SIEMENS

Industrial Edge - Security Overview 04/22

System Manual

04/2022

A5E50210335-AI

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

⚠DANGER

indicates that death or severe personal injury **will** result if proper precautions are not taken.

⚠WARNING

indicates that death or severe personal injury **may** result if proper precautions are not taken.

⚠CAUTION

indicates that minor personal injury can result if proper precautions are not taken.

NOTICE

indicates that property damage can result if proper precautions are not taken.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

⚠WARNING

Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

A5E50210335-AI
Ⓟ 04/2022 Subject to change

Preface

Purpose of this document

This documentation provides an overview with regard to security guidelines and requirements that apply to Industrial Edge and its components.

This documentation is aimed at all operators who operate and use the components of Industrial Edge.

Scope of this document

The security statements and guidelines in this documentation are valid for Industrial Edge and apply to the following manuals:

- Industrial Edge Management - Getting Started (https://support.industry.siemens.com/cs/us/en/view/109779989)
- Industrial Edge Management - Operation (https://support.industry.siemens.com/cs/us/en/view/109780393)
- Industrial Edge - Release Notes (https://support.industry.siemens.com/cs/us/en/view/109780394)
- Industrial Edge App Publisher - Operation (https://support.industry.siemens.com/cs/us/en/view/109780392)
- Industrial Edge Device - Operation (https://support.industry.siemens.com/cs/us/en/view/109783785)
- Industrial Edge - Update Procedures (https://support.industry.siemens.com/cs/us/en/view/109795343)
- Industrial Edge - Publishing Apps to the IE Hub (https://support.industry.siemens.com/cs/us/en/view/109803581)

Convention

The term "Edge Device" is used in this documentation to designate hardware with a configured Industrial Edge Device OS.

Instead of the product designation "Industrial Edge Apps", the short forms "Edge Apps" and "Apps" are also used.

Instead of the product designation "Industrial Edge System Apps", the short form "System Apps" is also used.

Instead of the product designation "Industrial Edge Device", the short form "Edge Device" is also used.

Instead of the product designations "Industrial Edge Databus" and "Industrial Edge Databus Configurator", the short forms "Databus" and "Databus Configurator" are also used respectively.

Instead of the product designations "Industrial Edge Cloud Connector" and "Industrial Edge Cloud Connector Configurator", the short forms "Cloud Connector" and "Cloud Connector Configurator" are also used respectively.

Table of contents

Industrial security 1

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit (http://www.siemens.com/industrialsecurity).

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed at (https://support.industry.siemens.com/cs/start?).

Security overview 2

2.1 General Data Protection Regulation (GDPR)

Siemens adheres to the principles of data protection, in particular the principles of data minimization (Privacy by Design).

For this product, Industrial Edge, this means:

Personal data

The product processes and stores the following personal data:

- First name and last name (Sign up)
- Email address
- Passwords
- Timestamp
- Location data (time zone)
- IP addresses
- MAC addresses

If the customer links the data mentioned above to other data (e.g. shift plans) or if the customer saves personal information on the same medium (e.g. hard disk) and thus creates a personal reference, the customer has to ensure that the guidelines regarding data protection are observed.

Purposes

The data mentioned above is required for the following purposes:

- Access protection and security measures (for example login, IP addresses)
- Process synchronization and integrity (for example information about time zones, IP addresses)
- Archiving system for traceability and verification of processes (for example access timestamps)
- Message system for traceability and availability (for example e-mail notification)

Storage of the data is affected for a suitable purpose and is limited to what is strictly necessary, as the information is indispensable in order to identify the authorized operators.

Securing of data

The above data will not be stored anonymously or pseudonymized, as the purpose (identification of the operating personnel) cannot be achieved otherwise. The data will be used only within the product and will not be automatically passed on to third parties or unauthorized persons.

The above data is secured by adequate encryption technologies

The customer must ensure the access protection as part of his process configuration.

