EcoStruxure Retail IMP
(Integrated Management Platform)

Hardening Guide

Legal Information

The information provided in this document contains general descriptions, technical characteristics and/or recommendations related to products/solutions.

This document is not intended as a substitute for a detailed study or operational and site-specific development or schematic plan. It is not to be used for determining suitability or reliability of the products/solutions for specific user applications. It is the duty of any such user to perform or have any professional expert of its choice (integrator, specifier or the like) perform the appropriate and comprehensive risk analysis, evaluation and testing of the products/solutions with respect to the relevant specific application or use thereof.

The Schneider Electric brand and any trademarks of Schneider Electric SE and its subsidiaries referred to in this document are the property of Schneider Electric SE or its subsidiaries. All other brands may be trademarks of their respective owner.

Schneider Electric does not grant any right or license for commercial use of the document or its content, except for a non-exclusive and personal license to consult it on an “as is” basis. Schneider Electric reserves the right to make changes or updates with respect to or in the content of this document or the format thereof, at any time without notice.

To the extent permitted by applicable law, no responsibility or liability is assumed by Schneider Electric and its subsidiaries for any errors or omissions in the informational content of this document, as well as any non-intended use or misuse of the content thereof.

Table of Contents

1 Safety Information

⚠ CAUTION

1.1 Important information

Read these instructions carefully and look at the equipment to become familiar with the device before trying to install, operate, service or maintain it. The following special messages may appear throughout this bulletin or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.

The addition of this symbol to a “Danger” or “Warning” safety label indicates that an electrical hazard exists which will result in personal injury if the instructions are not followed.

This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

⚠ DANGER
DANGER indicates a hazardous situation, which, if not avoided, will result in death or serious injury.

⚠ WARNING
WARNING indicates a hazardous situation, which if not avoided, could result in death or serious injury.

⚠ CAUTION
CAUTION indicates a hazardous situation, which if not avoided, could result in minor or moderate injury.

NOTICE
NOTICE is used to address practices not related to physical injury.

1.2 Please Note

Electrical equipment should be installed, operated, serviced, and maintained only by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material. A qualified person is one who has skills and knowledge related to the construction, installation, and operation of electrical equipment and has received safety training to recognize and avoid the hazards involved.

1.3 Cybersecurity Safety Notice

NOTICE

POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY

- Change default passwords at first use to help prevent unauthorized access to device settings, controls, and information.
- Change passwords regularly to help prevent unauthorized access to device settings, controls, and information.
- Do not share accounts. Each user must have their own account.
- When creating user and display names, it is important to avoid using personal information, and to consider regional privacy policies. Display names will appear in event logs to identify who performed operations on the device.
- It is recommended that log files be encrypted before transmission to help with security and privacy.
- Disable unused ports, services, and default accounts to help minimize pathways for malicious attackers.
- Place networked devices behind multiple layers of cyber defenses (such as firewalls, network segmentation, and network intrusion detection and protection).
- Use the recommended cybersecurity safety measures (for example, least privilege, separation of duties) to help prevent unauthorized exposure, loss, modification of data and logs, or interruption of services.

Failure to follow these instructions can result in loss of data, unauthorized system access, or equipment damage.

1.4 How to Report a Cybersecurity Vulnerability

If a security vulnerability is discovered or suspected, the portal found at www.se.com/ww/en/work/support/cybersecurity/report-a-vulnerability.jsp is to be used for reporting and to establish communication around suspected issues.

2 Introduction

2.1 About this guide

This guide provides information on the cybersecurity aspects for EcoStruxure™ Retail IMP (Integrated Management Platform) to help system designers and operators promote a secure operating environment for the platform. It describes how you can integrate Retail IMP into your IT environment, and it gives tips for improving the security of the system.

This guide is written for:

- IT departments, who need to understand how to incorporate Retail IMP into their IT environments.
- Engineers and technicians who need to deploy Retail IMP into their facilities.

