MiVoice MX-ONE

Release 7.6

SECURITY GUIDELINES

NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). Mitel makes no warranty of any kind with regards to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. 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.

TRADEMARKS

MiVoice MX-ONE Security Guidelines
Release 7.6
January 2023
9/154 31- ASP 113 01 Uen E 2023-12-21

General

Introduction

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

What is New in This Release

In this release, there are no updates impacting security guidelines.

Reference Documents

Following documents has been referenced within this document and can be found in MX-ONE O&M Library:

- *ACRONYMS ABBREVIATIONS AND GLOSSARY, Doc Id: 0033-ASP 113 01.*
- *SECURITY DESCRIPTION, Doc Id: 19/1551-ASP 113 01.*
- *CERTIFICATE MANAGEMENT, Doc Id: 132/154 31-ANF 901 14.*
- *VOIP SECURITY, Doc Id: 82/154 31-ANF 901 14.*

INSTALLING AND CONFIGURING MIVOICE MX-ONE, Doc Id: 4/1531-ANF 901 43.

Glossary

For a complete list of abbreviations and glossary, see the description for *ACRONYMS ABBREVIATIONS, AND GLOSSARY*.

Prerequisites

The required system components, such as the MiVoice MX-ONE Service Node(s), Managers, media gateways, certificates, and terminals/clients must be available.

The system administrator must have root authority.

Tools

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

References

The description for *SECURITY*.

Execution

Operating Systems

Linux

Unnecessary software must 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 with which the tool performs the integrity check of the file system.

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, it is recommended that customers implement security policies that cover patch management and anti-virus software updates. It is also recommended that they have an anti-virus software and activate automatic updates of the security patches.

SSH

Secure Shell (SSHv2) provides secure, console-based access to IP phones (H.323) and the MX-ONE Service Node. To manage the server using the Command Line Interface, SSHv2 is the recommended solution.

SSHv2 is enabled by default on the MX-ONE Service Node. To increase security, direct root access is disabled by default. A system administrator who needs to perform tasks that require root access must log in as a non-root administrator and then use the command su - to run as root.

As an extra precaution, unauthorized access can be limited by ACL in MX-ONE with iptables.

The following list shows the SSHv2 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
- umac-128-etm@openssh.com
- hmac-sha2-512
- hmac-sha2-256
- umac-128@openssh.com

Telnet

Telnet is disabled by default on the MX-ONE Service Node. Telnet sends user name/password in clear text over the wire, which might become a potential threat if sniffed. For remote access, SSH 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 be decrypted only with the public key. If a message is encrypted with the public key, it can be decrypted only 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*.

Digital Signature Algorithms

In MX-ONE , the certificates used by the encryption mechanisms can be signed by RSA or ECDSA algorithms digitally.

The following services support either RSA or ECDSA certificates:

- SIPLP (TCP Port 5061, 22223)
- Configure Server (TCP Port 22226)
- CSTA server (TCP Port 8883)
- Provisioning Manager and Service Node Manager (TCP Port 443)

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 IP phones and the Media Gateway Unit (MGU). 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 about 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 with 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)

The following sections describe the operation and maintenance security pertaining to management applications.

MX-ONE Service Node Manager (SNM)

Even if the SNM usually runs on the same server as the Service Node, it is recommended to use HTTPS with TLS 1.3. During the installation, the MX-ONE is configured to use 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*.

MX-ONE Provisioning Manager (PM)

It is recommended to use HTTPS with TLS 1.3. During the installation, the MX-ONE is configured to use HTTPS. With HTTPS, it is necessary to configure a private key, and a digital certificate either RSA or ECDSA, 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 support for TLS. In the configuration file for the IP telephones, TLS and its associated parameters such as the certificates must be set.

There are also some other security parameters that must be defined in the configuration file if:

- a validation of the certificate should be done
- the password should be stored in the telephone
- the registration should be allowed although the TLS negotiation fails (valid only 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

Compatibility (TLS protocol version and SHA version)	**SIP Trunks**	**SIP extensions (68XX and 69XX family)**	**Configuration Server**	**CSTA III**	**SIP extensions (67XX family)**	**H.323 extension**	**H.323 trunk**
TLS 1.0 / SHA-1	Legacy	Legacy	Legacy	Legacy	Legacy	Legacy	Legacy
TLS 1.1 / SHA-1	Legacy, Medium	Legacy, Medium	Legacy, Medium	Legacy, Medium	Not supported	Not supported	Not supported
TLS 1.1 / SHA-2	Not supported	Not supported	Not supported	Not supported	Not supported	Not supported	Not supported
TLS 1.2 / SHA-2	Legacy, Medium, High	Legacy, Medium, High	Legacy, Medium, High	Legacy, Medium, High	Not supported	Not supported	Not supported
TLS 1.3 / SHA-2	Legacy, Medium, High, Modern	Not supported	Legacy, Medium, High, Modern	Legacy, Medium, High, Modern	Not supported	Not supported	Not supported

NOTE: TLS 1.3 does not support SHA-1.

