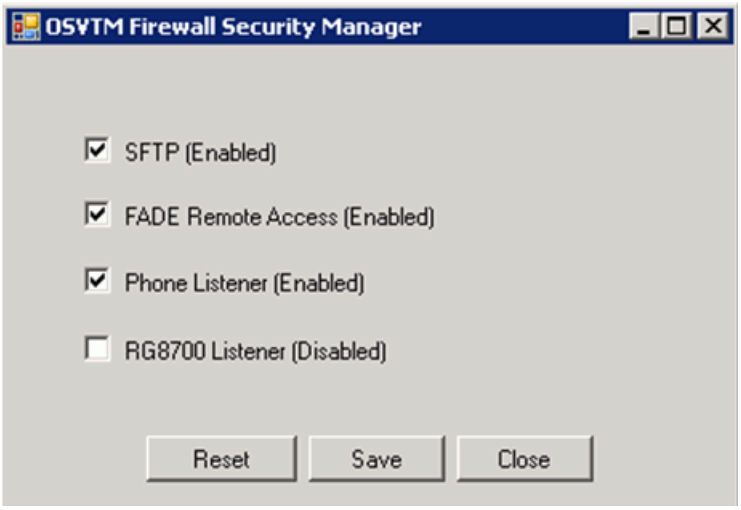
Follow the instructions to run the "OSV-TM Firewall Security Manager" utility in the "Enabling\Disabling OSV-TM Communication Ports with the OSV-TM Firewall Security Manager" section then enable the ports:

a) Check mark the "Phone Listener" option.

The (Enabled) label should show up.

b) Click Save.
The message "Updating Firewall rules" is displayed.

c) Click "Close" to exit the utility.



The Phone Listener ports are now opened.

To deactivate the Phone Listener communication ports, uncheck the same "Phone Listener" option.

2) Configure the Phone Listener:

Only one Phone Listener is configured per OpenScape Voice system and correspondingly per OSV-TM system.

NOTICE:

Important Restriction: When configuring Phone Listeners for multiple systems on the OSV-TM server, the Trace and Trap port numbers must be unique for each OSV-TM system. Do not use the same port number.

Phones are configured via the Administration view -> "Manage Phones" tab on the FADE Web interface.

3) Click view **Administration** > **Manage Phones**

4) There are three possible options in the Manage Phones tab: add, delete or modify phones depending on the existing phone configuration.

- Add Phone

  If there is no phone configured for the current system, then the **Add Phone** button is displayed.

  Continue with step 4.
- Delete Phone

  Continue with step 5.
- Modify Phone

  Continue with step 7.

5) Enter the required information for the Phone:

a) Phone Trap Port: It must be a value between 17000 and 18000 (unique port number).

b) Phone Trace Port: It must be a value between 500 and 600 (unique port number).

c) Max CAP File Size (MB): 2MB (default)

If the file exceeds this size then a new CAP file is created.

d) Max Trace File Size (MB): 2MB (default)

If the file exceeds this size then a new Trace file is created.

e) Continue with step 10.

6) Go to the Phone entry to delete.

7) Click **Delete** right to the Phone entry. Continue with step 10.

The existing Phone trace files and data are not deleted from the system but are aged by the DIPAZ monitor.

8) Go to the Phone entry to modify.

9) Click **Modify** right to the Phone.

10) Change, if necessary, its ports or the file sizes (allowed values: see step 4).

11) Click **Save**

A message indicates that the changes will take effect in 2 minutes.

Note: Cancel discards the current changes.

Related tasks

How to Configure Phone Devices to Send QoS Data to OSV-TM Listener on page 182

8.13 Configuring Tracing on Devices to Integrate with the OSV-TM Server

Each device that integrates with OSV-TM is configured independently for tracing and to send the trace data files to the OSV-TM server.

Support for IPV4 and IPV6

OSV-TM V7 supports IPV4 and IPV6 addressing from the OSV V6 and higher traces and QoS traps from OpenStage phones.

Trace data files with IPV6 addresses format will be processed normally and displayed through the view on the OSV-TM Web Portal -FADE.

QoS traps received from the IPV6 OpenStage phones will be received and handled by the Phone Listener.

No special configuration is needed in OSV-TM for this feature; it is enabled by default.

Setting Up Tracing on the OpenScape Voice Server

Configuring tracing on the OpenScape Voice V7R1 and above is done from the OSV Common Management Platform (CMP).

For lower OpenScape Voice versions (V4 through V7) tracing configuration and administration is done via the Real Time Trace (RTT) Trace Management Tool.

Older OpenScape Voice versions, V3.1 PS0035 and Below, use transfer scripts to set up tracing.

Important Notes:

If setting up the OpenScape Voice Server in OSV-TM for the first time all the steps in this section are necessary.

If the OpenScape Voice Server configuration is a dual node (i.e., duplex/cluster) system, the process must be followed for each node.

Both nodes in the cluster are identified by the same "system name" in OSV-TM (i.e.:SYS1); therefore, use the same "system name" when configuring the FTP transfer process on each node.

All trace files for both nodes are transferred to the same system folder under the `\tracedata\<system-name>` directory.

Verify connectivity from the OpenScape Voice Server to the OSV-TM server.

Test pinging the OSV-TM server:

```
>ping <OSV-TM server IP>
```

If ping fails, verify the network route configuration and ensure connectivity to the OSV-TM server.

If the OSV-TM Server lies outside of the Admin subnet, it may be necessary to setup a static route to make it accessible.

Contact your OpenScape Voice Server technician for support if necessary.

Related concepts
Configuration Requirements
Related tasks
How to Perform an Upgrade Installation on page 143

8.13.1 Pre-Setup for Trace File Exporting (FTPing) to OSV-TM Server

For OpenScape Voice Server V3.1, the transfer of traces to the OSV-TM server is controlled by a cron job that spawns an FTP session to the OSV-TM server. For OpenScape Voice Server V4.0, exporting trace files to the OSV-TM server is done using an active mode FTP session initiated from the OpenScape Voice system by the PrttReader process. To allow a connection and transfers to the OSV-TM server, it is necessary to configure Packet Filtering and Denial-of-Service rules on the OpenScape Voice Server.

8.13.1.1 How to Set Up Packet Filtering Role for FTP Connection

Prerequisites

Adequate administrative permissions

Step by Step

1) Open the RTP CLI menu, entering "`StartCli`" from srx.

   srx>`startCli`
2) Login as `sysad`
3) Create a packet filter rule.
4) Create a packet filter rule, navigate: **Application-level Management(6)** > **Network Element Security Management(8)** > **Packet Filter Rules Security management(4)** > **Create(1)**
5) Set the values:
   - Packet Filter Rule Name: OSV-TMContTraceServer (rule name)
   - Description: Allow FTP with OSV-TM Server (description)
   - Remote FQDN: <blank>
   - Remote IP Address: OSV-TM server IP address (nnn.nnn.nnn.nnn format)
   - Remote NetMask: 255.255.255.255
   - Remote Port Begin: 0
   - Remote Port End: 0
   - Direction: Incoming
   - Local Host: <blank>
   - Local Port Begin: 0
   - Local Port End: 0
   - Transport Protocol: ALL
   - Action: Allow
6) Save and close.

8.13.1.2 How to Configure Denial-of-Service Prevention

The OSV-TM server's IP address must be added to the Snort whitelist to prevent triggering of a Denial-Of-Service handling when transferring data.

Prerequisites

Adequate administrative permissions.

Step by Step

1) Open the RTP CLI menu by typing "`StartCli`" from srx `>startCli`.
2) Login as `sysad`.
3) Navigate through menu sequence: **Application-level Management(6)** > **Softswitch Management(1)** > **Softswitch Information(1)** > **Denial of Service Management** > **Denial of Service Trusted Hosts Mgmt(2)** > **Assign a Trusted Host(1)**
4) Set the value:
   - Trusted Host IP Address: OSV-TM server IP address (nnn.nnn.nnn.nnn format)
5) The **Denial of Service Management** value is different for OSV V3.1 and V4.
   - For OSV V3.1 the value is **7**: Denial of Service Management (7)
   - For OSV V4 the value is **6**: Denial of Service Management (6).

   IMPORTANT:

   The above procedure needs to be repeated on each node if the OpenScape Voice system is configured as duplex for load balancing.

6) Save and close.

8.13.2 Configuring OpenScape Voice Server V3.1R2 and V3.1R3

Configuring the OSV-TM involves several tasks: setting up tracing for the OpenScape Voice Server with the steps Pre-Setup for Trace File Exporting (FTPing) to OSV-TM Server, setting up a Packet Filtering Rule for the FTP connection, configuring Denial-Of-Service Prevention, and configuring for OpenScape Voice Server V3.1R2 and V3.1R3.

8.13.2.1 Transfer Tracing Scripts to the OpenScape Voice Server

The set of tracing scripts that must be copied to configure continuous tracing in OpenScape Voice Server V3.1 is based on the installed patch set level.

For V3.1 PS0035 and prior, the required "24_7" tracing scripts are not included in the OpenScape Voice Server installation; they must be copied along with the configuration scripts from the OSV-TM installation directory.

For V3.1 PS0036 and above, the "24x7" tracing scripts are already included in the OpenScape Voice Server node and only the configuration scripts need to be copied.

NOTICE:

A 3rd party application such as WinSCP is required to transfer the configuration scripts from the OSV-TM server to the OpenScape Voice Server. This application must be installed in the OSV-TM server (not included in the OSV-TM installation package).

8.13.2.2 How to Transfer Tracing and Configuration Scripts to OSV Server V3.1 PS0035 and Prior Releases

The tracing and configuration scripts must be transferred from the OSV-TM installation directory to the rtt_trace_script directory under "srx" home in the OpenScape Voice Server node.

Prerequisites

Adequate administrative permissions.

IMPORTANT:

These instructions apply ONLY to OpenScape Voice Server nodes running V3.1 Pre-PS0036.

Step by Step

1) On the OSV-TM server, using Windows Explorer, locate the **Siemens OpenScape Voice TM - V1R2** folder extracted during the OSV-TM installation (e.g.,: `C:\temp\Siemens OpenScape Voice TM - V1R2`).
2) Using a 3rd party software, transfer the scripts from the OSV-TM server to the OpenScape Voice Server.
3) Locate the `C:\<extracted_path>\Siemens OpenScape Voice TM - V1R2\Scripts\HiPath\V3.1_Pre-PS0036` directory on the OSV-TM server.
4) Transfer all files under the `V3.1_Pre-PS0036` folder to the `~srx/rtt_trace_scripts` directory (`/unisphere/srx3000/srx/rtt_trace_scripts`) in the OpenScape Voice switch.

