

MiVoice MX-ONE Security

DESCRIPTION



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.

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 for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website: <http://www.mitel.com/trademarks>.

© Copyright 2017, Mitel Networks Corporation

All rights reserved

1

INTRODUCTION

Integration of voice services into an IS/IT data infrastructure raises several questions and concerns as how to guarantee the same level of security, availability, and quality of service as the classic circuit-switched telephony infrastructure.

This document provides an overview of the security mechanisms available to protect the MX-ONE™ solution from threats that are typical of the IS/IT infrastructure. The described measures are either enabled in the system by default, enabled during the installation/configuration phase of the systems, or need to be enabled manually by the system administrator.

The security measures available for the MX-ONE system are mainly based on the following open standard technologies:

SSL (or TLS)

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

SSH

Secure Shell (SSH) provides secure console-based access to IP phones, the MX-ONE Service Node and the Media Gateway (MGU)

SRTP

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

Additionally, other mechanisms to protect the MX-ONE solution are based on the following:

- Correct configuration of the corporate Local Area Network (LAN) infrastructure
- Authentication and authorization of all users of the system, including end-users and administrators
- Security mechanisms provided by the target operating systems (SuSe® Linux and Microsoft Windows®) as well as hardening measures

Beside the security functions described in this document, there are a number of general security aspects that need to be covered and taken care of by a system administrator. Every organization must have a clearly defined IT security policy in place, defining goals, assets, trust levels, processes, incident handling procedure, etc. The security mechanisms available in the MX-ONE system must be covered by and deployed according to this policy. An important security measure to be implemented is to preserve physical security. Only authorized personnel shall have access to server locations, since many data-exposure attacks can be mounted by having physical access to a host. Further, the IT data infrastructure must have a solid design, security mechanisms and protocols must be enabled and all components of the whole system must be correctly configured and maintained.

2

DEFINITIONS

For definitions, see *ACRONYMS, ABBREVIATIONS AND GLOSSARY*.

3

MIVOICE MX-ONE ARCHITECTURE

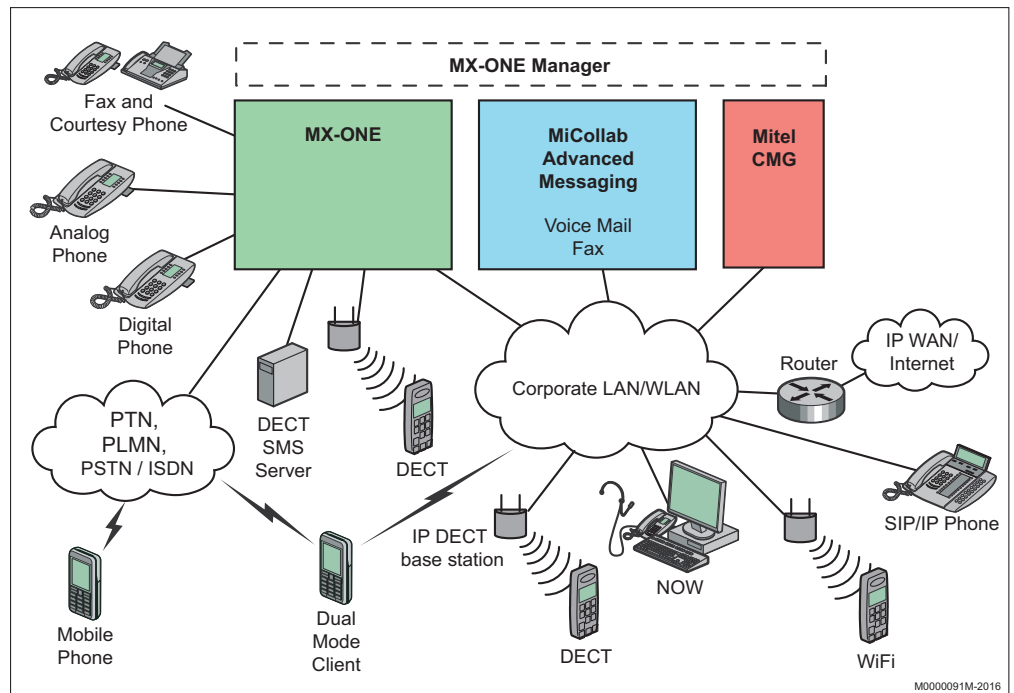


Figure 1: MX-ONE Architecture

The MX-ONE system comprises a number of components that communicate within an existing IT infrastructure, see Figure 1. The following sections illustrate the mechanisms that are available to protect MX-ONE from the architectural point of view.

3.1

LAN CONFIGURATION

The MX-ONE components communicate using the corporate LAN infrastructure, usually based on IEEE 802.3 (Ethernet). This is typically an open environment, and communication can be easily intercepted, eavesdropped, and hijacked if a number of configuration measures are not taken when setting up the network.

It is recommended that the LAN connecting the system nodes is fully switched, to avoid eavesdropping attacks that are extremely easy to perform in an Ethernet infrastructure only equipped with hubs. An eavesdropping attack is more difficult to carry out on a switched infrastructure, as Address Resolution Protocol (ARP) messages need to be intercepted and answered. However, ARP attacks have become quite frequent and software tools able to carry them out are widely available.

To make eavesdropping attacks more difficult to carry out, traffic on the LAN should be grouped together depending on the node functions and on their trust level. This can be achieved by the means of Virtual LANs (IEEE 802.1Q and port-based VLANs) that allow separating the communication for example for server-to-server signaling, server-to-client signaling, voice traffic, and so on, providing additional isolation and making the system more robust against virus-based and network flooding attacks. In particular, if Voice over Internet Protocol (VoIP) traffic is grouped into a single VLAN, and the nodes on such VLAN are strongly protected, a worm-based attack causing network overload originated on a node located on another VLAN might only marginally

affect the VoIP LAN. As a completion, the use of VLAN should be integrated with the use of different traffic priorities. Additionally, if the voice traffic must cross IP core networks, it is recommended to make use of Layer 3 techniques (such as DiffServ) to also provide traffic isolation when crossing Layer 3 devices.

The communication between the MX-ONE Service Node and the Media Gateway (valid for all types of media gateways) must occur on the corporate LAN, if full support of the available redundancy functions is needed. If support of the redundancy functions is not needed, it is possible to use a dedicated LAN segment to connect the MX-ONE Service Node to the Media Gateway. This is true for the Media Gateway Classic, but not for the media gateways built on the MGU board. A possible setup is the following:

- 1) One VLAN grouping the VoIP Servers (MX-ONE Service Node, Media Gateways)
- 2) One or several VLANs grouping the IP phones
- 3) One or several VLANs for data traffic

If traffic priorities are implemented in the network, the VLAN grouping the VoIP servers shall have the highest priority and the VLAN used for data services shall have the lowest priority. Usually, each VLAN is associated to an IP subnet. Hosts or devices belonging to different VLANs can communicate only through a Layer 3 router. This means that broadcast traffic is blocked across VLANs. Additionally, some routers are enhanced with Intrusion Detection/Prevention Systems (IDS/IPS), able to block more advanced types of attacks.

All MX-ONE components (MX-ONE Service Nodes, MGU, IPLU boards, and IP telephones) support the use and configuration of VLANs and DiffServ.

3.2 VOICE OVER IP TRAFFIC

Attention to the security aspects of an IP telephony infrastructure is increasingly growing by corporate Chief Information Officers (CIOs), IT administrators, and end-users. Voice over IP traffic (both signaling and media) must be protected from a number of attacks, such as media streams eavesdropping, toll-fraud attacks, signaling modification, and so on. For this reason, it is necessary to protect both the VoIP signaling messages as well as the media streams.

The following security measures are supported in the MX-ONE:

- Secure Real-time Transport Protocol (SRTP) to protect media streams
- TLS to protect signaling messages
- Support for a number of flexible security policies, in order to support environment with different security requirements

TLS guarantees the signaling privacy when the SRTP keys are interchanged between the parties.

The main principle for the security policy is that it directs if an extension is allowed to register to the system or not. Once the extension is registered, the calls to any other party is allowed from a security perspective.

