

MiVoice MX-ONE  
Security Guidelines  
Release 7.3  
August 31, 2020



## Notice

The information contained in this document is believed to be accurate in all respects but is not warranted by **Mitel Networks™ Corporation (MITEL®)**. 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") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at [legal@mitel.com](mailto:legal@mitel.com) for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website: <http://www.mitel.com/trademarks>.

®, ™ Trademark of Mitel Networks Corporation  
© Copyright 2020, Mitel Networks Corporation  
All rights reserved

---

# Contents

<b>Chapter: 1</b>	<b>General . . . . .</b>	<b>1</b>
	Introduction . . . . .	1
	Glossary . . . . .	1
<b>Chapter: 2</b>	<b>Prerequisites . . . . .</b>	<b>2</b>
<b>Chapter: 3</b>	<b>Tools . . . . .</b>	<b>3</b>
<b>Chapter: 4</b>	<b>References . . . . .</b>	<b>4</b>
<b>Chapter: 5</b>	<b>Execution . . . . .</b>	<b>5</b>
	Operating Systems . . . . .	5
	Linux . . . . .	5
	Operating System (OS) Patches . . . . .	5
	Hardening . . . . .	5
	SSH . . . . .	5
	Telnet . . . . .	6
	Certificate Management . . . . .	6
	VoIP Security . . . . .	6
	Media Encryption . . . . .	7
	Signaling Encryption . . . . .	7
	Security Policy Management . . . . .	7
	Operation and Maintenance Security (Management Applications) . . . . .	7
	MX-ONE Service Node Manager (SNM) . . . . .	7
	MX-ONE Provisioning Manager (PM) . . . . .	9
	Terminals/Clients . . . . .	9
	TLS/SHA Support in MX-ONE . . . . .	9
<b>Chapter: 6</b>	<b>Termination . . . . .</b>	<b>11</b>

# General

## Introduction

This document provides an overview of security guidelines for the MiVoice MX-ONE solution, that is, operational directions for security measures that are recommended, for servers, media gateways and end-points. It thus describes how to implement a secure system.

## Glossary

For a complete list of abbreviations and glossary, see the description for *Acronyms*, *Abbreviations*, and *Glossary*.

# Prerequisites

The wanted system components, like the MiVoice MX-ONE Service Node(s), Managers, media gateways, certificates and terminals/clients are available.

An individual account with less privileges (same as **mxone\_user**) is required to manage some parts of the system; for the normal operation, it is not required. This account must have bash as shell.

The most common maintenance tasks can be performed in the system via **mxone\_maintenance**. To do it, logon with the individual account and then do **su – mxone\_admin** to have a proper authority to run **mxone\_maintenance**.

The system accounts must be used only when it is required by the system.

# Tools

Management applications and/or I/O terminal for O&M commands.

# References

The description for *SECURITY*.

# Execution

## Operating Systems

### Linux

Unnecessary software should not be installed on the server. Certain types of software can compromise the hardening of the operating system.

To guarantee the integrity of the system and detect possible unauthorized or unwanted changes to the file system, the AIDE (Advanced Intrusion Detection Environment) tool has been installed and can be activated and configured on the MX-ONE Service Node. All relevant system files can then be monitored, and changes notified as soon as they are detected. The system administrator can change the default settings to further increase the security level by increasing the frequency when the tool performs the integrity check of the file system.

### Operating System (OS) Patches

Operating System patch packages are delivered once a month and placed in the Mitel Knowledge base. It is strongly recommended to keep the customer system up to date with the latest patches.

### Hardening

The servers in MX-ONE run on operating systems that have been hardened to resist the most common network attacks. Known vulnerable services are shut down and file integrity is checked periodically. Additionally, customers are recommended to implement security policies that cover patch management and anti-virus software updates. It is recommended to use an anti-virus software and to have automatic updates of the security patches activated.

### SSH

Secure Shell (SSH) version 2 provides secure console-based access to IP phones and the MX-ONE Service Node. To manage the server using the Command Line Interface, SSH is the recommended solution.

SSH is enabled by default on the MX-ONE Service Node. To increase security, direct root access is disabled by default. If a system administrator needs to carry out tasks that require root access, the administrator must log on as a non-root administrator and then use the command **su -** to run as root.

The list below shows the SSH cipher list support in MX-ONE.

