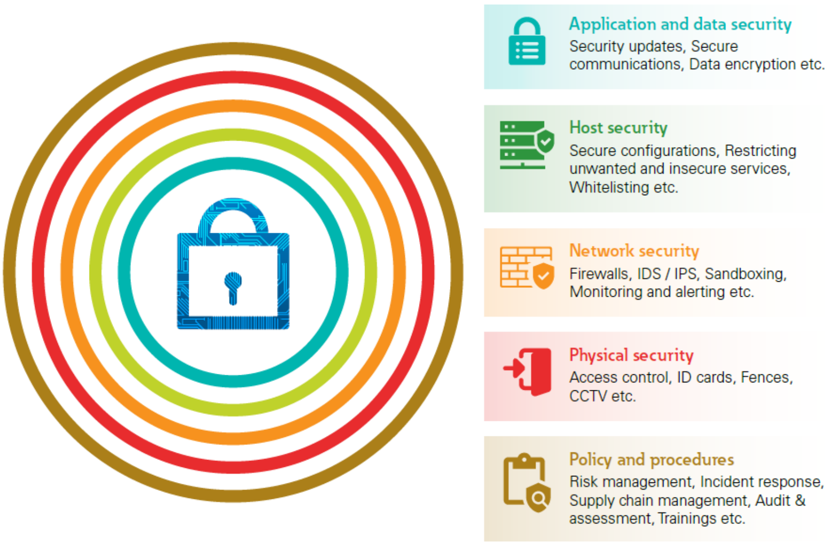
MN152296EN Effective February, 2025 Foreseer 7.9.200

Foreseer

Message Manager Recommended Security Hardening Guidelines

EATON
Powering Business Worldwide

Message Manager Secure Configuration Guidelines

Category	Description
Intended Use and Deployment	Message Manager is a component of Foreseer and is designed to allow alarm and events generated and managed by the system to be communicated across SMTP, SNMP and other services as they are added and supported into the product platform.
Asset identification and Inventory	Keeping track of all the devices in the system is a prerequisite for effective management of Cybersecurity of a system. Ensure you maintain an inventory of all the components in your system in a manner that uniquely identifies each component.
Defense in Depth	Defense in Depth basically means applying multiple counter-measures for mitigating risks, in a layered or step wise manner. A layered approach to security as shown in the below diagram is what is recommended. Defense in Depth is the responsibility of both the manufacturer and the customer.  Application and data security Security updates, Secure communications, Data encryption etc. Host security Secure configurations, Restricting unwanted and insecure services, Whitelisting etc. Network security Firewalls, IDS / IPS, Sandboxing, Monitoring and alerting etc. Physical security Access control, ID cards, Fences, CCTV etc. Policy and procedures Risk management, Incident response, Supply chain management, Audit & assessment, Trainings etc.
COTS Platform Security	Eaton recommends that customers harden third-party commercial off-the-shelf (COTS) operating systems or platforms that are used to run Eaton applications / products (e.g., third party hardware, operating systems and hypervisors, such as those made available by Dell, Microsoft, VMware, Cisco, etc.).

Category	Description
	- Eaton recommends that customers refer to the COTS vendor's documentation for guidance on how to harden these components. - Vendor-neutral guidance is made available by the Center for Internet Security https://www.cisecurity.org/ Irrespective of the platform, customers should consider the following best practices: - Install all security updates made available by the COTS manufacturer. - Change default credentials upon first login. - Disable or lock unused built-in accounts. - Limit use of privileged generic accounts (e.g., disable interactive login). - Change default SNMP community strings. - Restrict SNMP access using access control lists. - Disable unneeded ports & services.
Account Management	Logical access to the system | device should be restricted to legitimate users, who should be assigned only the privileges necessary to complete their job roles/functions. Some of the following best practices may need to be implemented by incorporating them into the organization's written policies: - Ensure default credentials are changed upon first login - Message Manager should not be deployed in production environments with default credentials, as default credentials are publicly known. - No account sharing – Each user should be provisioned a unique account instead of sharing accounts and passwords. Security monitoring/logging features in the product are designed based on each user having a unique account. Allowing users to share credentials weakens security. - Restrict administrative privileges - Attackers seek to gain control of legitimate credentials, especially those for highly privileged accounts. Administrative privileges should be