3.2.1 MEDIA ENCRYPTION

3.2.1.1 *General*

Support for SRTP is given in the IP phones (DBC 42x 02, DBC 43x 01, DBC 44x 01 and Mitel 6900/6800/6700) and in the Media Server, the MGU type of media gateway and in the Media Gateway Classic (IPLU/1 boards).

Note: SRTP support is not implemented in the Media Gateway version 1 (BFJ 901 03), in the Operator Assistant media device, or in Softphones like the ECC.

3.2.1.2 *Function*

SRTP makes use of the Advanced Encryption Standard (AES) with a 128, 192 or 256 bits key to protect the media streams. The encryption keys are exchanged according to the ITU-T H.235.8 specification for H.323, or to RFC 4568, RFC 5116, RFC 5282 and RFC 6188 for SIP end-points.

For a two-party phone call, four keys will be needed to be exchanged between the two parties. Each party originating a media stream will generate two keys, a Master Key and a Master Salt and send them to the other party during the call control phase. These values are generated using high-entropy pseudo-random number generators in the IP telephones and in the MX-ONE Service Nodes, the actual keys used by SRTP (one encryption key for each direction, one integrity key for each direction) are calculated using the procedures defined by the SRTP specification. The signaling messages carrying the encryption keys are encrypted by TLS before being sent.

3.2.1.3 *H.323 Trunks (tie-lines)*

Media encryption using the SRTP protocol is supported for calls over H.323 trunks. H.323 signaling messages that carry the encryption keys can be encrypted by configuring the route parameters to support or require TLS. In case it is set to support (but not require) TLS, but the secure TLS connection fails, a fall back to TCP can be done.

3.2.1.4 *SIP Trunks*

Media encryption using the SRTP protocol is supported for calls over SIP trunks. SIP trunk signaling is secured with TLS, but note that the certificate is shared with SIP extension. No fall back to TCP option exists.

3.2.1.5 *Gateway Calls*

SRTP is available in the MX-ONE Lite and in the MX-ONE Classic, either with the MGU or IPLU/1 boards, i.e. GW calls via the MGU or IPLU boards can be media encrypted.

Whenever there is a change in the Non-GW and GW conditions of the calls, the media encryption has to be negotiated. Whenever pause and rerouting is executed the media encryption capabilities are re-negotiated.

3.2.1.6 *Non-Gateway Calls*

For non-GW calls media encryption depends on the H.323 endpoints. The H.323 trunk is transparent in non-GW scenarios. An H.323 trunk does not decide on the media

encryption of the non-GW calls. However due to pause and rerouting if the call condition changes to gateway then again the trunk decides about the media encryption.

3.2.1.7 *Trunk Calls towards MD110*

MD110 does not support media encryption. So if a trunk call is made between an MX-ONE and an MD110, media encryption is disabled in the MX-ONE during the H245 negotiation. Hence calls towards an MD110 are plain RTP calls.

3.2.2 SIGNALING ENCRYPTION

To enable support for TLS in MX-ONE IP phones, see the Installation Instructions for *DBC 433/DBC 434, DBC 425, DBC 422, DBC 420 and Mitel 6900/6800/6700*.

3.2.2.1 *TLS Signalling*

The primary goal of the TLS Protocol is to provide privacy and data integrity between two communicating applications.

By use of asymmetric key encryption, parameters for the data transfer are negotiated in a safe way. Each transferred data packet is encrypted. By adding a modified message digest with each message (each data packet) the receiving application can verify the data integrity.

TLS consists of two protocols (layers), the handshake layer and the record layer.

The Handshake layer allows the server and client to authenticate each other and to negotiate for an encryption algorithm and keys before the application transmits or receives its first byte of data. The Handshake layer performs this operation using the certificates and asymmetric keys.

The Record layer provides connection security. Each record is encrypted using the symmetric key established in the handshake. The symmetric key is a secret key shared by the two parties.

3.2.2.2 *Terminal Signaling Encryption and Decryption*

Logon procedure

When the user presses the logon button the phone prompts the user to enter a PIN code. The Regional Authorization Code (RAC) configured for the terminal is the PIN code.

- In case the user does not enter the PIN code the RRQ (for H.323) or Register (for SIP) is sent insecurely. If this registration is accepted or not depends on the Security Policy set in the MX-ONE Service Node.
- If the user enters the PIN code the client (the IP extension) starts the TLS negotiation. After the session keys are established the client sends the encrypted RRQ or Register. The server decrypts it and checks whether the correct PIN code is received.

3.2.2.3 *H.323 trunk signaling Encryption and Decryption*

MX-ONE supports the encryption of the trunk signaling messages exchanged over H.323 trunk using TLS. This functionality is optional and can be configured by administrator.

A TLS session is established when both the end points support TLS. The call originating PBX acts as TLS client and starts the TLS negotiation with the other end point (PBX), which acts as server.

If the other end does not support TLS then the session will fall back to use normal TCP connection, based on the configuration given by the administrator. If the fall back option is not configured then the call does not proceed.

3.2.3 TLS AND SRTP INTERACTION

TLS ensures signaling encryption and SRTP ensures media encryption.

The TLS procedures are exchanged with the MX-ONE Service Node Server only. Hence once an extension is registered via TLS the signaling, will be encrypted until the extension is logged off. If both TLS and SRTP is used end-to-end, a security icon is shown on the telephone display.

Media encryption by SRTP depends on the type of media gateway that is used. It is supported in the MX-ONE Lite and in the MX-ONE Classic, either with MGU or (LSU-E plus) IPLU. For each call SRTP support is negotiated with the MX-ONE Service Node. Hence in case of extensions registered towards a Media Gateway where media encryption is not possible, the signaling can still be encrypted. Although an extension with both TLS and SRTP capabilities is logged on, the media may not be encrypted.

3.2.4 SIP

The MX-ONE system includes support for HTTP digest authentication for the SIP interface. Each time a SIP phone registers itself to the SIP Registrar, it will also be required to authenticate itself.

3.2.5 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.

The keys can be generated by different algorithms. For example, for large keys generated with the RSA algorithm, no practical method has yet been found to retrieve the encrypted data without access to the private (secret) key.

In order for the telephone to be able to authenticate the server, the telephone has a certificate repository with a number of root and trusted certificates. These certificates cannot be changed or increased in number.

The X.509 certificate has to be stored in each MX-ONE Service Node. The respective signed certificate with the generated public key is sent by each party in the TLS communication.

For further information, see the installation instructions for *INSTALLING AND CONFIGURING MIVOICE MX-ONE*.

3.2.6 SECURITY POLICIES

Security policies have been defined to give flexibility in administration and to provide sufficient system security. The administrator must be judicious in choosing the security policy for the system. A security license is needed for assigning security policies.

For the MX-ONE system three security policies, 1, 2, or 3, can be set for the system. When no policy is set the system is open for all types of terminals that are defined for the system.

1. In the ALL SECURE system policy only Secure Extensions are allowed to register in the system. Both TLS and SRTP must be supported by the extensions.
2. In the ALL SECURE + EXC EXT policy the All Secure policy is modified by giving a security exception to specified extension numbers. Users at these numbers are allowed to logon insecurely.
3. In the ALL SECURE + EXC TYPE policy the All Secure policy is modified by giving a security exception for the telephone type. This can be used, for example, to enable softphones to use the system.

For further information on security policies, see the operational directions for *VOIP SECURITY* and the command *sec_policy*.

3.3 TRAFFIC AMONG SERVERS

In a modern IS/IT infrastructure, servers are generally grouped together and located in server farms. These locations need to be physically protected and only authorized personnel should be allowed to access them. This means that traffic among servers is likely to never leave the physical locations where servers are stored. Layer-2 and Layer-3 network devices are also located in the same locations and contribute to guarantee the physical separation of server traffic from other kind of network traffic. As a further measure to protect server-to-server traffic, it is recommended to set up a specific VLAN just for grouping servers, see chapter 3.1 LAN Configuration on page 4.

If servers are located at remote locations, it is highly recommended to set up a Virtual Private Network (VPN) system, and firewalls to protect and monitor the communication among them.

If SIP trunks are to be used, protecting them with VPN should also be considered

3.4 CLIENT SERVER COMMUNICATION

Generally, no assumption can be made as to the location of the clients within the Intranet. This is a major difference compared to the server-to-server communication. For this reason, it is important to protect the communication from the MX-ONE clients to the MX-ONE servers.