Deletion policy

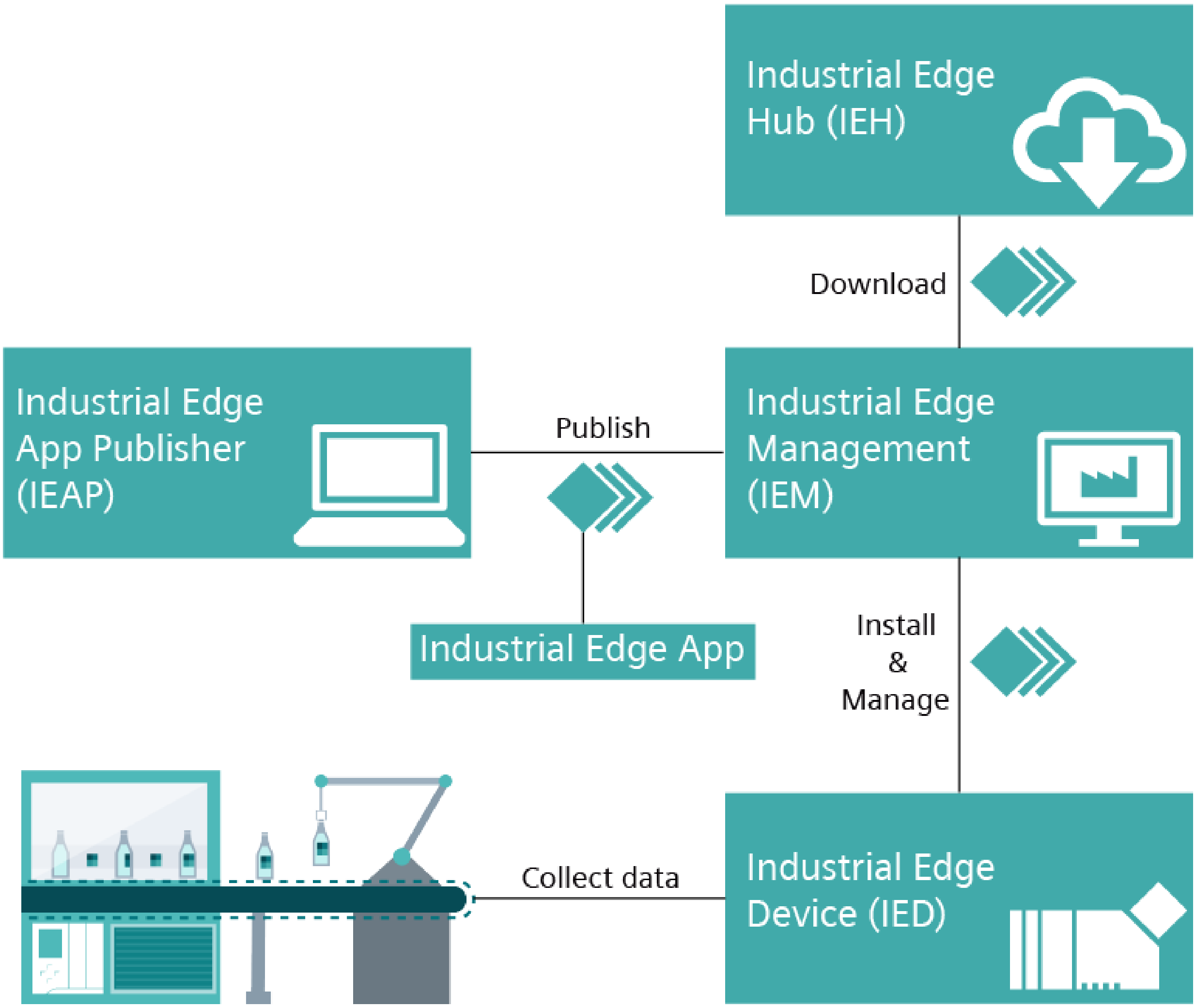
This product does not provide an automatic deletion of the data mentioned above.

Cookies

Regarding cookies, please refer to the Siemens cookie guidelines (https://new.siemens.com/global/en/general/cookie-notice.html).

2.2 System overview

The Industrial Edge Ecosystem provides a vertical integration of the shop floor to the cloud services. The Edge App and Edge Device management features are provided on a secured platform at all instances.

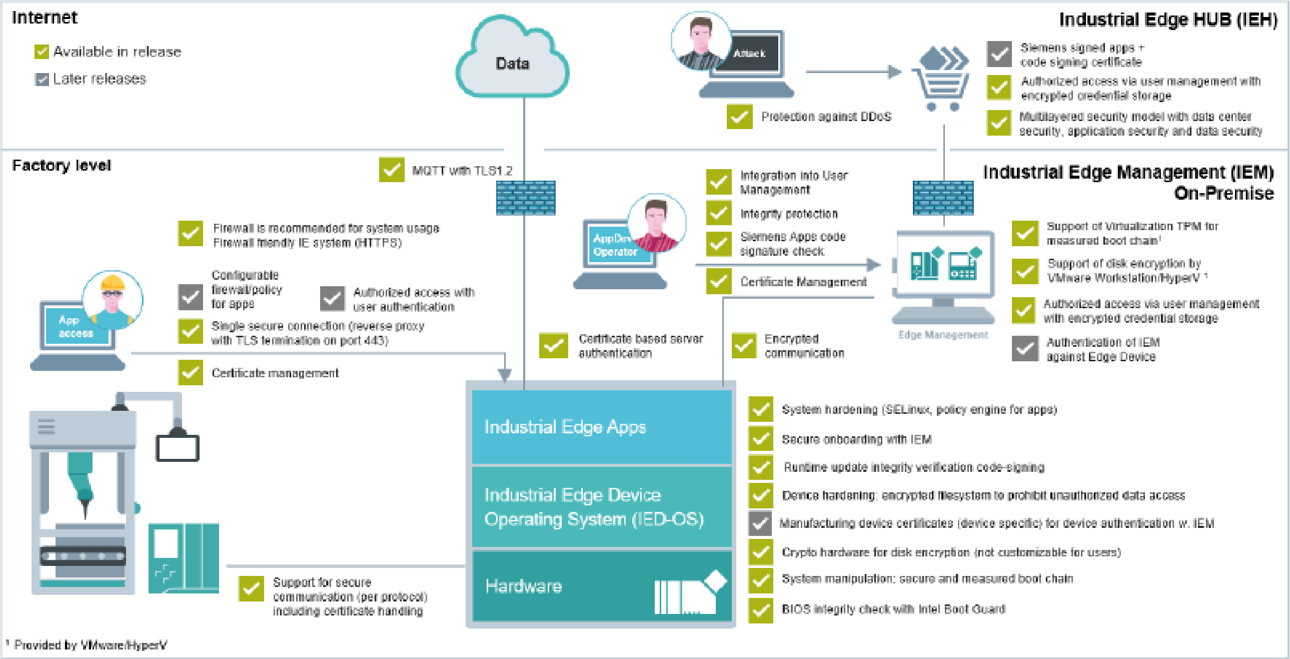

Industrial Edge Hub (IEH)
Download
Industrial Edge App Publisher (IEAP)
Publish
Industrial Edge Management (IEM)
Industrial Edge App
Install & Manage
Collect data
Industrial Edge Device (IED)

The main components of Industrial Edge are:

Component	Description
Industrial Edge HUB (IEH)	Download and manage system software and Edge Apps
Industrial Edge Management (IEM)	App and Edge Device management for Industrial Edge
Industrial Edge Device (IED)	Decentral Industrial Edge computing unit
Industrial Edge App Publisher (IEAP)	Create and publish Edge Apps
Industrial Edge App	Self-contained entity based on Docker containing functionality for intelligent processing of automation data