Category	Description
	assigned only to accounts specifically designated for administrative duties and not for regular use. • Leverage the roles / access privileges to provide tiered access to the users as per the business /operational need. Follow the principle of least privilege (allocate the minimum authority level and access to system resources required for the role). • Perform periodic account maintenance (remove unused accounts). • Ensure password length, complexity and expiration requirements are appropriately set, particularly for all administrative accounts (e.g., minimum 10 characters, mix of upper- and lower-case and special characters, and expire every 90 days, or otherwise in accordance with your organization’s policies). • Enforce session time-out after a period of inactivity.
Time Synchronization	Many operations in power grids and IT networks heavily depend on precise timing information. Ensure the system clock is synchronized with an authoritative time source (using manual configuration, NTP, SNTP, or IEEE 1588). For additional information on server time synchronization, refer to Windows operating system embedded help for additional details. Refer to the following link as a starting point: https://learn.microsoft.com/en-us/windows-server/networking/windows-time-service/windows-time-service-tools-and-settings
Physical Protection	Industrial control devices lack cryptographic protections at protocol level, at physical ports and at controller mode switches leaving them exposed to Cybersecurity risk. Physical security is an important layer of defense in such cases. Foreseer is designed with the consideration that it would be deployed and operated in a physically secure location.

Category	Description
	For details on how to securely deploy Message Manager, please refer to the Message Manager Guide for additional information.
Authorization and Access Control	Message Manager runs as a Windows service with no remote external user interface. Should configuration changes be necessary, access to the operating system is required by a privileged user. It is extremely important to securely configure the logical access mechanisms provided in the core operating system to safeguard from unauthorized access. Eaton recommends to use proper configuration ans ensure access to the system is restricted to legitimate users only. And, such users are restricted to only the privilege levels necessary to complete their job roles/functions. • Ensure default credentials are changed upon first login. Foreseer should not be commissioned for production with Default credentials; it’s a serious Cybersecurity flaw as default credentials may be published in manuals. • No password sharing – Make sure each user is assigned their own unique and dedicated password vs. sharing passwords. Security monitoring features of Foreseer are created with the expectation that each user has their own unique password. Security controls are weakened as soon as the users start sharing the password. • Restrict administrative privileges - Threat actors are increasingly focused on gaining control of legitimate credentials, especially those associated with highly privileged accounts. Limit privileges to only those needed for a user’s duties. • Perform periodic account maintenance (remove unused accounts). • Change passwords and other system access credentials whenever there is a personnel change.
Network Security	Message Manager is designed to send alarm and event notifications generated by the Foreseer software platform as SMTP email messages, SNMP trap notifications, as well as other services as they are supported and added to the product. The default configuration of Message Manager assumes that it will be installed on the same application server where Foreseer resides, and uses a secured connection.

Category	Description
	Message Manager can also be deployed on a remote machine for the purpose of redundancy. In order for a remote machine with Message Manager installed to be used, the Foreseer instance must be configured to explicitly permit a Message Manager connection from a remote machine by defining it's IP address or resolvable name. Refer to the Foreseer Server Guide for details on how to do so. From a high level: • Eaton recommends segmentation of networks into logical enclaves and restricting the communication to host-to-host paths. This helps protect sensitive information and critical services, and limits damage from network perimeter breaches. At a minimum, a utility Industrial Control Systems network should be segmented into a three-tiered architecture (as recommended by NIST SP800-82[R3]) for better security control. • Deploy adequate network protection devices like Firewalls, Intrusion Detection / Protection devices. • Work with your Network Service Provider (local or service-based) to ensure inbound and outbound data streams are secured and maintained in according with your organization's local policies. Please review detailed information about various Network level protection strategies in Eaton Cybersecurity Considerations for Electrical Distribution Systems [R1]. Use the below information for configuring the firewalls to allow needed access for Foreseer to operate smoothly. The following additional network security controls should be considered when deploying Message Manager for use with Foreseer. • Message Manager uses port 444 to establish an encrypted connect to Foreseer for receiving alarm and event data. This ports should be allowed in firewall for uninterrupted operation. The port may be modified to suit your site's specific security implementation. Consult the *Foreseer Server Guide* as well as *Message Manager Configuration Guide* for information on changing this port. • Email restrictions: If you are using SMTP mail services with Message Manager, only permit access to the necessary mail server ports defined by the mail service provider. In addition, you should use TLS/STARTTLS options whenever

