A MITEL
PRODUCT
GUIDE

Unify OpenScape Voice Trace Manager V8

Security Checklist

Security Checklist

07/2024

A31003-H8080-P103-05-76A9

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.

Contents

Contents

1 Introduction

1.1 General Remarks

Information and communication and their seamless integration in Unified Communications and Collaboration (UCC) are important and valuable assets for an enterprise and are the core parts of their business processes. Therefore, they have to be adequately protected. Every enterprise may require a specific level of protection, which depends on individual requirements for availability, confidentiality, integrity and compliance of the IT and communication systems being used.

Unify attempts to provide a common standard of features and settings of security parameters within the delivered products. Beyond this, we generally recommend:

- to adapt these default settings to the needs of the individual customer and the specific characteristic of the solution to be deployed.
- to weigh the costs (of implementing security measures) against the risks (of omitting a security measure) and to “harden” the systems accordingly.

As a basis for that, the Security Checklists are published. They support the customer and the service both directly and indirectly, as well as those wanting to maintain it themselves, to agree on the settings and to document the decisions that are made.

The Security Checklists can be used for two purposes:

1. In the planning and design phase of a particular customer project. Use the Security Checklists of every relevant product to evaluate if all of the products that form a part of the solution can be aligned with the customer’s security requirements. Document in the Checklist how they can be aligned. This ensures that security measures are appropriately considered and included in the Statement of Work to build the basis for the agreement between Unify and the customer. The customer will be responsible for the individual security measures:
   - during installation and setup of the solution
   - during operation
2. During installation and during major enhancements or software upgrade activities. The Security Checklists (ideally documented as described in the previous step) are used to apply and/or control the security settings of every individual product.

1.1.1 Update and Feedback

By their nature, security-relevant topics are prone to continuous changes and updates. New findings, corrections and enhancements of this checklist are being included as soon as possible. Therefore, we recommend always using the latest version of the Security Checklists of the products that are part of your solution. They can be retrieved from the partner portal at the relevant product information site.

We encourage you to provide feedback on anything that is not clear or about problems with the application of this checklist.

Please contact the OpenScale Baseline Security Office (obso@unify.com).

1.2 Customer Deployment - Overview

This Security Checklist covers the product OpenScape Voice V7 Trace Manager and lists the security relevant topics and settings in a comprehensive form.

	Customer	Supplier
Company		
Name		
Address		
Telephone		
E-mail		
Covered Systems (e.g. System, SW version, devices, MAC/IP-addresses)		
Referenced Master Security Checklist	Version:	
	Date:	
General Remarks		
Open issues to be resolved until		
Date		

1.3 Security Models for OSV-TM Environments

The security model to be adopted for OSV-TM will depend on the environment where the server resides:

- Safe Environment Security Model: The OSV-TM server, the OpenScape devices, and the OSV-TM users all reside on a Network that is secured by your company standards
- Strict Security Model: The OSV-TM server resides on a network that is not secured or your company policy requires a strict access control to the server and data.

1.3.1 Configuring OSV-TM for a Safe Environment Security Model

The OSV-TM server resides on a Network that is secured by your company standards, the OpenScape devices that send the traces to the server are on the same network, and OSV-TM users access the Portal on the same secured network.

On this model, the standard OSV-TM functionality is safe to be run with no additional restrictions.

The General Security Configurations outlined in Sect. 4.1 through Sect. 4.6 in Chapter 4, “Hardening” must be applied.

1.3.2 Configuring OSV-TM for a Strict Security Model

The OSV-TM server resides on a network that is not secure or your company policy requires a strict access control to the server.

This environment requires Windows configuration changes and to completely disable remote access to the OSV-TM Web Portal.

After the changes outlined in this section are made, FADE, the OSV-TM Web Portal, is accessible only locally from within the OSV-TM server console; the FTP functionality in FADE to export trace files for further analysis is disabled -trace files can be gathered with the "Zip and Download" feature and saved to a DVD or a USB drive; and tracing transfers from Phones and RG8700 via UDP ports are disabled.

The General Security Configurations outlined in Sect. 4.7 though Sect. 4.12 in Chapter 4, “Hardening” must be applied.