**For key exchange:**

- curve25519-sha256@libssh.org
- diffie-hellman-group-exchange-sha256

**For authentication:**

- RSA using 4096-bits



**Allowed host key types:**

- Ed25519
- RSA

**Symmetric ciphers (data encryption):**

- chacha20-poly1305@openssh.com
- aes256-cbc
- aes192-cbc
- aes256-ctr
- aes192-ctr
- aes128-cbc
- aes128-ctr

**Message authentication codes:**

- hmac-sha2-512-etm@openssh.com
- hmac-sha2-256-etm@openssh.com
- hmac-ripemd160-etm@openssh.com
- umac-128-etm@openssh.com
- hmac-sha2-512
- hmac-sha2-256
- hmac-ripemd160
- umac-128@openssh.com

SSH ciphers can be configured in the **mxone\_maintenance** menu in the Service Node.

## Telnet

Telnet is disabled by default on the MX ONE Service Node. Telnet sends user-name/password in clear text over the wire, which may become a potential threat if sniffed. For remote access, SSHv2 is the recommended solution.

## Certificate Management

The certificates are used to authenticate the communicating parties in the handshake procedure. Each server has a private key and a public key. A message that is encrypted with the private key can only be decrypted with the public key. If a message is encrypted with the public key it can only be decrypted by the owner of the private key. For more information about certificate management, see the description for *SECURITY* and the operational directions for *CERTIFICATE MANAGEMENT*.

## VoIP Security

The Voice over IP (VoIP) signaling between IP terminals and the SIP proxy or the H.323 Gatekeeper (the MX-ONE Service Node) is protected by the Transport Layer Secure (TLS) cryptographic protocol. TLS provides a secure way to interchange the cipher keys needed in the later Secure Real-time Transport

Protocol (SRTP) media transfer session. For more information about VoIP, see the operational directions for *VOIP SECURITY*.

## Media Encryption

Secure Real-time Transport Protocol (SRTP) is used to protect the media streams of the voice communication.

MX-ONE supports the use of SRTP for media encryption in the IP phones and the Media Gateway Lite and MX-ONE Classic. SRTP makes use of the Advanced Encryption Standard (AES) with different key lengths to protect the media streams.

For information about how to enable or disable SRTP, see the operational directions for *VOIP SECURITY*.

## Signaling Encryption

The Transport Layer Security (TLS) provides secure access to IP phones and web services and secure signaling between IP phones and MX-ONE Service Nodes.

For information on how to enable/disable TLS, see operational directions for *CERTIFICATE MANAGEMENT*.

## Security Policy Management

The Security Policy determines how IP entities in the system are allowed to register in the system. If security exceptions are allowed certain directory numbers or terminal types can be allowed to be used even if they do not support TLS or SRTP. For more information about the security policy and how to set it up, see the operational directions for *VOIP SECURITY*.

# Operation and Maintenance Security (Management Applications)

## MX-ONE Service Node Manager (SNM)

Even if the SNM usually runs on the same server as the Service Node, it is strongly recommended to use HTTPS, but HTTP can also be used. During the installation, the MX-ONE is configured to use either standard HTTP or HTTPS. With HTTPS, it is necessary to configure a private key, and a digital certificate, to be used in the system. For more information, see the installation instructions for *INSTALLING AND CONFIGURING MIVOICE MX-ONE*.

In Service Node Manager under **Tools** menu, there is a task called Command Line, enabled by default. It is recommended that customers and partners use SSH version 2 to access the system instead of this task. As this feature uses a direct call to the Operating System some scanning tools might highlight security issues on it.

It is also recommended that this task is disabled from the admin if that is not in use. To disable it, logon as System Setup Admin in Provisioning Manager and go to Administrators, Security Profile and then select the Security Profile Name where the function will be disabled.

**Uncheck the SNM:** Command Line Interface, note that the whole Tools task (Command Line, Quality of Service and Signal Trace) is removed from the Admin.

In the example below, the task is removed from **AlaCarte Service Provider** profile.