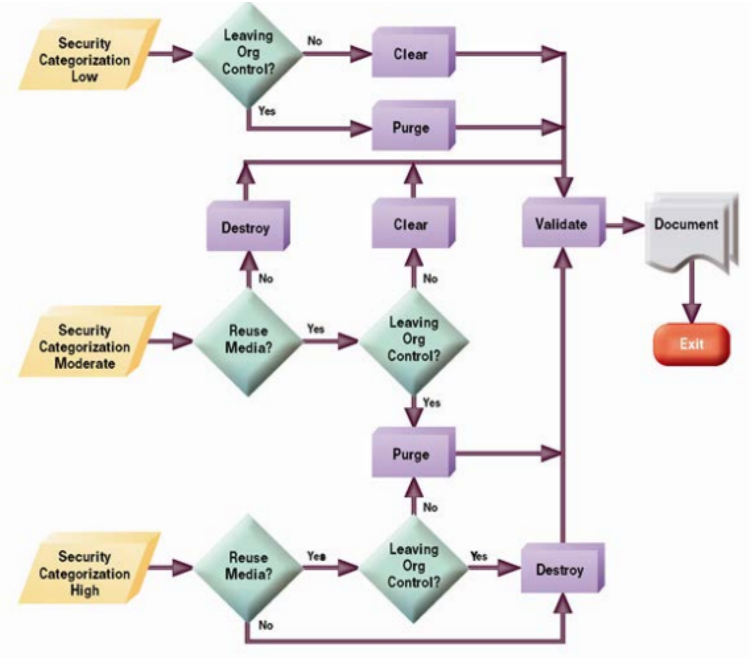
Category	Description
	possible along with secure credentials. Some mail providers now require you to create an "app-password" dedicated solely to a mail client like Message Manager. Refer to the service provider for additional assistance. TCP port configuration will vary depending on the mail service provider. • Simple Network Management Protocol (SNMP): Simple SNMP uses UDP Port 162 for trap transmission. The port should be allowed in firewall for uninterrupted operation. The port may be modified to suit your site's specific security implementation or to match a destination endpoint. • SNMPv1 & v2c Information: SNMPv1 and v2c are inherently insecure. Data is sent in plain text with no encryption or privacy options. Support for trap messages using either revision must be explicitly enabled in Message Manager. Ensure you are taking additional measures to secure traffic on these protocol versions beyond the scope of Message Manager. • SNMPv3 information: SNMPv3 provides additional security measures beyond that of v1 and v2c. Support for v3 by third-party network management software products vary. Ensure you are taking additional security measures to secure traffic on this protocol version beyond the scope of Message Manager. • Use the SNMPv3 User Security Model (USM): The User Security Model (USM) of v3 is intended to provide additional security measures beyond v1 and v2c. USM supports both an authentication protocol using secure digest, as well as a privacy protocol using select encryption protocol standards. v3 can be used without USM for backwards compatibility - which sends data in plain-text. More so, v3 standards also date back to using MD5 and DES standard which are now considered inherently insecure. Always use both authentication and privacy protocols whenever possible with a minimum of SHA256/AES256. Endpoint destinations are responsible for controlling what is possible for USM. Message Manager must match the same username, authentication and privacy protocols, along with their respective passwords. • Traffic control and filtering: Configure your host based firewall to limit unnecessary traffic. Please refer to the *Message Manager Configuration Guide* for more information on product setup.
	Remote access to device/systems creates another entry point

Category	Description
Remote Access	into the network. Strict management and validation of termination of such access is vital for maintaining control over overall ICS security. As a software service to Windows with no remote access, no additional steps are needed to secure the Message Manager service itself for Remote Access.
Logging and Event Management	• Eaton recommends logging all relevant system and application events, including all administrative and maintenance activities. • Logs should be protected from tampering and other risks to their integrity (for example, by restricting permissions to access and modify logs, transmitting logs to a security information and event management system, etc.). • Ensure that logs are retained for a reasonable and appropriate length of time. • Review the logs regularly. The frequency of review should be reasonable, taking into account the sensitivity and criticality of the system or device and any data it processes. By default, basic logging of data is enabled with the Message Manager application. Data is stored securely in the Windows Event Viewer application and can be accessed by well privileged users of the operating system. In certain situations where additional output is needed for troubleshooting purposes. Refer to the *Testing Notifications* section of the Message Manager Configuration Guide for more details.
Vulnerability Scanning	It is possible to install and use third-party software with Message Manager. Any known critical or high severity vulnerabilities on third party component/libraries used to run software /applications should be remediated before putting the device | system into production. • Eaton recommends running a vulnerability scan to identify known vulnerabilities for software used with the product. For COTS components (e.g., applications running on Windows), vulnerabilities can be tracked on the National Vulnerability Database (NVD), available at https://nvd.nist.gov/. • Keep software updated by monitoring security patches made available by COTS vendors and installing them as soon as