2.3 Integrated security measures

Security measures overview

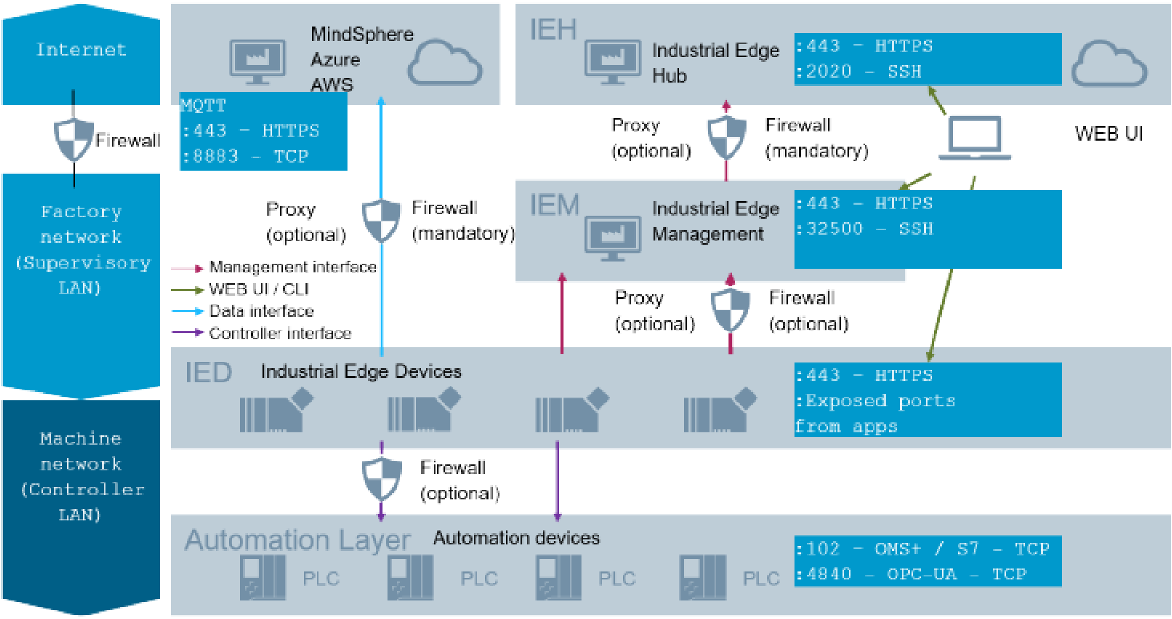

Internet
Available in release
Later releases
Data
Attack
Protection against DDoS
Industrial Edge HUB (IEH)
Siemens signed apps + code signing certificate
Authorized access via user management with encrypted credential storage
Multilayered security model with data center security, application security and data security
Factory level
MQTT with TLS1.2
Firewall is recommended for system usage
Firewall friendly IE system (HTTPS)
Configurable firewall/policy for apps
Authorized access with user authentication
Single secure connection (reverse proxy with TLS termination on port 443)
Certificate management
App access
AppDev Operator
Integration into User Management
Integrity protection
Siemens Apps code signature check
Certificate Management
Certificate based server authentication
Encrypted communication
Industrial Edge Management (IEM) On-Premise
Support of Virtualization TPM for measured boot chain¹
Support of disk encryption by VMware Workstation/HyperV ¹
Authorized access via user management with encrypted credential storage
Authentication of IEM against Edge Device
Edge Management
Industrial Edge Apps
Industrial Edge Device Operating System (IED-OS)
Hardware
System hardening (SELinux, policy engine for apps)
Secure onboarding with IEM
Runtime update integrity verification code-signing
Device hardening: encrypted filesystem to prohibit unauthorized data access
Manufacturing device certificates (device specific) for device authentication w. IEM
Crypto hardware for disk encryption (not customizable for users)
System manipulation: secure and measured boot chain
BIOS integrity check with Intel Boot Guard
Support for secure communication (per protocol) including certificate handling
¹ Provided by VMware/HyperV

Data

The data connection depends on the installed Apps. Siemens proposes the usage of an encrypted protocol like MQTT with TLS 1.2.

2.4 Operational environment - Example

The following figure shows the setup of the Industrial Edge system as an example.



The customer IT security concept needs to decide and adjust the setup and network protection concept. The Industrial Edge Management and Edge Devices must not be operated in zero trust networks.

In general, all system components are initializing connections from lower level to upper level using a secured communication channel.

Note

Source Network Address Translation (SNAT)

Industrial Edge is not supporting Source Network Address Translation for Edge Devices and IEMs.

Apps

Apps can run behind a central incoming traffic endpoint which is responsible for TLS termination, secure HTTP header injection and minimizing certificate management in 1 location.

2.4.1 Contacted domain names

For a flawless operation of Industrial Edge, customers must enable access to the following domains to ensure the required connectivity between all Industrial Edge components. All services are using dynamic set of IP addresses and are subject to change at any time, so resolving the domain names and using the IP addresses within the proxy or firewall is not recommended.

Communication from IEM to IE Hub:

- portal.eu1.edge.siemens.cloud
- portal-hub.eu1.edge.siemens.cloud
- portalhub.eu1.edge.siemens.cloud
- portal-relay.eu1.edge.siemens.cloud
- portalauth.eu1.edge.siemens.cloud
- artifacts.eu1.edge.siemens.cloud
- oss.eu1.edge.siemens.cloud
- applications.eu1.edge.siemens.cloud

User communication via browser to IE Hub:

- *.iehub.eu1.edge.siemens.cloud
- artifacts.eu1.edge.siemens.cloud
- oss.eu1.edge.siemens.cloud
- upload.applications.eu1.edge.siemens.cloud
- applications.eu1.edge.siemens.cloud

Email sending domains:

- siemens.com
- eu-west-1.amazonses.com
- edge.siemens.cloud
- eu1.edge.siemens.cloud

User authentication flow to log in to IE Hub:

- siemens-00035.eu.auth0
- login.siemens.com
- cdn.login.siemens.com
- cdn.auth0.com
- cdn.eu.auth0.com
- s.gravatar.com
- i2.wp.com

Note

User authentication flow domains

These domains might change due to system optimizations.