If the clients are used from the public Internet, the use of an IPSec-based VPN system is the best solution as it is not a recommended practice to open the corporate firewall for all ports used by the Personal Assistant clients.

3.5 CONNECTION TO PSTN AND PLMN

The MX-ONE can communicate with the Public Switched Telephony Network (PSTN) or the Public Land Mobile Network (PLMN) using the trunk interfaces. Such trunks are always located in the Media Gateway Classic or Media Gateway Lite.

To enhance the security of the system, ISDN signaling is always terminated in the Media Gateway Lite, or Media Gateway Classic. Communication with the MX-ONE Service Node is done by internal signaling protocols. Additionally, ISDN D-channel services are not implemented. This means that for example X.25 over an ISDN

D-channel is not allowed and it is thus not possible to access the LAN from an external line.

3.6 MOBILE EXTENSION

When using the Mobile Extension feature, security of the system is provided by mechanisms available in the mobile operator's network. It is recommended that the user make use of a PIN code to protect access to the phone and to prevent possible misuses of the system if the phone is lost.

3.7 ANALOG CONNECTIONS

The MX-ONE system supports the use of analog extensions. Only telephony services are supported through such interfaces. Data connections through Point-to-Point Protocol (PPP) using a modem are not possible to get access to the corporate LAN infrastructure.

4 PLATFORM SECURITY

The MX-ONE servers run on commercially available operating systems. From a security point of view, this is both an advantage and a disadvantage. The advantage is that these operating systems are being used by millions of users and security vulnerabilities are quickly discovered, announced and fixed. However the disadvantage is that these operating systems are the preferred target of the malicious crackers community.

4.1 MIVOICE MX-ONE

4.1.1 MX-ONE SERVICE NODE

The MX-ONE Service Node runs on the SUSE Linux Enterprise Server (SLES) operating system, which is the enterprise version of the well-known Linux distribution. One of the main advantages of this operating system is the enhanced security features that it is equipped with. It is worth mentioning that SLES is being evaluated for compliance with the Common Criteria Evaluation Assurance Level (EAL) 4+.

The MX-ONE Service Node is the most relevant node in the system whose security must be guaranteed to keep the system available. For this reason, beside the already strict security features of the operating system, a number of additional measures are enabled by default on the MX-ONE Service Node to improve its security, its reliability, and its resiliency to a number of malicious attacks.

Only needed packages of the operating system are installed on the MX-ONE Service Node. The SLES operating system is extremely feature-rich but the more features that are installed and enabled, the more are the potential security breaches. To decrease the risk of security vulnerabilities, the MX-ONE Service Node is delivered with only the necessary operating system packages installed by default.

Another important security measure is to only enable services and network ports that are necessary for the system's correct functioning. As an example, well known insecure services, such as Telnet and FTP are disabled by default. Additionally, the Linux packet filter IPTables has been configured to block access to certain services that are needed for the system but should not be reachable from the network interfaces connected to the corporate LAN. IPTables is also able to block certain kinds of attacks that have a well-known pattern and make use of certain deficiencies of the TCP/IP protocol stack.

To manage the server using the Command Line Interface, SSH is the preferred 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 need root access, the administrator first needs to log on as a non-root administrator and then require the system to be granted root privilege by performing a second authentication procedure.

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. It is however not activated default. All relevant system files can if AIDE is activated, be monitored and changes notified as soon as they are detected. The system administrator can of course 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.

The SLES operating system is equipped with a security tool named Seccheck. This tool is installed and enabled by default on the MX-ONE Service Node. Seccheck comprises three scripts that are run respectively each day, each week and each month. If some-

thing is detected that might indicate a security breach, a mail is sent to the root user with a description of the problem.

File permissions have to be accurately set, especially for those files that are relevant to the correct functioning of the system. The Linux operating system allows the use of the Least Necessary Privilege approach, the security golden rule that protects sensitive files of the system and avoids malfunctioning due to wrong configuration actions done by inexperienced users having accidentally gained access to the system.

4.1.2

MX-ONE MEDIA GATEWAY

The Media Gateway using the MGU provides VoIP security according to the SRTP protocol (RFC 3711), using data flow encryption with AES in Counter Mode (CM) and authentication with HMAC-SHA1.

To manage the Media Gateway using the Command Line Interface, SSH is the preferred solution. The Media Gateway can thus for trouble-shooting activities be logged on using SSH. To increase security, direct root access is disabled by default. If the system administrator needs to carry out some task that requires root access, the administrator first needs to log on as a non-root administrator, and then require the system to grant root privilege by performing a second authentication procedure.

See the Media Gateway Unit description for details.

4.2

MX-ONE MIVoice ADVANCED MESSAGING

The MX-ONE MiVoice Advanced Messaging server runs on the Microsoft Windows Server 2008 R2 or Microsoft Windows Server 2012 operating system. These versions of the well-known Windows operating system are supplied with much stronger security than its previous versions. For this reason, no further security measures are performed beside the ones already enabled by default on the operating system.

4.3

PATCH MANAGEMENT POLICY

As the MX-ONE components run on commercially available operating systems, vulnerabilities to these systems are discovered and fixed with high frequency. It is necessary to make sure that the MX-ONE components are always updated and equipped with all critical patches to guarantee the highest level of security. On the other hand, Mitel must guarantee the availability of the MX-ONE servers. In the unlikely event that a patch released by an operating system vendor should conflict with the MX-ONE software, the installation of such patch without prior testing would jeopardize the availability of the system.

To guarantee the availability of the MX-ONE system and hence the customer's satisfaction, Mitel recommends its customer not to modify (by for example installing not approved software) the Mitel products without prior verification and approval from Mitel.

Mitel has developed best practices as the management and installation of security patches released by the operating system vendors aiming to guarantee the highest level of security and the correct functioning of the system.

4.3.1

MX-ONE SERVICE NODE

Mitel constantly monitors updates released by the Operating System supplier. Concerning the Linux OS, patches and updates fixing several types of problems are

released daily. Some of them address security vulnerabilities that can be exploited to attack the system; such patches and updates must be installed as soon as possible.

In order to allow customers to keep a high security level without compromising the system's functionality, Mitel tests all patches and updates released by the OS suppliers that can be installed on the MX-ONE. In case one of these packages breaks the MX-ONE software preventing its correct functionality, Mitel will provide a hot fix solving the conflict, if deemed necessary by the nature of the update. A fix will always be provided for all security-related updates that conflict with the system functionality.

Mitel will make all OS patches and updates including possible conflict-fixing hot fixes available to customers regularly. Mitel is continuously working to decrease the time from the release date by the OS supplier until the OS patches and updates are available, but it is always guaranteed that the system functionality is not compromised.

4.3.2

MX-ONE MIVOICE ADVANCED MESSAGING

The MX-ONE MiVoice Advanced Messaging server runs on the Microsoft Windows 2008/2012 server. Microsoft has developed an efficient way of managing and classifying updates to their operating systems.

All updates released by Microsoft that are classified as *Critical updates* can be installed on the above-mentioned products without prior explicit approval from Mitel. In the unlikely event of a malfunctioning caused by any of these updates, the customer should contact Mitel (or its service partner) immediately and a Service Ticket with Priority A will be issued. This guarantees that the problem will be solved with the highest priority.

All updates released by Microsoft that are classified as *Recommended updates* should not be installed by the customer without prior approval from Mitel. Mitel guarantees to verify these updates before the release of the next service pack.

Occasionally, Microsoft releases service packs for their operating systems. Service packs have a broad scope and address problems of application compatibility, driver updates, reliability, security, and so on. Since Microsoft service packs include a broad range of changes, Mitel must thoroughly test all Computer Telephony Integration (CTI) products running on each service pack before we can support these service packs in the field. Therefore, before installing any new Microsoft service pack, it is necessary to check that it has been fully tested and qualified by Mitel. Use of unqualified service packs may prevent Mitel Technical Support from properly supporting customer installation.

4.4

ANTI-VIRUS POLICY

Virus attacks on the IS/IT infrastructure are becoming increasingly frequent. For this reason, a valid anti-virus policy is a necessary aspect of any valid security policy. The formulation of such a policy is a task that must be carried out by the IS/IT system administrator. Mitel, as a supplier of equipment that might be subject of a virus attack, guarantees that their products do not contrast with anti-virus policies in force in the IT environment.