2 OSV-TM Interfaces

2.1 OpenScape Voice (OSV) Trace Manager (TM) Overview

The OpenScape Voice Trace Manager (OSV-TM) is an application that allows for the collection of OpenScape Voice trace data (OSV), RG8700, Phone Quality of Service (QoS), OpenScape Branch (OSB), Session Border Control (SBC), OpenScape Unified Communications (OSUC), and HiPath Media Server (HMS), and Xpressions (XPR) data that can be used for analysis and troubleshooting of communication 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.

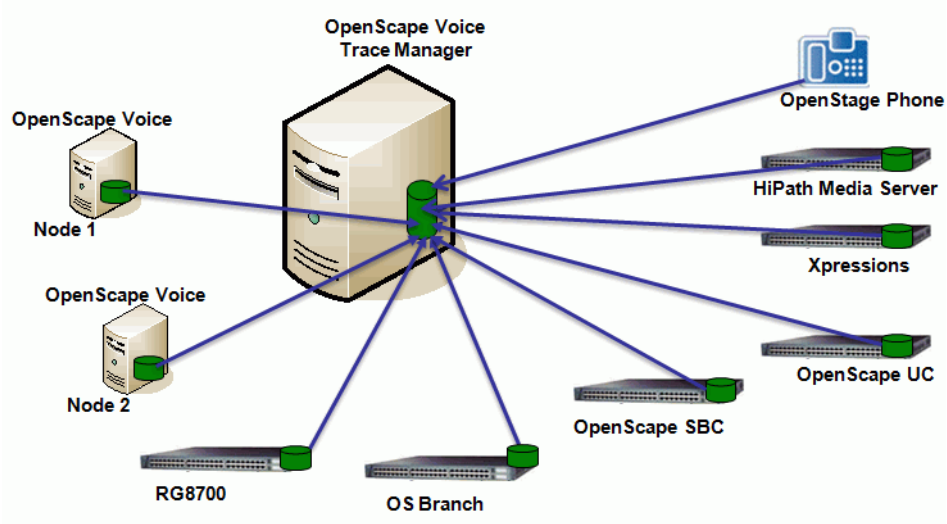
Presumably, the OSV-TM server and integrated OSC devices are hosted on a secured network based on the safety measures of your company. If there is a concern about the accessibility of the data in the trace files and the processed data by OSV-TM then a Strict Security OSV-TM configuration model is presented in this document.

NOTE: This Security Checklist document only addresses hardening the OSV-TM server. Hardening the of components that connect to the OSV-TM server are outside of the scope of this document.

2.2 OSV-TM Operating Architecture

The figure below reflects the component interfaces for OSV-TM.

NOTE: This Security Checklist document only addresses hardening the OSV-TM server.



The tracing and data files collection sequence is as follows.

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

The RG8700 Gateway is configured for continuous tracing and it streams data to the RG8700 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.

2.3 Hardening Restrictions

These security guidelines apply only to OSV-TM installations running on Windows 2008 R2 Standard, 64-bit.

The general security configuration can be applied to Windows 2003, but specific instructions are not given for this operating system.

Secure FTP is only supported for environments running OpenScape Voice server V4.1 and above and OSV-TM V2R0.4.2 and above.

3 OSV-TM Hardening Measures at a Glance

To tighten security on the OSV-TM, the following measures are recommended:

- Windows 2008 Hardening
- Windows Administrator Accounts
  - Create one access group for Windows Administrator and OSV-TM processes (FADE, DIPAZ, RG-listener, phone-listener) with the following access rights:
    - Read/write/execute
    - Logs
    - SQLite
    - Config files (including password file)
    - Trace files
  - Create a second access group [i.e., a Local User Account(s)] for SFTP user (trace data):
    - Trace files
- OSVTM default password
- Define packet filter rules that only allow incoming FTP traffic from specified sources
- Create different trace file export user names and passwords for different devices
- Block all ports not used by OSV-TM

3.1 Windows OS Updates

Windows Server OS specific security updates are the responsibility of the administration team in charge of the OSV-TM server. The Microsoft security updates must be applied as recommended by the vendor.

3.2 Windows Configuration Requirements

3.2.1 Windows Administrator Account

By default when Windows 2008 R2 is installed, the "Administrator" local account is created on the server. This account provides the rights required to administer the server's OS and all its applications.

During the installation process a password needs to be typed for this account. The password settings should follow the strictest procedures to protect its confidentiality.

3.2.2 OSV-TM Administrator Windows Account

In order for the OSV-TM administrator to install the software on the server, he requires a Windows local login account with administration rights to the server.