2.4.2 IP protocols and ports

The following table shows the required network settings of Industrial Edge. Customers need to apply ingress and egress rules in their firewalls to ensure the required connectivity between all Industrial Edge components:

Component	Port	Protocol	Direction	Usage
Industrial Edge Management	123, UDP	NTP	Egress	Network time synchronization
Industrial Edge Management	53, UDP	DNS	Egress	Domain name resolution
Industrial Edge Management	123, UDP	NTP	Ingress	Network time synchronization, acting as server
Industrial Edge Management	443	HTTPS	Ingress	IE Management UI (DNS-based setup)
Industrial Edge Management	9443, 9444	HTTPS	Ingress	IE Management UI (IP-based setup)
Industrial Edge Management	2020	SSH	Egress	Remote support channel for the IEM
Relay server in the Industrial Edge Management	32500 - 32700	SSH	Ingress	Remote access for Edge Devices
Industrial Edge Hub	443	HTTPS	Ingress	Industrial Edge Hub UI
Industrial Edge Hub	2020	SSH	Egress	Remote support channel for the IEM
Industrial Edge Device	443	HTTPS	Egress	IE Management UI (DNS-based setup)
Industrial Edge Device	123, UDP	NTP	Egress	Network time synchronization
Industrial Edge Device	443	HTTPS	Ingress	Edge Device UI
Industrial Edge Device	9443, 9444	HTTPS	Egress	IE Management UI (with IEM self-signed certificates, IP-based setup)
Industrial Edge Device	32500 - 32700	SSH	Egress	Remote access for Edge Devices
Industrial Edge App Publisher	443, 9443	HTTPS	Egress	IE Management UI

Customer-reachable UIs

IE component	IP-based setup	DNS-based setup	Remark
IEM-OS	https://<IP>:443	-	DNS not possible
IEMA	https://<IP>:9443	https://<hub-name>:443	-
IED	https://<IP>:443	https://<IP>:443	If DNS is used, name must be included in certificate

2.5 Industrial Edge components - Security measures

2.5.1 Industrial Edge Hub security

Component	Purpose	Description
Single sign-on with multifactor authentication	To allow only authenticated and authorized access to resources	User logins are protected by a strict password policy.
Certified data center provider	Ensure professional, secure and highly available operations of data centers	The IE Hub is hosted on platforms of certified data center providers only. Shared responsibilities principles are applied between data center provider and the IE Hub operator. Data center provider is certified according to SOC 2 and ISO 27001.
Shared responsibility principle and certified data center provider	To separate data and operation from platform and service	Shared responsibilities principles are applied between data center provider and IE Hub operator. Data center provider is certified at least according to SOC 2 and ISO 27001.
Firewall	Firewall configuration of data center services	Web Application Firewall (WAF) or Next-Generation Firewall (NGFW) are used within data centers to protect the endpoints.

2.5.2 Industrial Edge Management security

Component	Purpose	Description
IMA	Linux Integrity Measurement Architecture	Industrial Edge implements the Linux Integrity Measurement Architecture (IMA) to guarantee the integrity of the loaded modules.
Measured boot	Measure trusted boot and update channels	The measured boot checks the integrity of the whole boot chain and compares it with the trusted initial deployment. The fingerprints are stored in crypto hardware.*
Full disk encryption	Encrypted rootfs and data partitions	All system partitions are encrypted and locked by crypto hardware.*
Policy engine	Supervise app policies	The policy engine checks the associated app policy and enforces that only applied capabilities and resources are used by the app.
No root user login	Allow only user access	The Industrial Edge Management Operating System (IEM-OS) does not provide any possibility to login as root user.
System update	Keep the system updated and secure	A system update functionality is provided by the Industrial Edge Management. Security patches and system updates are published in the IE Hub shortly after vulnerabilities are known and issues are fixed.

*For deployments on hosting environments with Trusted Platform Module (TPM).

2.5.3 Industrial Edge Device security

The Industrial Edge Device is hosting apps as well as the app and device management software. These components are secured in respect to CIA (Confidentiality, Integrity, Availability) through the feature set listed below.

Component	Purpose	Description
Trusted deployment	Trusted environment for first installation	The Edge Device is delivered with a fully installed Industrial Edge Device OS (IED-OS), secured by default from the manufacturer site.*
Secure Boot	Verified boot artifacts	With Secure Boot, UEFI will only launch verified and unaltered Industrial Edge boot artifacts which are digitally signed by Siemens.
IMA	Linux Integrity Measurement Architecture	Industrial Edge implements the Linux Integrity Measurement Architecture (IMA) to guarantee the integrity of the loaded modules.
Measured boot	Measure trusted boot and update channels	The measured boot checks the integrity of the whole boot chain and compares it with the trusted initial deployment. The fingerprints are stored in crypto hardware.
Full disk encryption	Encrypted rootfs and data partitions	All system partitions are encrypted and locked by crypto hardware.
No root user login	Prevents access to the administrative root account trough console or the network	The Industrial Edge Device Operating System (IED-OS) does not provide any possibility to login as root user.
Digital signatures for Industrial Edge software artifacts	Integrity and authenticity of the software artifacts	CMS (Cryptographic Message Syntax) signatures and dedicated Industrial Edge code signing certificates ensure that the code has not been corrupted and the origin of the software has not been altered.
Secure onboarding	Trust establishment from Edge Devices to the Industrial Edge Management	The onboarding process is secured by an expiring session token from the Industrial Edge Management backend. The onboarding file is encrypted for confidentiality.*
System update	Keep the system updated and secure. Possible from the IEM and schedule possible.	A remote system update functionality is provided by the Ecosystem. The operator of the Industrial Edge Management is notified on the availability of new IED-OS. Updating Edge Devices can be directly initiated and scheduled in the IEM.