**Figure 5.1:** Security Profile - Change - AlaCarte Service Provider

**Security Profile - Change - AlaCarte Service Provider**

Apply Cancel

Security Profile Name: \* AlaCarte Service Provide

Description:

**Privileges**

End user self service:	<input checked="" type="checkbox"/>	End user group service:	<input type="checkbox"/>
Manage configuration data:	<input checked="" type="checkbox"/>	Manage user data:	<input checked="" type="checkbox"/>
View user data:	<input checked="" type="checkbox"/>	Manage service data:	<input checked="" type="checkbox"/>
View service data:	<input checked="" type="checkbox"/>	Manage administrators:	<input checked="" type="checkbox"/>
View administrators:	<input checked="" type="checkbox"/>	Manage security profiles:	<input type="checkbox"/>
View security profiles:	<input type="checkbox"/>	Import/Export user data:	<input checked="" type="checkbox"/>
Auto unlock:	<input checked="" type="checkbox"/>	Manage UDF data:	<input checked="" type="checkbox"/>
SNM: Manage advanced feature:	<input checked="" type="checkbox"/>	<b>SNM: Command line interface:</b>	<input type="checkbox"/>
SNM: Manage extension data:	<input checked="" type="checkbox"/>	View subsystems:	<input checked="" type="checkbox"/>
Tenant configuration data:	<input type="checkbox"/>	AlaCarte:	<input checked="" type="checkbox"/>
Feature level configuration data:	<input type="checkbox"/>	View logs:	<input checked="" type="checkbox"/>
Manage individual diversion:	<input checked="" type="checkbox"/>	Manage available extensions:	<input checked="" type="checkbox"/>
Manage Batch Operation:	<input checked="" type="checkbox"/>	SNM: View Logs:	<input checked="" type="checkbox"/>
SNM: Manage Secure Data:	<input checked="" type="checkbox"/>	SNM: Backup:	<input checked="" type="checkbox"/>
SNM: IP Phone Configuration:	<input checked="" type="checkbox"/>	Manage Secure Data:	<input checked="" type="checkbox"/>
Manage Featurebased System:	<input type="checkbox"/>		

After the Admin page view, the command line is disabled.

**Figure 5.2:** Admin Page View

**Mitel | Service Node Manager** Logged in as About User Guide Site Map Logout

Initial Setup Number Analysis Telephony Services System Logs

**Welcome**

This application handles the system settings for the MiVoice MX-ONE Service Node.  
For user settings please use the "MiVoice MX-ONE Provisioning Manager" application.

## MX-ONE Provisioning Manager (PM)

It is strongly recommended to use HTTPS, but HTTP can also be used. During the installation, the MX-ONE is configured to use either standard HTTP or HTTPS. With HTTPS, it is necessary to configure a private key, and a digital certificate, to be used in the system. For more information, see the installation instructions for *INSTALLING AND CONFIGURING MIVOICE MX-ONE*.

## Terminals/Clients

All Mitel IP (SIP and H.323) end-points with a few exceptions have support for TLS. In the configuration file for the IP telephones, TLS and its associated parameters like certificates must be set. It is strongly recommended to use TLS 1.2.

There are also some other security parameters to define in the configuration file, such as:

- If a validation of the certificate should be done.
- If the password should be stored in the telephone.
- If the registration should be allowed although the TLS negotiation fails (only valid for H.323 based phones).

For more information about parameters in the configuration file, see the description for respective end-point.

To make changes in the IP telephone configuration file, use the **IP Phone Configuration File** task in **MX-ONE Service Node Manager**.

For more information about the security features in the IP telephones, see installation instructions for the terminals/end-points.

## TLS/SHA Support in MX-ONE

Compati- bility (TLS 1.0 and SHA-1)	SIP Trunks	SIP extension s (68XX and 69XX family)	Configurat i- on Server	CSTA III	SIP extension s (67XX family)	H.323 extension	H.323 trunk
TLS 1.0 / SHA-1	support- ed	support- ed	supported	support- ed	supported	supported	supported
TLS 1.1 / SHA-1	support- ed	support- ed	supported	support- ed	not supported	not supported	not supported
TLS 1.2 / SHA-1	support- ed	support- ed	supported	support- ed	not supported	not supported	not supported

<b>Compati- bility (TLS 1.1 and SHA-2)</b>	<b>SIP Trunks</b>	<b>SIP extension s (68XX and 69XX family)</b>	<b>Configur- ation Server</b>	<b>CSTA III</b>	<b>SIP extensions (67XX family)</b>	<b>H.323 extension</b>	<b>H.323 trunk</b>
TLS 1.1 / SHA-2	support- ed	supported	supported	support- ed	not supported	not supported	not supported
TLS 1.2 / SHA-2	support- ed	supported	supported	support- ed	not supported	not supported	not supported

# Termination

Check that the security measures seem to have taken effect, for example that media is encrypted as it should be, and ditto for signaling channels.