If an Active Directory domain account is used, this account also requires the local administration rights to the server.

This account will be used to install OSV-TM and its processes and require the following access rights:

- Read/write/execute permissions to:
  - Install software: store files on the local disks, modify the server's registry, and modify firewall settings
  - Read/write to logs
  - SQLite databases administration
  - Read/write to configuration files (including OSV-TM user accounts and password management file)
  - Trace Files from the devices integrated with OSV-TM

3.2.3 OSV-TM local User account(s)

A Windows local user account is required for the FTP/SFTP transfer process. A single account can be configured and shared by all devices to transfer data; for a higher security policy, multiple accounts can be configured for SFTP, one for each device integrating with OSV-TM.

These accounts should only be used as the ftp/sftp login accounts to transfer the files to the OSV-TM server and should have exclusively regular local user rights.

The passwords for these accounts should be secured and only distributed to the administrators of the other OpenScape devices that will integrate with the OSV-TM server for tracing management. These devices could include: OpenScape Voice, RG8700, Telephones, OpenScape Branch, OpenScape Session Border Controller, Xpressions, HiPath Media Server, and OpenScape UC.

These accounts have access to these devices trace files only via the FTP/SFTP service.

The recommended name for a single shared account is "tracedata".

4 Hardening

The security parameters identified in the following sections should be configured for all OSV-TM server installations.

4.1 3rd Party Applications and Windows OS Updates

OSV-TM incorporates 3rd party applications in its structure. OSV-TM users are responsible for downloading and installing on their client machine the security updates or latest versions of these 3rd party applications from their respective vendors. See the Administration Tasks section in the *OpenScape Voice V8 Trace Manager, Service Documentation*, for detailed information.

Customers that have installed any earlier version of an OSV-TM server must either uninstall older components or upgrade them to the latest version for security compliance.

Security updates for OpenScape Voice Trace Manager software components are made available only with new OSV-TM releases via re-installation or via hot fixes if required.

3rd party applications required to be manually installed on the OSV-TM server should be upgraded only to the recommended version listed on the OSV-TM Release Note.

Windows Server OS specific security updates are the responsibility of the administration team in charge of the OSV-TM server. The Microsoft security updates must be applied as recommended by the vendor.

CL-OSV-TM_3rd_Party	**Verify 3rd Party Security Updates**
Measures	Verify that all security updates and latest versions of all 3rd Party Applications have been installed.
References	Refer to the 3rd party Application's vendor website.
Needed Access Rights	n/a
Executed	Yes  No: 
Customer Comments and Reasons	

4.1.1 Use of antivirus

The use of antivirus software on the server that hosts OSVTM is allowed with the following exceptions:

1. There is no list of compatible antivirus software. The server administrator must ensure that the installed antivirus will not interfere with the OSVTM software by issuing false positive alerts for the Trace manager components.
2. Due to intensive disk IO from Antivirus and OSVTM, performance issues can occur. In this case, it is recommended to disable the antivirus real time protection. Manual scans during off-peak hours can take place instead.

Exclude the following folders:

- ${Installation Drive}\MTC
- ${Installation Drive}\OSV-TM
- ${Installation Drive}\Program Files\OSVTM
- ${Installation Drive}\Program Files (x86)\OSVTM
- ${Installation Drive}\Webdata

Also, exclude the Root Path of the SFTP. The default path is the following:

- ${Installation Drive}\Tracedata

NOTE: When you use a different root path, for the SFTP, than the default, then you must exclude it from the antivirus.

When you enable the RAM Drive disk feature of the OSV-TM, you must exclude the created RAM Drive from the antivirus too.

4.2 Windows Administrator Account

By default when Windows 2008 R2 is installed, the "Administrator" local account is created on the server. This account provides the rights required to administer the server's OS and all its applications.

During the installation process a password needs to be typed for this account. The password settings should follow the strictest procedures to protect its confidentiality.

The "Administrator" password should be reset if the default one was used during installation.

CL-OSV-TM_Windows_Admin	**Change Default PW for Windows Admin**
Measures	Change the Windows Administrator password from the default password to a password that follows the requirements outlined in the OpenScape Voice V7 Trace Manager Service Documentation, Administration Tasks Section.
References	OpenScape Voice V7 Trace Manager Service Documentation, Administration Tasks Section
Needed Access Rights	n/a
Executed	Yes  No: 
Customer Comments and Reasons	

4.3 OSV-TM Local Administrator Account

In order for the OSV-TM administrator to install the software on the server, the administrator requires a Windows local login account with administration rights to the server.