   Example: Transfer all files: 24_7, 24_7_extern, 24_7_min, setup_tracing.ksh, and setup_trace_transfer.ksh from `C:\temp\Siemens OpenScape Voice TM - V1R2\ Scripts\HiPath\V3.1_Pre-PS0036\` to `~srx\rtt_trace_scripts\` directory in the OpenScape Voice switch.
5) On the OpenScape Voice server, go to the `~srx\rtt_trace_scripts\` directory and verify that the above files were copied correctly.

8.13.2.3 How to Transfer Tracing and Configuration Scripts to OSV Server V3.1 PS0036 and Above

The tracing and configuration scripts must be transferred from the OSV-TM installation directory to the rtt_trace_script directory under "srx" home in the OpenScape Voice Server node.

Prerequisites

Adequate administrative permissions.

NOTICE:

These instructions ONLY apply to OpenScape Voice Server nodes running V3.1 PS0036 and PS0036+.

Step by Step

1) On the OSV-TM server, using Windows Explorer, locate the `Siemens OpenScape Voice TM - V1R2` folder extracted during the OSV-TM installation (e.g.,: `C:\temp\Siemens OpenScape Voice TM - V1R2`).
2) Using a 3rd party software, transfer the scripts from the OSV-TM server to the OpenScape Voice Server.
3) Locate the `C:\<extracted_path>\Siemens OpenScape Voice TM - V1R2\Scripts\HiPath` directory on the OSV-TM server.
4) Transfer the `setup_tracing.ksh` and `setup_trace_transfer.ksh` scripts to the `~srx/rtt_trace_scripts` directory (`/unisphere/srx3000/srx/rtt_trace_scripts`) in the OpenScape Voice switch.

   Example: Transfer /copy: `C:\temp\Siemens OpenScape Voice TM - V1R2\ Scripts\HiPath\setup_tracing.ksh`, `C:\temp\Siemens OpenScape Voice TM - V1R2\ Scripts\HiPath\setup_trace_transfer.ksh` to `~srx\rtt_trace_scripts\` directory on the OpenScape Voice switch.
5) On the OpenScape Voice server, go to the ~srx\rtt_trace_scripts\ directory and verify that the above files were correctly copied.

   The "24_7" tracing scripts are already included in the OpenScape Voice V3.1 PS0036+ installation under the `/unisphere/srx3000/srx/rtt_trace_scripts` directory. These files should not be copied.

8.13.2.4 Set Up Tracing and Configure FTP Transfer to OSV-TM Server

When tracing is enabled, the RTT trace files are stored in a local directory on the OpenScape Voice Server (`/software/RTT/`). The two scripts (`setup_tracing.ksh` and `setup_trace_transfer.ksh`) copied from the OSV-TM installation folder must be run to enable tracing and to setup the FTP jobs to transfer the trace files to the OSV-TM server for processing and analysis.

IMPORTANT:

These procedures apply to all OpenScape Voice Server V3.1 patch set levels.

8.13.2.5 Configuration Script "setup_tracing.ksh"

The "setup_tracing.ksh" script calls the 24_7_extern script (default) which enables a subset of trace facilities and flags for ccm and ttudProc. The script also calls OP_RTT_READ with the parameters of 75 files, 10 Mb file size, and file wrapping enabled. If the user wants to change these default value,s then the script needs to be rerun. The setup_tracing.ksh script has two optional parameters: the tracing mode/level (-24_7|-24_7_extern|-24_7_min) and the tracing file size.

Functional Sequence

USAGE: `setup_tracing.ksh [-24_7|-24_7_extern|-24_7_min] [-size <1-29>]`

- Default trace level is: 24_7_extern
- Default trace file wrap size (in MB):
  - 10 <24_7_extern/24_7_min>
  - 20 <24_7>

Trace Levels

- 24_7_extern: Enables a subset of trace facilities and flags for ccm and ttudProc.
- 24_7: Enables a subset of trace facilities and flags for sip, sipRegistrar, uce, cstasm, ccm and ttudProc.
- 24_7_min: Enables a smaller subset of 24_7 trace facilities and flags for sip, sipRegistrar, uce, cstasm, ccm and ttudProc.

For example: If the user requires more trace data with 24_7 trace levels and also needs to lower the default file wrap size to 10M, the user can run: `> ./setup_tracing.ksh -24_7 -size 10`

8.13.2.6 Transfer Script "setup_trace_transfer.ksh"

The "setup_trace_transfer.ksh" script modifies the `.netrc` file, and creates a second script that is run via a cron job. This cron script compresses the raw trace files, sends the trace files via FTP to the OSV-TM server, deletes the FTP'd files from the local directory (`/software/RTT/`), and generates a ".pid" file to keep track of the transfers. The FTP transfer script maintains a log file in `/var/log/rttftp.log`.

8.13.2.7 How to Set Script Permissions and Modes

Prerequisites

Adequate administrative permissions.

Step by Step

1) On the OSV server: Change the owner and group of the "setup_tracing.ksh" script to srx:other with command:

   `>chown srx:other setup_tracing.ksh`

2) Change the owner and group of the "setup_trace_transfer.ksh" script to root:root with command:

   `>chown root:root setup_trace_transfer.ksh`

3) Set the executable permissions for both scripts:

   - `>chmod +x setup_trace_transfer.ksh`
   - `>chmod +x setup_tracing.ksh`

4) Disable the OpenScape Voice Server PrttReader process from reading the trace buffer. This is done via CLI and setting the parameter Srx/PrttReader/ReadFromDriver to 0.

5) **Stop the tracing job**, if tracing has already been configured in the OpenScape Voice Server:

   a) Stop all oprtt_read processes on each node before running the configuration scripts:

      `>ps -ef | grep oprtt_read` (get process id).

      `>kill -9 <process id>`

   b) Remove all existing "raw" files from the `/software/RTT` directory

   Invalid *.raw* files will prevent the transfer process from working properly.

6) **Start RTT tracing:**

   a) Run the setup_tracing.ksh script to configure the tracing process:

      `>setup_tracing.ksh` (run as srx user)

   b) Verify that the oprtt process is running:

      >ps -ef | grep oprtt_read

   c) Verify that the trace files (<filename>.raw) are being written to the correct directory:

      `/software/RTT`

7) **Configure the FTP transfer process:**

   a) Run the setup_trace_transfer.ksh script to configure the FTP transfer process:

      `> setup_trace_transfer.ksh` (run as user "root")

   b) Enter Trace Management (OSV-TM server IP address: Type the OSV-TM server's IP address.

   c) Enter OSV-TM FTP login: Type the FTP user id configured in OSV-TM.

   d) FTP password: Type the FTP password for the user id configured in OSV-TM.

   e) Enter the system name or ID as created on the OSV-TM server, i.e. System1. System ID: Type the system name given to the OpenScape Voice Server node in OSV-TM.

   f) Enter trace file upload interval (minutes) [1|2|3|4|5|10|15]: Type the frequency (in minutes) that you want the trace files to be transferred to the OSV-TM server.

   Note: After the "setup_trace_transfer.ksh" script is run, it creates a cron script and sets up a cron job that is run based on the frequency that isset as the "trace file upload interval". The recommended value is 2 minutes.

8) Verify that the root cron job was set correctly:

`> crontab -l` (look for the rttftp2.ksh job)

9) **Optional:** Test the ftp connectivity between the OpenScape Voice Server and the OSV-TM server:

a) `>ftp <osv-tm_IP_address> username=tracedata passwd=<ftp-tracedata-passwd>`

b) >quit

The OpenScape Voice Server is now configured to generate and transfer trace data to the OSV-TM server.

10) Verify that the trace files (<filename>.raw) are being written to the correct OpenScape Voice Server directory: `/software/RTT`

11) Verify that the files are transferred to the OSV-TM shared folder `\\<OSV-TM-server-address>\tracedata\<system-name>` (e.g.: `\\my-osvtm-serv.mydomain.com\tracedata\SYS1`).

12) When rebooting or after patching the OpenScape Voice server, restart the setup_tracing process:

a) Run the setup_tracing.ksh script:

`> setup_tracing.ksh` (run as srx user)

b) Verify that the trace files (<filename>.raw) are being written to the correct directory: `/software/RTT`

8.13.3 Configuration of Tracing and File Transferring for OpenScape Voice Server V7R1 and Later Releases

Configuring tracing on the OpenScape Voice V7R1 and later is done from the OSV Common Management Platform (CMP) via the following path: **Configuration** > **OpenScape Voice** > **Administration Wheel** > **Tools** > **Continuous Tracing**

Detailed instructions on how to configure and administer OSV tracing for V7R1 and higher releases can be found in the "OpenScape Voice V7R1 Service Manual" in E-Doku.

Traces are sent via SFTP to the OSV-TM server and stored in the trace data storage for processing: "tracedata\<system-name>\" directory

These traces are automatically processed by DIPAZ and their data saved into the SQLite database as they are received.

No further configuration is required in OSV-TM.

8.14 Setting up Tracing for OpenScape SBC

The OpenScape SBC device needs to be setup to enable tracing.

For detailed information on configuring the OpenScape SBC device, please refer to the Service, OpenScape SBC Vx.x Rx Install and Maintenance Manual.

OpenScape SBC tracing modes can be configured through the FADE Web Interface. The "Adding, Removing and Configuring OpenScape SBC Tracing on an OSV-TM System" section provides the detailed instructions to add and configure the OpenScape SBC parameters in OSV-TM.

Please note that the OpenScape SBC device has three IP Addresses:

- Admin IP Address
- SIP Signaling IP Address
- Media IP Address

The "SIP signaling IP address" is used when adding or configuring and OpenScape SBC in OSV-TM.

Once the OpenScape SBC is configured in the OSV-TM system, it starts polling and listening for traces.

There are two methods to enable tracing on the OpenScape SBC:

- Via the OSV Assistant CMP console
- From the OpenScape SBC CLI interface.

8.14.1 How to Enable OpenScape SBC Tracing from the OSV Assistant CMP

This is the simpler and preferred method to enable tracing.

Prerequisites

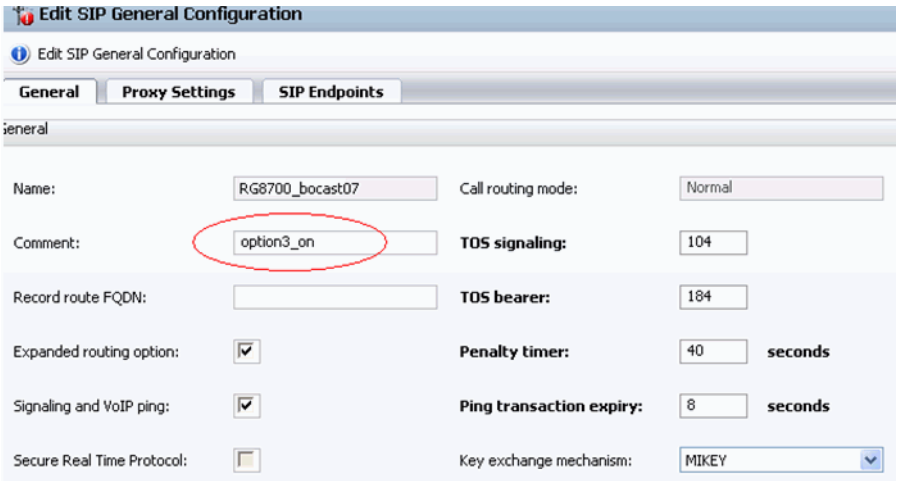
Adequate administrative permissions.