This guide does not address the more general topic of how to secure your operational technology network, or your company Ethernet network. For a general introduction to cybersecurity threats and how to address them, refer to *How Can I Reduce Vulnerability to Cyber Attacks?* .

NOTE: In this guide, the term **security** is used to refer to cybersecurity.

2.2 About Retail IMP (Integrated Management Platform)

Retail IMP (Integrated Management Platform) is a cloud-based analytical software solution that connects field devices, onsite systems, cloud software, and analytics enabling you to monitor the health of your entire business, including stores and sites across the globe with multiple systems ranging from BMS to HVAC, and refrigeration to lighting. Customers can use Retail IMP to monitor, track, and analyze all their data in one master dashboard. The solution provides seamless control of facility applications and 24/7 monitoring and alarming to help increase business profitability, enhance energy efficiency, maintain service continuity and simplify maintenance.

2.3 About Schneider Electric data confidentiality and security

Retail IMP collects operational energy system data and a small amount of personally identifiable information (PII). PII information includes the usernames and email addresses that users enter at the time of registration. For more details on what data is collected, see the Retail IMP Terms of Use (available on the upper right corner of the Retail IMP solution under the “?” symbol).

Schneider Electric is committed to protecting the confidentiality and security of customer data. Retail IMP complies with Schneider Electric’s global policies and procedures on cybersecurity and data protection.

For more information on the Schneider Electric cybersecurity and data protection policies and procedures, see the Resources section in this guide.

3 Connectivity Overview

3.1 Design

Retail IMP is designed following the Schneider Electric Secure Development Lifecycle, that is based on the IEC 62443-4-1-series standards for information security. This means security is considered and integrated into the design of Retail IMP right from the start.

The following are examples of the Secure Development Lifecycle practices that we use:

- Periodic authorized simulated cyberattacks (penetration tests) on Retail IMP, performed by Schneider Electric cybersecurity specialists to evaluate the security of the system.
- Ongoing cybersecurity threat modeling and analysis by development teams for Retail IMP.
- Ongoing cybersecurity and data privacy training for all Retail IMP designers and developers.

3.2 Network Architecture

The following shows a high-level conceptual view of a Retail IMP system:

3.3 Data collection and transmission

All data for Retail IMP is sent through a compatible IoT gateway. The gateways use secure protocols for data transmission. The following are some of the characteristics of the secure data collection:

- Data transmission between the onsite gateways and the Schneider Electric cloud services is encrypted using TLS 1.2 (HTTPS) protocol.
- Only device measurement data and events are sent to the cloud services.
- Only the gateway can start the connection with the cloud services. Data flow can be bi-directional.

This end-to-end cybersecurity, from gateway to cloud, makes sure that all data sent to Retail IMP is from a trusted source. The following gateways are compatible with Retail IMP:

- Automation Server (AS-P, AS-B)

For more information on the IoT gateways, see the Resources section in this guide.

3.4 Cloud-based software

Retail IMP data is hosted in a secure Microsoft Azure environment, certified to ISO/IEC 27001. More information about Microsoft cloud services security can be found on the Microsoft Trust Portal.

The Retail IMP application includes many operational security features, such as:

- Strong password enforcement
- (Optional) Two-factor authentication
- Role-based access control
- Session timeout after 24 hours of inactivity
- Regular security updates are automatically applied to the Retail IMP cloud servers

3.5 Site connection at edge level

The Retail IMP platform is cloud-based and can be accessed in a web browser without any software installation. The monitoring devices and IoT gateways that provide the operational data are installed locally in the customer facility. For Retail IMP to receive the data from the Automation Server, the gateway must be able to connect to the Schneider Electric cloud services. The connection between the Automation Server and the Integrated Management Platform is divided into two parts, with the WAN connection acting as a bridge between the two parts:

- WAN Connection: The Wide-Area Network is the internet connection between the router and Schneider Electric's data centers.
- LAN Connection: The Local-Area Network is the network connection between the router and the Automation Server, at the customer's site.