If an Active Directory domain account is used, this account also requires the local administration rights to the server.

This account is used to install OSV-TM and its processes and it requires the following access rights:

- Read/write/execute permissions to:
  - Install software: store files on the local disks, modify the server's registry, and modify firewall settings
  - Read/write to logs
  - SQLite databases administration
  - Read/write to configuration files (including OSV-TM user accounts and password management file)
  - Trace Files from the devices integrated with OSV-TM

CL-OSV-TM_Windows_Admin_Permissions	**Create Windows Local Login Account for OSV-TM Administrator**
Measures	Create a Windows Local Login Account for the OSV-TM Administrator with the following read/write/execute permissions: – Install software: store files on the local disks, modify the server's registry, and modify firewall settings – Read/write to logs – SQLite databases administration – Read/write to configuration files (including OSV-TM user accounts and password management file) Trace Files from the devices integrated with OSV-TM.
References	OpenScape Voice V7 Trace Manager Service Documentation, Administration Tasks Section
Needed Access Rights	n/a
Executed	Yes  No: 
Customer Comments and Reasons	

4.4 OSV-TM Local User Account(s)

A Windows local user account is required for the FTP/SFTP transfer process. A single account can be configured and shared by all devices to transfer data; for a higher security policy, multiple accounts can be configured for SFTP, one for each device integrating with OSV-TM.

These accounts should only be used as the ftp/sftp login accounts to transfer the files to the OSV-TM server and should have exclusively *regular local user rights*.

The passwords for these accounts should be secured and only distributed to the administrators of the other OpenScape devices that will integrate with the OSV-TM server for tracing management. These devices could include: OpenScape Voice, RG8700, Telephones, OpenScape Branch, OpenScape Session Border Controller, Xpressions, HiPath Media Server, and OpenScape UC.

These accounts have access to these devices trace files only via the FTP/SFTP service.

The recommended name for a single shared account is "tracedata".

CL-OSV-TM_Local_Accounts	**Create Windows Local Uers Account**
Measures	Create the FTP/SFTP local accounts: 3.
References	OpenScape Voice V7 Trace Manager Service Documentation, Administration Tasks Section
Needed Access Rights	n/a
Executed	Yes  No: 
Customer Comments and Reasons	

4.4.1 How to Create Windows Local Users Account

1. Login to the Windows OSV-TM server as Administrator
2. From the Control Panel, open “Administrative Tools”
3. From the menu, Select “Computer Management”
4. Expand “Local Users and Groups“
5. Click on the "Users" folder
6. From the “Action” menu select “New User”
7. On the field “New User” write it down for the FTP/SFTP setup during OSV-TM installation.
8. Uncheck the option “User must change password at next logon”.
9. Check the option “Password never expires”
10. Click “Create” button then “Close”

4.5 Secured HTTPS Configuration for 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 SLL to connect to the OSV-TM server.

Port 28081 is the secured port configured for HTTPS in the OSV-TM server. The unsecured HTTP port 28080 is also automatically configured to redirect the traffic through the 28081 port.

A default digital certificate is included in the OSV-TM server installation with 10 year expiration; however, it is recommended that a personalized certificate for the server is generated by the OSV-TM administrator.

CL-OSV-TM_Personalized_DC	**Personalized Digital Certificate for the OSV-TM Server**
Measures	Generate a Personalized Digital Certificate for the OSV-TM Server
References	Section 4.5.1, “Install the Self-Signed Certificate”
Needed Access Rights	n/a
Executed	Yes  No: 
Customer Comments and Reasons	

4.5.1 Install the Self-Signed Certificate

NOTE: If you wish to create your own certificate then follow this link to Section 4.5.1.1, “How to Generate a Self-Signed Certificate for the OSV-TM Server”, on page 23.

Sect. 4.5.1.1, contains a link back to this location.

NOTE: If you have generated a certificate and key using your own PKI:

- rename your certificate and key to **server.crt** and **server.key** (without a passpharase on the key) and

-then simply copy it the same location.

Then continue at step 2 below (i.e., restart Apache as per instructions.).

1. Copy the files "server.crt" and "server.key" into the Apache web server "conf" folder:

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

2. 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**"

3. Test the certificate:
   - Connect to FADE web client:

     https://<server-name>:28081/FADE/public/index.php/login

     You should be warned to accept the certificate.
   - Accept the certificate.