Step by Step

1) Open the OSV Assistant CMP.

2) Navigate to **Edit SIP General Configuration** > **General**

3) In the field **Comment**, enter the value `option3_on`.



8.14.2 How to Disable OpenScape SBC Tracing from the OSV Assistant CMP

Prerequisites

Adequate administrative permissions.

Step by Step

1) Open the OSV Assistant CMP.
2) Navigate to **-** > **SIP Management** > **General Configuration** > **Edit SIP General Configuration** > **General**
3) In the field **Comment**, enter the value `option3_off`.

NOTICE:

This is the preferred method to disable tracing.

8.14.3 How to Enable OpenScape SBC Tracing from the SIP Object CLI Interface

Prerequisites

Adequate administrative permissions.

Step by Step

1) Login onto the OpenScape SBC.
2) Enter user id = **admin** and <*admin password*>

   The system prompts with:
   `admin#`
3) Display the SIP object on the OpenScape SBC with the following commands:

   `dir/sip`

   `show /sip/xxx.sip`

   where xxx is the name or ID of the OpenScape SBC device (i.e., OpenScape SBC_bocast07.sip)
4) To enable tracing, modify the SIP object and set the comment field to option3_on with the following command:

   `mod /sip/xxx.sip comment option3_on`

Example

This is an example of the output screen on the OpenScape SBC when typing the above-mentioned cli commands for our sample OpenScape SBC_bocast07.sip device:

```
admin# dir /sip

10-21-2009 20:07 <SIP> 00000001 /sip/OpenScape
SBC_bocast07.sip

admin# show /sip/OpenScape SBC_bocast07.sip

Name: /sip/OpenScape SBC_bocast07.sip

Last Modified: 2009-21-10T20:07:27-0000

Comment:

Mg Ctrlr IP Address: 10.237.71.142

Mg Ctrlr Port Number: 5060
```

```
Backup Mg Ctrlr IP Address: 0.0.0.0
Backup Mg Ctrlr Port Number: 0
Proxy IP Address: 0.0.0.0
Proxy Port Number: 0
Mg Ctrlr Transport Protocol: tcp
Mg Ctrlr Heart Beat Interval: 32 (seconds)
Soap Server IP Address: 10.237.14.11
Soap Server Port Number: 8767
Backup Soap Server IP Address: 0.0.0.0
Backup Soap Server Port Number: 0
Soap Server Query Interval: 60 (minutes)
Penalty Timer Interval: 40 (seconds)
Timer F Interval: 32 (seconds)
Timer B Interval: 32 (seconds)
Record Route FQDN:
Survivability Mode: No
Expanded Routing Option: Enabled
SRTP: Disabled
Signaling and VoIP Ping: Disabled
TOS Signaling: 0
TOS Bearer: 0
New Soap Server Method: Disabled
Geo Redundancy Option: Disabled
Trans Record-Route: Disabled
UDP MTU Check: Disabled
bFqdn Cid Suppression: Disabled
Spare Flag 1: Disabled
Spare Flag 2: Disabled
Spare Flag 3: Disabled
Spare Flag 4: Disabled
Mg Ctrlr Domain Name:
Mg Ctrlr Dns: Disabled
SIPQ v2 Protocol: Enabled
Srtp Key Mechanism: mikey
Max Number of Failed Options: 3
SEP Assignments:
/sep/node2.sep
```

```
/sep/node1.sep
```

8.14.4 How to Disable OpenScape SBC Tracing from the SIP Object CLI Interface

Prerequisites

Adequate administrative permissions.

Step by Step

1) Login onto the OpenScape SBC.
2) Enter user id = **admin** and *<admin password>*

   The system prompts with:
   `admin#`
3) Display the SIP object on the OpenScape SBC with the following commands:

   `dir/sip`

   `show /sip/xxx.sip`

   where xxx is the name or ID of the OpenScape SBC device (i.e., OpenScape SBC_bocast07.sip)
4) To disable tracing, enter the following command:

   `mod /sip/xxx.sip comment option3_off`

8.15 Configuring Phone Devices to Send QoS Data and Tracing to OSV-TM

Phone traces can be generated from manually configuring a phone to send traces or from a user-initiated action that automatically triggers the start of tracing.

User-Initiated Tracing from OpenStage Phones

Phone traces can be initiated by a user from an OpenStage phone.

The SEN customer service representative provides the user with a pre-determined prefix to dial before his destination phone number (DN) and asks him to retry the call.

Traces are generated and collected for a limited time when the 'test call' prefix is recognized by the OpenStage phone and is replaced with an internal "TraceId" that is used to identify the call. The OpenStage phone traces are sent to the OSV-TM server by DLS via SFTP. The OpenScape Voice server traces the call for its duration, and the traced data is sent to the OSV-TM server via trace files. Once the traces are processed in the OSV-TM server, they are displayed through FADE (OSV-TM web portal) and the corresponding "cap" files can be downloaded for analysis.

NOTICE:

Continuous tracing has to be activated on the OpenScape Voice server before initiating the test call, so the tracing can be triggered.

NOTICE:

Only OpenStage and OptiPoint phone devices (Deprecated) are supported by OSV Trace Manager.

No further configuration is required in OSV-TM for User-Initiated tracing processing.

Detailed instructions on how to configure DLS to send traces to the OSV-TM server can be found in the DLS V7 Administration and Installation Manual that can be found in E-Doku.

8.16 How to Configure Phone Devices to Send QoS Data to OSV-TM Listener

Telephone QoS data collection and tracing need to be configured in the OSV-TM server for each system, and the corresponding telephone devices also need to be setup to send the data to the specified OSV-TM server port.

Prerequisites

Adequate administrative permissions.

You need first to identify the Phone Listener parameters configured in OSV-TM then configure the phone devices to complete the integration. See the "Manage Phones in an OSV-TM System" section for detailed instructions on how to add an OSV-TM Phone Listener.

Step by Step

1) Login to Trace Manager Portal (FADE) web interface as administrator.
2) Navigate to **Administration** > **Manage Phones**
3) The **Phone Trap Port** field indicates the default Trap port configured for the OSV-TM system. The **Phone Trace Port** field indicates the default Trace port configured for the system.
   - Trap Port

     Use the **Trap Port** value as the **Trap destination port** and **QCU Host Port Number** when configuring the phone devices

     Use the IP address of the OSV-TM server as the **trap destination** so that the phone can send the QoS data to the correct destination.
   - Trace Port

     Use the Trace Port value as the **Phone Trace Host Port Number** or **Remote Server Port** when configuring the phone devices to send phone traces to the OSV-TM (example: 500).

     Use the IP address of the OSV-TM server as the **Phone Trace Host IP Address** or **Remote Server IP** so that the phone can send the trace data to the correct destination.

   When changing the port number for the OSV-TM Phone Listener or TrapCollector, the phone also needs to be reconfigured to send the data to that new port.

Related tasks

How to Manage Phones in an OSV-TM System on page 168

8.16.1 How to Configure OptiPoint Phone Devices to Send QoS Data to OSV-TM

Prerequisites

Adequate administrative permissions.

NOTICE:

Changing the configuration of the telephones should be performed after business hours as the device requires a restart.

Configuring OptiPoint Phone Devices

Step by Step

1) Open the **DLS tool**
2) Expand folder **DeploymentService**
3) Navigate to **IP Devices** > **IP Phone Configuration** > **QoS Data Collection** The **QoS Data Collection** window opens.
4) Scroll down to the Server Data section.
5) Select check box **Send Traps QCU**
6) In the field **QCU Home Address**, enter the ***<IP address>*** of the OSV-TM server.
7) In the field **QCU Host Port Number,** enter the ***<port number>*** configured in OSV-TM for the corresponding system.
8) Click tab **Report Setting**
9) Set **Report Mode** value to: EOS (End of Session).
10) Click **Save**
11) Close the window.

8.16.2 How to Configure OpenStage Devices

Prerequisites

Adequate administrative permissions.

NOTICE:

Changing the configuration of the telephones should be performed after business hours as the device requires a restart.

Configuring OpenStage Phone Devices: (Steps 1 - 9)

Step by Step

1) Login to the OpenStage web administration interface as administrator.
2) Select System -> SNMP from the left pane.
3) Check mark the "Trap sending enabled" box.
4) In the "Trap destination" field enter the ip address of the OSV-TM server.
5) Set the "Trap destination port" field to the Trap Port configured in the OSV-TM Listener as identified above (example Trap port = 17000).
6) Check mark the "QoS traps to QCU" box
7) In the "QCU address" field enter the ip address of the OSV-TM server.
8) Set the "QCU port" field to the same Trap Port configured in the OSV-TM Listener as identified above (example Trap port = 17000).
9) Click on Submit when done.

   Completing the QoS setting on the OpenStage phone: (Steps 10 - 14)
10) Login to the OpenStage web administration interface as administrator.
11) Select Diagnostics -> QoS Reports -> Generation from the left pane.
12) On the Report mode select "EOS (End of Session)".
13) You can leave the other fields with the default parameters.
14) Click on Submit when done.

    Alternatively, the Deployment Service (DLS) server can be used to configure the OpenStage phone device for QoS listening as follows: (Steps 15 - 24)
15) Open the DLS tool.
16) Expand the DeploymentService folder.
17) Navigate to: IP Devices -> IP Phone Configuration -> QoS Data Collection.
18) On the QoS Data Collection window scroll down to the "Server Data" section.
19) Select the "Send Traps QCU" check box.
20) On the "QCU Home Address" field, enter the IP address of the OSV-TM server.
21) On the "QCU Host Port Number" field, enter the port number configured in OSV-TM for the corresponding system.
22) Click on the Report Setting tab.
23) Set the "Report Mode" value to: EOS (End of Session.
24) Click the "Save" button and close the window.

The QoS Data Collection configuration will be downloaded to the phone.

8.16.3 How to Configure OpenStage Phone Devices

Prerequisites

Adequate administrative permissions.

NOTICE:

Changing the configuration of the telephones should be performed after business hours as the device requires a restart.

Configure the Trace settings on the OpenStage phone as follows: (Steps 1 - 6)

Step by Step

1) Login to the OpenStage web administration interface as administrator.

2) Select Maintenance -> Remote Trace from the left pane.

3) Check mark the "Remote Trace Status" field.

4) In the Remote Server IP field enter the IP address of the OSV-TM server.

5) Set the Remote Server Port field to the Trace Port configured in the OSV-TM Listener as identified above (example Trap port = 500).

