

# Recommended Security Hardening Guide



## Contents

Recommended Security Hardening Guidelines .....	3
Foreseer – Secure Configuration Guidelines.....	3
References .....	10

# 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. 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 whitepapers to its customers that can be referenced at [www.eaton.com/cybersecurity](http://www.eaton.com/cybersecurity)



Apache version v2.4.41 and OpenSSL version v1.1.1d are installed with this release of Foreseer.

## Foreseer – Secure Configuration Guidelines

Category	Description
Asset identification and Inventory	<p>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.</p> <p>For more details, refer to the Using <i>WebViews Reports</i> section in the <i>WebViews Guide</i> help file for a description on using WebViews Reports.</p>
Physical Protection	<p>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.</p>

Category	Description
	<p>For details on how to securely deploy Foreseer, please refer to the <i>Hardware and Security Considerations</i> section in the <i>Server Guide</i> help file.</p>
<p>Authorization and Access Control</p>	<p>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.</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> <li>• 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.</li> <li>• Perform periodic account maintenance (remove unused accounts).</li> <li>• Change passwords and other system access credentials whenever there is a personnel change.</li> </ul> <p>Eaton recommends that following secure considerations be implemented by customers while deploying Foreseer:</p> <ol style="list-style-type: none"> <li>1. Securely configuring User groups, roles and privileges.  See the <i>Security and User Groups</i> section in the <i>Server Guide</i> help file.</li> <li>2. Securely configuring webserver and client whitelisting</li> </ol>

Category	Description
	<p>See <i>Security and User Groups / Whitelisting</i> in the <i>Server Guide</i> help file.</p> <p>3. LDAP configuration and Windows security configuration</p> <p>See <i>System Administration / LDAP Properties</i> in the <i>Server Guide</i> help file.</p> <p>4. Security User Group Access Information</p> <p>See <i>Security and User Groups / Authorization Levels</i> in the <i>Server Guide</i> help file.</p> <p>5. Changing Foreseer default user account</p> <p>See <i>Running Foreseer Services with Minimum Privileges</i> in the <i>Server Guide</i> help file.</p> <p>6. Configuring Interactive Remote Access</p> <p>See <i>Security Considerations for Interactive Remote Access</i> in the <i>Server Guide</i> help file.</p>
Network Security	<p>Foreseer provides network access to facilitate communication with other devices in the systems and configuration. But this capability could open a big security hole if it's not configured securely.</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Deploy adequate network protection devices like Firewalls, Intrusion Detection / Protection devices.</li> </ul> <p>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.</p>

Category	Description
	<p>The following additional network security controls should be considered when deploying Foreseer.</p> <ul style="list-style-type: none"> <li>• Internet/ Email restrictions: Internet and email traffic to Foreseer is not recommended. Additional network controls and Windows Firewall should be used to filter unnecessary traffic from Foreseer nodes.</li> <li>• Traffic control and filtering: Configure Windows Firewall to limit unnecessary traffic to Foreseer</li> <li>• Foreseer uses port 80, 81 for accessing webserver over HTTP. These ports should be allowed in firewall for uninterrupted operation of Foreseer application. HTTP is by default disabled on Foreseer webserver.</li> <li>• Usage of HTTPS is recommended as HTTP communication is unencrypted and can lead to compromise of sensitive information.</li> <li>• Foreseer uses port 443,444 for accessing webserver over HTTPS. These ports should be allowed in firewall for uninterrupted operation of Foreseer application.</li> <li>• Foreseer supports Remote/Redundant Servers on TCP port 2100. If Foreseer is configured to support remote/redundant servers, allow TCP port 2100 in firewall.</li> </ul> <p>Please refer to the <i>Server Guide help file</i> for more details</p> <p>It is possible to obtain a System Configuration report from Foreseer. Information regarding IP addresses and Ports used can be found in this report.</p>
Database Security	<p>Foreseer supports Microsoft SQL Server. Eaton recommends following best practices for securely maintaining the database:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> </ul>