You should be logged in to port 28081.

4.5.1.1 How to Generate a Self-Signed Certificate for the OSV-TM Server

The default OpenSSL configuration enforces the generation of 1024 bit keys.

1. For greater security, increase this default value in the openssl.cnf file to 2048 bit:

   Open the openssl.cnf file with Notepad:

   ```
   <system-drive>:\programfiles (x86)\Apache Software
   Foundation\Apache2.2\conf\openssl.cnf
   ```

   Change the value of the " default_bits" to 2048:

   ```
   default_bits = 2048
   ```

2. .All the following procedures need to be run from the command line interface using the Windows Command Prompt (CMD) shell.

   Open the CMD shell:

   From the "**Start**" menu click on "**Run**"

   On the Open field type: **cmd**

3. On the CMD shell type:

   ```
   cd %programfiles (x86)%\Apache Software
   Foundation\Apache2.2\bin
   ```

4. Press "**Enter**"

5. Type the following command:

   ```
   openssl req -config ../conf/openssl.cnf -new -out server.csr
   -keyout server.pem
   ```

6. Press the "**Enter**"

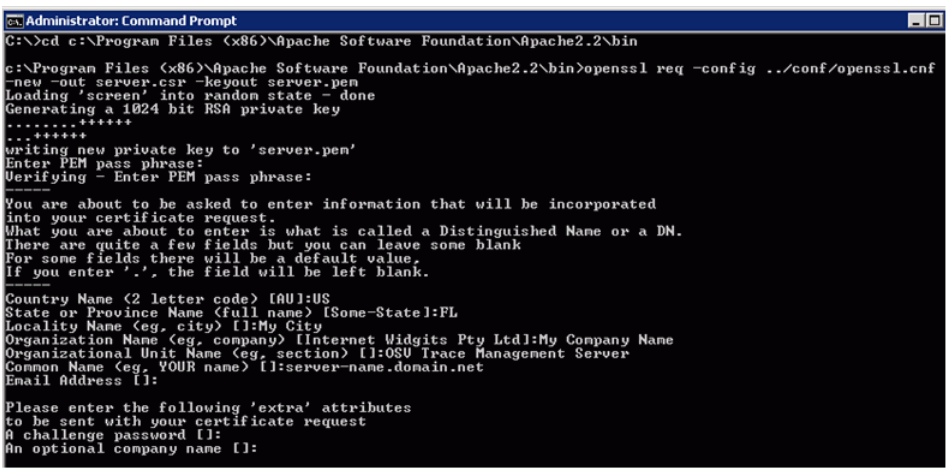
7. At the "*Enter PEM pass phrase:*" prompt, type a password to secure the access to the digital key.

NOTE: Write down the password phrase since it will be required for administering the SSL certificates.

You need to 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>
- 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 if your company enforces it.



NOTE: This step generates a digital key for this server. You can use this same key to submit a certificate signing request (CSR) to apply for a signed certificate by a Certificate Authority (CA). Once you get the certificate (server.crt) from the CA, you can use this certificate and proceed to the last step in this section.

This step removes the password that was created for the key in the previous step. This is necessary for Apache to be able to automatically start in SSL mode. You should store the private key in a secure folder that is accessible only by the Administrator, SYSTEM, and user accounts that run the Apache service.

If your security policy enforces the use of a password, you will need to start Apache manually from the command line and enter the password when prompted.

8. Type the following command:

   openssl rsa -in server.pem -out server.key

9. Press the "**Enter**"

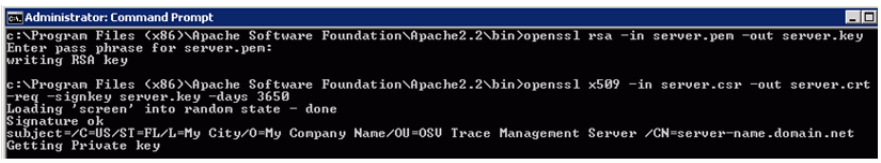
10. At the "**Enter pass phrase for server.pem:**" prompt, type the password you set in the step above.

11. Type the following command to create your self-signed certificate:

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

12. Press the "**Enter**"

NOTE: 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.



The steps above generated a valid certificate.

NOTE: Follow this link to return to Section 4.5.1, “Install the Self-Signed Certificate”, on page 22.