The Automation Server must be configured to be visible on the same LAN (Local Area Network) as the routers. The Teltonika RUT240 is a recommended 4G router by Schneider Electric. Schneider Electric has set up the following rules within the modem:

- Traffic through Wireguard VPN
- Allow HTTPs with HTTP redirect to HTTPs (Port 443, 80)
- Allow SSH (Port 22)
- Port forwarded device (Automation Server IP only)

The Teltonika router has the following security features built-in:

SECURITY	
Authentication	Pre-shared key, digital certificates, X.509 certificates
Firewall	Pre-configured firewall rules can be enabled via WebUI, unlimited firewall configuration via CLI; DMZ; NAT; NAT-T
Attack prevention	DDOS prevention (SYN flood protection, SSH attack prevention, HTTP/HTTPS attack prevention), port scan prevention (SYN-FIN, SYN-RST, X-mas, NULL flags, FIN scan attacks)
VLAN	Port and tag based VLAN separation
Mobile quota control	Set up custom data limits for the SIM card
WEB filter	Blacklist for blocking out unwanted websites, whitelist for specifying allowed sites only
Access control	Flexible access control of TCP, UDP, ICMP packets, MAC address filter

For more documentation on Teltonika's routers, please visit their website here.

3.6 WAN connection between Retail IMP and the 4G router

There are two options for connecting the Retail IMP platform and the router. The customer can either use a 4G connection or the customer's existing internet connection. We recommend you review the options with your IT team to decide the most suitable WAN connection for your sites.

- **Using a 4G connection**
  The router is connected to the Retail IMP platform using a 4G connection. The 4G solution is the simplest to set up, but it comes with an additional cost for the 4G data subscription.

- **Using the customer's existing internet connection**
  The router is connected to the Retail IMP platform using the customer's existing internet connection. This solution utilizes the existing network structure but requires the customer's IT organization to allow communication through their infrastructure.

3.7 LAN connection between the 4G router and the Automation Server

There are three options for connecting the router and the Automation Server.

- **Direct connection**
  In this case, the Automation Server is connected directly to the 4G router. This is the simplest setup for a site with only one Automation Server.

- **Direct connection with extra devices**
  The Automation Server is connected directly to the 4G router. The Automation Server also acts as a bridge that allows other servers and devices on the local network to connect to Retail IMP

- **Connection through a switch**
  The Automation Server is connected to the 4G router through a local network.

4 Third Party Router Management

This section describes how to maintain the 4G router to connect to the Integrated Management Platform. The router must be secured to prevent unauthorized access to the gateways, the end devices on site and the Retail IMP solution.

NOTE: For best practices and the latest updates on the Teltonika router or the third-party router of your choice, always refer to the manufacturer's website and documents for information. Refer here for the latest updates on the Teltonika's routers.

4.1 Firmware Update

Download and install your router's latest firmware to ensure you have the latest functionality and security updates.

- For Teltonika routers, go to the manufacturer's webpage FW & SDK Downloads. For other third-party routers refer to the manufacturer's website and documents for instructions.
- Find the product in the list and download the latest firmware.
- Install the latest firmware on the router according to the manufacturer's recommendation.

4.2 Connecting to the Router

You connect to the Teltonika Router to configure the Wireguard VPN, the firewall, and port forwarding.

- Connect your computer to the LAN port of the router and browse to the default address 192.168.1.1 to open the user interface.
- The first time you log on, use the default username and password, and then change the password. You find the username and password on the label of the router.

4.3 Enabling the NTP Client

You enable the NTP client to make sure that the router has the correct time. This is essential for logging events in the system.

- Log on to the router.
- In the menu, click on Services and then click on NTP.
- In the menu, click on NTP.
- In the NTP Client section, turn on Enable NTP Client.
- In the Hostname section, enter the address of the NTP server you want to use.
- Click on the Save & Apply button.
- If you're using a third-party router of your choice, follow the manufacturer's instructions on how to enable the NTP client.