4.4.1

MX-ONE SERVICE NODE

The MX-ONE Service Node is based on the Linux OS, which has traditionally only marginally been object of virus-related attacks. However, since there is a slight possibility to be hit by a virus targeting the Linux OS, it is possible to install anti-virus software on the MX-ONE Service Node, if desired.

When installing an anti-virus application containing more than anti-virus, all features except anti-virus must be disabled. Features such as firewall and integrity protection can safely be disabled in the anti-virus application since they are already covered by the hardening installed with the MX-ONE Service Node application.

When deploying anti-virus software, it is important to guarantee that the virus definition files are always updated.

Note: Mitel does not provide any anti virus applications with MX-ONE.

For mission critical applications, customers may want to use Trend Micro ServerProtect3.

However the following is recommended:

- Stop the AntiVirus service when upgrading the MX-ONE.
- Run the updates during low traffic time.
- Increase swap size on MX-ONE Service Node for matching your demand.
- As On-access real-time Anti Virus scanning is CPU and memory intensive task, customer may want to scan only a subset of all the files on the MX-ONE Service Node to avoid any performance degradation (for example, users directories only). Especially including logging directories in scan-list may incur some performance degradation in the MX-ONE Service Node.

4.4.2

MX-ONE MESSAGING

As a real-time system performing business-critical and computationally-intensive functions, MX-ONE Messaging cannot be expected to perform to specification if a third party application periodically makes essential Central Processor Unit (CPU), memory, and disk resources unavailable. The preferred solution is naturally to schedule virus scanning on a daily basis and during low server activity. The selected time should not coincide with scheduled daily maintenance or updates to the system. Should a periodic scan not be acceptable, the virus scanning software may have multiple configurations or approaches for continuous or active scans.

All virus scan solutions including periodic, active and continuous background scans of directories or disks may significantly impede operating system resources, and prevent Mitel products from responding as specified. It is the customer's responsibility to test the virus scanning software in conjunction with Mitel products during a high load condition to assure correct system operation. When configuring the virus scan software, the preferred choice will be the one that uses the least amount of CPU and generates the least amount of disk activity.

4.5

IP PHONES

The IP phones for the MX-ONE system are based on a Real-Time OS (RTOS) with strict control over which applications are running on the phones and with limited privileges. Additionally, only signed firmware can be uploaded on the phones. For these reasons, it is unlikely that such a phone can be infected by a virus or some other form of mal-ware. The IP phones are endowed with an SSH server to perform configuration and troubleshooting activities. The SSH server public and private keys are hard-coded in the phones and cannot be updated.

4.6

FIREWALLS

If an *external* firewall has to be used between MiVoice MX-ONE and IP terminals or between MiVoice MX-ONE, MiContact Center Enterprise and MiCollab Advanced Messaging or similar applications, where dynamic ports are involved, it is recommended to use a stateful firewall.

Stateless firewalls identify protocols connected on well-known ports like H.323-Q.931 on TCP port 1720. Although all the RTCP and RTP streams are negotiated by H.245, packet classifiers are unable to relate them to the parent protocols because they don't decode the protocols and recognize the dynamic port negotiations. Hence, all the subsequent audio (and video) streams are classified as general UDP traffic, unrelated to the H.323 application and can get blocked.

While in an alternative solution, stateful firewalls start analyzing packets at the beginning of the application, and maintain flow entries in a flow database to track and analyze the relationship of the evolving dynamic flows, which empowers the policy engine to correctly process every packet in every related flow to the end-application. All hierarchical (parent-child) relations are preserved.

5

OPERATION AND MAINTENANCE SECURITY

Management of the MX-ONE system is performed according to the FCAPS paradigm. In particular, the following mechanisms are available to manage the system:

- MX-ONE Service Node Manager: Web-based tool located on the MX-ONE Service Node used for system-wide configuration.
- MX-ONE Provisioning Manager: Web-based tool for user and extension management.
- Windows GUIs located on the MiCollab Advanced Messaging.
- Command Line Interface-based management of the MX-ONE Service Node.

5.1

MX-ONE SERVICE NODE MANAGER

The MX-ONE Service Node Manager is a Web-based tool that allows monitoring and configuration of a number of relevant objects.

To protect access to this tool, SSL in server authentication mode can be enabled during the installation procedure. The administrator (client/Web browser) will be authenticated by the means of username/password. It is assumed that the Web server has a valid pair of RSA keys and a digital certificate that can be verified by the client. This certificate can either be a self-signed certificate or issued by a well-known Certification Authority (CA). After successful authentication, the administrator is mapped to one of four possible administrator profiles, each of them holding different access privileges. The following four profiles are defined within MX-ONE Service Node Manager:

- Secretary/Administrator
- System Administrator
- Engineer
- Advanced Troubleshooter

For each operation requested by the administrator, the access privileges are checked against the requested privileges for that specific operation, thus implementing a fine-grained access control policy. The system administrator can configure the access privileges assigned to each role.

5.2

MX-ONE PROVISIONING MANAGER

Users and extensions are defined in MX-ONE Provisioning Manager and the data is automatically updated in the MX-ONE Service Node.

For more information, see the description for *MX-ONE Provisioning Manager*.

5.3 ENVIRONMENTS ENCRYPTION AND DECRYPTION FOR PM, SNM & CSTA PHASE III APPLICATIONS

5.3.1 INTRODUCTION

As part of 6.2 enhancement, you can encrypt entire environment. Also, you can encrypt the Server Logs and Database Backup files.

Whenever you enable the Environment encryption, files from below directories get encrypted.

Provisioning Manager Related Database Backup files:

- 1) /var/opt/eri_mp_config/
- 2) /var/opt/eri_mp
- 3) /var/opt/eri_mp/postgresdata/<pm_version_directories>

Service Node Manager Database Backup Files:

- 1) /var/opt/eri_om
- 2) /var/opt/eri_om/postgresdata/<SNM_version_directories>

Server Logs:

- 1) /opt/jboss/server/default/log/server.log
- 2) /opt/jboss/server/default/log/eri_jboss.log

Common Database Backup of all DBs(WBM,MP,QoS,Quartz):

- 1) /var/tmp/psql_data_archives/PM_SNM

5.3.2 ENABLING THE ENCRYPTION OF ENVIRONMENT

To enable the encryption of environment, execute the below commands:

- 1) Open webserver_config utility by executing `sudo -H webserver_config` command as `mxone_admin` user; or
- 2) Execute `sudo -H mxone_maintenance` as `mxone_admin` user, then select `webmanagement`.
- 3) Select Enable or Disable of Encryption of Environment as mentioned in the below screen.

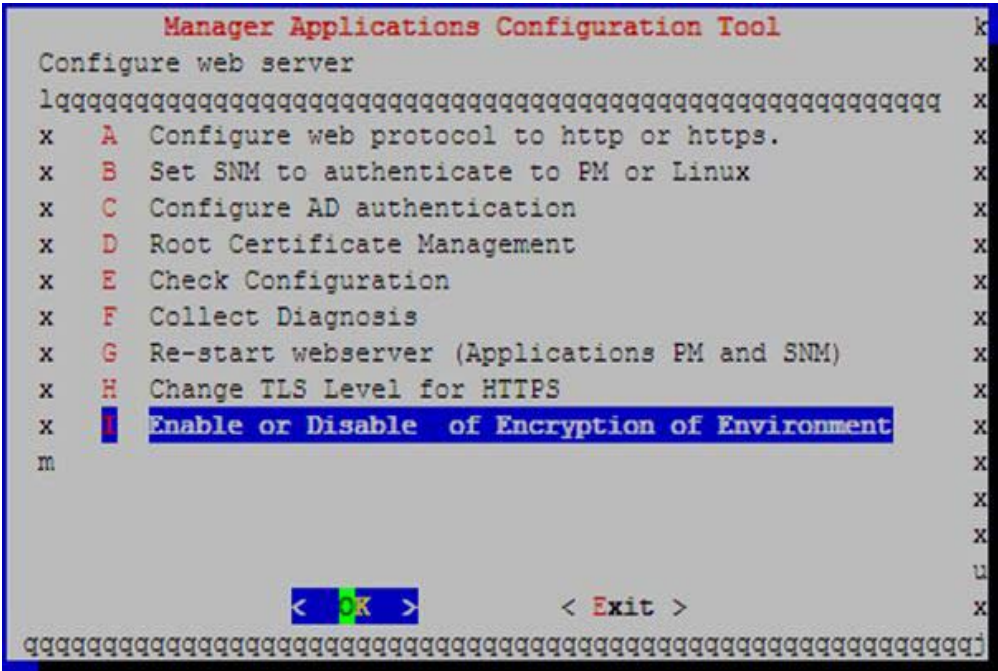


Figure 2: Selection of Option Enable or Disable of Environment

4) If Encryption is not enabled, it asks for confirmation to enable the Encryption.