4.6 Password Hardening for the OSV-TM Admin Account

The OSV-TM installation creates a default OSV-TM user account with administration rights and password which grants access to the Trace Management Portal (FADE); A password change will be enforced when logging into FADE with this Admin account.

CL-OSV-TM_TM_Admin_Acct	OSV-TM Admin Account Password Hardening
Measures	Change the default Password for the OSV-TM System Administrator Account
References	Section 4.6.1, “How to Change the Default Password for the OSV-TM System Administrator Account”
Needed Access Rights	n/a
Executed	Yes  No: 
Customer Comments and Reasons	

4.6.1 How to Change the Default Password for the OSV-TM System Administrator Account

1. Login locally into the Windows OSV-TM server.
2. From the server’s Desktop:
   Click on the “**FADE**” icon. This opens the Trace Management Portal (FADE) web interface.
3. Login to the FADE Portal with the OSV-TM administration account:
   User Name: **Admin** (case sensitive)
   Default password: **Admin** (case sensitive)

   You will be prompted to change the “Admin” account password.

   NOTE: 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 (!@#$%^&*()
4. Enter New Password, Re-type the password, and **Save** the changes.

4.7 Close Communication Ports

OSV-TM uses the following communication ports and automatically opens them during its installation:

- 21 (ftp),
- 22 (sftp),
- 500-600 (udp),

- 17000-18000 (udp),
- 41390 (udp), 3
- 2000-33000 (udp)

For a highly secured environment where no remote access to the OSV-TM information is allowed, some of these ports need to be manually closed by the administrator.

CL-OSV-TM_Close_Ports	**Close Communication Ports**
Measures	Close the Communications Ports when remote access to the OSV-TM is not allowed.
References	Section 4.7.1, “How to Close the Communications Ports”
Needed Access Rights	n/a
Executed	Yes  No: 
Customer Comments and Reasons	

4.7.1 How to Close the Communications Ports

1. To disable these ports, you need to be logged into the Windows OSV-TM server with the administrator account and access the Windows Firewall configuration rules:
2. Go to “**Control Panel**” > **System and Security** > **Windows Firewall**
3. Click on “**Advanced Settings**”
4. Locate the corresponding “**Inbound Rules**” and “**Outbound Rules”**
5. Close the FTP port
   On highly secure environments where only secure FTP is allowed, the non-secured FTP port 21 should be disabled.
   - Disable the ports:
     - From the “Inbound Rules”, select the “**OSV-TM FTP Port**” rule
     - Click on “**Disable Rule**” on the right pane
     - Select the “**FTP CMD IN**” rule
     - Click on “Disable Rule” on the right pane
     - From the “Outbound Rules”, select the “**FTP CMD OUT**” rule

- Click on “**Disable Rule**” on the right pane

6. Close the OSV-TM Phone Listener ports
   The Phone Listener utility uses UDP ports 500-600 and 17000-18000 for trap and trace functionality. Disable these ports if UDP traffic is not allowed.
   – Disable the ports from the “Inbound Rules”:
     - Select the “OSV-TM Phone Trace Listen Ports” rule
     - Click on “Disable Rule” on the right pane
     - Select the “OSV-TM Phone Trap Listen Ports” rule
     - Click on “Disable Rule” on the right pane

7. Close the RG8700 Listener ports
   The RG8700 Listener utility sends trace information to the OSV-TM server via UDP ports 41390 and 32000-33000.
   – Disable the ports:
     - From the “Inbound Rules”, select the “OSV-TM RG8700 Listen Ports” rule
     - Click on “Disable Rule” on the right pane
     - From the “Outbound Rules”, select the “
     - OSV-TM RG8700 Control Ports” rule
     - Click on “Disable Rule” on the right pane

4.8 Block FTP Port

One of the Pre-Installation Requirements outlined in the OSV-TM Administrators Guide is to install a FTP server.

Because FTP is not a secured protocol, it should not be installed on highly secured environments. SFTP is included by default on all OSV-TM installations and should be used instead.

If FTP is already installed on the server, make sure that the FTP port is blocked to all traffic.

