Industrial Edge Security Guidelines

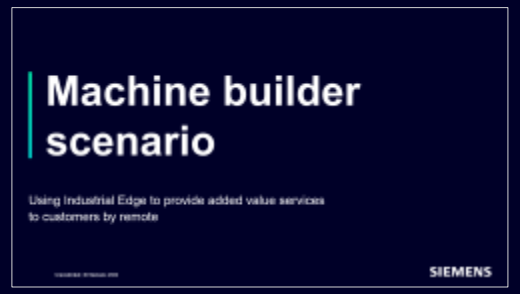
A comprehensive guide to secure your Edge solution

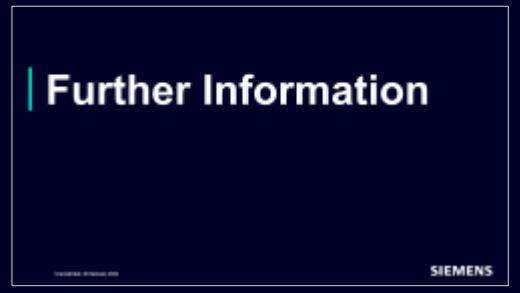
SIEMENS

Industrial Edge Security Guidelines
A comprehensive guide to secure your Edge solution

Document description

- This document acts as guideline to be considered when implementing your Industrial Edge solution in production.
- It gives comprehensive guidelines to get started either as plant operator or machine builder including all relevant tasks to be done such as certificate creation and firewall configurations
- For all of our guidelines we rely on guiding principles according to IEC 62443





SIEMENS

Glossary

Abbreviation	Meaning	Description
IE HUB	Industrial Edge HUB	Online Edge platform including app store. → Hosted by Siemens
IEM	Industrial Edge Management	Management system for Edge devices running in the customers architecture → Hosted by end customer or machine builder
IED	Industrial Edge Device	Device which is running apps managed by IEM → Hosted next to the machine
DHCP	Dynamic Host Control Protocol	Protocol used to automatically assign IP addresses to devices in the network
DNS	Domain Name Server	Server which translates FQDN into IP addresses
FQDN	Fully qualified domain name	Domain name of a device - stored in DNS server with IP address
NTP	Network Time Protocol	Protocol used to synchronize the system time of devices connected to the network
Proxy Server		Server which acts as an intermediary for requests →Usually located in IT networks
PKI	Public Key Infrastructure	Set of policies with hardware and software to manage digital certificates
CA	Certificate Authority	Entity that issues digital certificates
Root CA	Root Certificate Authority	Certificate Authority that owns one or more trusted roots. Usually the first (top level) CA in the trust chain
Intermediate CA	Intermediate Certificate Authority	Certificate Authority that issue a intermediate trust chains. Also known as “Sub CA”
On-premise		Software that runs on computers of the user (rather than cloud hosted software as a service)
(D)DoS	(Distributed) Denial of Service	Attack with the aim of making the server unavailable

Security Introduction

SIEMENS

Siemens Industrial IoT Stack

Applications

with a strong need for responsiveness, privacy, reliability and cost-efficiency can now be additionally deployed **on-premise** with Edge Computing, while still benefitting of the available IT- and OT-technology

Low-Code platform
Build apps faster for cloud, on-premise or hybrid infrastructure

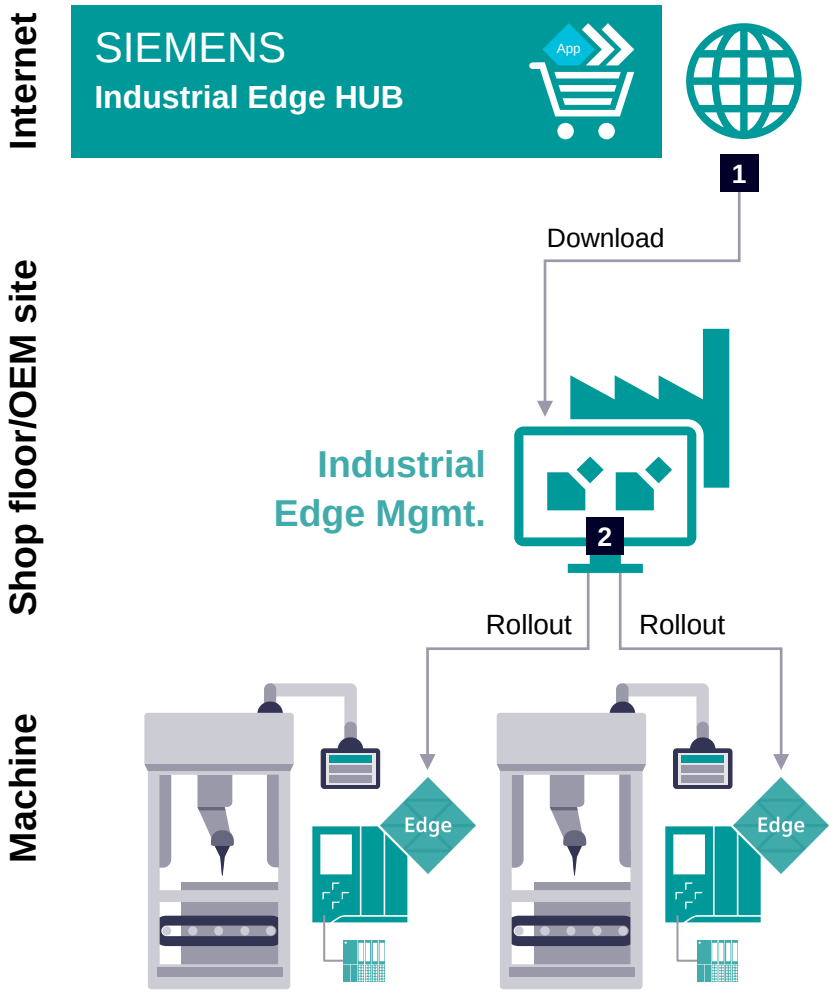
IIoT as a service
Centralized computing & storage, with solutions, apps & services

Edge Computing
Decentral computing & storage with device runtime, apps and management

Field/Control
Automation runtime and engineering connectivity

SIEMENS

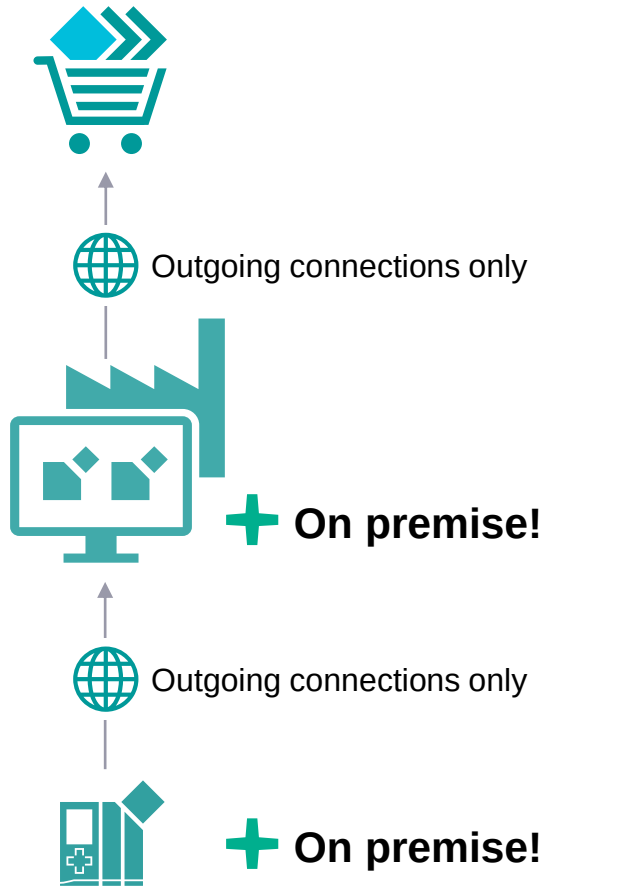
Industrial Edge
App Installation Workflow



IE HUB
App Store/Update provisioning

IE Management
Management of IE Devices
Rollout of configuration and apps

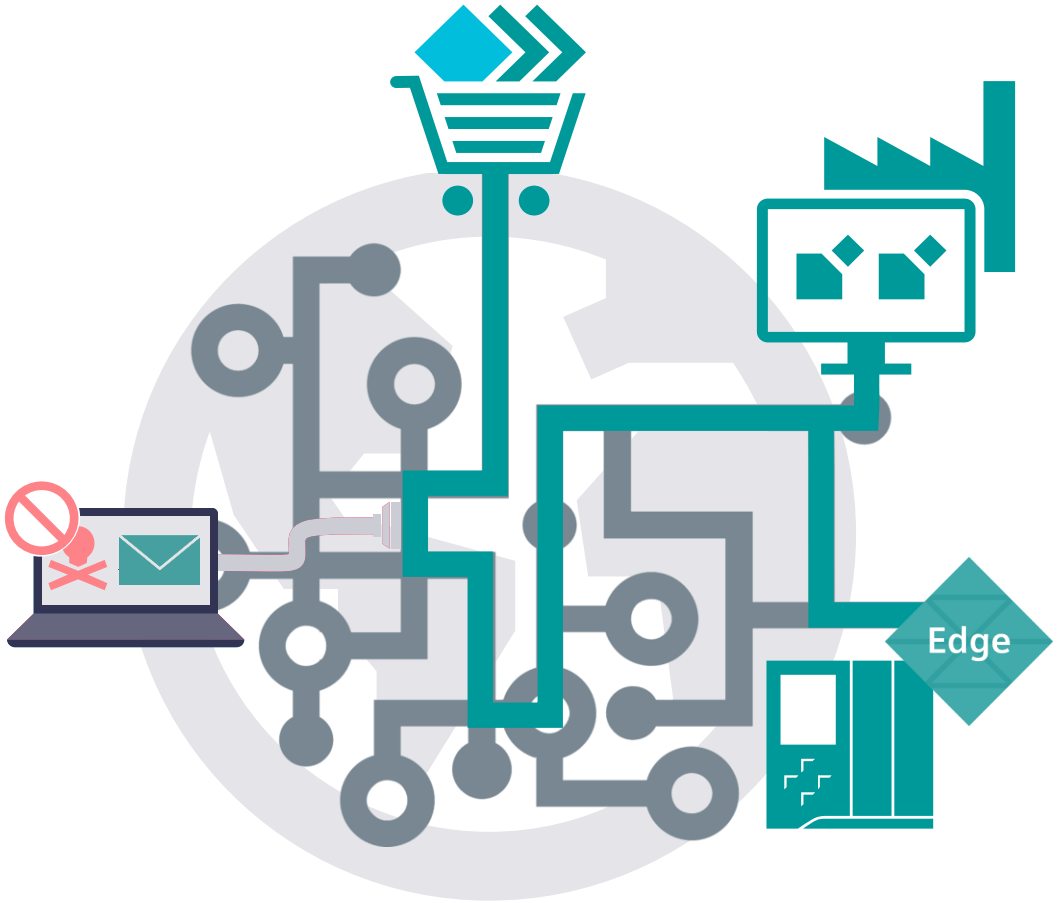
IE Device
Execution platform for apps



Edge App decides which data is uploaded to higher level systems

SIEMENS

Challenges due to internet-based connectivity
Encryption



Prevent eavesdropping or manipulation

- Detect manipulation due to signatures
- Ensure confidentiality by use of encryption

IEC 62443-3-3 – SR 4.1 RE 1
“Provide the capability to protect the confidentiality of information at rest and remote access sessions traversing an untrusted network.”