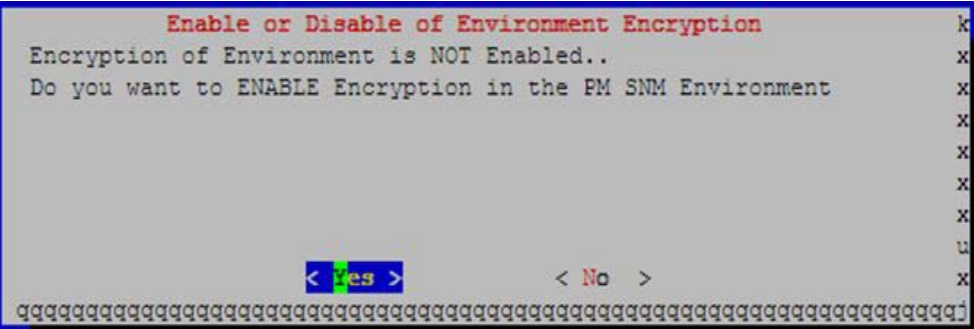


Figure 3: Confirmation of Encryption of Environment

5) Click **Yes** to view all the below screens.

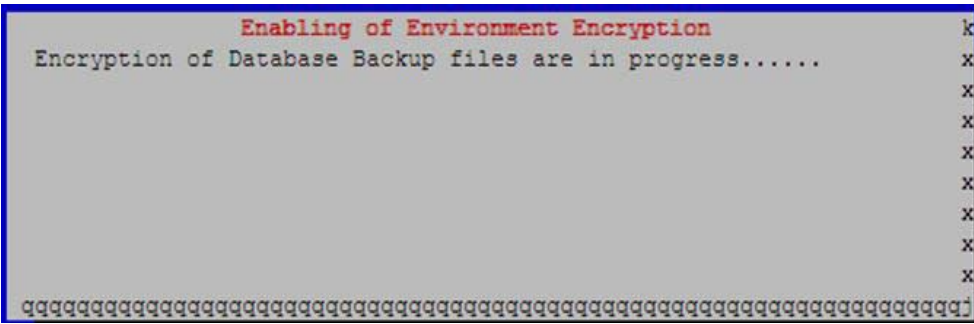


Figure 4: Environment Encryption is in progress

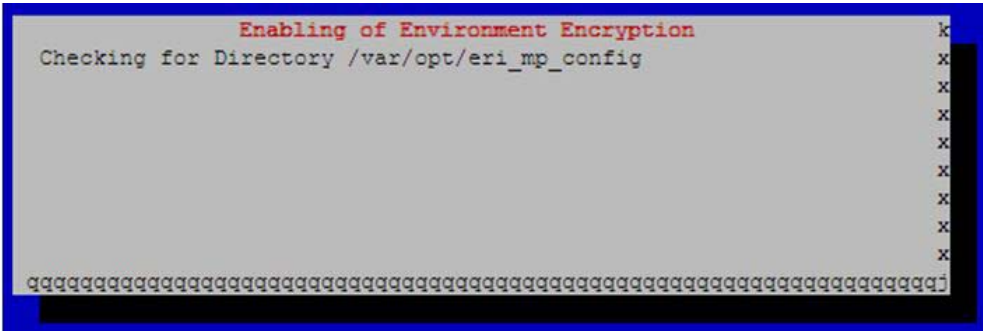


Figure 5: Environment Encryption is in progress

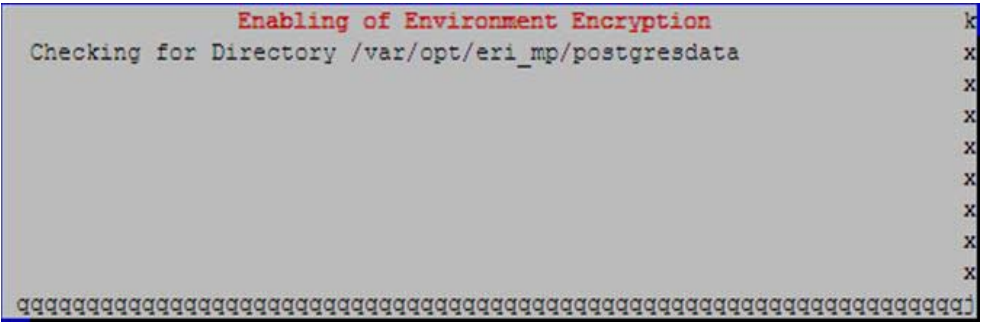


Figure 6: Environment Encryption is in progress

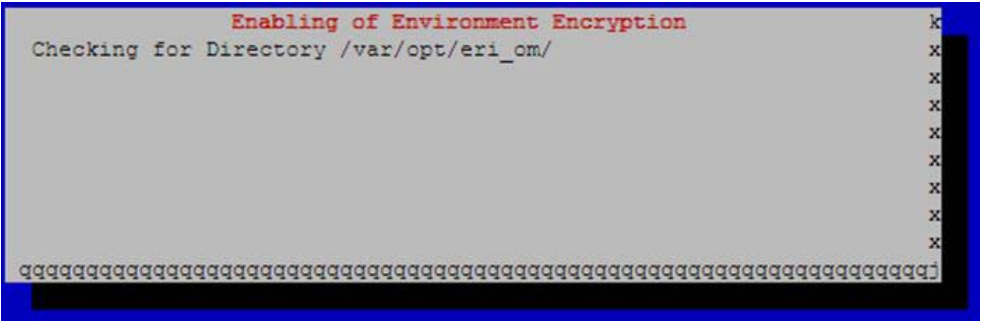


Figure 7: Environment Encryption is in progress

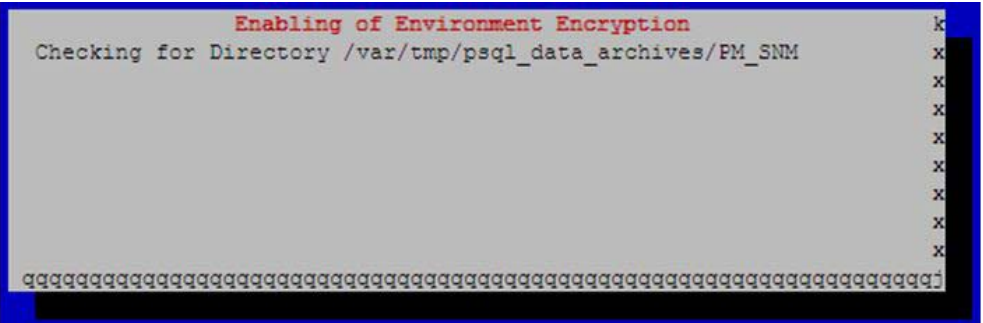


Figure 8: Environment Encryption is in progress

Once this procedure is completed, it encrypts all the files from above directories.

Note: Going forward in the environment whenever upgrade happens for PM/SNM/CSTA Phase III, the database related Backup files and Server Logs are encrypted.

A cron job is enabled, which encrypts the server logs (server.log, eri_jboss.log) in /opt/jboss/server/default/log.