CL-OSV-TM_FTP_Port_Blocked	**FTP Port is Blocked**
Measures	Close the FTP Port.
References	Section 4.7.1, “How to Close the Communications Ports”
Needed Access Rights	n/a
Executed	Yes  No: 
Customer Comments and Reasons	

4.9 Dedicated SFTP Accounts Configured for Integrated Devices

1. Navigate to: **Control Panel > All Control Panel Items > User Accounts**
2. Select **Manage Another Account**
3. Select **Add a user account**
4. Insert the Name and password for the new User
5. Click on **Next** and **Finish**

4.10 Configure SFTP to Allow Connectivity Only from Allowed IP Addresses

1. Navigate to: **C:\ProgramData\ssh**
2. Edit the file **sshd_config**
3. Find the line `#PasswordAuthentication yes`
   1. Uncomment this line (Remove the # character)
   2. Change from `yes` to `no`
4. At the end of the file, add the following lines:

```
1. Match Address <ip_address_to_accept>
   PasswordAuthentication yes
```

When you want to enable access for multiple IP addresses, you can add the two last lines multiple times with the appropriate matching IP.

4.11 Disable the OSV-TM Web Portal FTP Export Feature

CL-OSV-TM_Disable_FTP_Export	**Disabling FTP Export Feature**
Measures	Disable the OSV-TM Web Portal FTP Export Feature
References	Section 4.11.1, “How to Disable the OSV-TM Web Portal FTP Export Feature”
Needed Access Rights	n/a
Executed	Yes  No: 
Customer Comments and Reasons	

4.11.1 How to Disable the OSV-TM Web Portal FTP Export Feature

Disable the "Send Files via FTP" functionality:

1. Login to FADE with the Admin account.
2. Navigate to the “Administration” view -> "TM_System_Configuration" -> “Other” tab.
3. Change the “Allow FTP access” option to “No”
4. Click “Save”
5. To ensure the FTP feature is completely disabled, ensure that the FTP communication ports are disabled on the Windows Firewall. Follow the steps in Section 4.7.1, “How to Close the Communications Ports”, on page 27.

   FTP Inbound/outbound firewall rules should close port 21 to disable FTP traffic.

4.12 Verify that no Listeners are configured in OSV-TM

The Phones and RG8700 devices send trace information to the OSV-TM server via UDP ports. Since this traffic is not protected, these devices must not be configured in an OSV-TM environment with strict security policies.

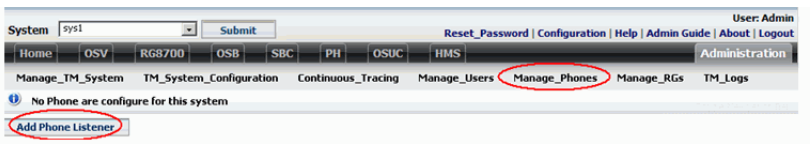
Phones report Quality of Service (QoS) data to the OSV-TM server; however, the traces received from the OpenScape Voice also contain QoS information that is sufficient data for trace analysis.

OSV-TM does not enable the RG listener or the phone listener during installation by default; they have to be manually configured in OSV-TM by the Admin. If these listeners have been already configured, they need to be removed.

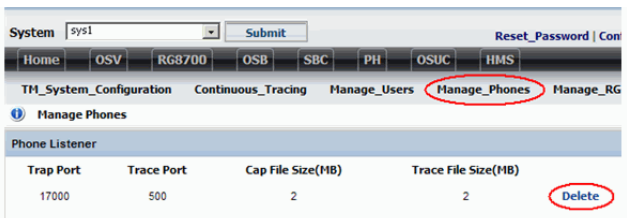
CL-OSV-TM_Listeners	**No RG or Phone Listeners Configured**
Measures	Verify that no phone listeners or RG listeners are configured in OSV-TM
References	Section 4.12.1, “How to Verify that no Phone Listeners are configured in OSV-TM”
Needed Access Rights	n/a
Executed	Yes No:
Customer Comments and Reasons	

4.12.1 How to Verify that no Phone Listeners are configured in OSV-TM

1. Click on the "Administration" view > Manage_Phones tab
2. This page should be blank and display only the "Add Phone Listener"



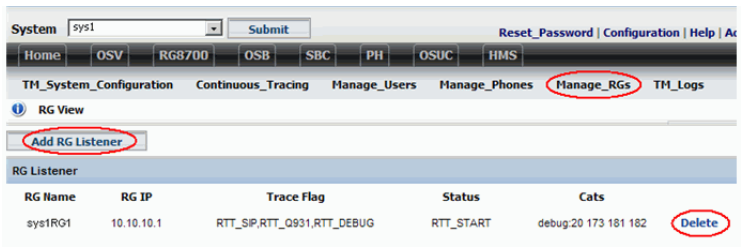
3. If a Phone Listener has been configured in the system, delete it:
   – Click the "Delete" action to the right of the Phone configuration to remove the Listener



4.12.2 How to Verify that no RG Listeners are configured in OSV-TM

1. Click on the “Administration” view > Manage_RGs tab
2. This page should be blank and no RG Listeners listed

3. If RG Listeners have been configured in the system, delete them:
   – Click the "Delete" action to the right of the RG to remove the RG.