*planned

2.5.4 Industrial Edge App Publisher security

The Industrial Edge App Publisher communicates with the IEM using secured HTTPS communication. It is treated as component of the Industrial Edge Management and must therefore run inside the customer's internal network (intranet).

2.5.5 Industrial Edge App security

The Industrial Edge Ecosystem provides certain features for secure Edge App operation.

Note

Edge Apps are operated in a containerized environment and are only receiving the privileges they require to run properly, hence following the least privilege principle. Privileges can be reviewed by the operator.

During deployment of the Edge App, the operator is notified about privileges and resources requested from the Edge App. The operator can either accept or deny these privileges. Siemens Edge Apps are digitally signed by Siemens, and are presented to the operator as trusted Edge Apps.

Requirement	Purpose	IE offering & app partner responsibility
Confidentiality	Encrypted communication for the UI	• Reverse Proxy • Central TLS termination for system and apps authentication
	Encrypted communication for data traffic: • Datac sent to the cloud • Data collected from PLCs	To be done by App Provider
	Secure storage of data and configuration (e.g cloud access credentials)	IED disk encryption
	Separation from other Apps on IED	-
Integrity	App File Integrity	Digital signing of apps
Availability	Backup of App	Provided by IED backup
	Backup of configuration	To be done by App Provider
	Offline Operation	IED and apps can operate completely offline. Even when the administrative connection is lost, data is still collected and forwarded. Connection is only required for maintenance purposes, for example for updates or new app deployments, and are fully controlled by the operator.
	Read and write of PLC tags	Apps may be capable of reading and writing all PLC tags and therefore impact the plant severely. Apps should describe the possibility to secure this like the S7 connector.

2.5.6 Hardware security

The Industrial Edge portfolio contains security hardened hardware. Edge Devices provide a set of built in features to securely protect the system.

Component	Purpose	Description
Intel® Boot Guard	Protect BIOS	Intel® Boot Guard provides hardware enforced boot controls and ensure that only authorized and unaltered BIOS code can be run on the Edge Devices.
BIOS signature	Protect BIOS	The Edge Device BIOS is protected over the whole lifecycle through signatures.
Secure Boot	Verify boot artifacts	With Secure Boot, UEFI will only launch verified and unaltered Industrial Edge boot artifacts which are digitally signed by Siemens.
Crypto hardware	Disk encryption	The Industrial Edge provides hardware modules to encrypt the storage.
Crypto hardware	Measured boot	The crypto hardware measures and supervises the boot chain.
Manufacturer device certificate	Hardware authenticity	The manufacturer device certificate provides a proof-of-origin of the Edge Device provisioned during the manufacturing process.*
Separate network interfaces	Separation of IT and OT networks	Industrial Edge hardware provides at least 2 separate physical network interfaces, which may be used to segregate OT and IT networks.*

*planned

2.5.7 Network security

This section applies to all user sessions in the Industrial Edge Ecosystem.

Component	Purpose	Description
System firewall	Minimize attacks for Industrial Edge Devices (IED)	By default, on the IED only port 443 is open, protected through Transport Layer Security (TLS). Incoming traffic is routed through this port. Apps on the IED can open further ports on demand. By default, on the IEM the port 443/9433/9444 is exclusively open, and the customer can configure a specific port range for the relay server functionality.
Web interfaces	Common termination of TLS for all services	All web interfaces are secured through TLS 1.2 and strong cipher suites. Secure HTTP headers and cookies with Secure-Flag are applied on all web interfaces to mitigate common web vulnerabilities.
User authentication on web services	Allow only authenticated and authorized access to web services	The user is authenticated through username and password by a central authentication service and gives him the rights defined by the administrator. The session is protected by an expiring session token.
DoS	Denial-of-Service attacks	Each user session is protected against Denial-of-Service attacks by applying IP-based rate limiting.

2.6 Industrial Edge standards

Industrial Edge is developed by Siemens in accordance with open and internal standards.

Standards and Organization

Standard	Processes	Comment
Charter of Trust	Guidance for cyber security	Siemens is core member of the Charter of Trust which is applied in Industrial Edge.

Secure operation recommendations 3

3.1 Setup guidelines and recommendations

All components of the Industrial Edge Ecosystem follow the security by default paradigm. In addition, the operation of components needs to consider several aspects.

Securing first setup of the Industrial Edge Management

The first setup of the Industrial Edge Management must be performed in a protected LAN network to ensure that the initial credentials and settings are given by an authorized administrator. No default certificates are being used to ensure the identity of the servers and system during the first setup.

Customers are responsible for protecting and securing the first setup of the Industrial Edge Management in a protected LAN network and for preventing unauthorized access to it.

Securing Industrial Edge Management PCs and the VM

The Industrial Edge Management is provided as an installation medium (ISO image) that needs to be set up in a virtual machine (VM).

Customers are responsible for storing the VM in a secure environment prior to installation and for protecting the Industrial Edge Management and the VM by external measures and firewalls against direct access from the Internet.

Customers are responsible for securely handling the medium during transition, storage, installation and operations. Furthermore, customers are responsible for protecting the Industrial Edge Management PCs prior to installation and during operation and for preventing unauthorized access to the Industrial Edge Management PCs.

It is strongly recommended to install the Industrial Edge Management on a server or PC which is locked in a cabinet and to provide a virtual TPM for the VM by the virtualization environment.