6) Click on Submit to save the changes.

To send standard SIP trace data from an OpenStage phone to the OSV-TM server this additional configuration is required: (Steps 7 - 11)

7) Log in to the OpenStage web administration interface as administrator.

8) Select Diagnostics -> Easy Trace Profiles -> SIP standard singleline from the left.

9) Set File size = <preferred value> (example: 1,048,576 bytes).

10) Set the Trace timeout parameter in minutes (example: 99999).

11) Select Submit

The phone should be ready to start sending standard SIP trace data to the OSV-TM server.

8.17 Setting up Tracing for OpenScape Branch

The OSV-TM support for OpenScape Branch (OSB) tracing analysis is enabled by default in all OSV-TM systems.

Tracing for the OpenScape Branch is configured through the OpenScape Branch Assistant. Please refer to the service document for the OpenScape Branch V7, Administrator Documentation, Issue x (where x is the current version).

Once configured for tracing, the OpenScape Branch sends its trace files directly via SFTP to the OSV-TM server; these trace files are stored in the "tracedata \<system-name>\OB" directory.

The traces are automatically unzipped by DIPAZ every five minutes and the files are processed into the SQLite database as they are received.

No further configuration is required in OSV-TM for OpenScape Branch tracing integration; however, for OSV-TM to process and display OSB .performance data, the information (IP address and device name) of the branches to be monitored should be added to an OSV-TM configuration file.

8.18 Setting up Tracing for OpenScape Session Border Controller

OSV-TM support for OpenScape Session Border Controller tracing analysis is enabled by default in all OSV-TM systems.

Tracing for the OpenScape Session Border Controller is configured through the OpenScape Branch Assistant interface. For additional information, please refer to the administration documentation for the OpenScape Branch, Administrator Documentation.

Once configured for tracing, the OpenScape Session Border Controller sends its trace files directly via SFTP to the OSV-TM server. The SBC trace files are stored in the same location where the OpenScape Branch traces are stored, i.e., in the **tracedata\<system name>\OB** directory. For identification purposes, “OSS” in included in the filename.

The traces are automatically unzipped by DIPAZ every five minutes and processed into the SQLite database as they are received.

No further configuration is required in OSV-TM for OpenScape Session Border Controller tracing;. however, for OSV-TM to process and display OSS performance data, the information (IP address and device name) of the gateways to be monitored should be added to an OSV-TM configuration file.

8.19 Setting up Tracing for OpenScape UC

OSV-TM support for OpenScape UC (OSUC) tracing analysis is enabled by default in all OSV-TM systems.

Tracing for the OpenScape UC is enabled and configured from the CMP administration interface of the OSUC device.

If the OSUC and HMS are collocated in the same server, the traces from both devices are set in a single file.

If the OpenScape UC is configured to send its traces to the OSV-TM server, the trace files are directly transferred via SFTP; the trace files are received by the SFTP service on the OSV-TM server and stored under the "tracedata\<system-name>\OSUC" directory.

The traces are automatically unzipped and processed as they are received by DIPAZ, and the data is parsed into the SQLite database.

No further configuration is required in OSV-TM for OpenScape UC tracing.

Detailed instructions on how to configure the OSUC to send traces to the OSV-TM server can be found in the "OpenScape Common Management Platform Vx, Administrator Documentation (where x is the corrent version), in the Remote Logging for OSV-Trace Manager Section (e-Doku).

8.20 Setting up Tracing for the HiPath Media Server

OSV-TM support for processing HiPath Media Server (HMS) traces is handled by default in all OSV-TM systems.

The tracing configuration for the HiPath Media Server is done from the CMP administration interface. If the HMS and OSUC are collocated in the same server, the traces from both devices are set in a single file.

If the HiPath Media Server is configured to send its traces to the OSV-TM server, the trace files are directly transferred via SFTP; the trace files are received by the SFTP service on the OSV-TM server and stored under the "tracedata\<system-name>\HMS" directory.

The traces are automatically unzipped by the DIPAZ process as they are received, and the data is parsed into the SQLite database.

No further configuration is required in OSV-TM for HiPath Media Server tracing.

Detailed instructions on how to configure the OSUC to send traces to the OSV-TM server can be found in the "OpenScape Common Management Platform Vx, Administrator Documentation, (where x is the current version) in the Remote logging for OSV-Trace Manager Section (e-Doku).

8.21 Setting up Tracing for Xpressions

OSV-TM support for processing Xpressions (XPR) traces is handled by default in all OSV-TM systems.

The traces are automatically unzipped by the DIPAZ process as they are received, and the data is parsed into the corresponding SQLite database.

No further configuration is required in OSV-TM for Xpressions trace processing.

Detailed instructions on how to configure the OpenScape Xpressions device to send traces to the OSV-TM server can be found in the "OpenScape Xpressions Vx, Server Administration, Administrator Documentation, in the section describing the OpenScape Voice Trace Manager (where x is the current version).

8.22 Setting up Tracing for Contact Center Extensions (OSCCE)

OSV-TM collects and stores OpenScape Contact Center Extensions (OSCCE) trace files to support only trace file filtering and access. The trace data is not processed by OSV-TM.

No further configuration is required in OSV-TM for OSCCE trace collection.

The instructions on how to configure Contact Center Extensions to send traces to the OSV-TM server can be found in the latest issue of the "OpenScape Contact Center Extensions V3, Configuration Concierge, Administrator Documentation".

8.23 Stopping or Re-starting OSV-TM Services

The DIPAZ Monitor is the main service that controls the OSV-TM processes. The DIPAZ Monitor service ensures that all processes are started after a system update or after a server reboot. This service automatically starts after a server

restarts. If the DIPAZ Monitor process is not running, the user must manually start the service.

8.23.1 How to Restart DIPAZ Monitor

The DIPAZ Monitor service ensures that all processes are restarted after a system update or after a server reboot. This service should start automatically after a reboot.

Prerequisites

Adequate administrative permissions.

The DIPAZ process is not running.

Step by Step

1) Navigate to **Start** > **Control Panel** > **Administrative Tools** > **Services**
2) Locate the **Dipaz Monitor**
3) Right mouse click and select **Start**

   The DIPAZ process starts a few seconds later.

Stopping and starting the DIPAZ Monitor service will force all other OSV-TM services to be restarted and to re-read the OSV-TM configuration files. This may be necessary when manual changes are made to the OSV-TM configuration.

Related tasks

How to Migrate Data Between Source and Target OSV-TM
How to Replace Configuration Files
How to Change Location of the Trace Data Storage Directory

8.24 User Accounts Administration

All user accounts are administered through FADE. Only users with an Admin access level can execute the User Management and Configuration of administrative tasks, e.g., create, delete, or modify user accounts. All user accounts are administered through the Administration view -> "Manage Users" tab in FADE.

OSV-TM enforces strict password rules on all accounts. These rules can be individually disabled by the OSV-TM administrator; however, it is recommended to keep all rules active to maintain a more secure framework. The list of rules and configuration are included in the last section of this chapter.

8.24.1 How to Create a User Account

Prerequisites

Adequate administrative permissions.

Step by Step

1) Login to Trace Manager Portal (FADE).
2) Navigate to **Administration** > **Manage Users**
3) Select **Add User**

4) Fill in all the blanks for: User ID, User Name, and Email fields.
5) Create a password.

   The password must be at least 8 characters and must contain a combination of [A-Z], lowercase [a-z], numeric[0-9], and special charters (!@#$%^&*()

   See additional rules in the "Password Security Rules" section.
6) Select the **Access Level**

   The default is **User**

   If the new account is an administrator, change the level to Admin. The "Advanced" user role has the following functionality:

   - It is allowed to see the **TM_Logs** tab in the **Administration** view
   - Allowed to Zip and download the TM logs
   - Access to the OSV-TM **Configuration** link on the top menu of the FADE portal
7) Retype ***<password>***
8) Click **Save**

8.24.2 How to Delete a User Account

Prerequisites

Adequate administrative permissions.

Step by Step

1) Login to Trace Manager Portal (FADE).
2) Navigate to **Administration** > **Manage Users**
3) Select the user to delete from list (column **UID**).
4) Click **Delete**

   A confirmation prompt displays.
5) Click **OK**

   The user no longer appears in the users list.

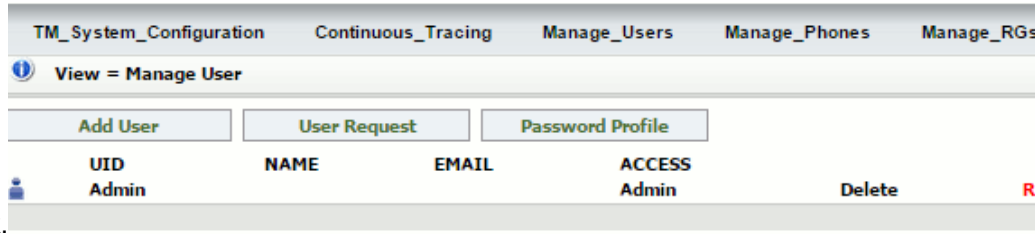
8.24.3 How to Reset Password

Prerequisites

Adequate administrative permissions.

Step by Step

1) Login to Trace Manager Portal (FADE).
2) Navigate to **Administration** > **Manage Users**
3) Select the user needing the password reset from the user list.
4) Click on the **Reset Password**



link.

5) Enter the new ***<password>***

   The password must be at least 8 characters and must contain a combination of [A-Z], lowercase [a-z], numeric[0-9], and special charters (!@#$%^&*()

   See additional rules in the "Password Security Rules" section.
6) Retype ***<password>***
7) Click **Save**

8.24.4 How to Change Access Level

There are two access modes: Admin and User.

Prerequisites

Adequate administrative permissions.

Step by Step

1) Login to Trace Manager Portal (FADE).
2) Navigate to **Administration** > **Manage Users**
3) Select the user from list (column **UID**).
4) Click the User ID that needs changing.
   The **Modify User** window opens.
5) Go to **Access Level** drop down box and change the level.

   (There are three levels: User, Advanced, and Admin.)

   The access level default is User.

   If the new account is an administrator account, change the level to **Admin**
6) Click **Save**

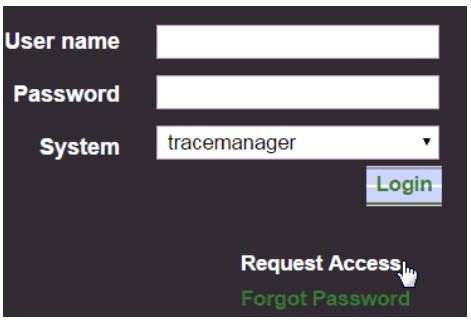
8.24.5 How to Manage User Account Request

Users request accounts by clicking on the **Request Access** link on FADE's welcome page. This action generates a user account request and adds an entry to the request queue. The administrator must then approve or reject the request.