4.4 Configuring the WAN Connection

The router is already configured to connect to the Internet. In most cases you do not need to change anything. The interface list contains three interfaces by default:

- WAN: The WAN Ethernet port. This interface uses IPv4.
- WAN6: The WAN Ethernet port. This interface uses IPv6.
- Mob1s1a1: The 4G connection

The router will try to connect using one interface at a time, in the order they are listed. To change the order, drag and drop the interfaces in the list. To configure the WAN connection:

- Log on to the router.
- In the menu, click on Network and then click on WAN.
- Click on the Edit button on the interface you want to configure.
- Enter the settings. If you are connecting the system over 4G, the settings are provided either by Schneider Electric or the Partner. If you are connecting the system using the customer's internet connection, the settings are provided by the customer's IT organization.
- When you are done, click on the Save & Apply button.

4.5 Configuring the Wireguard VPN

You configure the Wireguard VPN to create a secure way for the Automation Server to communicate with the platform. To configure the Wireguard VPN:

NOTICE
POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY The VPN key files are critical. Losing or distributing these beyond your control can compromise the cybersecurity of the system. If you lose control of the key, immediately contact IT Operations. **Failure to follow these instructions can result in loss of data or equipment damage.**

- Log on to the router.
- In the menu, click on Services, then click on VPN, and then click on Wireguard.
- In the Add new instance section, enter a logical name, for example IMP_CUST, and click Add.
- On the General Settings tab, set these parameters:
    - Private Key: Copy the private key from the document you received from the IT Operations Team.
    - Public Key: This connection does not use a public key. Do not press the Generate button.
    - Listen port: Enter 51820
    - IP Addresses: Copy the IP address from the config file and add /24 at the end.
- Click on the Save & Apply button.
- Click on the pen icon on the VPN instance you just created.
- In the Peers section, on the General Setup tab, set these parameters:
    - Public Key: Copy the public key from the document you received from the Operations Team.

    - Allowed IPs: Copy the allowed IPs from the document you received from the Operations Team. To add more IP addresses, click on the + button.
- On the Advanced Setup tab, set these parameters:
    - Pre-shared Key: Copy the pre-shared key from the document you received from the Operations Team.
    - Turn on Route Allowed IPs.
    - Endpoint Host: Copy the endpoint host from the document you received from the Operations Team.
    - Endpoint Port: Copy the endpoint port from the document you received from the Operations Team.
    - Persistent Keep Alive: Enter 50.
- Click the Save & Apply button.
- In the Wireguard Interface window, click the Save & Apply button.
- Under Wireguard Configuration, under Tunnel Name, turn on the VPN tunnel you just created.

4.6 Checking the Wireguard VPN

You check the Wireguard VPN to see that the router is accessible to the portal.

- Go to System, then click on Administration, then click on Troubleshoot.
- In the Diagnostics section, in the Method dropdown box, select Ping.
- In the Protocol dropdown box, select the used protocol.
- In the Address text box, add the IP address for the VPN server. The IP address is the same as the Allowed IP address, but with the fourth group replaced with 1.
- Click on the Perform button to ping the VPN server. If the ping succeeds, the VPN is correctly configured.
- If you can't ping the VPN server, ping the address 1.1.1.1 to check that your router is connected to the Internet. If you can connect to the Internet but not the VPN server, check all VPN settings again.
- To reset the connection and start again, remove the Public Key from the peer, and then start setting up the VPN again.

4.7 Configuring the Firewall

The firewall should be configured to allow the platform to communicate with the automation or enterprise servers on your internal network.