Protection of USB flash drives

Onboarding Edge Devices to the Industrial Edge Management can be done through an USB flash drive. When onboarding the Edge Device to the Industrial Edge Management, unencrypted configuration data, sensitive system data and customer's network data (proxy password is encrypted) are stored on the USB flash drive. Customers are responsible for keeping the configuration data on the USB flash drive, and in general the configuration file, safe (confidential and integrity protected).

Customers are responsible to securely store the USB flash drive that contains the sensitive configuration data for connection of Edge Devices and prevent unauthorized access to the USB flash drive.

Customers are also responsible for applying the security guidelines regarding the use of USB flash drives in production facilities.

Passwords

Use only strong passwords containing upper- and lower-case letters as well as non-alpha numerical characters with a minimum length of 12 characters. The system assists you in setting strong passwords.

Industrial Edge Management administrators

During the setup of the Industrial Edge Management, the admin users for the IEM-OS and for the Industrial Edge Management are created by the operator of the setup.

Subdomains for IEM with system services

For the Industrial Edge Management, several subdomains are established during the setup. DNS entries must be setup by the administrator.

BIOS

SIMATIC Edge Devices are not delivered with a BIOS password. Customers are strongly recommended to set a BIOS password.

To secure the boot process and of Industrial Edge Devices, it is recommended to set an individual, strong BIOS password during the setup.

Secure onboarding of Edge Devices

The onboarding process of Edge Devices must be in a secure environment, as there might be unencrypted configuration data, sensitive system data and customer's network data exchanged in this process.

Web server authentication

During the initial setup, each component (Industrial Edge Management and Edge Device) will be associated with a unique ID known to the upper level. The operator must perform this association of unique IDs on a protected network connection respectively when connecting the Edge Device to the Industrial Edge Management through an USB flash drive.

3.2 Network security and segmentation

Client access to Industrial Edge Management

The Industrial Edge Management should not be accessed through the Internet. Clients that want to access the Industrial Edge Management or Edge Devices must be located in the plant network or the Supervisory LAN.

Protection of Configurators within Industrial Edge Management

In Industrial Edge, the following Configurators, for example, are used for a flawless functionality of the Industrial Edge Management:

- SIMATIC S7 Connector Configurator
- Industrial Edge Databus Configurator
- Industrial Edge Cloud Connector Configurator

Customers are responsible for implementing appropriate security measures to ensure the secure operations of the configurators within the Industrial Edge Management and for preventing unauthorized access to the configurators.

Ethernet communication

With Ethernet-based communication, customers are responsible for the security of their data network because proper functioning cannot be guaranteed under all circumstances, for example, in the event of targeted attacks that result in an overload of the Industrial Edge Management PCs or Edge Devices.

Protection of the internal network

The Industrial Edge Management is located and runs inside the customer's internal network (intranet).

Customers are responsible for protecting their internal network (intranet) and thus for protecting the Industrial Edge Management and for preventing unauthorized access to their internal network.

Network communication

The Industrial Edge Management and its components must be installed in a protected zone that does not include other untrusted systems and software.

The Transmission Control Protocol (TCP) is exposed in plain text and is strictly limited to the internal network which is trusted and protected from external access. The interface of the Industrial Edge Management is exposed encrypted to other than internal networks and requires authentication.

IT infrastructure

Customers are responsible for an IT infrastructure that is administrated and operated according to common IT security rules and guidelines. For example, virus scanned and up to date IT infrastructure.

Protection of Industrial Edge Management and Edge Devices

Customers are responsible for implementing appropriate security measures to ensure the secure operations of the Industrial Edge Management and Edge Devices.

In the Industrial Edge Management, relay servers are in use. Relay servers are required when Edge Devices are placed in a plant network that is separated for example by NAT Gateway from the control plane network in which the IEM is running. This relay server allows to access the Edge Devices from the control plane network. Customers are responsible for protecting the relay servers within the Industrial Edge Management and for preventing unauthorized access to the relay servers.

3.3 Identity and access management

The identity and access management is the process of granting authorized users the right to use a service, while preventing access to non-authorized users. Identity and access management can also be referred to as rights management.

The identity and access management ensures the right for users to be able to use a service or group of services. Access management is the execution of information security policies and actions. It also protects the Confidentiality, Integrity and Availability (CIA).

The identity and access management has the following tasks:

- Grant access to services, service groups, data or functions only if the entity is entitled to that access
- Remove access when people change roles or jobs
- Regular audits of the access permissions to ensure they are still correct

Industrial Edge provides an integrated user management for the IE Hub, the IE Management and for Edge Devices.

Brute force protection

Login attempts are limited to 5 attempts for 15 minutes. In this period, this user cannot log in and must wait.

Notes on protecting administrator accounts

A user with administrator rights has extensive access and manipulation options available in the system.

Therefore, customers must ensure that adequate security guards for protecting the administrator accounts are in use to prevent unauthorized changes. Therefore, secure passwords and a standard user account for normal operation shall be used. Other measures, such as the use of security policies, should be applied as needed.

Following the segregation of duties principle, only administrative tasks are done with privileged accounts whereas daily operation tasks are to be handled with non-privileged user accounts.

3.4 Secure channels and encryption

Certificates

In Industrial Edge, certificates are used for accessing the Industrial Edge Management and Edge Devices. For security reasons, customers can import their own certificates for the Industrial Edge Management and Edge Devices. Managing certificates is possible through the UI of the IEM and the Edge Devices which are secured through TLS 1.2 with strong cipher suites. The certificates are internally stored within a secure trust store.

If you are running the IEM and Industrial Edge Devices with self-signed certificates, consider the information from this FAQ (https://support.industry.siemens.com/cs/ww/en/view/109795516).