Prerequisites

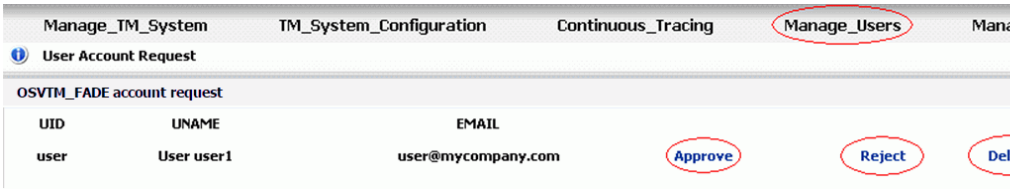
Adequate administrative permissions.

A user has clicked on **Request Access** on FADE's welcome screen.



Step by Step

1) Navigate to **Administration** > **Manage Users**
2) Click tab **Manage User Request**
3) Click **Approve** to the right of the User Account request.



Approving a request for an account creates the account. An e-mail message is sent to the user's address with the UID and password.

The user will be prompted to change the password on his first login.

8.24.6 Password Security Rules

OSV-TM enforces the following password rules to ensure better security on user accounts:

- Minimum password length = 8 characters
- Maximum password length = 20 characters
- Password should contain at least 1 uppercase character
- Password should contain at least 1 lowercase character
- Password should contain at least 1 number
- User account name should not be part of the password
- Password should contain at least 1 special character
- Password should not contain more than 3 sequential characters in a row
- Password should not contain more than 3 identical characters in a

- A changed password should have at least 2 characters difference from the original password
- User password reset every 90 days
- User account name in reverse should not be part of the password

The default configuration enables all rules except these two:

- Password should not contain more than 3 sequential characters in a row
- Password should not contain more than 3 identical characters in a row

8.24.7 How to Disable Password Security Rules

It is recommended to keep the default rules enabled. Customers that find these rules too restrictive for their environment can disable individual rules via FADE.

Prerequisites

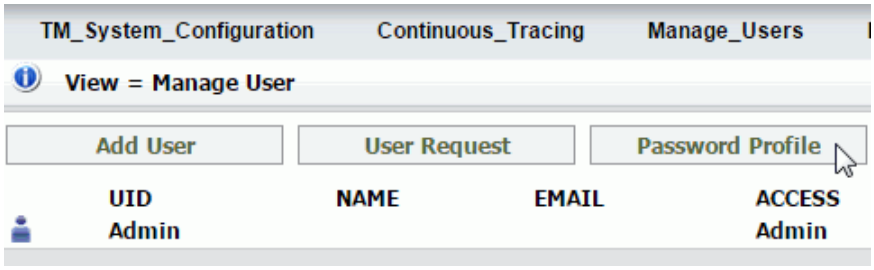
Adequate administrative permissions.

Step by Step

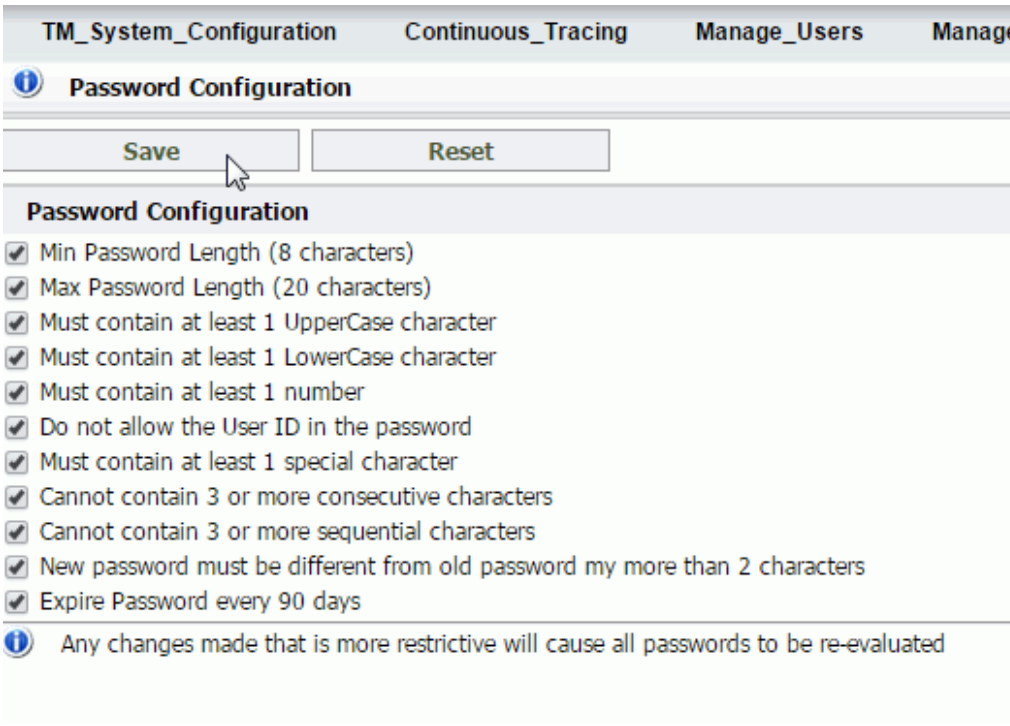
1) Login to Trace Manager Portal (FADE).

2) Navigate to **Administration** > **Manage Users**

3) Click on the "Password Profile" button



4) Disable a rule by removing the "Check Mark" in front



5) Click on the "Save" button.

These changes take effect immediately and will apply to any user who logs into the system after they are saved.

8.25 OSV-TM Database Optimization Schemes

To improve overall performance on an OSV-TM server integrated with devices that have medium or high call processing load, a database partitioning scheme is now available. Having smaller databases, each storing the processed traces from the individual devices integrated with OSV-TM, gives better performance and more efficient processing.

8.25.1 Types of OSV-TM Database Partitioning Schemes

Three partition schemes are available in OSV-TM:

- DB Partition 1

  This is the default configuration for upgraded and new systems. An OSV-TM system is configured with multiple databases to store the processed data per device: OSV, OpenScape SBC, Phones, OSB, SBC, OSUC, HMS, and Xpressions.

  This configuration is designed for integrated systems with low call processing loads.

  Data can be queried in FADE normally with no restriction on Filter starting and ending dates.

- DB Partition 2

  Daily database storage configuration. This scheme distributes processed trace data into daily databases. A database is created per device per day.

  NOTICE:

  This scheme is intended only for OSV-TM customers that run very high tracing loads and that experience performance issues with the DB Partition schemes 3. High call processing loads on devices averaging over 10 calls per second.

  Filtering data in FADE is restricted on a per day basis; it is not possible to query the system for multiple days on one filter.

  For example, if a user wants to query data for two consecutive days, he will have to run two different filters/queries -one for each day.

  Graphs in FADE will display data for a single day; it is not possible to display data for a multiple days on the same graph; the date filter for the Graph needs to be changed as needed.
- DB Partition 3 (default configuration for new systems)

  Weekly database storage configuration. This scheme distributes processed trace data in weekly databases. A database is created per device per week.

  Designed for medium call processing loads on devices averaging 10 calls per second or less.

  Filtering data in FADE is restricted on a per week basis; it is not possible to query the system for days across multiple weeks. Users will be required to change the filter to a "weekly" period: Sunday through Saturday. For example: if DIPAZ is configured with "Days in Rear" = 10, and the user wants to query the system for the whole 10 day period, he will have to run two separate queries, one for each week period.

  Graphs in FADE will display data only for a week; it is not possible to display data for days that cross the week boundaries, Sunday through Saturday, on the same graph; the date filter for the Graph needs to be changed as needed.

8.25.2 DB Partitioning Screen for New Systems

The default configuration when creating an OSV-TM V7 system is DB Partition 3.

The partition scheme can be changed from "Weekly" (3) and be set to "Daily" (2) or "None" (1) during the creation of new systems in FADE as described in the section: "Adding an OSV-TM system".

8.25.3 Database Partitioning Scheme for Existing Systems

The DB Partition of an existing OSV-TM system can be changed to a different configuration.Be aware of the following constraints when switching DB Partitions:

- It is recommended to change the DB Partition configuration for a system only if OSV-TM displays performance degradation when processing trace data and FADE delays.
- The OSV-TM Administrator must verify that there is enough hard disk space before initiating this procedure: at least 70% of the space used by the current databases.
- Changing the DB configuration of a system will restrict how processed data is filtered and graphed in FADE as it was described in the section above.
- All trace data files under the tracedata\<system>\<date> folders corresponding to the system will be reprocessed. This task will take time and data filtered in FADE will be displayed as the traces are parsed.

8.25.4 How to Change the DB Partition Scheme

Prerequisites

Adequate administrative permissions.

Step by Step

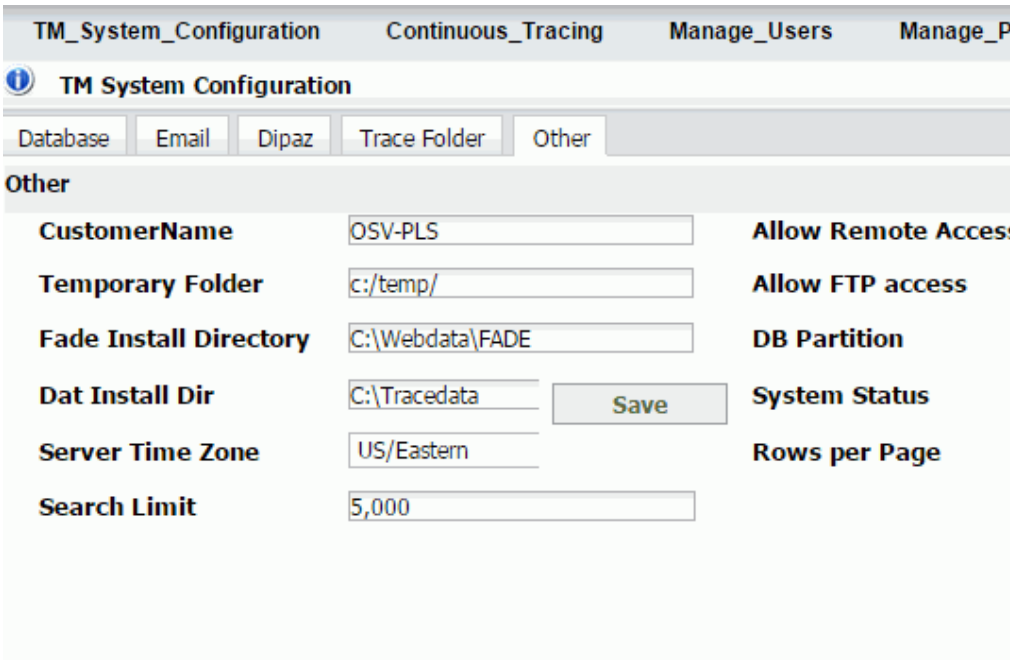
1) Login locally into the OSV-TM Windows server with an OSV-TM Windows administrative account.