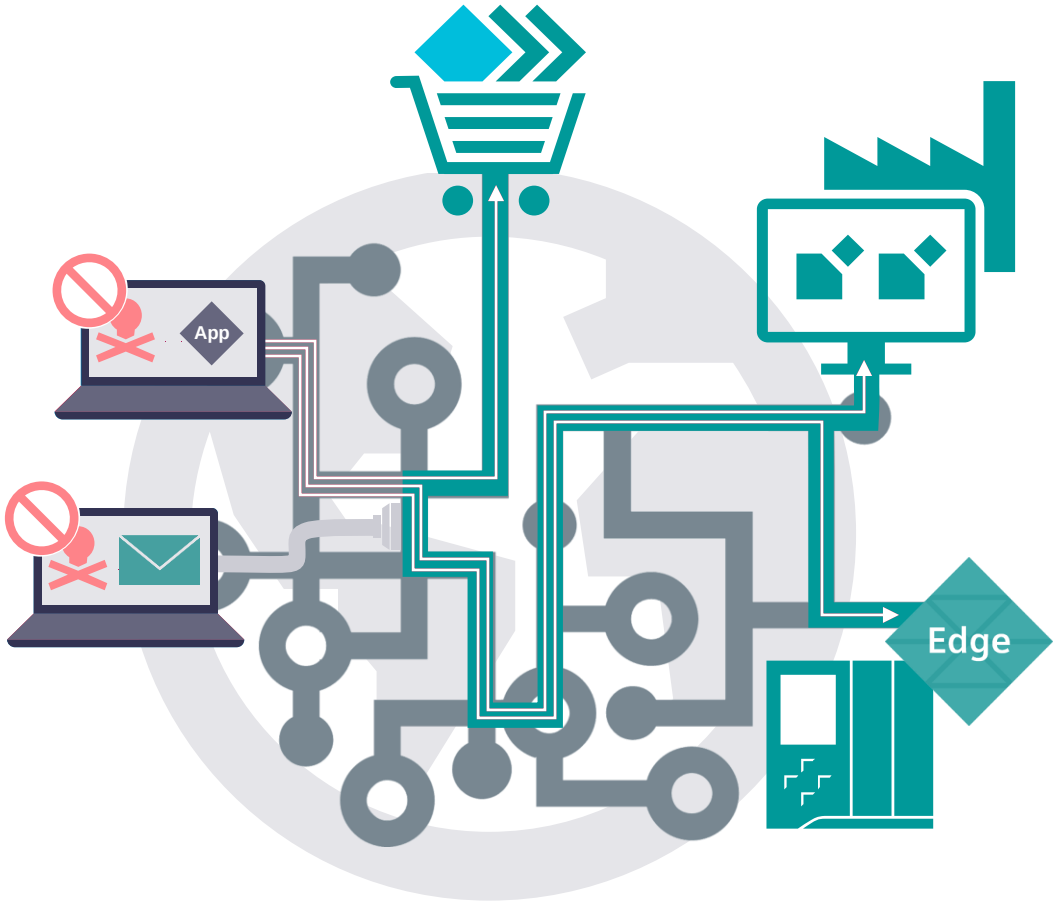
IEC 62443-3-3 – SR 4.1 RE 2
“Provide the capability to protect the confidentiality of information traversing any zone boundary.”

HTTPS to protect communication between Industrial Edge components

SSH-Tunneling to protect remote access

SIEMENS

Challenges due to internet-based connectivity
Authentication



Prevent unauthorized access

- Validate IED and IEM identities
- Identify and authenticate users

IEC 62443-3-3 – SR 1.1
“The control system shall provide the capability to uniquely identify and authenticate all human users.”

IEC 62443-3-3 – SR 1.2
“The control system shall provide the capability to identify and authenticate all software processes and devices.”

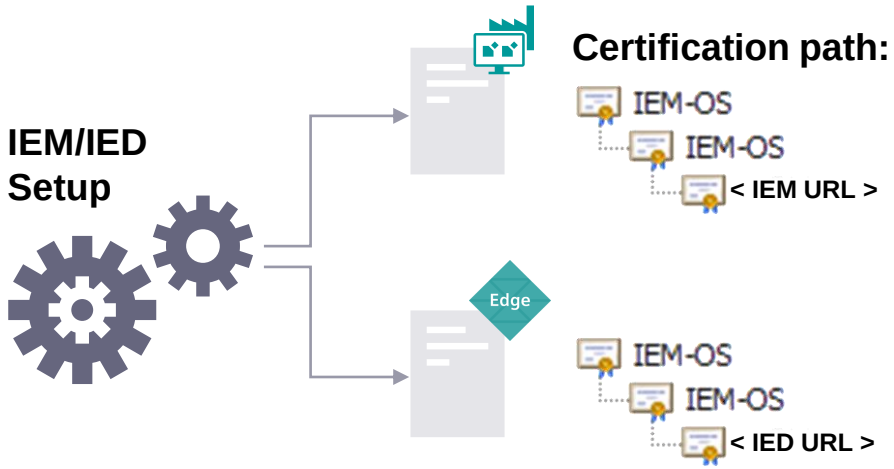
User accounts in IE HUB, IEM and IED

Certificates to identify and authenticate IEM and IEDs

SIEMENS

Challenges due to internet-based connectivity
Certificate management

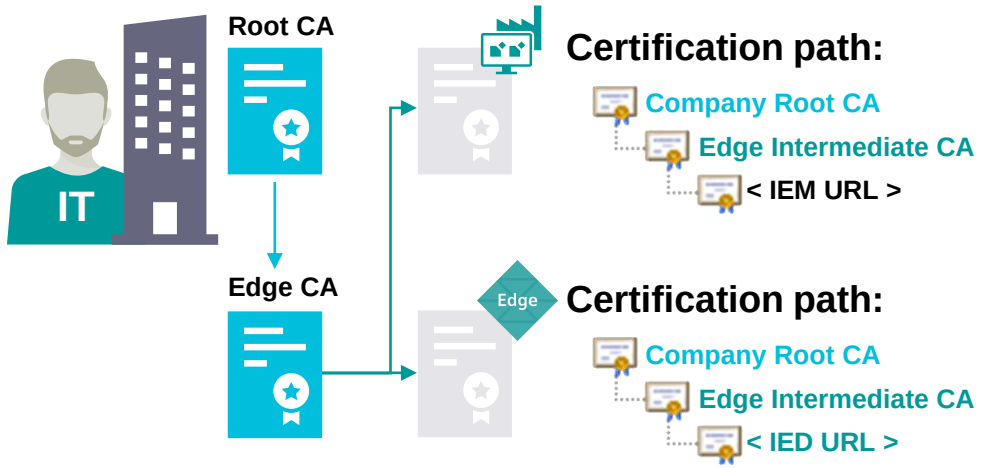
Use of default certificates



Create certificate automatically during setup

- \+ Easy setup
- − No further prove of identity
- − Installation of certificates on every PC required

Use certificates signed by PKI



Create certificates with a Public Key Infrastructure (PKI)

- − More complex setup
- \+ Proves that the device belongs to the company
- \+ No further certificate installation on PCs required

Challenge of this use case!

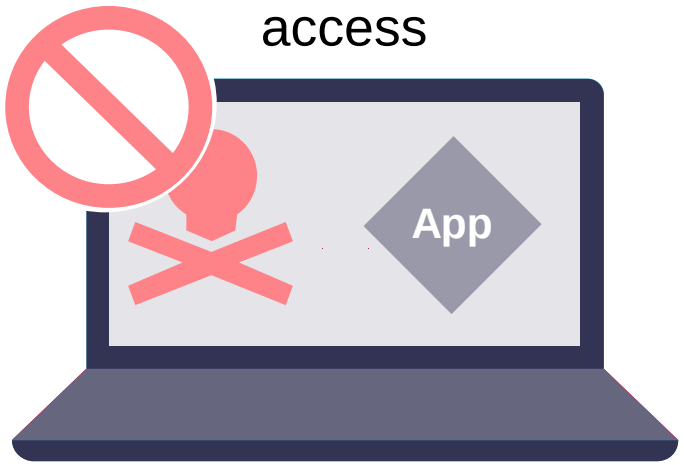
SIEMENS

Challenges due to internet-based connectivity
Further threads

Eavesdropping/ manipulation

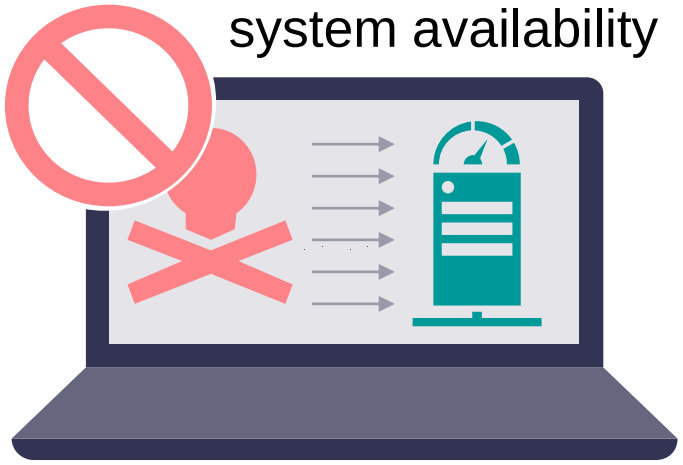
HTTPS with TLS
(Certificates and Encryption)

Unauthorized access



User accounts

Attacks against system availability

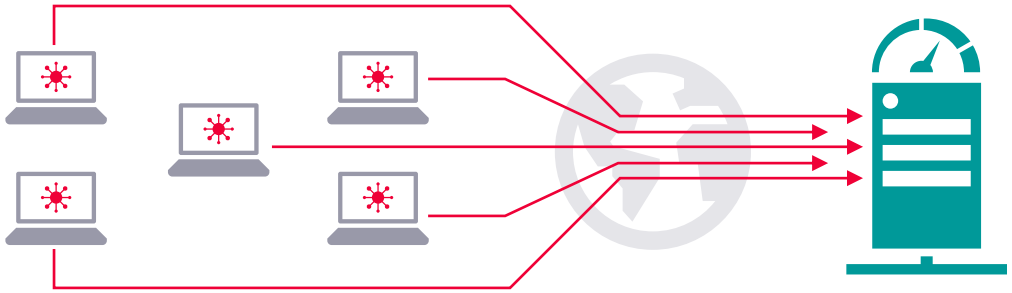


Backup & Restore

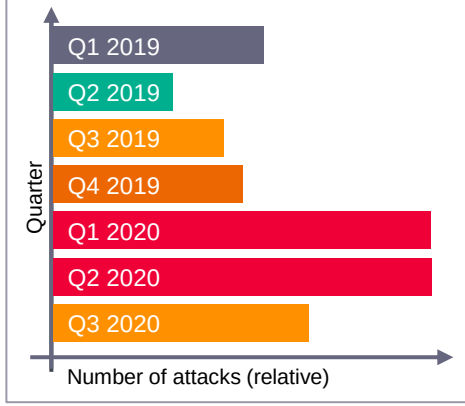
SIEMENS

Challenges due to internet-based connectivity
Example: Distributed Denial of Service (DDoS) attacks

Distributed Denial of Service (DDoS)



Trend of DDoS attacks[1]



Potential threat to any internet exposed server

Countermeasures are complex and expensive

Industrial Edge

Only IE-HUB is exposed to the Internet

- Siemens is responsible for protection
- Certified data center provider
- Web Application Firewall (WAF)

IEM and IED use outgoing connections

- Minimized attack surface
- **Less online dependencies** (on-premise installation)
- Easy integration in existing networks