Category	Description
	<ul style="list-style-type: none"> <li>• 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.</li> <li>• Backup &amp; 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.</li> <li>• Patching and Updating: Regularly update database software to latest secure supported version.</li> <li>• Database should be store behind firewalls and, by default all traffic should be disabled.</li> </ul>
Logging and Event Management	<ul style="list-style-type: none"> <li>• Eaton recommends that all remote interactive sessions are encrypted, logged, and monitored; including all administrative and maintenance activities.</li> <li>• Ensure that logs are backed up; retain the backups for a minimum of 3 months or as per organization's security policy.</li> <li>• Perform log review at a minimum every 15 days.</li> <li>• Eaton recommends configuring Windows audit policy on Foreseer Server. Please find the recommended configurations below:</li> <li>• If Windows Authentication is used, it can be configured to log user logins</li> <li>• All successful and failed log in attempts and successful logoff attempts should be configured in Windows audit policy.</li> <li>• If LDAP Authentication is used, LDAP servers can be configured to log authentication</li> <li>• Foreseer can generate an Audit History Report. This report will give configuration change information.</li> </ul> <p>Please refer the Using <i>WebViews Reports</i> section in the <i>WebViews Guide</i> help file for a description on using WebViews Reports.</p> <ul style="list-style-type: none"> <li>• Foreseer can generate Log File Report. This report will give errors, warning information for the application. Please refer the Using <i>WebViews Reports</i> section in the <i>WebViews Guide</i> help file for a description on using WebViews Reports.</li> </ul>

Category	Description
Secure Maintenance	<ul style="list-style-type: none"> <li>• Apply Firmware updates and patches regularly</li> <li>• 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.</li> <li>• CST, Customer Success Team is available for customer to contact at: <ul style="list-style-type: none"> <li>○ <b>For callers within the domestic United States.</b> <ul style="list-style-type: none"> <li>▪ <b>1-877-386-2273, Opt 2, 4, 1, then 2</b></li> </ul> </li> <li>○ <b>For callers outside of the United States</b> <ul style="list-style-type: none"> <li>▪ <b>1-828-651-0786, Opt 2, 4, 1, then 2</b></li> </ul> </li> <li>○ <b>Email</b> <ul style="list-style-type: none"> <li>▪ <a href="mailto:cst@eaton.com">cst@eaton.com</a></li> </ul> </li> </ul> </li> <li>• 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.</li> <li>• 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 - <a href="http://eaton.com/cybersecurity">http://eaton.com/cybersecurity</a></li> <li>• Please contact CST, immediately in case of any vulnerability found in Foreseer.</li> <li>• Conduct regular Cybersecurity risk analyses of the organization /system.</li> </ul> <p>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.</p>



Category	Description
	<p data-bbox="619 210 1342 282">Plan for Business Continuity / Cybersecurity Disaster Recovery</p> <p data-bbox="619 327 1406 517">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:</p> <ul data-bbox="667 528 1417 797" style="list-style-type: none"> <li data-bbox="667 528 1417 640">• Backup of the latest f/w copy of Foreseer. Make it a part of SOP to update the backup copy as soon as the latest f/w is updated on Foreseer.</li> <li data-bbox="667 647 1305 680">• Backup of the most current configurations.</li> <li data-bbox="667 687 1337 721">• Documentation of the most current User List.</li> <li data-bbox="667 728 1406 797">• Save and store securely the current configurations of the device.</li> </ul>

# References

[R1] Cybersecurity Considerations for Electrical Distribution Systems (WP152002EN):  
[http://www.eaton.com/ecm/groups/public/@pub/@eaton/@corp/documents/content/pct\\_1603172.pdf](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](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>

# Recommended Security Hardening Guide – Foreseer 7.2.210

Publication date 12/2019

Copyright © 2019 by Eaton Corporation. All rights reserved. Specifications contained herein are subject to change without notice.

Foreseer is a registered trademark of Eaton Corporation.

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.