Ciphers List in MX-ONE

The encryption mechanisms used by MX-ONE Service Node and MX-ONE Management are different. Therefore, the ciphers lists are different.

MX-ONE Service Node

The ciphers supported by MX-ONE Service Node are divided into four groups: Modern, High, Medium, and Legacy level of security.

Modern Level

With security level Modern in MX-ONE, the following ciphers are supported by Service Node.

TLS 1.3: CSTA server (TCP Port 8883) and SIPLP (TCP Port 5061, 22223), Configure Server (TCP Port 22226), ciphers:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256

High Level

With security level High in MX-ONE, the following ciphers are supported by Service Node.

TLS 1.3: CSTA server (TCP Port 8883) and SIPLP (TCP Port 5061, 22223), Configure Server (TCP Port 22226), ciphers:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256

TLS 1.2: CSTA server (TCP Port 8883) and SIPLP (TCP Port 5061, 22223), Configure Server (TCP Port 22226) ciphers:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256

Medium Level

With security level Medium in MX-ONE, the following ciphers are supported by Service Node.

TLS 1.3: CSTA server (TCP Port 8883) and SIPLP (TCP Port 5061, 22223), Configure Server (TCP Port 22226), ciphers:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256

TLS 1.1: Configure Server (TCP Port 22226), CSTA server (TCP Port 8883), SIPLP (TCP Port 5061, 22223), ciphers:

- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA

TLS 1.2: ciphers:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA

Legacy Level

With security level Legacy in MX-ONE, the following ciphers are supported by Service Node.

TLS 1.3: CSTA server (TCP Port 8883) and SIPLP (TCP Port 5061, 22223), Configure Server (TCP Port 22226), ciphers:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256

TLS 1: Configure Server (TCP Port 22226), CSTA server (TCP Port 8883), SIPLP (TCP Port 5061, 22223), ciphers:

- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA

TLS 1.1: ciphers:

- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

TLS 1.2: ciphers:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

MX-ONE Management - Provisioning Manager and Service Node Manager

The ciphers supported by MX-ONE Management are divided into four groups: TLS 1.3, TLS 1.2 only, TLS 1.2, and TLS 1.1 and 1.0. level of security.

TLS 1.3 is the only recommended version to be used as it will work with the modern browsers (Firefox, Google Chrome, and Microsoft Edge).

TLS 1.3, ciphers:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256

TLS 1.2 only, ciphers:

- SSL_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- SSL_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- SSL_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- SSL_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- SSL_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- SSL_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- SSL_RSA_WITH_AES_256_GCM_SHA384
- SSL_RSA_WITH_AES_256_CBC_SHA256
- SSL_ECDHE_RSA_WITH_AES_256_CBC_SHA

- SSL_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- SSL_RSA_WITH_AES_256_CBC_SHA

TLS 1.2, ciphers:

- SSL_RSA_WITH_AES_128_GCM_SHA256
- SSL_RSA_WITH_AES_128_CBC_SHA256
- SSL_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- SSL_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- SSL_ECDHE_RSA_WITH_AES_128_CBC_SHA
- SSL_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- SSL_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- SSL_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- SSL_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- SSL_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- SSL_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- SSL_RSA_WITH_AES_256_GCM_SHA384
- SSL_RSA_WITH_AES_256_CBC_SHA256
- SSL_ECDHE_RSA_WITH_AES_256_CBC_SHA
- SSL_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- SSL_RSA_WITH_AES_256_CBC_SHA

TLS 1.1 and TLS 1.0 (legacy browsers), ciphers

The number of ciphers were reduced to only 1 for TLS 1.1 and TLS 1.0 and now it is the same.

- SSL_RSA_WITH_AES_128_CBC_SHA4

Product Security Information

Mitel Product Security Vulnerabilities

The Product Security Policy discusses how Mitel assesses security risks, resolves confirmed security vulnerabilities, and how the reporting of security vulnerabilities is performed.

Mitel's Product Security Policy is available at:

https://www.mitel.com/support/security-advisories/mitel-product-security-policy

Mitel Product Security Advisories

Mitel Product Security Advisories are available at:

https://www.mitel.com/support/security-advisories

Mitel Security Documentation

Mitel security documentation includes product specific; Security Guidelines, Important Information for Customer GDPR Compliance Initiatives and Data Protection and Privacy Controls. Mitel also has Technical Papers and White papers that discuss network security and data center security.

Mitel Product Security Documentation is available at:

https://www.mitel.com/document-center

Disclaimer

THIS SOLUTIONS ENGINEERING DOCUMENT IS PROVIDED “AS IS” AND WITHOUT WARRANTY. IN NO EVENT WILL MITEL NETWORKS CORPORATION OR ITS AFFILIATES HAVE ANY LIABILITY WHATSOEVER ARISING FROM IN CONNECTION WITH THIS DOCUMENT. You acknowledge and agree that you are solely responsible to comply with any and all laws and regulations in association with your use of MiVoice MX-ONE and/or other Mitel products and solutions including without limitation, laws and regulations related to call recording and data privacy. The information contained in this document is not, and should not be construed as, legal advice. Should further analysis or explanation of the subject matter be required, please contact an attorney.