4.13 Apache users permissions configuration

CL-OSV-TM_Apache_Perm	Configure Apache Permissions
Measures	Non-admin users don't have access to Apache bin and logs folders
References	Section 4.13.1, “How to configure Apache users permissions”
Needed Access Rights	n/a
Executed	Yes No
Customer Comments and Reasons	

4.13.1 How to configure Apache users permissions

By default, Apache assigns read/execute rights to user group for all its folders. The read/execute (and any other permissions) that users have, can be safely removed if needed.

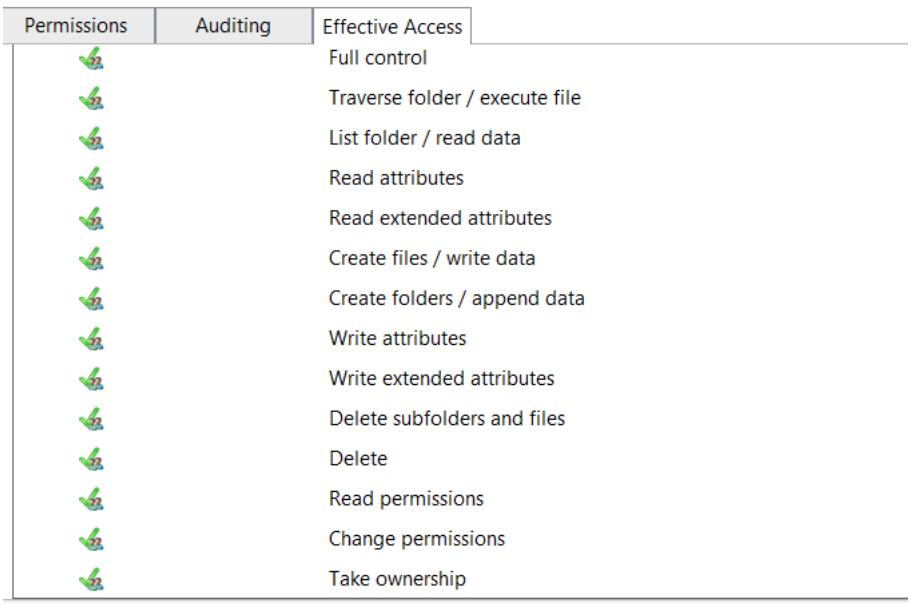
To remove users permissions:

1. Navigate to **..\Apache Software Foundation\Apache2.4**
2. Right-click on **folder logs -> Properties -> Security -> Edit**
3. Select the users or users' group and uncheck all checks for allow list (disable permissions inheritance from advanced settings if needed)

Repeat these steps for bin folder.

Administrator permissions should stay as they are, full for both folders.

Administrator permissions for Apache folders:



4.14 Encrypt Data at rest

This step is optional.

OS Filesystem encryptions provides an additional security measurement that prevents data leak in case of hard-disk loss.

The Filesystem is decrypted while the system is in a running state. Unauthorized access to the system (e.g. Remote Desktop, OSVTM Portal) will still lead to data leak.

Please note that this feature is not applicable for the RAM-Drive feature. Any data stored in the RAM are ephemeral only for the timeframe the system is in running state.

For the encryption of the OS Filesystem the BitLocker is proposed. The BitLocker may be deployed on Windows Server 2012 and later.

For installation instructions, please refer to the official Microsoft Documentation:

https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-how-to-deploy-on-windows-server

You may verify that the disk has been encrypted successfully using the following commands:

- manage-bde -status (CMD)
- Get-BitLockerVolume (PowerShell)

CL-OSV-TM FileSystemEncryption	**Enabling the OS Filesystem Encryption**
Measures	Encrypt OS Filesystem
References	
Needed Access Rights	Yes, System Administrator
Executed	
Customer Comments and Reasons