Category	Description
	possible. *Note: Many compliance frameworks and security best practices require a monthly vulnerability review. For many non-COTS products vulnerabilities will be communicated directly through the vendor site.*
Malware Defenses	Eaton recommends deploying adequate malware defenses to protect the product or the platforms used to run the Eaton product.
Secure Maintenance	● Apply Firmware updates and patches regularly ● Due to increasing Cyber Attacks on Industrial Control Systems, Eaton implements a comprehensive patch and update process for its products. Users are encouraged to maintain a consistent process to promptly monitor for fresh firmware updates, implement patching and updates as and when required or released. ● CST, Customer Success Team is available for customer to contact at: o **For callers within the domestic United States.** ▪ **1-800-498-2678, Opt 2, 5, 1, then 2** o **For callers outside of the United States** ▪ **1-828-651-0786, Opt 2, 5, 1, then 2** o **Email** ▪ **cst@eaton.com** ● Customer notification and update process is manually managed through our Customer Care Contracts administration and through CST. Future notification and delivery methods are being reviewed to determine how/if we can provide them electronically but that is currently not an option. ● Eaton also has a robust vulnerability response process. In the event of any security vulnerability getting discovered in its products, Eaton patches the vulnerability and releases information bulletin through its cybersecurity web site - http://eaton.com/cybersecurity ● Please contact CST, immediately in case of any vulnerability found in Foreseer. ● Conduct regular Cybersecurity risk analyses of the organization /system.

Category	Description
	Eaton has worked with third-party security firms to perform system audits, both as part of a specific customer's deployment and within Eaton's own development cycle process. Eaton can provide guidance and support to your organization's effort to perform regular cybersecurity audits or assessments. Plan for Business Continuity / Cybersecurity Disaster Recovery It's a Cybersecurity best practice for organizations to plan for Business continuity. Establish an OT Business Continuity plan, periodically review and, where possible, exercise the established continuity plans. Make sure offsite backups include: ● Backup of the latest software installation .MSI file of Foreseer. Make it a part of SOP to update the backup copy as soon as the latest version software installation .MSI file is installed on Foreseer. ● Backup of the most current configurations. ● Documentation of the most current User List. ● Save and store securely the current configurations of the device.
Business Continuity / Cybersecurity Disaster Recovery	**Plan for Business Continuity / Cybersecurity Disaster Recovery** Eaton recommends incorporating Message Manager into the organization's business continuity and disaster recovery plans. Organizations should establish a Business Continuity Plan and a Disaster Recovery Plan and should periodically review and, where possible, exercise these plans. As part of the plan, important system | device data should be backed up and securely stored, including: ● Updated firmware and software related to Message Manager. Make it a part of standard operating procedure to update the backup copy as soon as the latest firmware is updated. ● Maintain the current configuration. ● Documentation of the current permissions / access controls, if not backed up as part of the configuration. ● Create a full system image and backup of the Windows operating system in its entirety.

Category	Description
Customer Application Security	Message Manager provides a platform on which customers can customize and host applications according to their requirements. Security vulnerabilities in these applications may expose the underlying device to attack. Eaton recommends observing best practices for secure system development when customers develop and host an application on the device: • Privacy and Security by Design: The application should take security and privacy into consideration from the outset, including at the stage of defining requirements and assessing the associated risks. • Communication Protection: If the application communicates over the network, Eaton recommends encrypting the communications in accordance with the applicable level described by the FIPS 140-2 standard. • Access Enforcement: The application should provide the ability to enforce access controls to protect the application against unauthorized access and to protect accounts against unauthorized authentication attempts (for example, through account lockout). • Least Privilege: Any application developed by the customers should not run with root account privileges. The root account has full control over and access to the operating system. Therefore, if an application that requires root privileges has any security vulnerability, it endangers the entire system. • Input Checking: All input to the application should be sanitized before storing and processing by the application to protect against malicious code injection. • Output Handling: Data output by the application for user consumption, including error messages, should be appropriately handled to avoid revealing important information about the application and the underlying system. • Password Management: The application should securely store and transmit credentials (for example, encrypting authentication traffic, and salting and hashing passwords in transit and at rest). Password complexity should be implemented, and password should be masked when entered on-screen. • Secure Coding Practices: Follow secure coding practice while developing applications for the device (for example, implementing multiple security layers, verifying authorization for all requests, conducting code reviews, etc.).