1 Data calculated from Secure list DDoS attack reports (2019 – 2020)

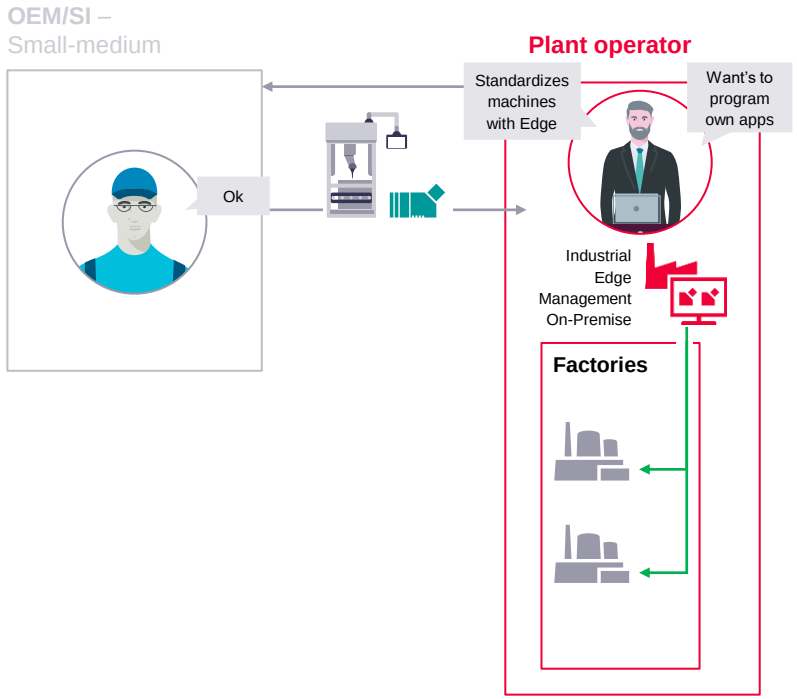
SIEMENS

Major customer scenarios for Industrial IoT

In the upcoming slides we will cover both of them security-wise

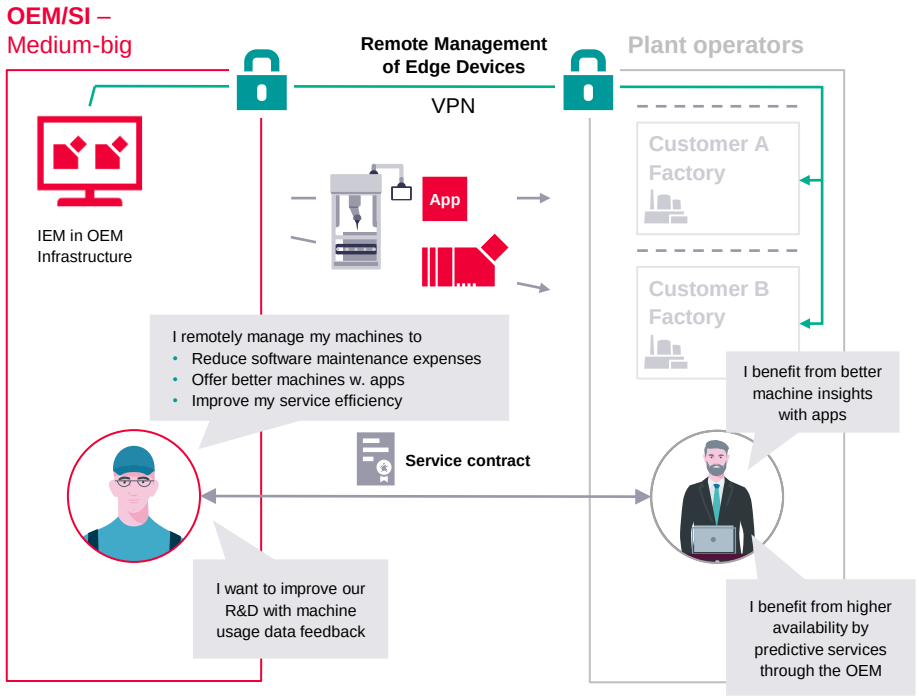
Plant operator standardization

on Industrial Edge to introduce digital solutions to manufacturing and improve OEE



OEM/System integrator remote management

of Edge solutions to utilize machine data to offer new digital solutions to my customers



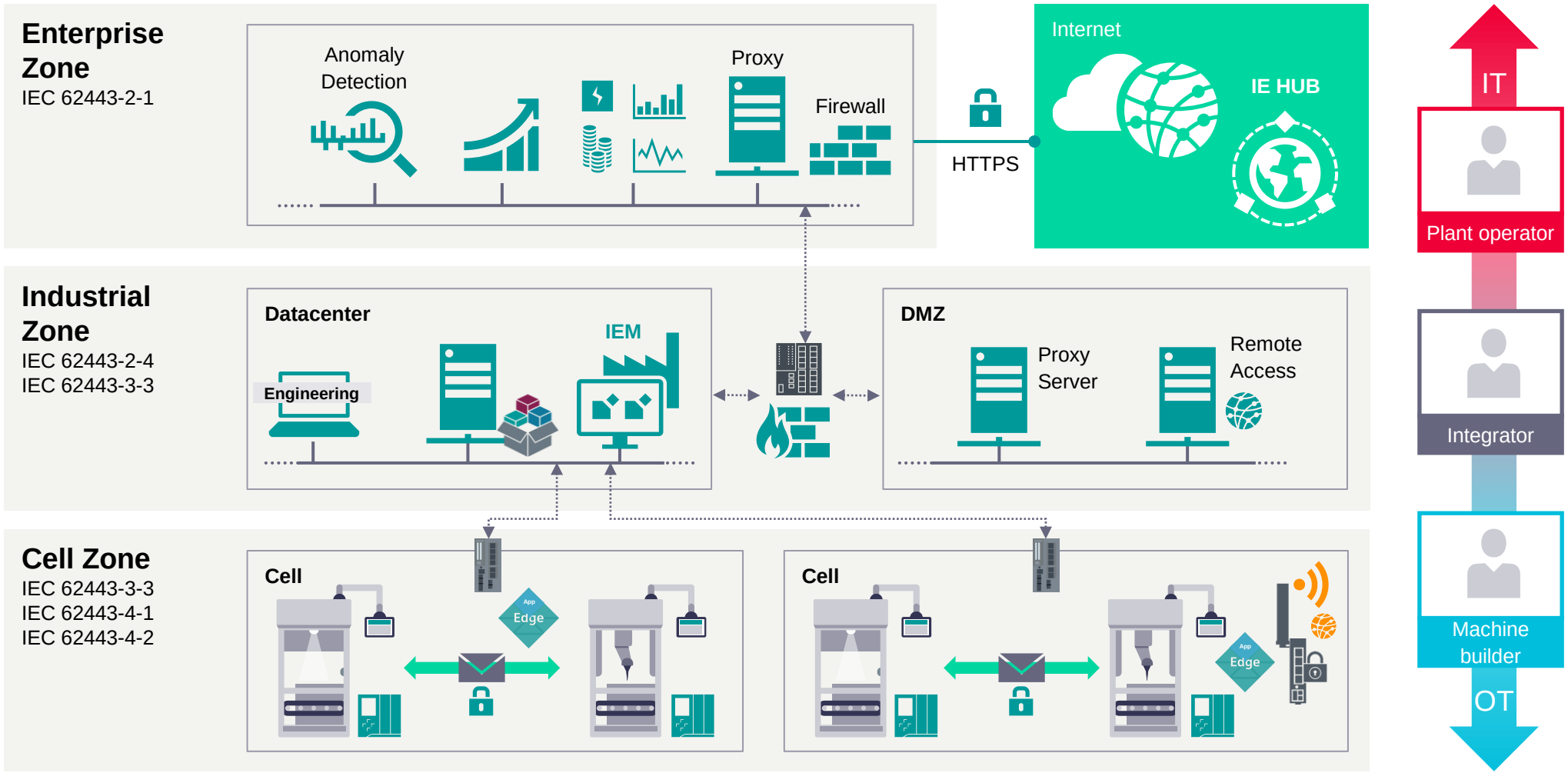
SIEMENS

Plant operator scenario

Standardizing on Industrial Edge to introduce digital solutions to manufacturing to improve OEE