- Click on Network, then click on Firewall, and then click on General Settings.
- In the Zones section, select these settings:

Zone => Forwarding	Input	Output	Forward	Masquerading	MSS Clamping
Lan => wan wireguard	Accept	Accept	Accept	On	Off
Wan => reject	Reject	Accept	Reject	On	On
Wireguard => lan	Accept	Accept	Reject	On	Off

- Click on the Save & Apply button.
- 4. Click on Network, then click on Firewall, and then click on Port forwards
- Add three port forward instances with the following settings:

Name	External Port	Internal IP	Internal Port
Remote	443	The IP address of the Teltonika router's LAN interface	443
IMP	8443	The IP address of the Automation Server	443
Upgrade	2222	The IP address of the Automation Server	22

TIP: If you have multiple Automation Servers at one site, connected to the same router, add one IMP and one Upgrade instance for each server. Give each instance a unique name.

- On each port forward, click on the pen icon and change the Source zone to Wireguard.
- Click on the Save & Apply button.
- Check that a PC allowed on the VPN and running Wireguard can perform the two actions authorized in the firewall rules:
    - Access the Teltonika web pages by typing the Teltonika VPN IP address in a browser using HTTPS, for example HTTPS://192.168.10.153
    - Access the AS WebStation by typing the Teltonika VPN IP address in a browser using port 8443, for example HTTPS://192.168.10.153:8443
    - If either one of these steps don’t work, check the default firewall rules and port forwarding rules. Verify that the port forwarding rule only allows communication from source zone Wireguard and not WAN.
- If you are unsuccessful and are running on a corporate IT network, check if it works better with a 4G connection and then contact the IT department to help solve the issue.

4.8 Accessing the Edge System through the VPN

You access the edge system through the VPN to verify that the Teltonika router is accessible to the Retail Integrated Management Platform.

- Download and install the Wireguard Client from www.wireguard.com/install/.
- When the installation is complete, open the Wireguard application.
- Click on Import tunnel(s) from file.
- Select the .conf-file you received from the IT support.
- Click Activate. IMPORTANT: You may need to change your computer's internet settings to be able to connect through the Wireguard VPN. Contact IT helpdesk for help with this.
- Click the Activate button.
- In the Peer box, under Transfer, check that the tunnel has sent and received data. If you can't get the VPN to connect, check all steps again, and then contact support.

Now you have verified that you can remotely access WebStation on the Automation Server. The next step is to verify the entire connection.

4.9 Checking the Connection

You check the connection to verify that the different components can communicate with each other.

- Start Wireguard on your computer.
- Open a web browser and go to https://[IP address of router]
- If the web page of the router doesn’t open, check the configuration of the WireGuard in the Router.
- In the browser's address field, add :8443 after the router's IP address.
- If the web page of the AS-B doesn’t open, check the configuration of the AS-B and the port forward rules in the router.
- In the web page of the router, click on System, then click on Administration, and then click on Troubleshoot.
- Click on Diagnostics
- In the Method field, select Traceroute.
- In the Protocol field, select IPv4.
- In the Address field, enter the address of the Integrated Management Platform. Example: venice.autumninsight.com
- Click the Perform button.
- If the command returns the IP address of the Integrated Management Platform server, your system is correctly set up.

5 Edge Security

This chapter describes how to improve the security of the BMS system at each site. Following the best practices in this section will ensure the overall security of the system, including BMS equipment, is maintained.

5.1 Guiding principles

When discussing any network-based installation, understanding the purpose and security capabilities of each component is key in achieving integration security. There are two general classes of network devices commonly used in BMS integrations:

- Network protective devices (Firewalls, VPNs, routers, switches, etc.) – Securing the 4G router was covered in the previous section.
- BMS products (BACnet / IP controllers, Automation Server gateways)

5.2 Best practices for BMS equipment

It is important to note that BMS products have been designed to provide building management functionality, not network management and security. The following “Requirements” are a MUST for all BMS network implementations:

Requirement #1 – BMS networks MUST BE isolated from the Internet. EcoStruxure BMS servers are NOT to be connected directly to the Internet. BMS system access to the Internet must be buffered by at least one, properly configured, router.