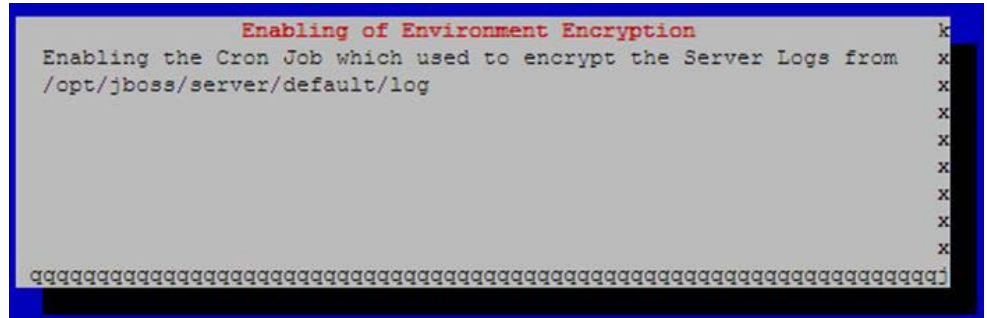


Figure 9: Enabling the Cron Job to encrypt the Logs in the environment

This cron job runs for every hour.



Figure 10: Enabling the Cron Job to encrypt the Logs in the environment

5.3.3

DISABLING THE ENCRYPTION OF ENVIRONMENT

To disable the encryption of environment, execute the below commands:

- 1) Open webserver_config utility by executing `sudo -H webserver_config` command as `mxone_admin` user; or,
- 2) Execute `sudo -H mxone_maintenance` as `mxone_admin` user, then select webmanagement.
- 3) Select Enable or Disable of Encryption of Environment as mentioned in the below screen.

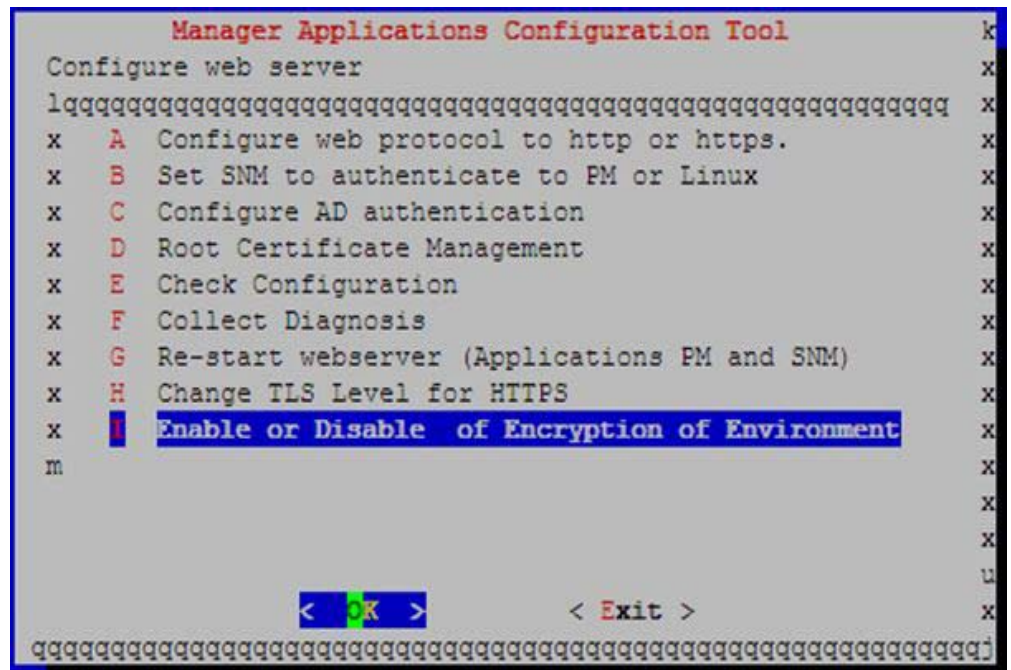


Figure 11: Selection of Option Enable or Disable of Environment

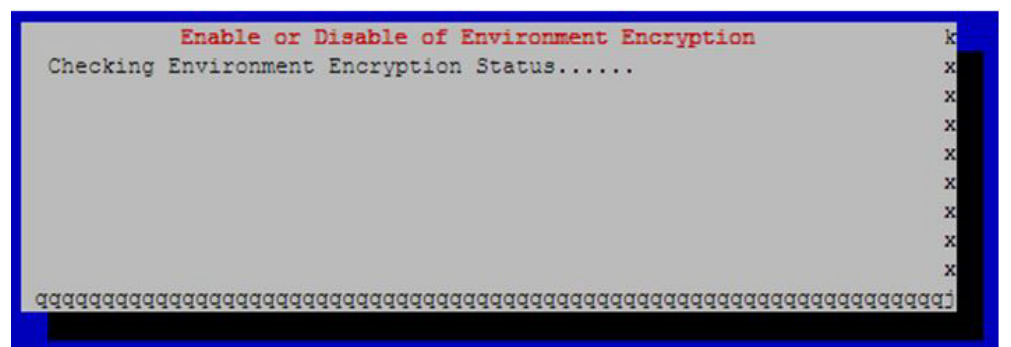


Figure 12: Checking Environment Encryption Status



Figure 13: Environment Encryption status confirmation

- 4) Click **Yes** to Disable the Encryption of Environment.

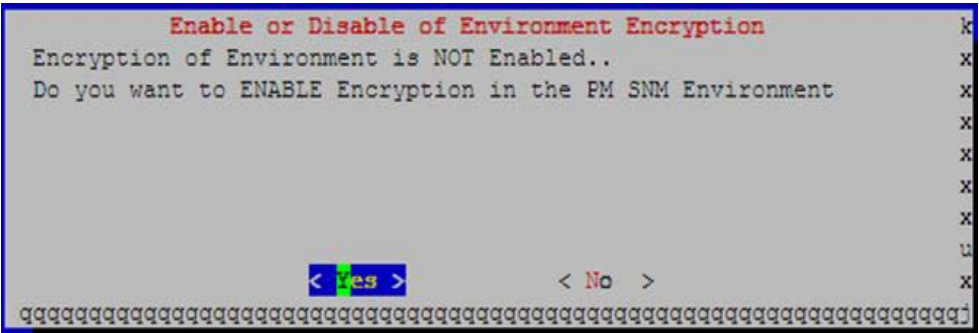


Figure 14: Confirmation of Encryption of Environment

- 5) Once clicked on **Yes**, it decrypts all the Database Backup and Server Logs (/opt/jboss/server/default/log/server.log,eri_jboss.log) from the below locations.