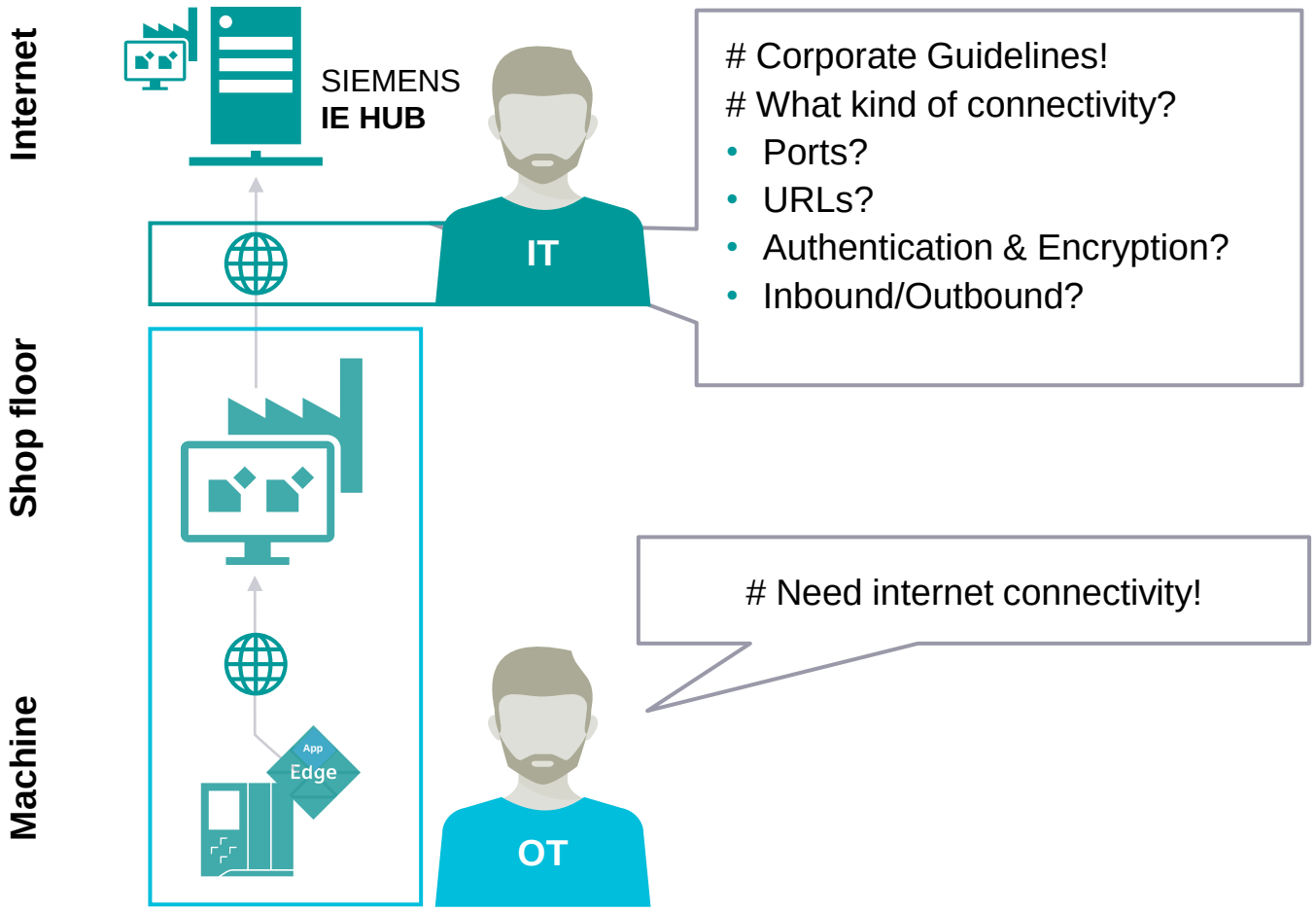
SIEMENS

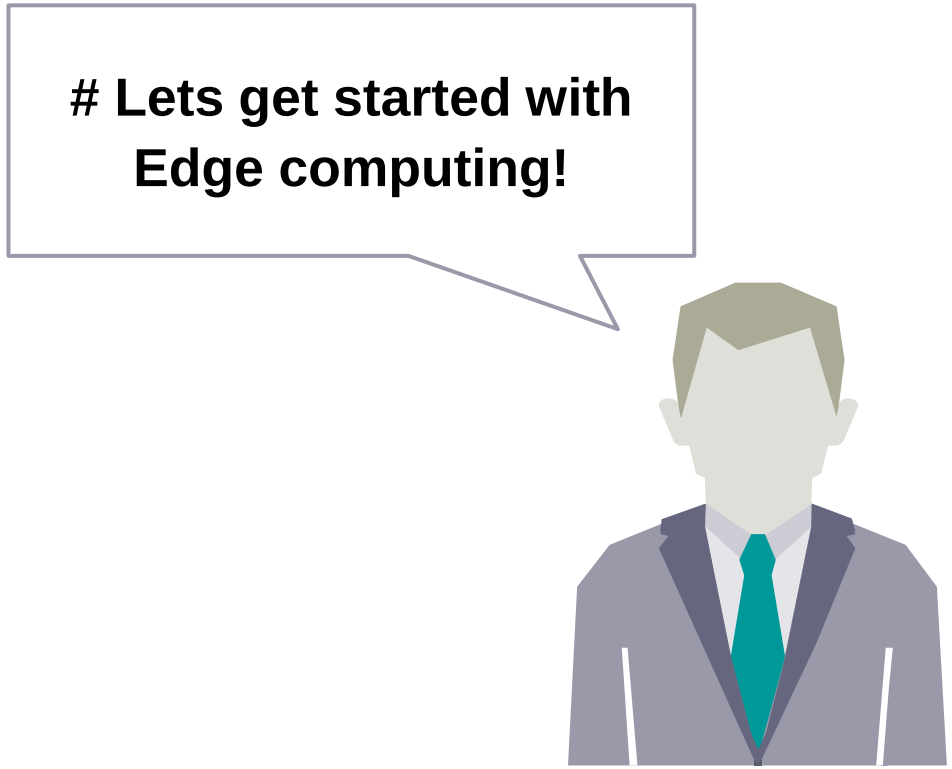
Plant operator
Architecture blueprint



SIEMENS

Industrial Edge
App Installation Workflow





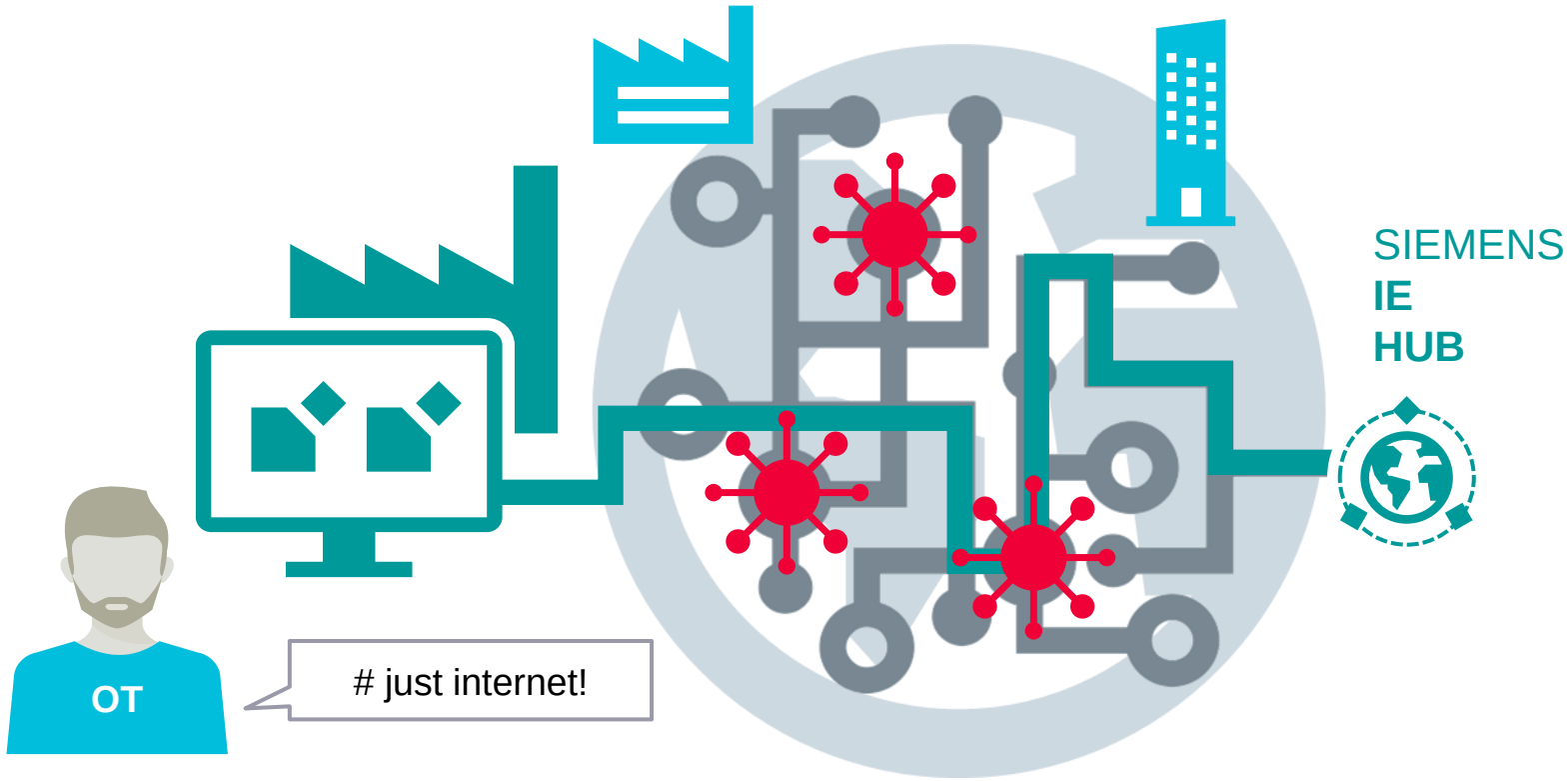
SIEMENS

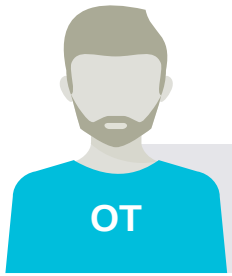
Security risks potentially arise due to internet connectivity

IEC 62443-3-3

Chapter 9.3.2:
“Access from the control system to the World Wide Web should be clearly justified based on control system operational requirements.”

SR 5.2 RE 1:
“The control system shall provide the capability to deny network traffic by default and allow network traffic by exception. (Also termed **deny all, permit by exception**)”





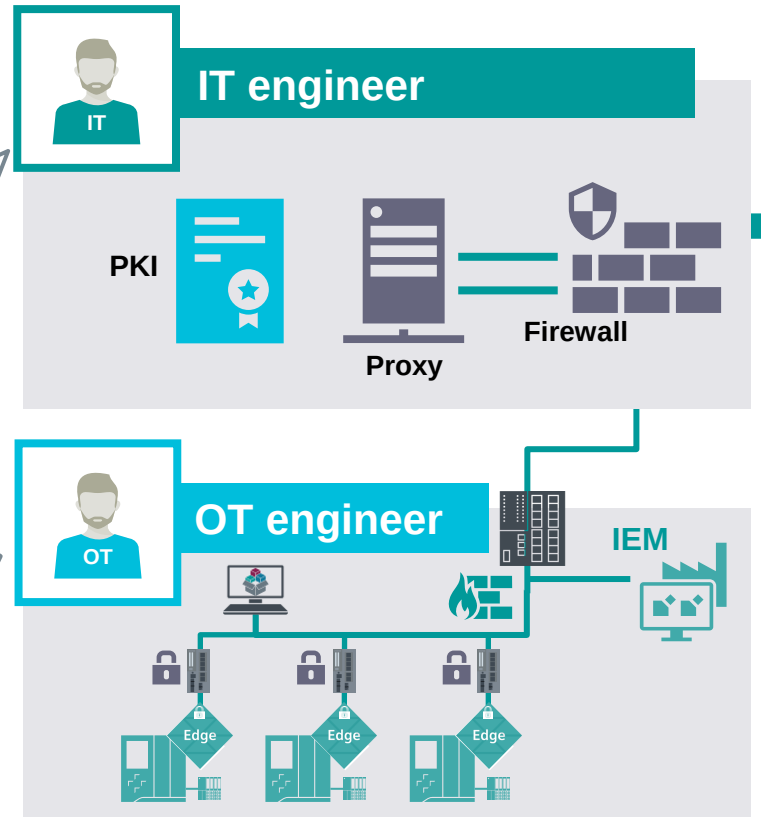
Challenge: Establish state of the art internet connection from IEM to IE HUB

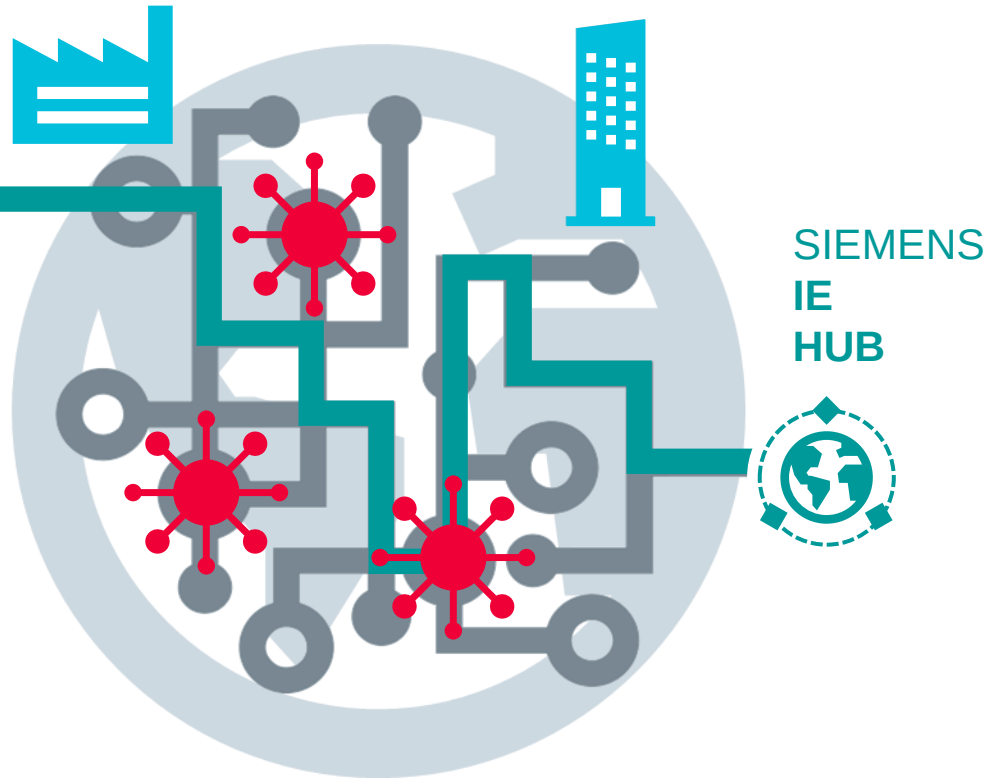
SIEMENS

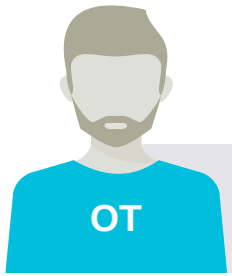
Security risks potentially arise due to internet connectivity

Daily business!
Lots of measures to avoid security threads.
→ “Just” need to extend this to shop floor

“Just” need to extend?
Never heard about:
- Firewalls
- PKI
- Proxy servers







Challenge: Comply with standards used in IT infrastructure

SIEMENS

Industrial Edge
Terms: Firewall, Proxy, CA

Firewalls are used to restrict access on network level

- Restrict IED network access to connections needed for IEM
- Restrict IEM network access to connections needed for Edge HUB

Firewalls can filter network traffic based on IP addresses and TCP/UDP Ports

---

Proxy

HTTPS Proxy server can provide security measures based on the web protocol itself