Requirement #2 – BMS components MUST BE connected to isolated network segments dedicated to BMS use. All BMS network segments must be isolated from all other networks using at least one router configured to ensure only appropriate external systems can interact with the BMS network components.

Requirement #3 – Remote access MUST USE a VPN for connectivity to the BMS network segments. It is common for maintenance operations to be performed remotely. The security of that connection is critical in ensuring maintenance is performed securely. The use of a VPN connection between the remote device and the BMS network is the only approved way to establish that connection. There are various architectural considerations associated with VPN connections; the Customer’s IT department can assist in the designing and implementing a solution that meets company policies.

Requirement #4 – BMS security patches MUST BE applied in a timely manner. Cybersecurity is a fast-moving field where new vulnerabilities are constantly being detected. While the network protective devices and isolated network segments provide the primary protection functions; eliminating unnecessary risks by regularly updating all BMS product security patches is REQUIRED to ensure availability of the latest security features.

Requirement #5 – BMS backups MUST BE routinely completed, validated and secured. A robust backup practice is the best insurance available for handling unexpected security issues. From Disaster Recovery to recovering a failed device, up-to-date backups speed recovery efforts. Beyond simply performing periodic backups, there should be a practice that validates each backup and ensures it is possible to restore it. All backups should be encrypted and securely stored.

Requirement #6 – User accounts MUST BE regularly maintained.

For the EcoStruxure Building Management line of products, the BACnet/IP controllers have been designed to connect to IP networks using the AS-P server. This device has been designed to provide the required isolation for IP based controllers on the BMS network segment.

The IP field network defined by the AS-P to the BACnet/IP controllers is normally implemented in a fully isolated mode. This limits each controller's attack surface to the IP Field Network to which it is connected. In such an architecture, additional network protective devices are not needed on the isolated subnet. If non-EBO IP controllers are introduced, additional network protective devices are used to limit the risk posed by these devices.

For more information on edge security and best practices for field controllers, refer to the EcoStruxure Building Management, System Hardening Guide.

6 General Recommendations

These guidelines will help the user ensure the security and integrity of not only the Retail IMP platform but also the overall system and the customer's network.

Confidentiality

Confidentiality is the ability not to disclose information to unauthorized persons, programs, or processes.

- Data should be handled based on the organization's required privacy.
- Data should be encrypted using 2FA.
- Keep access control lists and other file permissions up to date.
- Follow the rule of least privilege – offer user permissions limited to the actions the user needs to fulfil.

Session timeout

Retail IMP automatically ends inactive sessions after a certain time interval (24 hours). Before the session is ended, users are reminded of the timeout with an option to continue the session. If they continue the session, the timeout counter resets. The timeout interval is not configurable.

Usernames and passwords

These guidelines ensure the security and confidentiality of your username and password.

User Responsibility

Users are responsible for all activities performed with their individual username. Do not allow others to use your username or usernames belonging to other users.

Use of Usernames and Passwords

Do not use company identification like your email address and password to sign up for uncertified or unapproved platforms or systems.

Password Sharing

Under no circumstances should you share or reveal your password to anyone. Administrators and support personnel should never request password disclosure.

Strong Passwords

Choose passwords that are difficult to guess and follow the password & authentication requirement policy. Avoid using dictionary words, derivatives of your username, common character sequences, personal information details, common names, or work-related words.

Password Handling

Avoid typing passwords on a keyboard when others are watching as it may expose the accessed information to unauthorized individuals.

Password Storage

Do not write or store passwords in clear text, whether physically or electronically. Store passwords securely in the approved password vault software provided by your organization.

Lost Passwords

Immediately change your password if you suspect or know that it has been disclosed to an unauthorized party.

Virus Protection

To keep your user account secure and minimize the chance of information exposure, make sure your computer has reliable and up-to-date antivirus and antimalware protection. This will help maintain the integrity of your account. While the Retail IMP platform uses Microsoft Defender to scan external files, ensure what you are uploading is from a trusted source.