Category	Description
	• Administration Interface: The interface for administering the application should be separated from the end-user interface. • Session Controls: All application sessions should be encrypted, logged and monitored. • Event Log Generation: The application should have the capability to log security related events at a minimum, including the time, date, and user.
Sensitive Information Disclosure	Eaton recommends that sensitive information (i.e. connectivity, log data, personal information) that may be stored by Foreseer be adequately protected through the deployment of organizational security practices.
Decommissioning or Zeroization	It is a best practice to purge data before disposing of any device containing data. Guidelines for decommissioning are provided in NIST SP 800-88. Eaton recommends that products containing embedded flash memory be securely destroyed to ensure data is unrecoverable.  Security Categorization Low Leaving Org Control? No Yes Clear Purge Destroy Clear Validate Document Exit Security Categorization Moderate Reuse Media? Yes No Leaving Org Control? No Yes Purge No Security Categorization High Reuse Media? Yes No Leaving Org Control? Yes Destroy **Figure 4-1: Sanitization and Disposition Decision Flow** ** Figure and data from NIST SP800-88* • **Embedded Flash Memory on Boards and Devices** • Eaton recommends the following methods for disposing of

Category	Description
	motherboards, peripheral cards such as network adapters, or any other adapter containing non-volatile flash memory. • **Purge**: If the flash memory can be easily identified and removed from the board, the flash memory may be destroyed independently of the board that contained the flash memory. Otherwise, the whole board should be destroyed. • **Destroy**: Shred, disintegrate, pulverize, or incinerate by burning the device in a licensed incinerator.

References

[R1] Cybersecurity Considerations for Electrical Distribution Systems (WP152002EN): http://www.eaton.com/ecm/groups/public/@pub/@eaton/@corp/documents/content/pct_1603172.pdf

[R2] Cybersecurity Best Practices Checklist Reminder (WP910003EN): https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/white-papers/WP910003EN.pdf

[R3] NIST SP 800-82 Rev 2, Guide to Industrial Control Systems (ICS) Security, May 2015: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

[R4] National Institute of Technology (NIST) Interagency "Guidelines on Firewalls and Firewall Policy, NIST Special Publication 800-41", October 2009: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf

[R5] NIST SP 800-88, Guidelines for Media Sanitization, September 2006: http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=50819

[R6] A Summary of Cybersecurity Best Practices - Homeland Security https://www.hsdl.org/?view&did=806518

Copyright

Message Manager Recommended Security Hardening Guidelines – 7.9.200

Publication date 02/2025

EATON CORPORATION - CONFIDENTIAL AND PROPRIETARY NOTICE TO PERSONS RECEIVING THIS DOCUMENT AND/OR TECHNICAL INFORMATION THIS DOCUMENT, INCLUDING THE DRAWING AND INFORMATION CONTAINED THEREON, IS CONFIDENTIAL AND IS THE EXCLUSIVE PROPERTY OF EATON CORPORATION, AND IS MERELY ON LOAN AND SUBJECT TO RECALL BY EATON AT ANY TIME. BY TAKING POSSESSION OF THIS DOCUMENT, THE RECIPIENT ACKNOWLEDGES AND AGREES THAT THIS DOCUMENT CANNOT BE USED IN ANY MANNER ADVERSE TO THE INTERESTS OF EATON, AND THAT NO PORTION OF THIS DOCUMENT MAY BE COPIED OR OTHERWISE REPRODUCED WITHOUT THE PRIOR WRITTEN CONSENT OF EATON. IN THE CASE OF CONFLICTING CONTRACTUAL PROVISIONS, THIS NOTICE SHALL GOVERN THE STATUS OF THIS DOCUMENT.

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITY

The information, recommendations, descriptions and safety notations in this document are based on Eaton Corporation’s (“Eaton”) experience and judgment and may not cover all contingencies. If further information is required, an Eaton sales office should be consulted. Sale of the product shown in this literature is subject to the terms and conditions outlined in appropriate Eaton selling policies or other contractual agreement between Eaton and the purchaser.

THERE ARE NO UNDERSTANDINGS, AGREEMENTS, WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE OR MERCHANTABILITY, OTHER THAN THOSE SPECIFICALLY SET OUT IN ANY EXISTING CONTRACT BETWEEN THE PARTIES. ANY SUCH CONTRACT STATES THE ENTIRE OBLIGATION OF EATON. THE CONTENTS OF THIS DOCUMENT SHALL NOT BECOME PART OF OR MODIFY ANY CONTRACT BETWEEN THE PARTIES.

In no event will Eaton be responsible to the purchaser or user in contract, in tort (including negligence), strict liability or otherwise for any special, indirect, incidental or consequential damage or loss whatsoever, including but not limited to damage or loss of use of equipment, plant or power system, cost of capital, loss of power, additional expenses in the use of existing power facilities, or claims against the purchaser or user by its customers resulting from the use of the information, recommendations and descriptions contained herein.