- User authentication of internet access/Logging of internet traffic/
  Black- and whitelisting of certain websites/Malware scan of incoming traffic
- Usually placed at the Enterprise IT level and managed IT personnel

A firewall rule set is needed to restrict outgoing traffic to the proxy server

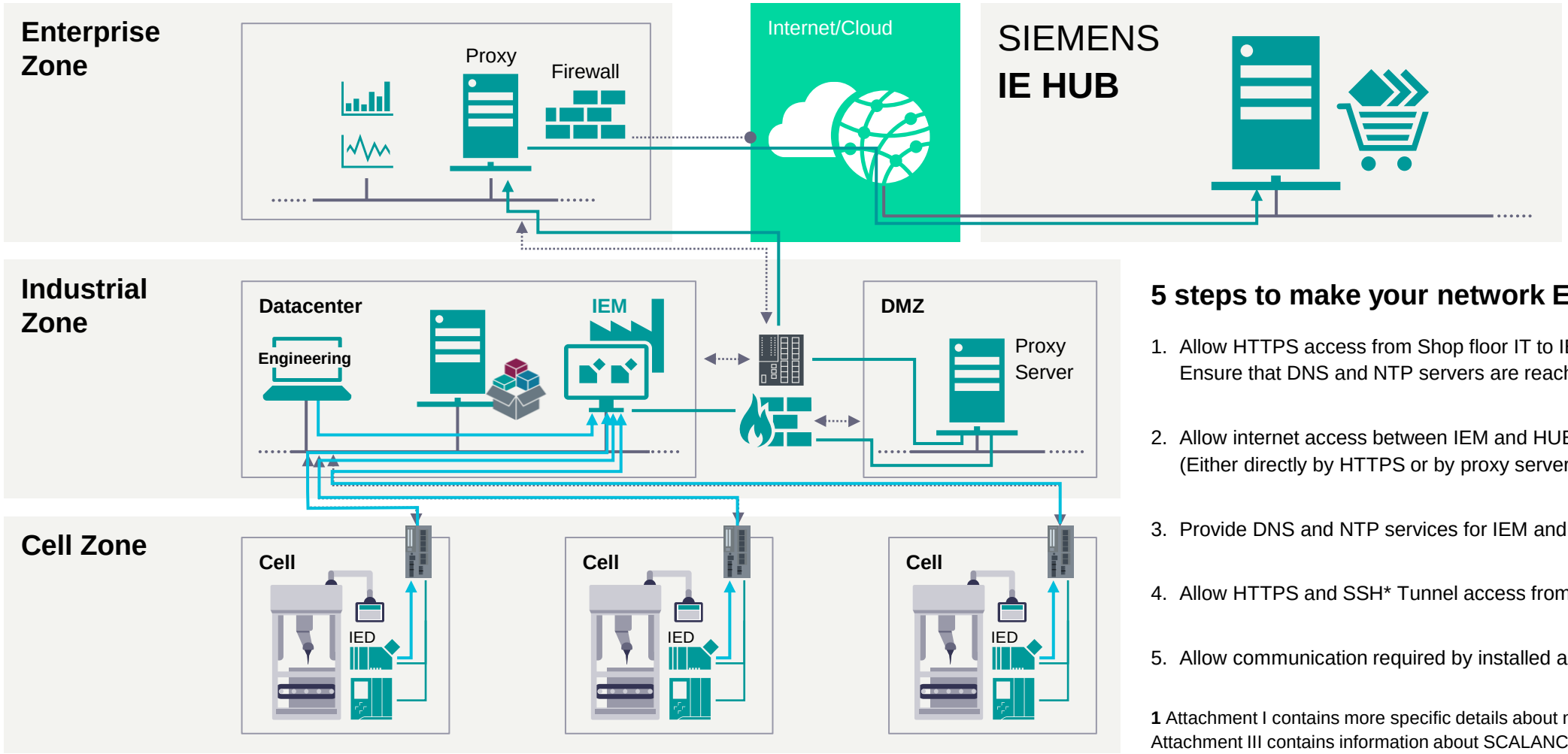
---

Public Key Infrastructures are used to authenticate devices

- Certificates are used by the devices as a proof of identity

State of the art security mechanism in IT infrastructure

Plant Operator hosting the Industrial Edge Management System
Network configuration



5 steps to make your network Edge ready

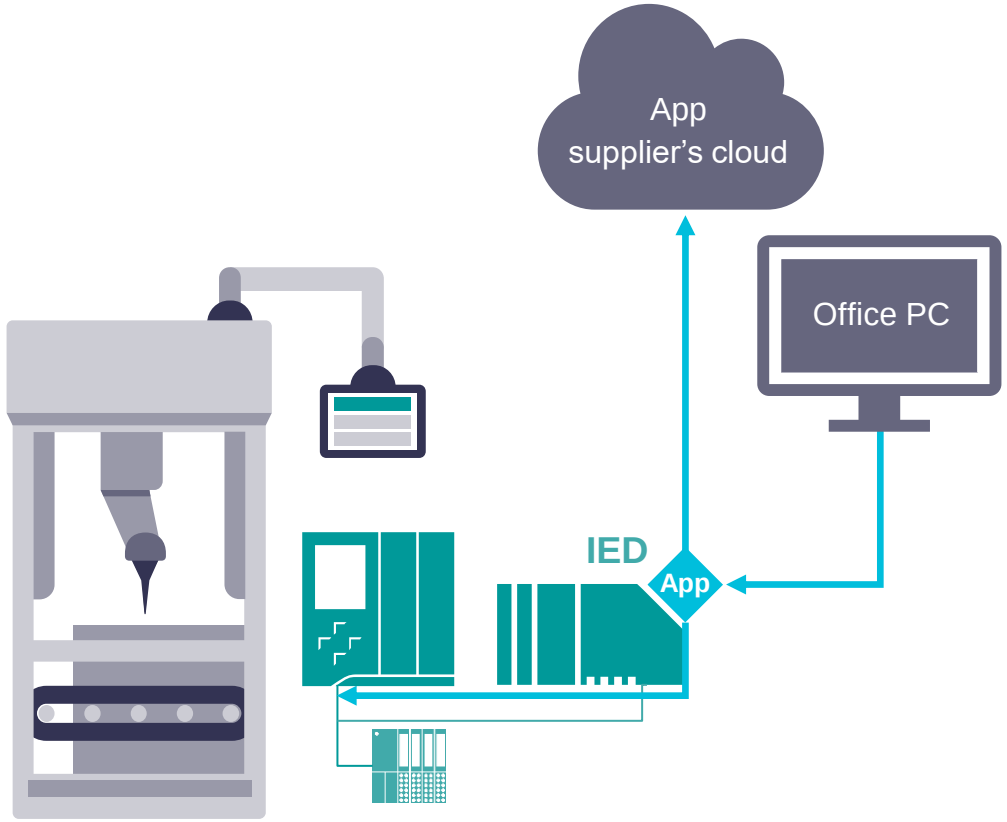
1. Allow HTTPS access from Shop floor IT to IEM.
   Ensure that DNS and NTP servers are reachable
2. Allow internet access between IEM and HUB
   (Either directly by HTTPS or by proxy servers)
3. Provide DNS and NTP services for IEM and IED
4. Allow HTTPS and SSH* Tunnel access from IEDs to IEM
5. Allow communication required by installed apps.

1 Attachment I contains more specific details about needed connections, Attachment III contains information about SCALANCE DHCP, DNS and NTP

* Allow SSH Tunnel only if it is necessary for your application

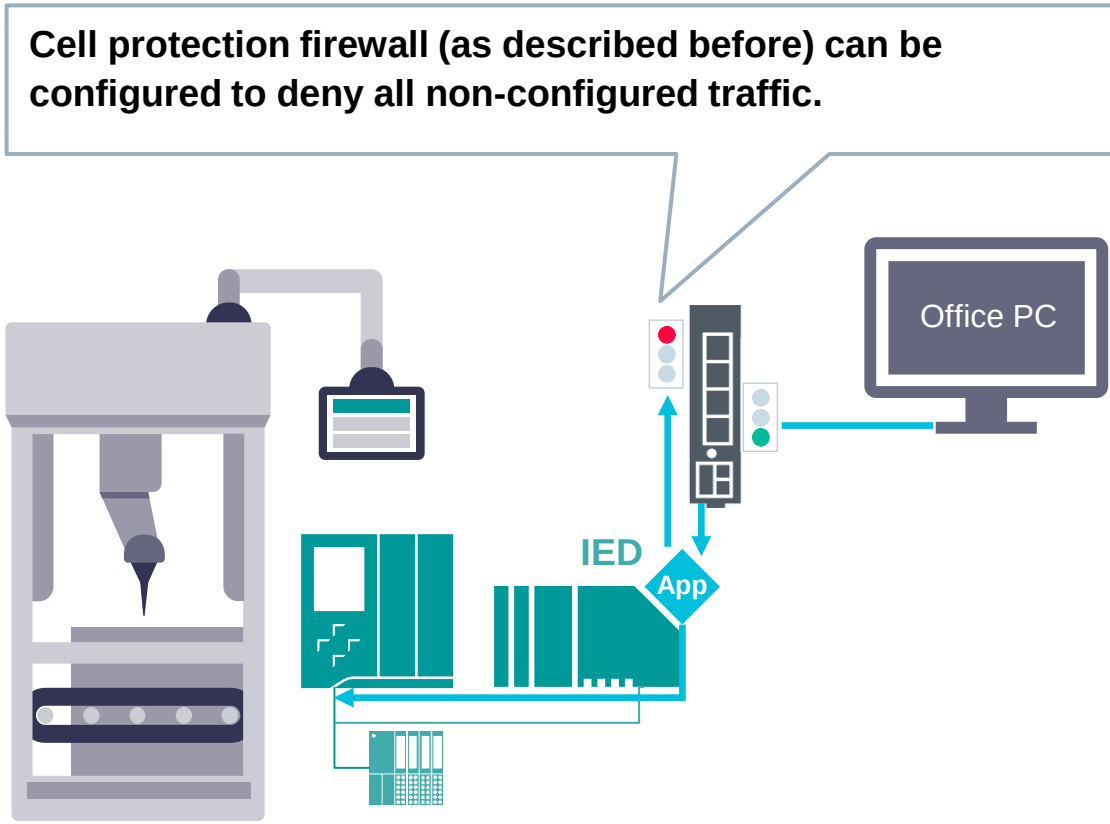
SIEMENS

Plant Operator
Network configuration: Apps



Challenge:
Apps might include communication services

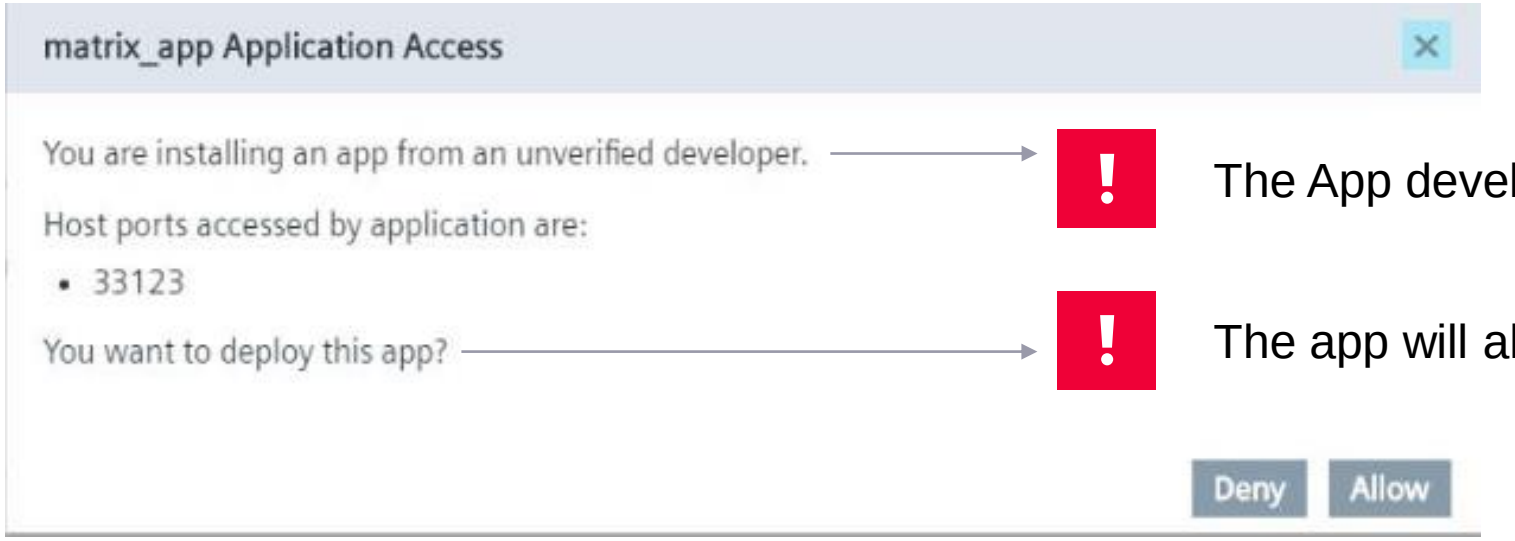
Cell protection firewall (as described before) can be configured to deny all non-configured traffic.