2) Login with an Admin account into FADE: Click on the FADE icon located on the server's Desktop.

3) Select the system name that you want to convert. Ex.: sys1

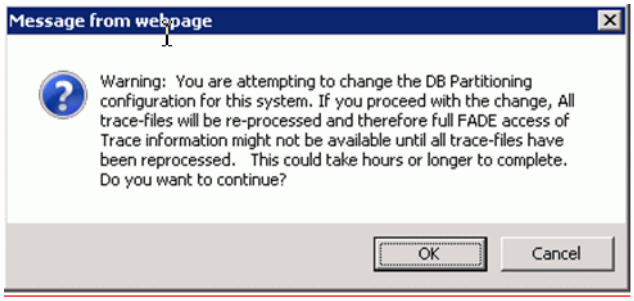
4) Navigate to the Administration view -> TM_System_Configuration -> Other tab.

5) Change the "DB Partition" field to the new scheme: None, Daily, Weekly.



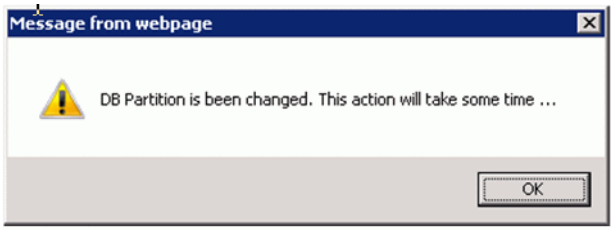
6) Click "Save"

A Warning will prompt you to confirm the change.



7) Click "OK"

A confirmation message will remind you of the delay caused by the conversion.



8) Click "OK"

All trace data files under the tracedata\<system>\<date> folders will be reprocessed for all devices.

8.26 Using a RAM Drive Storage for Performance Solutions

OSV-TM V7R0.7.x and above supports RAM drives as storage space for the OSV-TM databases. This configuration is only recommended for customers experiencing delays in processing their traces or OSV-TM performance problems.

Risk of Losing Data

RAM drives are volatile, therefore extreme caution need to be used using this configuration. There is a high risk for losing data if the OSV-TM server crashes or is not brought down gracefully. Trace files may need to be reprocessed to recover the data.

It is recommended that you stop the DIPAZ Monitor before any restart of the OSV-TM Server. Refer to the section, "Stopping or Re-starting OSV-TM Services".

DIPAZ is restarted nightly at 1:00AM. An OSV-TM internal process also backs up the daily databases from the RAM Drive to the OSV-TM installation physical drive.

If the RAM Drive gets 85% full an internal monitor process will age or delete the older databases from the OSV-TM system until the space is below the threshold.

OSV-TM System Limitations

OSV-TM systems stored in a RAM drive are constraint to the following configuration:

- Only one OSV-TM system can be hosted in the RAM drive storage
- The OSV-TM system only supports a "Daily" database partition configuration

RAM Drive Support Hardware and Software Requirements

RAM drive storage is only supported on servers with the following configuration:

- Windows Server 2019 - 64 bit Standard Edition /Windows 2016 /Windows 2012 R2 /Windows 2008 R2 x64
- Minimum 32GB of physical RAM
- Minimum 16GB free RAM

The OSV-TM installation package includes the "ImDisk" software required to setup a RAM Drive. This software should not be manually installed by the administrator.

The OSV-TM installation manager will create and configure the RAM Drive automatically if the hardware requirements are met.

The next available drive letter will be assigned to access the drive.

Enabling the Ram Drive Storage in OSV-TM

For new OSV-TM V7R0.7.x and above installations, the RAM Drive feature can be enabled during the OSV-TM setup.

On existing OSV-TM V7R0.7.x and above servers, the RAM Drive feature can be enabled via the OSV-TM Setup Utility. Once the RAM Drive is enabled, a new OSV-TM system can be configured to use the RAM Drive when the system is created via FADE, or an existing system can be converted or moved to the RAM Drive storage.

This feature is only available on new and existing installations if the above hardware requirements are met.

8.26.1 How to Enable RAM Drive on New OSV-TM Installations

RAM Drives support can be enabled during the fresh OSV-TM installation via the configuration window.

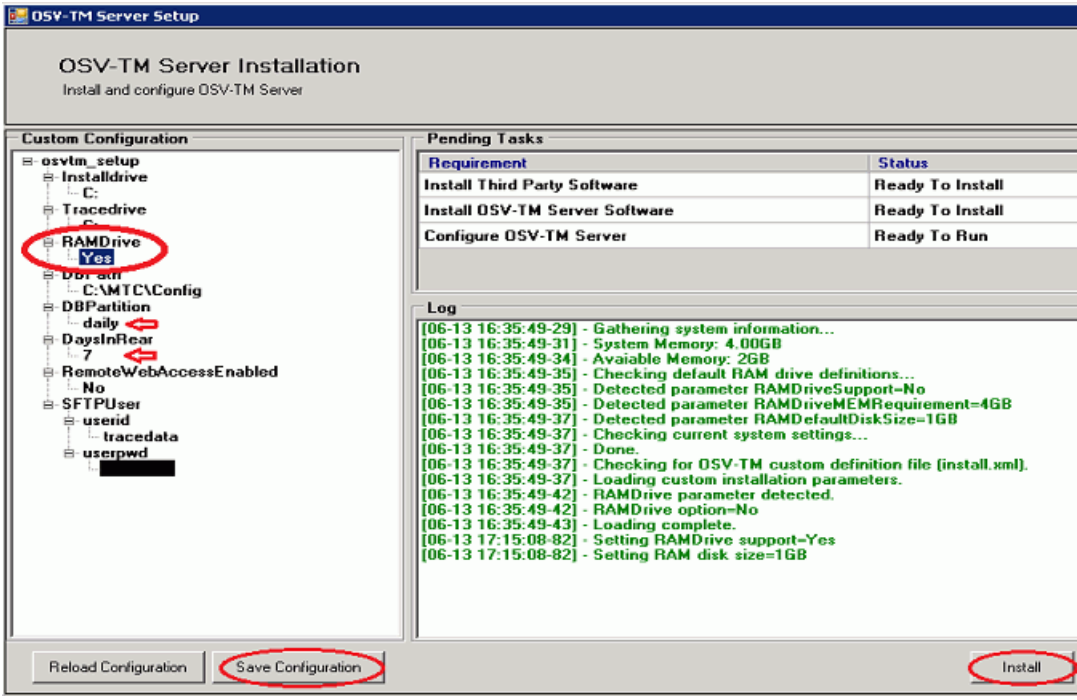
Follow the instructions in chapter How to install OSV-TM on Windows 2008 R2 or newer to start the fresh installation.

The installation process checks the server resources; if all the hardware requirements are met, the OSV-TM installation program allows you to setup the RAMDrive option.

Step by Step

1) Go to the "OSV-TM Server Installation Window."
2) Double-click on the "RAMDrive" option and change it to Yes. If this option is locked and cannot be changed from the "No" value, your server did not meet the requirements to support and enable a RAM Drive.

3) By default, the "DBPartition" option is changed to "daily" and the "DaysInRear" set to "7" days.
4) Click the "Save Configuration" button.
5) Click "Install" button to complete the installation.



OSV-TM installs with a RAM Drive configuration and available with a "Drive" letter, (i.e.: E:).

The instructions in the sections: "Migrate or Move an Existing OSV-TM System to a RAM Drive Configuration" or "Creating a New OSV-TM System on a RAM Drive" provide detailed information on using the RAM Drive configuration.

8.26.2 How to Enable RAM Drive Feature during an OSV-TM Upgrade

To be able to enable the RAM Drive feature when upgrading an OSV-TM server, the hardware requirements must be met before starting the upgrade process.

Follow the instructions from the "Upgrade Installation" section in this manual to start the upgrade process. The install process checks the server configuration; if all the conditions are met, the OSV-TM V7R0.7.x installation program allows you to setup the RAMDrive configuration.

Step by Step

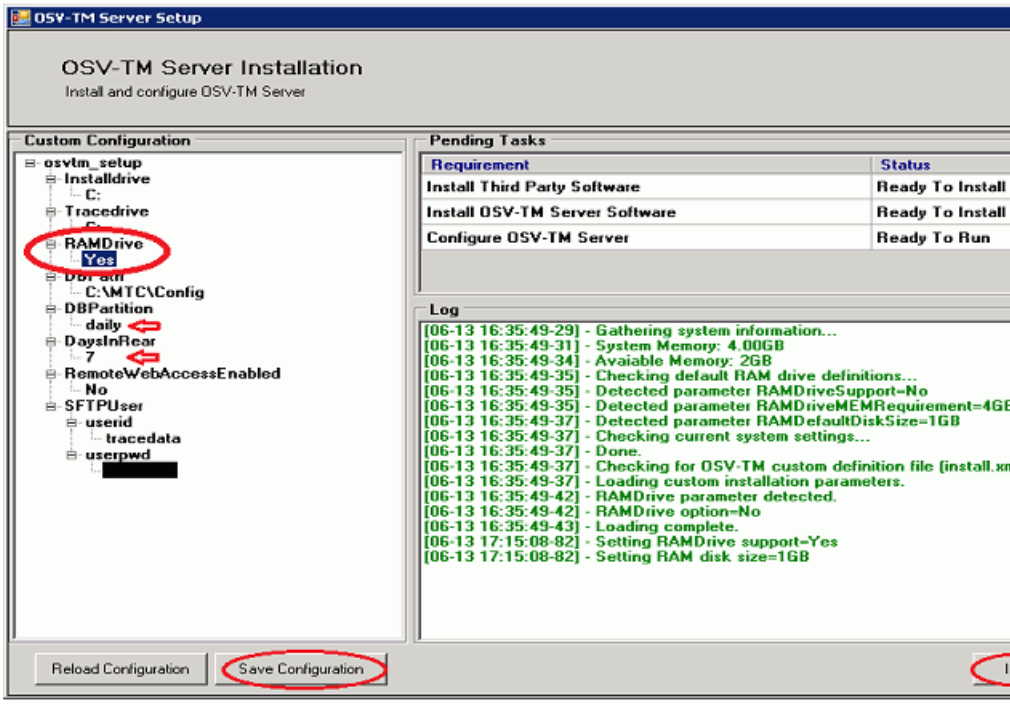
1) Go to the "OSV-TM Server Installation Window."
2) Double-click on the "RAMDrive" option and change it to Yes. If you are not allowed to edit this option, your server did not meet the requirements to configure a RAMDrive.

3) By default, the "DBPartition" option is set to "daily" and the "DaysInRear" set to "7" days.

   Note:These values apply to TM Systems that are created after this configuration is finished.

4) Click the "Save Configuration" button.

5) Click "Install" button to complete the upgrade.



