MN152104EN Effective September 2021 Foreseer 7.4.500

Foreseer Recommended Security Hardening Guidelines

Powering Business Worldwide

Table of contents

Foreseer Recommended Security Hardening Guidelines 3
Foreseer Secure Configuration Guidelines 4
References 10
Copyright 11

Foreseer Recommended Security Hardening Guidelines

Foreseer is designed with Cybersecurity as an important consideration. Several Cybersecurity features are now offered in the product which, if implemented as per the recommendations in this document, will minimize Cybersecurity risk. This document provides information and guidelines on how to securely deploy and maintain a Foreseer installation which can include Foreseer, Foreseer Reporting Service, Outpost, Message Manager, and/or Connectors for Foreseer. By following the guidelines provided here within, sites can play a proactive role in minimizing Cybersecurity risks.

Eaton is committed to minimizing the Cybersecurity risk in its products and deploys best practices and the latest technologies in its products and solutions; making them more secure, reliable and competitive for our customers. Eaton also offers Cybersecurity Best Practices technical papers to its customers that can be referenced at www.eaton.com/cybersecurity

Apache version v2.4.46 and OpenSSL version v1.1.1h are installed with this release of Foreseer.

Foreseer Secure Configuration Guidelines

Category	Description
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. To facilitate this, Foreseer is capable of generating a System Configuration Report. This report provides information about devices - including IP address and port assignment. For more details, refer to the Using *WebViews Reports* section in the *WebViews Guide* help file for a description on using WebViews Reports.
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. For details on how to securely deploy Foreseer, please refer to the *Hardware and Security Considerations* section in the *Server Guide* help file.
Authorization and Access Control	It is extremely important to securely configure the logical access mechanisms provided in Foreseer to safeguard from unauthorized access. Eaton recommends that the available access control mechanisms be used properly to ensure that 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

Category	Description
	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. Eaton recommends that following secure considerations be implemented by customers while deploying Foreseer: 1. Securely configuring User groups, roles and privileges. See the *Security and User Groups* section in the *Server Guide* help file. 2. Securely configuring web server and client allowlisting See *Security and User Groups / Allowlisting* in the *Server Guide* help file. 3. LDAP configuration and Windows security configuration 4. See *System Administration / LDAP Properties* in the *Server Guide* help file. 5. Security User Group Access Information 6. See *Security and User Groups / Authorization Levels* in the *Server Guide* help file. 7. Changing Foreseer default user account 8. See *Running Foreseer Services with Minimum Privileges* in the *Server Guide* help file. 9. Configuring Interactive Remote Access See *Security Considerations for Interactive Remote Access* in the *Server Guide* help file.
Network Security	Foreseer provides network access to facilitate communication with other devices in the systems and configuration. In addition to on-premises capabilities, Foreseer can push data to other Eaton cloud-based software solutions and provide data information to configured cloud clients via HTTPS. Leveraging these capabilities could present challenges if it's not configured securely within your organization. • 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

Category	Description
	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 Foreseer. • Internet/ Email restrictions: Internet and email traffic to Foreseer is not recommended. Additional network controls and a host based firewall should be used to filter unnecessary traffic from Foreseer nodes. • Traffic control and filtering: Configure your host based firewall to limit unnecessary traffic to Foreseer and its licensed options (e.g. Foreseer Cloud Agent). • Foreseer uses port 80, 81 for accessing web server over HTTP. These ports should be allowed in firewall for uninterrupted operation of Foreseer application. HTTP is by default disabled on the Foreseer web server. • Usage of HTTPS is recommended as HTTP is not encrypted and can lead to compromise of sensitive information. • Foreseer uses default port assignments of 443,444 for accessing web server information over HTTPS. These ports should be allowed in firewall configurations for uninterrupted operation of the Foreseer application. • Foreseer supports Remote/Redundant Servers on TCP port 2100. If Foreseer is configured to support remote/redundant servers, allow TCP port 2100 in firewall. • Foreseer's Cloud Agent feature uses ports 5443 and 443 for intake data operations and should be configured in a manner where it is accessible to the host only - meaning no accessibility outside of the local host. • This port should be accessible for uninterrupted operation of it and the Foreseer application.

Category	Description
	Please refer to the *Server Guide* help file for more details. For assistance with the Foreseer Cloud Agent, please refer to the documentation corresponding to the *Foreseer Cloud Agent* connector you are using. It is possible to obtain a System Configuration report from Foreseer. Information regarding IP addresses and Ports used can be found in this report.
Database Security	Foreseer supports Microsoft SQL Server. Eaton recommends following best practices for securely maintaining the database: • Physical Security: Verify physical security to the machine hosting the Foreseer server database. Physical access to these machines should be access controlled, monitored and logged at all times. • Logical access: Restrict logical access to database on the basis of roles and permissions. Change default credentials on first use. Do not share passwords of one account with multiple people. Change password on personnel change or as per the organization's password policy. • Auditing: All access to the database including administrative and maintenance activities should be logged and maintained for at least 3 months or as per organization's policy. • Backup & Restore: Databases should be properly backed up at a secure location so that it can be restored at any point of time in case of any failure. • Patching and Updating: Regularly update database software to latest secure supported version. • Database should be store behind firewalls and, by default all traffic should be disabled.
Logging and Event Management	• Eaton recommends that all remote interactive sessions are encrypted, logged, and monitored; including all administrative and maintenance activities. • Ensure that logs are backed up; retain the backups for a minimum of 3 months or as per organization's security policy. • Perform log review at a minimum every 15 days. • Eaton recommends configuring Windows audit policy on Foreseer Server. Please find the recommended configurations below: • If Windows Authentication is used, it can be configured to

Category	Description
	log user logins • All successful and failed log in attempts and successful logoff attempts should be configured in Windows audit policy. • If LDAP Authentication is used, LDAP servers can be configured to log authentication • Foreseer can generate an Audit History Report. This report will give configuration change information. Please refer the Using *WebViews Reports* section in the *WebViews Guide* help file for a description on using WebViews Reports. • Foreseer can generate Log File Report. This report will give errors, warning information for the application. • Please refer the Using *WebViews Reports* section in the *WebViews Guide* help file for a description on using WebViews Reports.
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.** ▪ **1-877-386-2273, Opt 2, 4, 1, then 2** o **For callers outside of the United States** ▪ **1-828-651-0786, Opt 2, 4, 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

Category	Description
	• Please contact CST, immediately in case of any vulnerability found in Foreseer. • Conduct regular Cybersecurity risk analyses of the organization /system. 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.

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):
http://www.cooperindustries.com/content/dam/public/powersystems/resources/library/1100_EAS/WP910003EN.pdf

[R3] NIST SP 800-82 Rev 2, Guide to Industrial Control Systems (ICS) Security, May 2015.
https://ics-cert.us-cert.gov/Standards-and-References

[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

Copyright

Foreseer Recommended Security Hardening Guidelines– 7.4.500

Publication date 09/2021