Security Controls

Do not circumvent or bypass any implemented security controls, including deleting logs on organizational assets.

Personal Computer Usage

Do not share your company-assigned systems with individuals outside the organization. Keep your system protected by logging out or activating a password-protected screen saver when unattended.

Security Assistance

Do not accept any form of assistance to improve system security without approval from the IT or Security team. Do not download free security software or employ free security evaluation services unless approved by the designated team.

Malicious Programs

Do not introduce or propagate any malicious programs (e.g., viruses, worms, Trojan horses, e-mail bombs) into the network, servers, or any information asset.

7 User management

User level security is designed to limit system access to users with valid credentials and with proper permissions. Using Retail IMP, you can manage each user's access by limiting the actions that can be performed and the information that can be accessed.

7.1 User authentication

User authentication is how a service provider determines if a user should be granted access to a requested service. For Retail IMP, User management is the specified method of validating a user's credentials. A user's credentials are the username and password associated with his/her account.

Best practices for maintaining user accounts and securing passwords are explained in the 'General recommendations' section and documented in the link here. It is especially important to periodically review all user accounts and to disable or remove all users who no longer have a valid reason for accessing the Retail IMP platform.

7.2 User and Group Permissions

User account permissions determine the level of access each user has to services offered in Retail IMP. The best approach to setting user permissions is to be as restrictive as possible. For example, if a customer's user only needs to monitor point values, then grant read-only access to the points he/she needs to monitor and no others. In this manner, limited damage can be inflicted if the user's credentials are compromised. Within Retail IMP, there are a few ways to limit user access.

Each user belongs to one or more user groups. Each user group has a role on a scope of entities. Each role defines the actions allowed and denied on the various elements of the platform. The actions are create, read, update, and delete.

These are the default roles:

- **Platform application admin:** This role has unrestricted access to the application.
- **Basic grant:** This role has read access to menus, users, blades, classes, dashboards, grants and maps.
- **Platform node admin:** This role provides unrestricted access to nodes and entities.
- **Platform twin admin:** This role provides unrestricted access to entities.
- **Entity Viewer:** This role granted on a site or on an equipment to have read-only access on associated control points and dashboards (visualization only)
- **Entity Operator:** This role is granted on a site or on an equipment to have read-write access on associated control points and read-only access on dashboards (visualization and control)
- **Entity Integrator:** This role is granted on a site or on an equipment to have read-write access on associated control points and dashboards (visualization, control and edition of dashboard).
- **Interface Group Integrator:** This role can manage interfaces within a group

You can add custom roles. Permissions are inherited in the model tree. For example, if a user has a role in a Region, they have the same role on all the Buildings in that Region.

8 Frequently Asked Questions

- Does Retail IMP support multi-factor authentication?
    - Yes. Multi-factor authentication is strictly enforced on the platform.
- How frequently is the session timeout performed for security?
    - The session timeout is performed after 24 hours.
- What is the default password policy enforced in Retail IMP?
    - Must be at least 8 characters
    - Must have at least 2 alphabetic characters
    - Must have at least 2 numeric characters
    - Must have at least 2 symbol characters

9 Resources

9.1 IoT Gateway resources

- Automation Server AS-P (Opens the Web Help page for the product)
- Automation Server AS-B (Opens the Web Help page for the product)
- Automation Server – User manual

9.2 Retail IMP resources

- Terms of Use – This can be found in the Retail IMP platform (Press the question mark symbol on the upper right corner of the platform)
- Retail IMP Commissioning Guide *(coming soon)*

9.3 General resources

- Schneider Electric Data Privacy Policy (Opens the policy webpage)
- Schneider Electric Cybersecurity and Data Protection Posture (Opens the posture webpage)
- Microsoft Service Trust Portal (Opens the portal webpage)
- EcoStruxure Building Management, System Hardening Guide. (Opens the EcoXpert Xtranet)