OSV-TM is upgraded and a RAM Drive is configured and available in the server with a "Drive" letter, (i.e.: E:).

Please follow the instructions on the "Migrate or Move an Existing OSV-TM System to a RAM Drive Configuration" section to move an existing OSV-TM system to a RAM Drive, or follow the instructions for "Create a New OSV-TM System on a RAM Drive".

8.26.3 How to Enable the RAM Drive on an Existing OSV-TM Installation

OSV-TM servers running V7R0.7.x and above can enable RAM Drive support via the "Setup OSV-TM Server" utility.

Running the "Setup OSV-TM Server" Utility:

Step by Step

1) Login locally to the OSV-TM server with a Windows administrator account.
2) From the "Start" menu navigate to: All Programs -> OSV-TM
3) Right-Click on the "Setup OSV-TM Server" utility and select: "Run as Administrator"

   The "OSV-TM Server Installation" window opens.

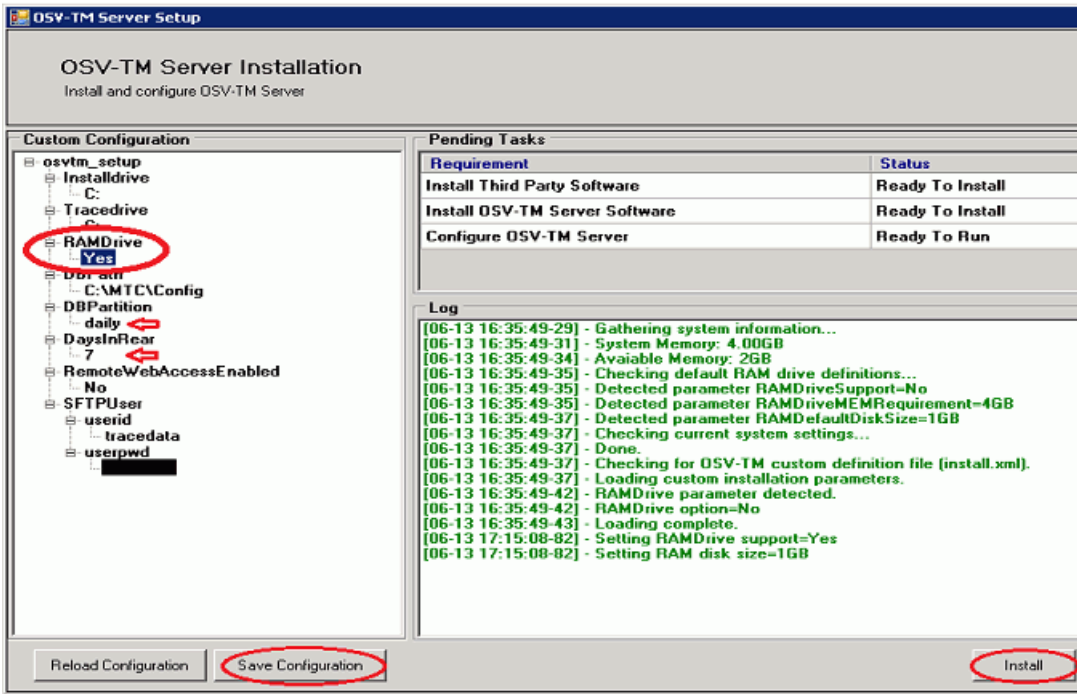
4) Double-click on the "RAMDrive" option and change it to Yes. If you are not allowed to edit this option, your server did not meet the requirements to configure a RAMDrive.

   By default, the "DBPartition" option is set to "daily" and the "DaysInRear" set to "7" days.

   Note: These values apply to TM Systems that are created after this configuration is finished.

5) Click the "Save Configuration" button.

6) Click the "Install" button to modify the exiting OSV-TM installation and enable the RAM Drive configuration.



7) Click "Finish" to exit the utility.

Follow the instructions on the "Migrate or Move an Existing OSV-TM System to a RAM Drive Configuration" section to move an existing OSV-TM system to a RAM Drive, or follow the instructions for "Create a New OSV-TM System on a RAM Drive".

8.26.4 How to Migrate or Move an Existing OSV-TM System to A RAM Drive

The RAM Drive feature needs to be enabled on the server to be able to host OSV-TM systems in a RAM Drive. Please refer to the previous sections for instructions.

If the system you want to move has a DB Partition configuration other than "Daily", you will not be able to migrate it to a RAM Drive. You need to change its DB Partition to "Daily" first. Follow the instructions on the "Change the DB Partition Scheme" section in this manual.

Login locally to the OSV-TM server and access the OSV-TM system you want to convert from the FADE Portal with the Admin account.

NOTICE:

Changing the configuration of an OSV-TM system to use the RAM Drive can only be done from a FADE session running locally on the OSV-TM server.

Step by Step

1) Go to the "Administration" view.
2) Click on the "TM System Configuration" link.
3) Navigate to the "Other" tab.
   The "DB Partition" parameter should indicate "Daily"
4) Click on the "Use Ram Drive" flag to move the current system to the RAM Drive.
5) Click the "Save" button.

IMPORTANT:

The migration process will take some time to complete. You will not be able to use the system while it is in migration mode!!

The current OSV-TM system is reconfigured to store its databases on the RAM Drive. Trace data files continue to be collected in the "Tracedata" folder on the physical disk

To move an existing OSV-TM system running on a RAM Drive off to the physical disk, uncheck the "Use RAM Drive" option. The current OSV-TM system is reconfigured to store its databases on the physical disk.

8.26.5 How to Create a New OSV-TM System on a RAM Drive

The RAM Drive feature needs to be enabled on the server to be able to create an OSV-TM system in a RAM Drive. Please refer to the previous sections for instructions.

Prerequisites

Follow the instructions from the section How to Add a System to create a new OSV-TM system.

NOTICE: Adding an OSV-TM System can only be done from a FADE session running locally on the OSV-TM server.

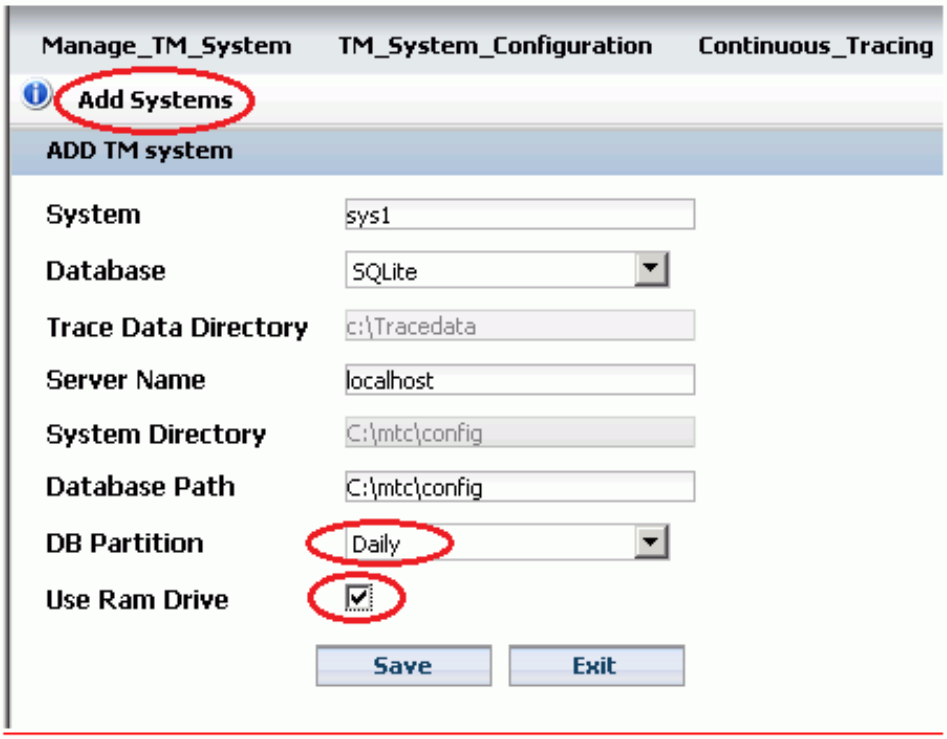
Step by Step

1) Go to the "Add System" configuration window in FADE.
2) Complete the system information.
3) Change the "DB Partition" option to "Daily".

4) Click on the "Use Ram Drive" flag to set the configuration to use the RAM Drive.

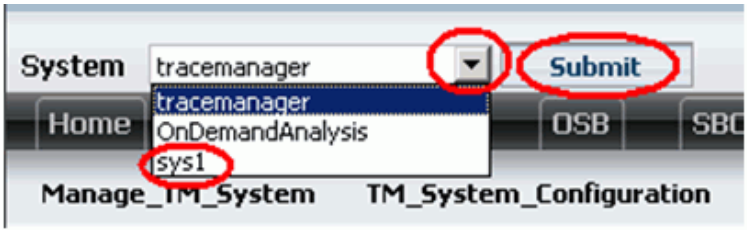
   If the RAM Drive functionality has not been enabled on the server, FADE will display a warning message.

5) Click the "Save" button.



The OSV-TM system is created and its databases stored in the RAM Drive.

You should see the new OSV-TM system listed in the "System" field in the FADE portal (i.e.: sys1), Select it and click the "Submit" button to access it in FADE.



IMPORTANT:

Configuring a RAM Drive only affects the databases where systems data is stored. Trace files continue to be collected in the "Tracedata" folder on the physical disk.

8.26.6 How to Increase the Size of the RAM Drive

The default OSV-TM RAM Drive configuration is set for 16GB of memory space set aside for the RAM drive. Once the RAM Drive is created, it cannot be extended in size. If the 16GB drive size is not enough, the drive has to be removed and created again.

Before performing this operation, any OSV-TM system running on a RAM Drive needs to be moved off to the physical disk first. Follow the instructions on the section above: "Migrate or Move an Existing OSV-TM System to a RAM Drive Configuration", and uncheck the "Use RAM Drive" option.

Change the OSV-TM configuration file to increase the default RAM Disk size variable:

Step by Step

1) On the OSV-TM server, open Windows Explorer and navigate to the folder where OSV-TM was installed. i.e.: <OSV-TM install drive>:\MTC\Config

2) Launch Notepad as Administrator:

- Start > Programs >Accessories

  Right click on Notepad and select "Run as administrator"

3) Edit the "OSV-TM.ini" file with Notepad.

4) Change the value of the "RAMDiskSize" value to the preferred size.

Important Note:

This must be an integer value, in Gigabytes, less than the "available" physical memory. If the value entered is incorrect the system will default the size to 16 (GB).

5) Do not modify any of the other variables in this file. The "RAMDriveSupport" variable should be already set to "True".

6) Save the changes and close the file.

Important Note:

It is recommended that you stop the DIPAZ Monitor before any restart of the OSV-TM Server. Refer to the section, "Stopping or Re-starting OSV-TM Services".