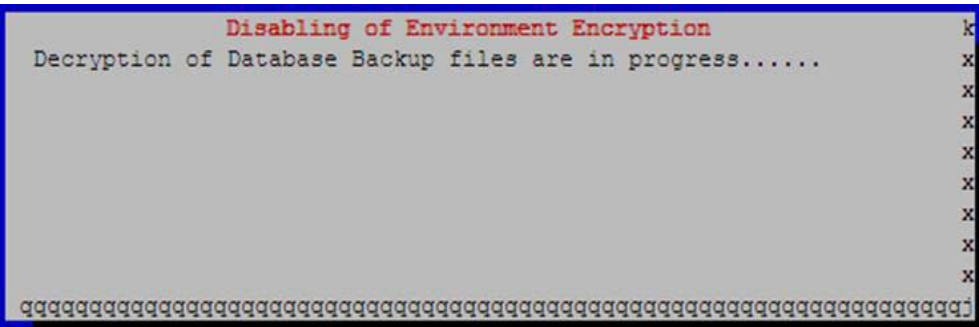


Figure 15: Decryption of Database Backup files are in progress

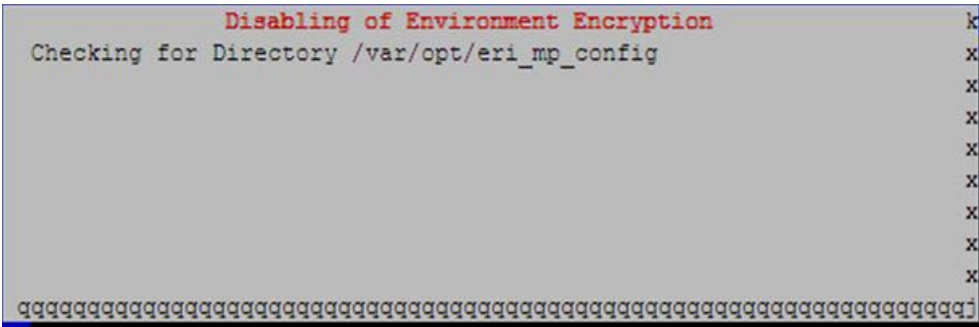


Figure 16: Disabling of Environment Encryption in progress

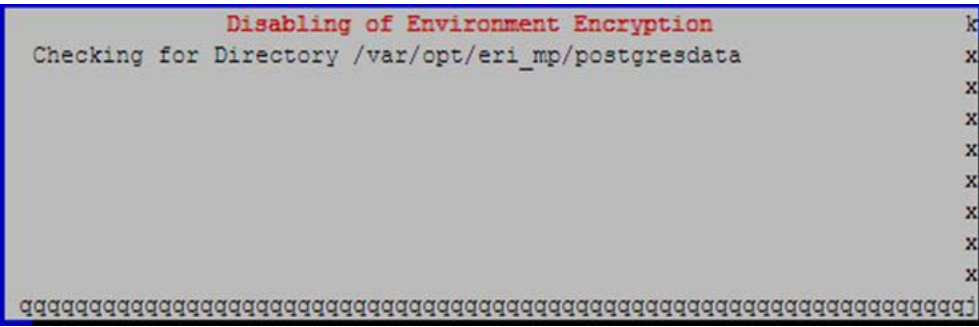


Figure 17: Disabling of Environment Encryption in progress

```

Disabling of Environment Encryption
Checking for Directory /var/opt/eri_om

```

Figure 18: Disabling of Environment Encryption in progress

```

Disabling of Environment Encryption
Checking for Directory /var/tmp/psql_data_archives/PM_SNM

```

Figure 19: Disabling of Environment Encryption in progress

Note: Since you have disabled Environment Encryption feature, going forward all the Backup and Server Logs will not be Encrypted.

It also disables the Cron Job entry from the system, which is used to encrypt the Server Logs periodically for every hour

```

Disabling of Environment Encryption
Disabling the Cron Job which used to encrypt the Server Logs from
/opt/jboss/server/default/log

```

Figure 20: Disable of Cron Job of Environment Encryption in progress

The cron job related field gets deleted from this location.

```

newmp-1:/opt/manager/webserver_config_sw # cd /etc/cron.d
newmp-1:/etc/cron.d # ls -lrt
total 8
-rw-r--r-- 1 root root 63 Jan 28 2015 novell.com-suse_register
-rw-r--r-- 1 root root 82 Oct 3 09:26 log_encryption_cron
newmp-1:/etc/cron.d #
newmp-1:/etc/cron.d #
newmp-1:/etc/cron.d # cat log_encryption_cron
0 * * * * root /etc/opt/webserver_install/webserver_templates/PMSNM_logencryption
newmp-1:/etc/cron.d #
newmp-1:/etc/cron.d #
newmp-1:/etc/cron.d #
newmp-1:/etc/cron.d #

```

Figure 21: Confirmation of Disable of Cron Job of Environment Encryption

5.3.4

DATABASE BACKUP FILE ENCRYPTION SCENARIOS

5.3.4.1

Provisioning Manager

5.3.4.1.1

mp_config utility

- a) **Database Backup:** When this option is selected and the environment is encrypted, the PM database (MP) backup file gets encrypted automatically and placed in `/var/opt/eri_mp_config`
- b) **Database Restore:** During the Restore, the Encrypted backup file will be decrypted and restored. Existing Backup file will remain encrypted. In case if the Environment Encryption is disabled, if the file is not encrypted, though it will restore the file.

5.3.4.1.2

Upgradation of PM Application

During the upgradation of PM application the temporary database backup files get encrypted if the Environment Encryption is enabled and Decrypted during the restore of post installation / upgrade of PM application.

All decrypted files get deleted and the existing encrypted files remain encrypted. During the upgrade scenario, PM Database data is taken as backup and stored in below directory with version specific directory. These backup files are used during the Roll-back.

`/var/opt/eri_mp/postgresdata/<Version Specific Directory>`

5.3.4.2

Service Node Manager

5.3.4.2.1

snm_backup

This is a new utility, which is created to take the backup of SNM database (WBM) data. When this utility is executed and the environment is encrypted, the SNM database (WBM) backup file is encrypted automatically and gets placed in `/var/opt/eri_om`.

5.3.4.2.2

snm_data_store

This utility is created to restore the SNM database data, which is taken as backup by snm_backup utility During the Restore. The Encrypted backup file is decrypted and restored. Existing Backup file remains encrypted. In case if the Environment Encryption is disabled, if the file is not encrypted, though it restores the file.

5.3.5

UPGRADATION OF SNM APPLICATION

During the upgradation of SNM application, the temporary database backup files get encrypted if the Environment Encryption is enabled and decrypted during the restore of post installation / upgrade of SNM application and those decrypted files get deleted. The Existing encrypted files remain encrypted.

During the upgrade scenario, SNM Database data is taken as backup and stored in below directory with version specific directory. These backup files are used during the Rollback.

/var/opt/eri_om/postgresdata/<Version Specific Directory>

5.3.6

PM_SNM_POSTGRESQL_DATA_BACKUP_AND_RESTORE UTILITY

This utility is created to take the backup of all Databases (MP, WBM, Qos, Quartz), which can be restored later. This utility is created for SLES upgrade scenario.

When this utility backup the databases if the Environment is encrypted and the backup file is encrypted. And, whenever you want to restore the above backup file. That file gets decrypted and restored. Those decrypted files are deleted. The Existing encrypted files remains encrypted.

5.4

SERVER LOG ENCRYPTION AND DECRYPTION

5.4.1

ENCRYPTION

These files get encrypted if the Environment encryption is enabled. As per the below screenshot the file names which end with numbers (for example, 1,2,3) are encrypted.

Note: Server.log and eri_jboss.log files are not encrypted, because these files still being locked by Jboss process.

```
newmp-1:/opt/jboss/server/default/log # ls -lrt
total 3516
drwxr-x---+ 10 jboss jboss    4096 Oct  3 06:10 mp
-rw-r-x---+  1 jboss jboss   221025 Oct  4 07:55 eri_jboss.log.3
-rw-r-x---+  1 jboss jboss    70431 Oct  4 08:09 boot.log
-rw-r-x---+  1 jboss jboss  2247253 Oct  4 23:21 server.log.3
-rw-r-x---+  1 jboss jboss    51310 Oct  4 23:21 server.log.2
-rw-r-x---+  1 jboss jboss    51261 Oct  4 23:21 server.log.1
-rw-r-----  1 root  root   162656 Oct  4 23:21 eri_jboss.log.3_temp
-rw-r-x---+  1 jboss jboss    51300 Oct  4 23:21 eri_jboss.log.2
-rw-r-x---+  1 jboss jboss    51322 Oct  4 23:21 eri_jboss.log.1
drwxr-x---+  7 jboss jboss    4096 Oct  5 00:00 setasm
-rw-r-x---+  1 jboss jboss   358853 Oct  5 00:54 server.log
-rw-r-x---+  1 jboss jboss   267217 Oct  5 00:54 eri_jboss.log
newmp-1:/opt/jboss/server/default/log #
```

Figure 22: Confirmation of Disable of Cron Job of Environment Encryption

5.5

SERVER LOG ENCRYPTION AND DECRYPTION

5.5.1

DECRYPTION

Execute below utility in your system:

