MiVoice MX-ONE

Security Guidelines

Release 7.3 SP1

February 13, 2021

Mitel®

Notice

Trademarks

Contents

General

Introduction

This document provides an overview of security guidelines for the MiVoice MX-ONE solution, i.e. 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.

The 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 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 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.

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.

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) 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

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, 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 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*.

Digital Signature Algorithms

In MX-ONE 7.3 SP1 and later 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 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 CERTIF-ICATE 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)

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 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* .

MX-ONE Provisioning Manager (PM)

It is recommended to use HTTPS with TLS 1.2, 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 either RSA or ECDSA, to be used in the system. For more information, see the installation instructions for *INSTALLING AND CONFIG-URING 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.

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

Compatibility (TLS 1.0 and SHA-1)	**SIP Trunks**	**SIP extensions (68XX and 69XX family)**	**ConfigurationServer**	**CSTA III**	**SIP extensions (67XX family)**	**H.323 extension**	**H.323 trunk**
TLS 1.0 / SHA-1	supported	supported	supported	supported	supported	supported	supported
TLS 1.1 / SHA-1	supported	supported	supported	supported	not supported	not supported	not supported
TLS 1.2 / SHA-1	supported	supported	supported	supported	not supported	not supported	not supported

Compatibility (TLS 1.1 and SHA-2)	**SIP Trunks**	**SIP extensions (68XX and 69XX family)**	**Configuration Server**	**CSTA III**	**SIP extensions (67XX family)**	**H.323 extension**	**H.323 trunk**
TLS 1.1 / SHA-2	supported	supported	supported	supported	not supported	not supported	not supported
TLS 1.2 / SHA-2	supported	supported	supported	supported	not supported	not supported	not supported

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 in three groups: High, Medium and Low (legacy) level of security.

High Level

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

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

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256

TLS 1.2: Configure Server (TCP Port 22226), ciphers:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- 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 1.1: 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

Low (legacy) Level

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

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 in four groups: TLS 1.0, TLS 1.1, TLS 1.2 and TLS 1.2 only level of security.

TLS 1.2 only is the recommended version to be used as it will work with the modern browsers (Firefox, Google Chrome and Microsoft Edge).

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

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.

Mitel
Powering connections

mitel.com