Recommendation:
Use Cell Protection concept with firewalls

SIEMENS

Plant Operator
Network configuration: App rollout



The App developer is not verified by Siemens

The app will allow incoming connection on port 33123

Feature: The app rollout process warns about potential hazards due to app installations

SIEMENS

Industrial Edge
Terms: Firewall, Proxy, CA

Firewalls are used to restrict access on network level

- Restrict IED network access to connections needed for IEM
- Restrict IEM network access to connections needed for Edge HUB

Firewalls can filter network traffic based on IP addresses and TCP/UDP Ports

---

HTTPS Proxy server can provide security measures based on the web protocol itself

- User authentication of internet access/Logging of internet traffic/
  Black- and whitelisting of certain websites/Malware scan of incoming traffic
- Usually placed at the Enterprise IT level and managed IT personnel

A firewall rule set is needed to restrict outgoing traffic to the proxy server

---

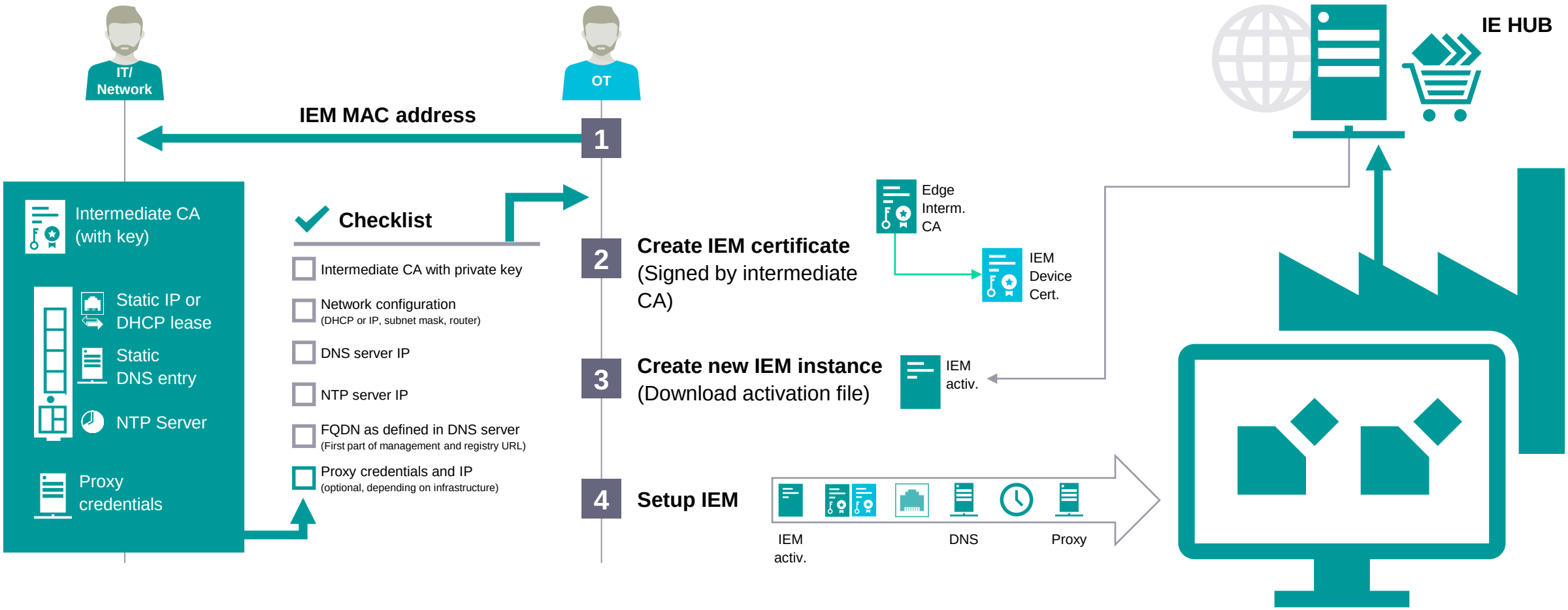
Public Key Infrastructures are used to authenticate devices

- Certificates are used by the devices as a proof of identity

State of the art security mechanism in IT infrastructure

SIEMENS

Plant Operator
Industrial Edge Management installation

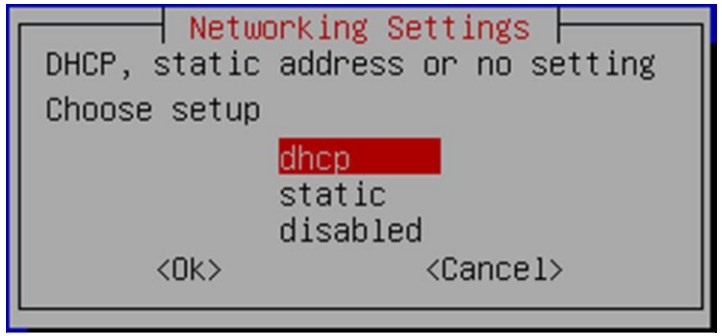


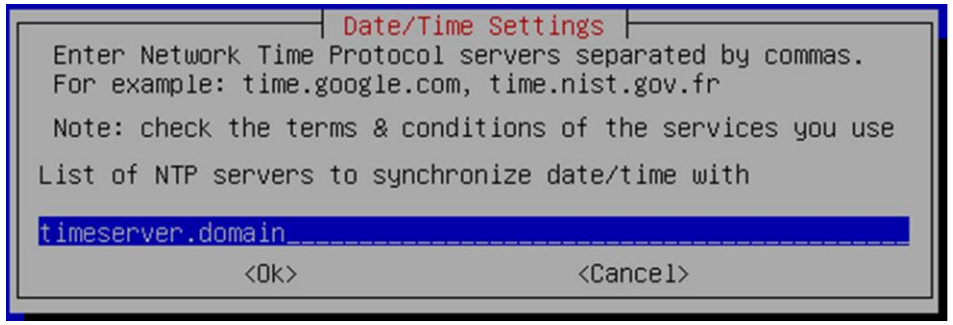
Please take notice: The workflow shown depends on the used infrastructure

SIEMENS

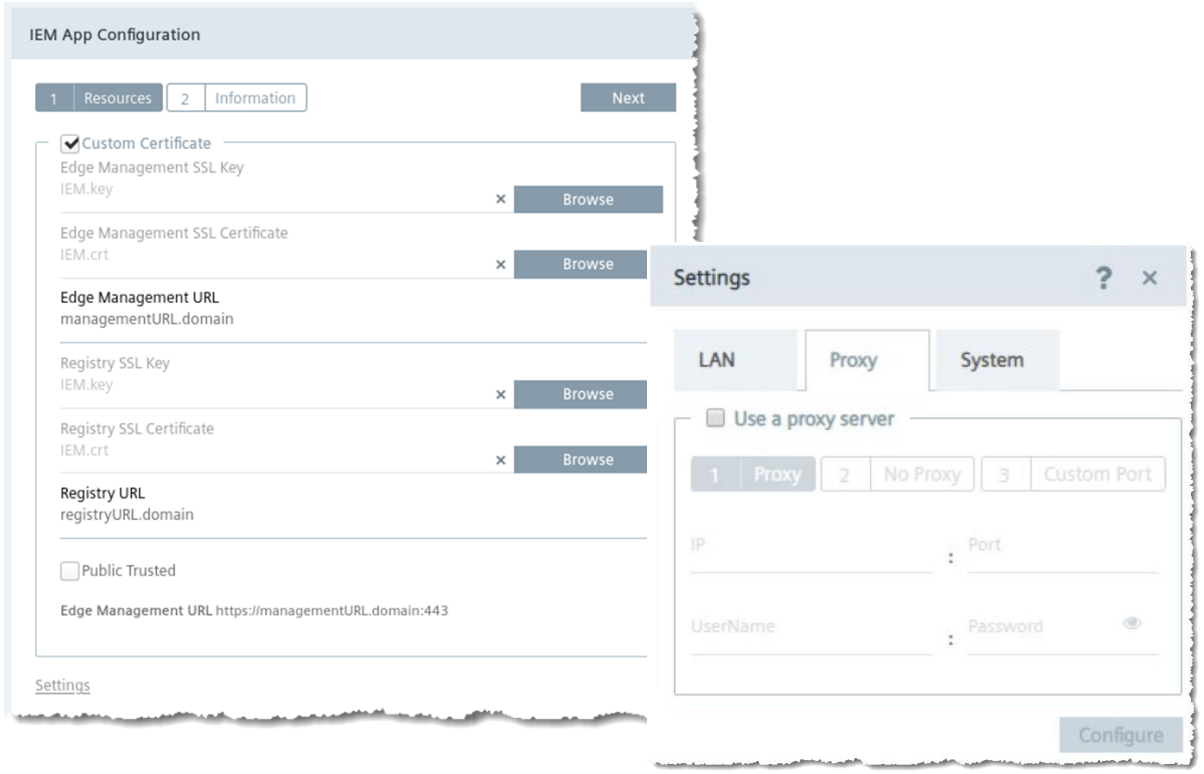
Plant Operator
Industrial Edge Management installation dialogue