- 1) In Sudo -H webserver_config, select **Other Utilities** and **Log Decryption**.
- 2) Displays all the encrypted server files column wise ([Sequence No.][File Details]) as displayed in the below screenshot.

```
Below are list of Encrypted Log Files available. You can select to decrypt the logs
selection pattern can be all/1-5/1,3-5,6
-----
[1]  -rw-r-xr--+ 1 jboss jboss 302080 Dec 30 05:40 /opt/jboss/server/default/log/server.log.14
[2]  -rw-r-xr--+ 1 jboss jboss 69510 Dec 30 05:41 /opt/jboss/server/default/log/server.log.13
[3]  -rw-r-xr--+ 1 jboss jboss 69400 Dec 30 05:41 /opt/jboss/server/default/log/server.log.12
[4]  -rw-r-xr--+ 1 jboss jboss 69400 Jan 4 05:31 /opt/jboss/server/default/log/server.log.11
[5]  -rw-r-xr--+ 1 jboss jboss 69420 Jan 4 05:32 /opt/jboss/server/default/log/server.log.10
[6]  -rw-r-xr--+ 1 jboss jboss 69400 Jan 4 05:33 /opt/jboss/server/default/log/server.log.9
[7]  -rw-r-xr--+ 1 jboss jboss 69400 Jan 5 00:31 /opt/jboss/server/default/log/server.log.8
[8]  -rw-r-xr--+ 1 jboss jboss 69420 Jan 5 00:32 /opt/jboss/server/default/log/server.log.7
[9]  -rw-r-xr--+ 1 jboss jboss 69400 Jan 5 00:32 /opt/jboss/server/default/log/server.log.6
[10] -rw-r-xr--+ 1 jboss jboss 69615 Jan 6 00:51 /opt/jboss/server/default/log/server.log.5
[11] -rw-r-xr--+ 1 jboss jboss 71005 Jan 6 00:51 /opt/jboss/server/default/log/server.log.4
[12] -rw-r-xr--+ 1 jboss jboss 69485 Jan 9 05:41 /opt/jboss/server/default/log/server.log.3
[13] -rw-r-xr--+ 1 jboss jboss 69530 Jan 9 05:41 /opt/jboss/server/default/log/server.log.2
[14] -rw-r-xr--+ 1 jboss jboss 69550 Jan 9 05:42 /opt/jboss/server/default/log/server.log.1
[15] -rw-r-xr--+ 1 jboss jboss 69510 Jan 4 05:33 /opt/jboss/server/default/log/eri_jboss.log.9
[16] -rw-r-xr--+ 1 jboss jboss 69380 Jan 4 05:34 /opt/jboss/server/default/log/eri_jboss.log.8
[17] -rw-r-xr--+ 1 jboss jboss 221793 Jan 5 00:30 /opt/jboss/server/default/log/eri_jboss.log.10
[18] -rw-r-xr--+ 1 jboss jboss 69445 Jan 5 00:32 /opt/jboss/server/default/log/eri_jboss.log.6
[19] -rw-r-xr--+ 1 jboss jboss 69420 Jan 5 00:33 /opt/jboss/server/default/log/eri_jboss.log.5
[20] -rw-r-xr--+ 1 jboss jboss 74515 Jan 6 00:51 /opt/jboss/server/default/log/eri_jboss.log.4
[21] -rw-r-xr--+ 1 jboss jboss 308393 Jan 9 05:40 /opt/jboss/server/default/log/eri_jboss.log.7
[22] -rw-r-xr--+ 1 jboss jboss 69510 Jan 9 05:42 /opt/jboss/server/default/log/eri_jboss.log.2
[23] -rw-r-xr--+ 1 jboss jboss 69380 Jan 9 05:42 /opt/jboss/server/default/log/eri_jboss.log.1
[24] -rw-r-xr--+ 1 jboss jboss 220505 Jan 9 05:45 /opt/jboss/server/default/log/eri_jboss.log.3
-----
Enter selection pattern:
```

Figure 23: Selection of Log Files

- 3) From the above list select the files to be decrypted.

Note: A set of pattern is followed to decrypt the files which is mentioned below.

- 4) Enter the file number to decrypt the file.
- 5) Enter the sequence pattern like 3-6 if you want to range files from sequence number 3 to sequence number 6.
- 6) If want to select the files in range and other individual files like range start from 3 to 6 and 7,9 as individual, the you can enter like 3-6,7,9, and so on.

Note: This always asks for confirmation to decrypt the files by displaying selected files. After confirmation it decrypts those files and stores with file extension of “_temp”.

```

newamp-1:/opt/jboss/server/default/log # ls -lrt
total 3516
drwxr-x---+ 10 jboss jboss    4096 Oct  3 06:10 mp
-rw-r-x---+  1 jboss jboss   221025 Oct  4 07:55 eri_jboss.log.3
-rw-r-x---+  1 jboss jboss    70431 Oct  4 08:09 boot.log
-rw-r-x---+  1 jboss jboss  2247253 Oct  4 23:21 server.log.3
-rw-r-x---+  1 jboss jboss    51310 Oct  4 23:21 server.log.2
-rw-r-x---+  1 jboss jboss    51261 Oct  4 23:21 server.log.1
-rw-r-x---+  1 jboss jboss    51300 Oct  4 23:21 eri_jboss.log.2
-rw-r-x---+  1 jboss jboss    51322 Oct  4 23:21 eri_jboss.log.1
drwxr-x---+  7 jboss jboss    4096 Oct  5 00:00 certsm
-rw-r-x---+  1 jboss jboss  358853 Oct  5 00:54 server.log
-rw-r-x---+  1 jboss jboss  267217 Oct  5 00:54 eri_jboss.log
-rw-r-----  1 root  root   162656 Oct  5 02:47 eri_jboss.log.3_temp
newamp-1:/opt/jboss/server/default/log #

```

Figure 24: Decryption of Files with File Extension

5.6 ROLLBACK SCENARIO

The rollback of PM/SNM application is required if the older version is less than 6.2. So, you need to disable the Environment Encryption and then trigger for rollback.

5.7 WINDOWS GUI

The Messaging server is running on the Microsoft Windows Server 2008 operating system. All management operations related to the operating system need to be carried out through Windows-specific GUIs. Additionally, the Messaging server is equipped with a proprietary GUI in order to carry out system configuration activities. Access to these GUIs requires physical access to the host where the tool is being installed. Standard Windows security applies for controlling access to the hosts.

It is possible to gain remote access to the host where the Messaging Server is installed by making use of the PcAnywhere tool, which has been tested for this purpose. In this case, security features provided by the tool apply.

5.8 CLI-BASED MANAGEMENT OF MIVOICE MX-ONE

Most of the management operations necessary on the MX-ONE are carried out through a proprietary Command Line Interface known as MD-shell. In order to have access to this tool remotely, SSH shall be used to log on to the system. It is obviously necessary to set up authentication keys before being able to use SSH.

5.8.1 PROTECTION MECHANISM OF THE MD-SHELL

The MD-shell is a console-based mechanism to manage the MX-ONE Service Node. All possible management operations can be performed by the means of this tool, which makes it very powerful but also potentially dangerous. It is built on top of the Linux bash shell, which in turn is built on top of the operating system kernel.

It is necessary to guarantee that only authorized users (administrators) can manage the system; additionally, different groups of administrators might have different privileges. The MX-ONE Service Node defines eight different levels of user privileges for managing the system. Each time a command is issued by an administrator, the required privilege level to issue that command is checked against the privilege level assigned to the administrator issuing the command: if it is higher, the command is not performed. The root user is automatically assigned the highest privilege level, that is seven.

The mapping between different commands to access privileges is stored in a configuration file that can only be modified by the root user. Additionally, it contains the mapping between Linux user groups and access privileges. The following briefly describes which operations are entitled to the different access privilege levels:

- Level 0: Visualizing of non-sensitive system configuration
- Level 1: Some Unix non-sensitive commands, call diversion, some operator-related operations
- Level 2: Operations on analog, IP, and generic extension, operations concerning abbreviated dialing
- Level 3: Simple accounting operations, number analysis, simple routing
- Level 4: Logging-related and dump operations, interception service, blocking operations, configuration, traffic recording
- Level 5: Inter-Server signaling, Control system, LIM switch
- Level 6: Advanced management operations
- Level 7: Advanced troubleshooting; advanced diagnostic tools; advanced configuration, system-critical operations

5.9

SNMP

When monitoring the system with SNMP, it is only possible to read data that is not considered sensitive. It is not possible to set the value of a MIB II object.

6

EVENT LOGGING

All MX-ONE components log relevant events using tools available on the target operating system and MX-ONE specific tools or files.

The MX-ONE has two main types of logs. The actual telephony application makes use of the common Linux logger known as Syslog. The MX-ONE Service Node Manager allows the administrator to view relevant logs through its Web interface.

The Mitel Advanced Messaging in MX-ONE is also equipped with a number of tools to monitor and visualize information concerning mailboxes, port usage, call handling statistics, network activity report, subscribers' setup, and so on.