3.5 Security logging and monitoring

Data logging and monitoring is the process of collecting and storing data over a period of time to analyze specific trends or record the data-based events of a system, network or IT environment. It enables tracking of all interactions. Interactions through which data, files, or applications are stored, accessed, or modified, whether on a storage device or application. Logging can produce technical information usable for the maintenance of applications. It supports:

- Identifying performance of the system/application
- Reporting errors, incidents, and other incorrect behavior
- Defining whether a reported bug is a bug
- Analyzing, reproducing and solving bugs
- Testing new features in a developmental stage

Currently, Industrial Edge only supports local storage of log files within IEDs and the IEM. The logs are write-protected from external.

Requirements for operation

Requirement	Remark
Set up logging and monitoring to a central system	Comprehensive Linux OS logging mechanisms in place for all components and applications
Log files need to be access-protected	Supported by Industrial Edge
All security relevant functionalities and all security relevant parts of the service need to be monitored	Supported by Industrial Edge
Review log files regularly, set up process	To be done by customer

3.6 Backup and restore

Recovering and reconstituting an automation control system to a known state after a disruption of failure is an important topic in the defense in depth concept and recommended in the IEC 62443.

In a backup and restore strategy, all the data which are necessary for recover and their location in the system are identified. The frequency of creating backups, the kind of backup (complete, differential or incremental) and the storage location of the backups are described in this strategy.

Backup will be categorized as following:

- System backup: The IEM is saved completely as full system using virtual machine snapshots.
- Data/Configuration backup: Apps and configurations are saved in the IED backup.

Restoring is more critical than the creation of backups. This process must be tested and reproduced to guarantee fast availability of the plant systems in case of emergency and minimizes downtimes.

Deleting of IEDs

If IEDs are deleted from the IEM, the respective backup is not deleted. It can be restored to any other IED (which will be overwritten).

Protection against power loss

Customers are responsible for integrating means to protect all operating Industrial Edge Devices and the PC respectively the host on which the Industrial Edge Management VM is running against power loss. Siemens recommends integrating an uninterruptible power supply (UPS) to back up data and to shut down the Industrial Edge Management VM correctly. In case of an unprotected power loss, the Industrial Edge Devices and the IEM might not work anymore and need to be restored or set up again.

Requirements for operation

- Create backup plan and implement regular backups
- Create disaster recovery plan and define responsibilities
- Implement regular recovery tests

3.7 Attack Surface Reduction

Physical access to IE components

The Industrial Edge Management and its components must be installed in a protected zone that ensures physical access is limited to authorized personnel only. Customers are responsible for the use of unauthorized removable devices, for example USB flash drives, and for its caused damages.

3.8 Vulnerability management

Siemens CERT

Siemens tracks and announces application specific vulnerabilities for all products. Customers can register under this link (https://siemens.com/industrialsecurity) to the mailing list to get updates on all known vulnerabilities.

Vulnerability Manager

Software and hardware components embedded in Automation Control Systems and products are regularly affected by security flaws that shall be mitigated to reduce the risk of cyber-attacks on plants and factories. As part of a global patch management concept, it is needed to monitor the individual hardware and software components over the time to identify the flaws affecting them.

The Siemens software solution is the Industrial Vulnerability Manager (https://support.industry.siemens.com/cs/us/en/sc/4990).

3.9 Patch management

Patch management is a strategy for managing patches or upgrades, for example OS and security patches, for software applications, services and technologies. A patch management plan can help handle these changes efficiently. Patches are often necessary to fix problems with software that are noticed after the initial release. Many of these patches relate to security. The specific functionality of programs and services could be affected.

Information on updates

Industrial Edge provides mail notifications on updates of IE components for registered users in the IE Hub.

The IVM can help monitoring the component versions and getting information on available updates on known vulnerabilities.

Update

Industrial Edge provides updates of the IEM directly in the IE Hub. You can download the current release from the IE Hub.

IEDs can be updated through the respective IEM. The version is downloaded in the Device Catalog in the Admin UI of the IEM, and released by the IEM admin to the IED update interface in the IEM.

Overview on updatable IE components

Rollback

You can select all released versions of an app to be able to roll back to an older version, if needed.

You should backup the IEM and IEDs before any updates, so you can restore the previous state. The procedure is described in the respective manuals.

Scheduling

With the option to schedule updates, it is easy to select a suitable maintenance timeslot.

Requirements for operation

Requirement	Remark
Monitor for available updates	Siemens regularly offers security updates
Test updates on test systems	Updates can be applied on individual test systems
Schedule updates of Edge Devices	Updates can be planned

3.10 Malware protection

The Industrial Edge Management is located and runs inside the customer's internal network (intranet).

Customers are responsible and must be capable of protecting the Industrial Edge Management, its components and the internal network from malware infection.

Software installation - Agents and Antivirus

Typically, system installations require endpoint security through software installations like antivirus software, endpoint security agents or whitelisting installation.

This is not possible in Industrial Edge (IEM and IEDs), as these are closed and hardened Linux-based appliances. Refer to the "Industrial Edge components - Security measures (Page 16)" chapter to check which measures are already taken to harden the devices.

Software hardening

Industrial Edge is in full control of the host operating system. The delivered artifacts are hardened according to the Siemens Industry development guidelines:

- Up to date patch level
- Virus scanned
- Penetration tested before delivery
- Integrity and authenticity of the artifacts is protected via PKI based code signatures

3.11 Read and write access to PLCs

Read and write access to controllers

Industrial Edge provides the "SIMATIC S7 Connector Configurator" which supports read and write access to controller data. By default, all tags have read access only.

When configuring tags, the following options are available as part of the access mode:

- Read: Tags will only be read from controllers. This option is selected by default.
- Read & Write: In this access mode, tags can be read and written. This access mode is not selected by default. If customers want to write tag values to controllers, they can change the access mode to "Read&Write" in the configurator.

Customers also can restrict writing of tag values to controllers by disabling the "Writable from HMI/OPC UA" column feature in the TIA Portal.