OS installation defines IP and NTP server



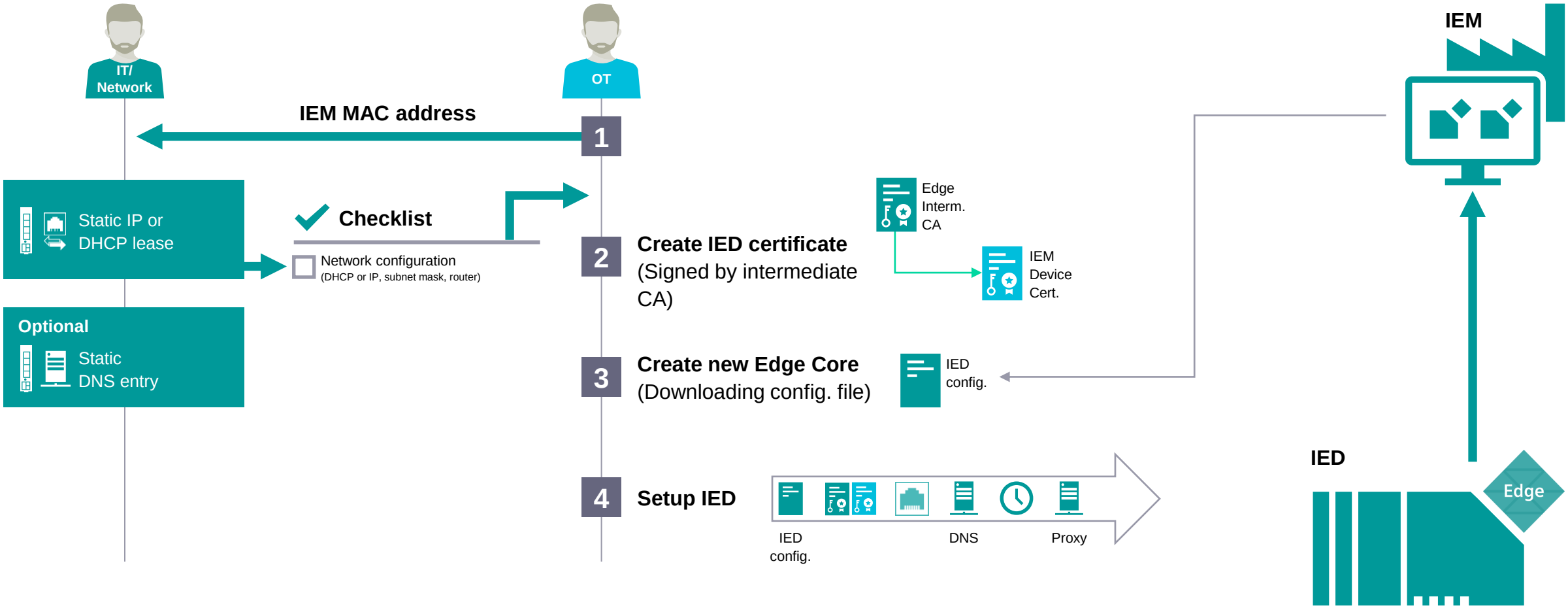


IEM activation defines URLs, certificates and proxy settings



SIEMENS

Plant Operator
Industrial Edge Device installation

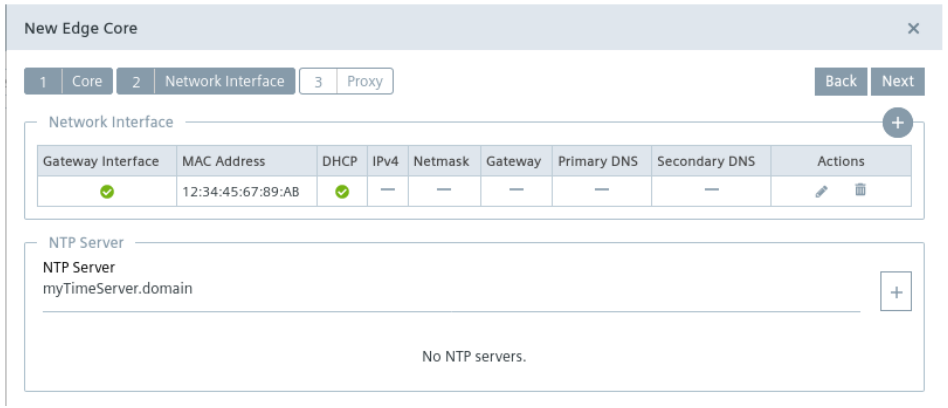


Please take notice: The workflow shown depends on the used infrastructure

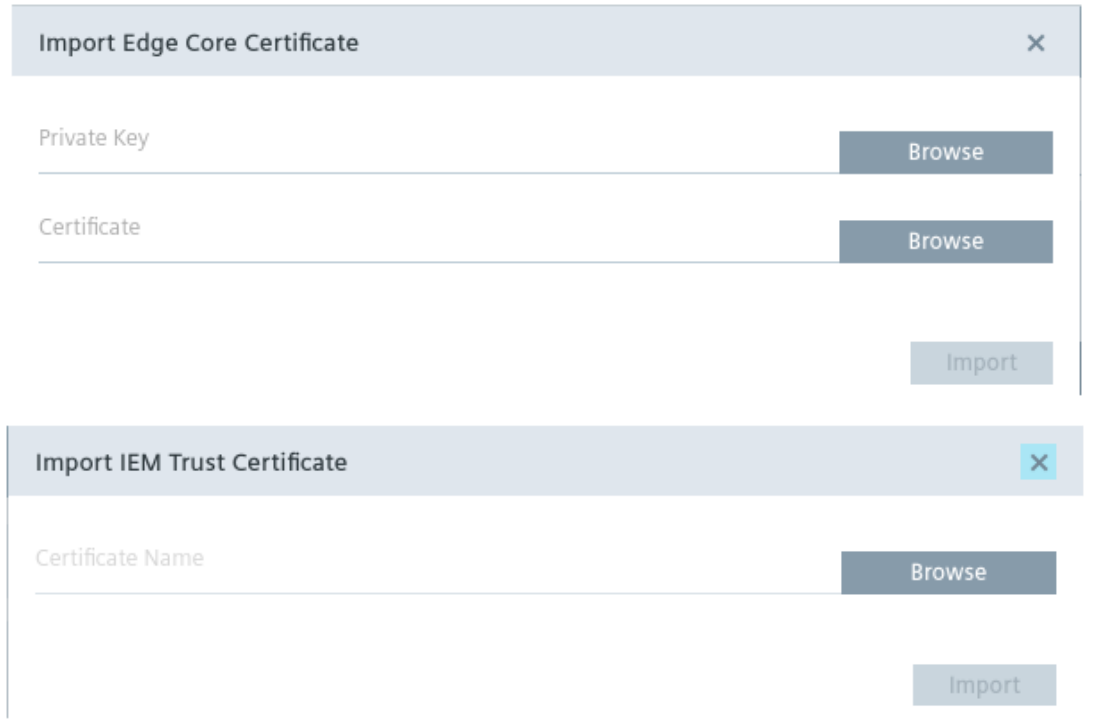
SIEMENS

Plant Operator
Industrial Edge Device installation dialogue

IP, DNS, NTP and Proxy settings are defined during creation in IEM



Certificates can be uploaded in the IED webserver



SIEMENS

Machine builder scenario

Using Industrial Edge to provide added value services to customers by remote

SIEMENS

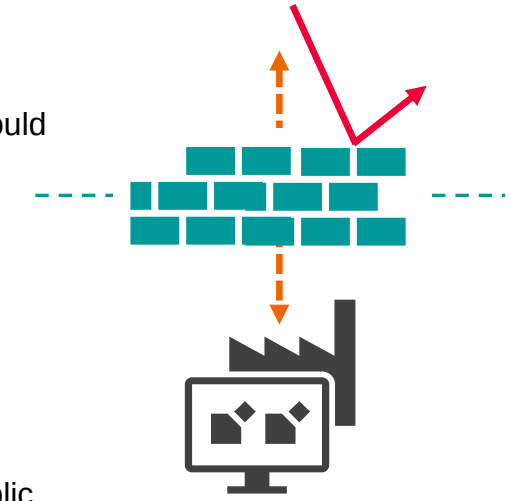
Industrial Edge Management
Operations guideline for Zero-Trust-Networks (!)

As of now Industrial Edge Management is designed for **On-premises use-cases** and operations within **trusted networks**.
For this operation scenario we provide a self-contained easy to setup & operatable On-premise solution as managed appliance.
In this case our customers provide the Infrastructure, but operations are being handled by Siemens, resulting in less IT-Operations required on customer site.

Today's solution

For scenarios with communication in **Zero-Trust-Networks** we therefore recommend to apply firewalls and VPNs for the communication between Industrial Edge Management and Industrial Edge Devices.

If this security protection measure is **not viable due to company policy or efforts linked to it**, there are also **other measures** which could be implemented e.g. **IP-Whitelisting, Proxy Servers or Geo-Blocking measures**.
For more information please consult our SUP FA Presales Team at simatic.industry@siemens.com



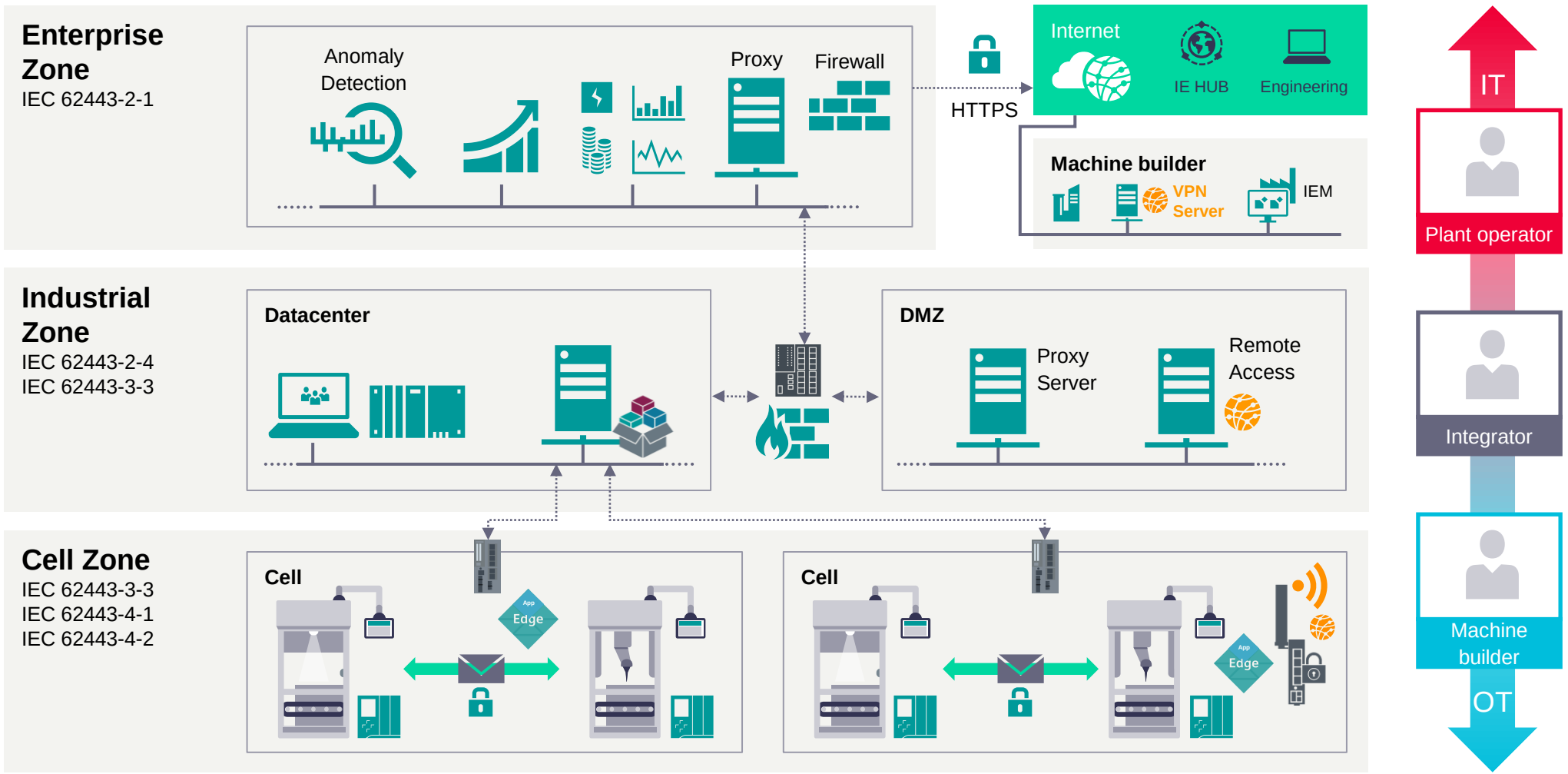
Future solution

In order to operate the Industrial Edge Management **directly exposed** to **Zero-Trust-Networks** while also fulfilling Siemens and our customers security standards, further IT and security features such as Audit Trail, DDOS protection and integrated product firewalls are required.

As we are aware of all of those (and further) requirements we are working on enhancing our Industrial Edge Management System for public internet operations over the next release versions.