7) Restart the OSV-TM server.

Upon start up, the OSV-TM services will recreate RAM drive with the new size.

To move the OSV-TM system to the new RAM Drive, follow the instructions on the section above: "Migrate or Move an Existing OSV-TM System to a RAM Drive Configuration".

8.26.7 Troubleshooting RAM Drive Issues

Problem:

Solution:

No recent trace data is displayed in FADE on a system that uses the RAM Drive feature. The TM Explorer shows the latest trace data files as "Pending".

If no traces are being processed, this could be a sign that the RAM Drive is full. Check the RAM Drive capacity, if it is full, you can move the system from the RAM Drive to the OSV-TM physical drive storage.

Follow the instructions under the "Migrate or Move an Existing OSV-TM System to a RAM Drive Configuration" section and uncheck the "Use Ram Drive" flag to move the system to the physical drive.

Problem:

Solution:

The OSV-TM was abruptly shutdown due to a power failure or without stopping the DIPAZ Monitor, and the system on the RAM Drive does not display data for today.

When the OSV-TM server is not shutdown in a graceful mode, the RAM Drive is automatically destroyed from memory and the data in it is lost. When the server is restarted, the OSV-TM internal processes will recreate the RAM Drive for the system that was configured on it and will reprocess the trace data files for "today".

DIPAZ is restarted nightly at 1:00AM. An OSV-TM internal process also backs up the daily databases from the RAM Drive to the OSV-TM installation physical drive.

8.27 OSV-TM Performance Guidelines

Following the aforementioned suggestions, please note that delays in trace and log parsing may be experienced in case of heavy traffic. Apart for the actual traffic, the log level may impact the performance as well.

Currently the only official improvement of the OSVTM performance is the use of the RAM Drive feature.

Increasing the Host OS number of CPUs beyond the suggested configurations specs (7.2 Hardware Requirements) does not seem to provide any improvements.

Increase of the total RAM size of the host OS, RAM Drive disk size as well as the free RAM used by the Windows OS, has improved the performance limits, by delaying the system congestion.

Currently, for Performance Profiles that exceed the scenarios as described in chapter Hardware Requirements (extremely heavy traffic scenarios) it is strongly advised to set up and use multiple OSVTM servers per component (OSV, OSB, SBC, OSUC, XPR, etc.).

IMPORTANT:

Delays in trace and log parsing may still be experienced.

In the OSVTM portal, under TM_Explorer -> Overview, the user can be informed regarding any files that are in “Pending” analysis status.

Please refer to Overview for more details.

8.28 OSV-TM Automated Maintenance Processes and Backup

Automated Maintenance Processes

For stability and data storage management of the OSV-TM server, four automated maintenance processes have been configured by default in the OSV-TM application: Trace data files deletion, processed trace data cleanup from the database, and database defragmentation and restarting DIZAP.

- The trace data file deletion process runs every hour on the hour based on the Days in Rear* configuration of DIPAZ. It deletes the files that have already been processed and stored in the tracedata\<system-name>\<date> directories.
- The OSV-TM aging process cleans up processed trace data from the database based on the DIPAZ Clean_Days_in_Rear* aging configuration.

  This procedure runs nightly at 2 AM, except on Sundays when it runs after the vacuuming process.
- The vacuuming maintenance procedure defragments the database caused by aging. This process runs weekly on Sundays at 2 AM and 3 AM.

  This process does not run on systems configured with Daily or Weekly DB Partition schemes.
- DIPAZ is restarted nightly at 1:00AM.

NOTICE:

* See the "How to Set DIPAZ Configuration" section for detailed information on this parameter.

NOTICE:

No traces are processed during the aging and vacuuming maintenance period.

If OSV-TM functionality issues arise from these cleaning processes, the OSV-TM administrator should report them to your service provider.

Automated Backup Process

The automated backup process is run by the Monitor and makes copies of all OSV-TM configuration files to be able to restore all systems to a previous configuration point.

Backup storage directory: <system-drive>:\TM\backup (system-drive is same drive where tracedata folder is located)

Backup schedule: runs every night at mid-night

Archival holding period: daily backups are kept for seven (7) days and a sequence of four (4) Saturday’s backups

NOTICE:

It is recommended to also backup the archived files stored in the Backup storage directory with your corporate backup software for longer archival periods.

8.29 Monitoring OSV-TM Status and Processes Logs

OSV-TM collects different types of logs that can be used by the administrator to determine the current the condition of the server and its processes or to find out about the root cause of a problem.

RapidStat Logs

The RapidStat logs collect OSV-TM server status statistics for a period of 24 hours.

The following RapidStat logs are available for analysis:

- RapidStat_DBSize: number of database records for each system being monitored by the OSV-TM server
- RapidStat_System_Configuration: current configuration for each OSV-TM system being monitored
- RapidStat_Memory_Usage: memory usage statistics on the OSV-TM server
- RapidStat_Dipaz_Status: current status of the DIPAZ process

Other Logs

Events related to the OSV-TM processes are recorded in their corresponding logs: Dipaz, Monitor, Fade, Phone, FTP, SFTP_Server, Schemas, and Configuration. Each of these logs captures the transactions handled by each process and the time at which the event occurred.

All logs are aged according to the OSV-TM aging scheme based on the "Days in Rear (Files)" flag found in the Dipaz tab under the Administration view > TM System Configuration. The default value is 10 days.

8.29.1 How to Access OSV-TM Administraton Logs

Users with OSV-TM "Admin" or "Advanced" access level can access the OSV-TM logs remotely using the FADE.

Prerequisites

Adequate administrative permissions.

Step by Step

1) Login to **FADE**

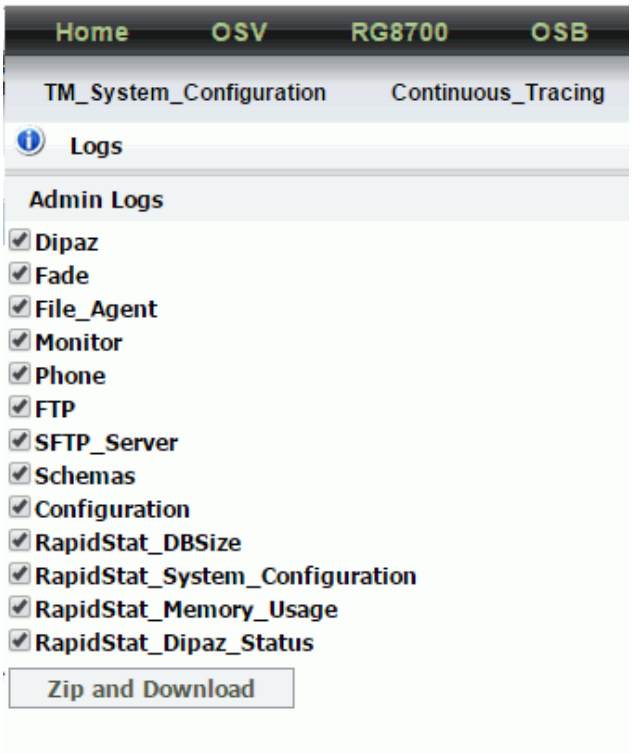
2) Go to the Administration view.

3) Click on the **TM_Logs** tab.

4) Click on any log to save it to your local client machine or to open the log.

5) To download all the logs at once, check mark all logs, then click on **Zip and Download**.

   These logs are also accessible locally on the server by the Administrator.



   Archived RapidStat logs are stored on the system-drive where OSV-TM is installed: <sys-drive>:\MTC\Rapidstat and can be accessed locally on the OSV-TM server by the administrator.

8.30 Configuring OSV-TM through configuration file

Every system contains a config.ini file with system wide configuration variables. Do not modify this file unless absolutely necessary. Change only the variables in this file, described in the following subsection.

8.30.1 How to Store SIP Notify Messages

"SIP notify" messages are by default disabled within the config.ini file on every system in order to ensure reduced performance issues. By default, you cannot view the "SIP Notify" messages through FADE, while the correlated CallID's are available. As a result, you cannot download the associated trace files through FADE. When you must enable the "SIP notify" messages, then follow the steps below.

Prerequisites

Adequate administrative permissions.

Step by Step

1) Navigate to: **Start** > **Control Panel** > **Administrative Tools** > **Services**

2) Locate the Dipaz Monitor
3) Right - click and select **Stop**
4) Find the config.ini file within the `C:\MTC\Config\<System Name>` directory
5) Edit the config.ini file and change the value of "SubNotifytoDB" from "False" to "True"
6) Navigate to: **Start** > **Control Panel** > **Administrative Tools** > **Services**
7) Locate the Dipaz Monitor
8) Right - click and select **Start**

IMPORTANT:

By enabling the "SIP Notify" messages, performance issues will occur due to the high load of the "SIP Notify" messages stored within the database

---

9 Reconfiguration Procedure after Restoring An OSV-TM Server from Windows Backup

When restoring an OSV-TM server from a previous image or with Windows Server Backup and Restore service, it is necessary to reset the permissions in the OSV-configuration files.

When the permissions are not reset, SSH connection errors are reported. i.e.:

06-03-2013 18:46:55 IP 172.25.5.10 SSH connection attempt.

06-03-2013 18:46:55 IP 172.25.5.10 SSH tracedata submitted a bad key.

Running the OSV-TM Configuration Utility

If you are running an OSV-TM V7R0.6.0 and above you can run the "Setup OSV-TM Server" utility from the Windows Start menu:

1) Login to the OSV-TM server with an account having Windows Administrator rights.
2) From the Windows Start menu, select "All Programs" > "OSV-TM"
3) Right click on "Setup OSV-TM Server" and select " Run as administrator"
4) Click the "Install" button. The utility will reconfigure all processes.
5) Click "Finish" when completed.

If you are running an OSV-TM version earlier than V7R0.6.0, run the utility manually:

1) Login to the OSV-TM server with an account having Windows Administrator rights.
2) Right Click on the fle "Configure_TM.bat" and select "Run as administrator"
3) The "Trace Management Server Configuration" window opens and displays the process messages
4) When the reconfiguration is completed, the window closes.

The reconfiguration process may take some time to run. After it completes, all services are restarted.Verify that the systems integrating with OSV-TM are sending their trace data files. The traces should start processing shortly after they are received in the "Tracedata" folder.

10 How to Report Problems/Bugs

Step by Step

Problems with the OpenScape Voice Trace Manager should be reported to your Unify service provider via the appropriate customer portal or GSI.Flow.

Index

A

About this guide 10
Audience 10

M

Migration to V1R3 115

T

Trace:filter 63

U

Upgrade 138

© 2024 Mitel Networks Corporation. All Rights Reserved. Mitel and the Mitel logo are trademark(s) of Mitel Networks Corporation. Unify and associated marks are trademarks of Unify Software and Solutions GmbH & Co. KG. All other trademarks herein are the property of their respective owners.