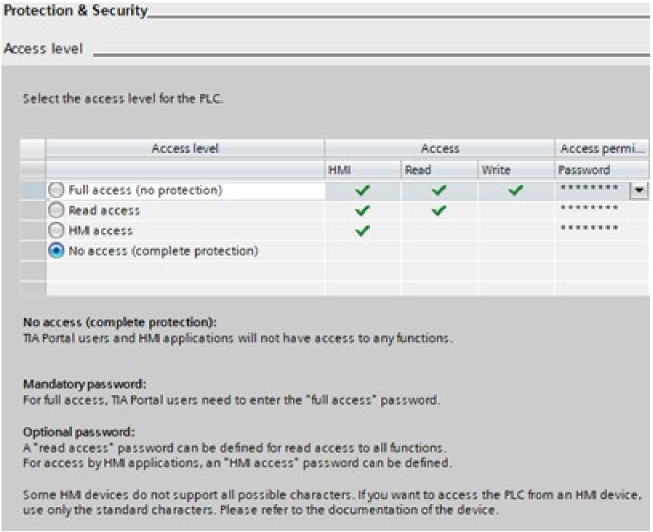
Furthermore, customers can implement apps with read and write access to controller data. Customers are responsible for Edge Apps and self-developed apps with read and write accesses to controller data. Customers are responsible for any damages that are caused by changing or overwriting controller data. In addition, customers are also responsible for protecting their self-developed apps that have write access to controller data with regard to security and preventing unauthorized access to these apps.

Securing in the PLC

Customers restrict access and writing of tag values in the controller by disabling the "Writable from HMI/OPC UA" column feature in the TIA Portal. For confidential process data or variables which should be read-only it is recommend restricting the access in the PLC directly as it is not depending on the configuration of any external program.

This should be used by PLC operators to further secure and limit the access to any PLC variable.

In the S7 Connector you can use the password for the respective PLC protection level:



Protection & Security

Access level

Select the access level for the PLC.

Access level	Access			Access permi...
	HMI	Read	Write	Password
○ Full access (no protection)	✓	✓	✓	********
○ Read access	✓	✓		********
○ HMI access	✓			********
● No access (complete protection)				

No access (complete protection):
TIA Portal users and HMI applications will not have access to any functions.

Mandatory password:
For full access, TIA Portal users need to enter the "full access" password.

Optional password:
A "read access" password can be defined for read access to all functions.
For access by HMI applications, an "HMI access" password can be defined.

Some HMI devices do not support all possible characters. If you want to access the PLC from an HMI device, use only the standard characters. Please refer to the documentation of the device.

3.12 Secure app development

Docker security policies

Industrial Edge supports the use of Docker and Docker containers.

By publishing this product, Siemens provides the latest Docker security policies.

Usage of trustworthy Docker images

Customers are responsible for the content and security of their apps. Furthermore, customers are responsible for using only trustworthy Docker images from a trustworthy Docker registry respectively from trusted resources for their own apps and check them accordingly. Customers also must ensure to deliver security patches in a certain time.

Protection of the customer's development environment

Customers are responsible for protecting their own development environment and preventing unauthorized access to their development PCs. Furthermore, development PCs are expected to be protected according to latest security standards which usually demands virus scans, update procedures and disk encryption.

3.13 App security

Protection of customer apps

Customers are responsible for implementing all required security measures protecting their self-developed apps with regard to security, and for preventing unauthorized access to their own apps.

Access control of customer apps

Customers are responsible for the access control of each own developed app and for preventing unauthorized access to their apps.

Data protection

In Industrial Edge, customers have the possibility to store data outside of Edge Devices such as in their cloud infrastructure.

Customers are responsible for the confidentiality, integrity and availability (CIA) of data stored outside of Edge Devices and for preventing unauthorized access to the stored data.

Sensitive resources and secrets in Edge Apps

In Industrial Edge, customers can develop their own Edge Apps, upload the apps to the IEM and install and run the apps on Edge Devices.

Do not store secrets and do not use sensitive system resources in mounted volumes of the host system in custom-developed and installed Edge Apps.

Encrypted communication between Edge Apps

Customers are responsible for implementing encrypted and secure communication (e.g. HTTPS using TLS 1.2 with strong cipher suites) for their apps.

Encrypted communication between multiple Edge Devices

Customers are responsible for implementing encrypted and secure communication (e.g. HTTPS using TLS 1.2 with strong cipher suites) between their Edge Devices.

Secure exposure of app communication

To secure the exposure of apps to the outer world, the apps can configure a reverse proxy which is already provided by the IED.

Customers may allow to host other apps too but must ensure and guarantee that the app provides the necessary security measures and standards.

List of abbreviations/acronyms 4

Abbreviation	Description
IE	Industrial Edge
IED	Industrial Edge Device
IEH	Industrial Edge Hub
IEM	Industrial Edge Management
IERT	Industrial Edge Runtime
IEAP	Industrial Edge App Publisher
IED-OS	Industrial Edge Device Operating System
IEM-OS	Industrial Edge Management Operating System
VM	Virtual Machine
UI	User Interface
CLI	Command Line Interface
IEFC	Industrial Edge Flow Creator
SAS	Shared Access Signature
SSH	Secure Shell
IoT	Internet of Things
DHCP	Dynamic Host Configuration Protocol
API	Application Programming Interface
TPM	Trusted Platform Module
LAN	Local Area Network
FQDN	Fully Qualified Domain Name
NTP	Network Time Protocol
L2	Layer 2
LLDP	Link Layer Discovery Protocol
CIDR	Classless Inter-Domain Routing
IEACS	Industrial Edge Application Configuration Service
IEDK	Industrial Edge Device Kit
IECTL	Industrial Edge Control
IESS	Industrial Edge State Service
DEX	Digital Exchange