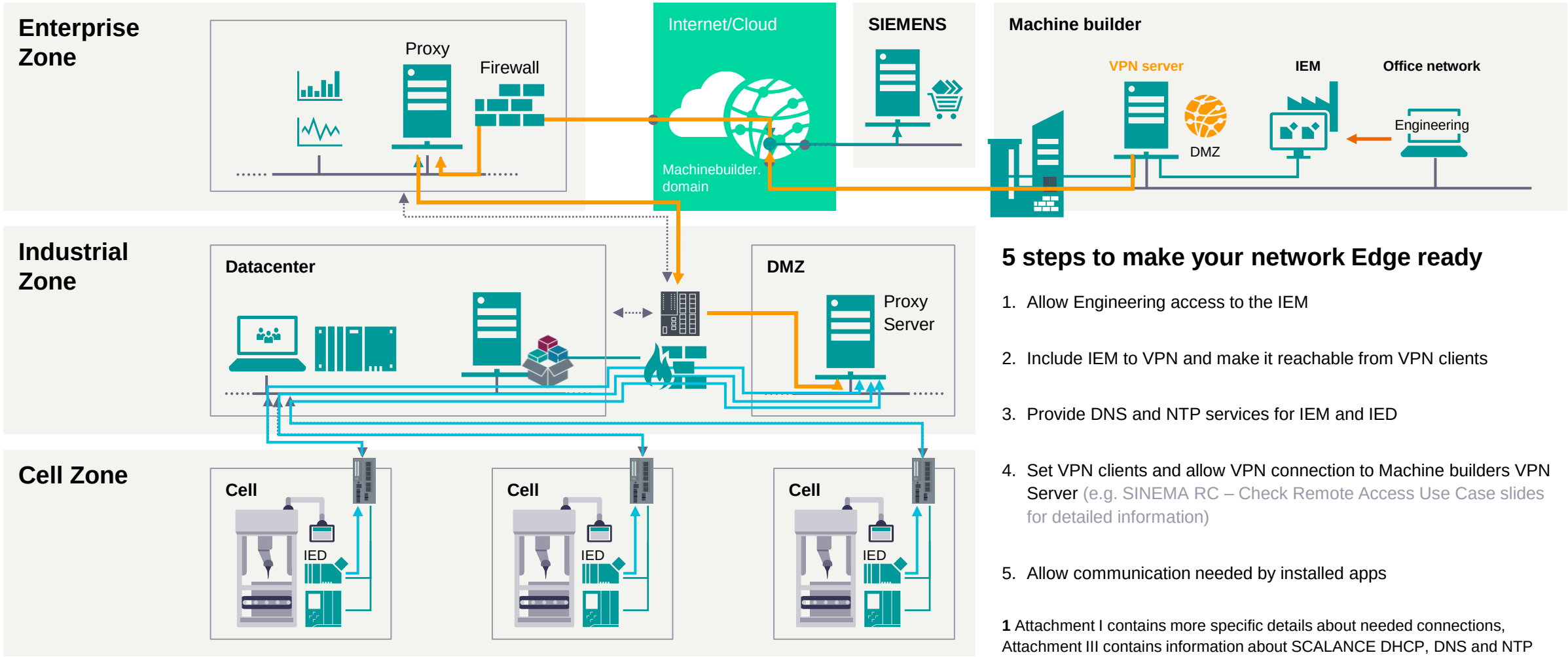
SIEMENS

Machine Builder
Architecture blueprint



SIEMENS

Machine builder
Industrial Edge Management System hosting – Network configuration



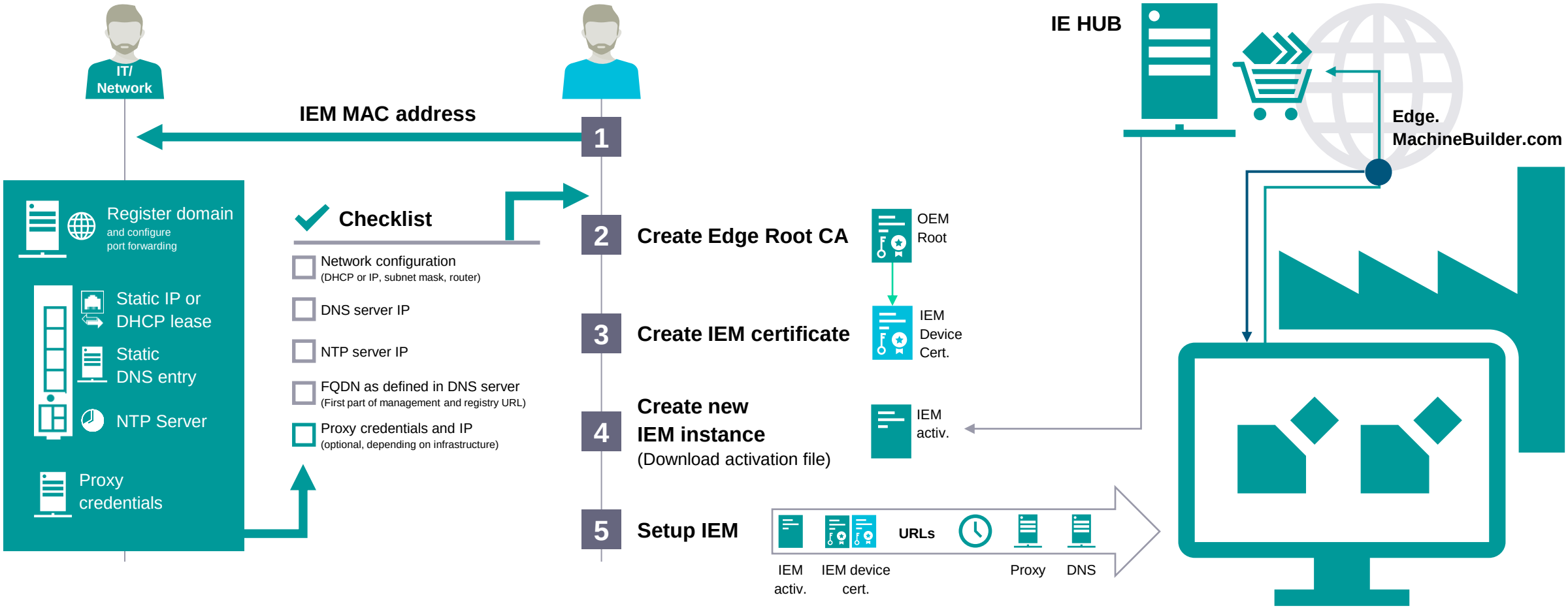
5 steps to make your network Edge ready

1. Allow Engineering access to the IEM
2. Include IEM to VPN and make it reachable from VPN clients
3. Provide DNS and NTP services for IEM and IED
4. Set VPN clients and allow VPN connection to Machine builders VPN Server (e.g. SINEMA RC – Check Remote Access Use Case slides for detailed information)
5. Allow communication needed by installed apps

1 Attachment I contains more specific details about needed connections, Attachment III contains information about SCALANCE DHCP, DNS and NTP

SIEMENS

Machine builder
Industrial Edge Management installation

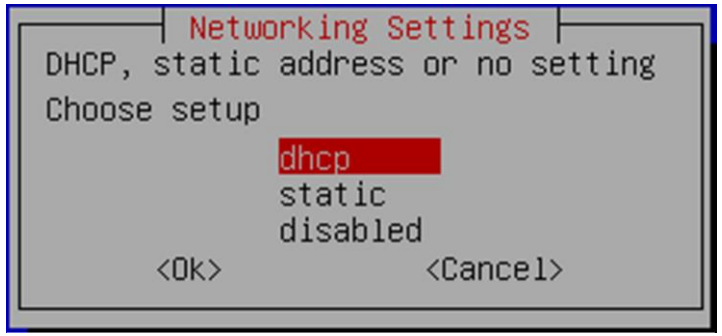


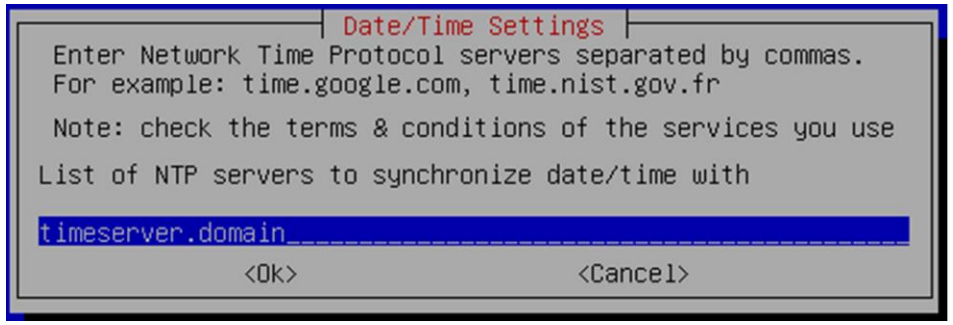
Please take notice: The workflow shown depends on the used infrastructure

SIEMENS

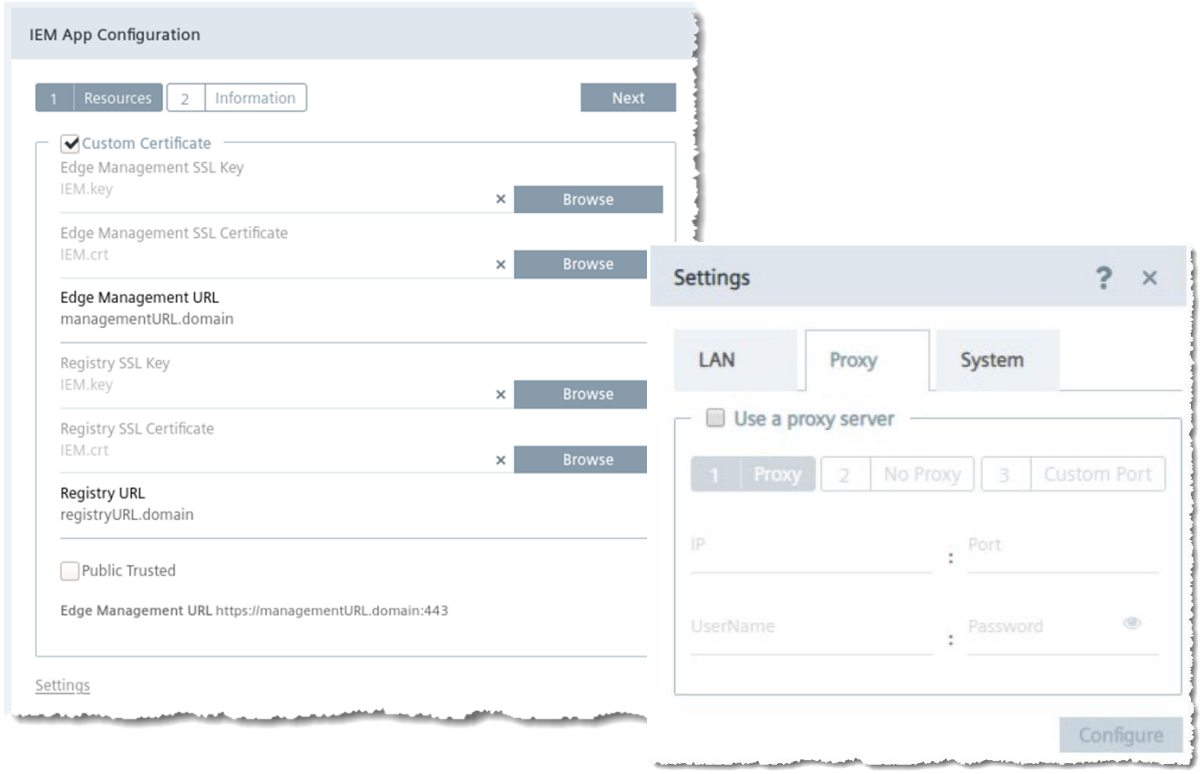
Machine builder –
Industrial Edge Management installation dialogue

OS installation defines IP and NTP server



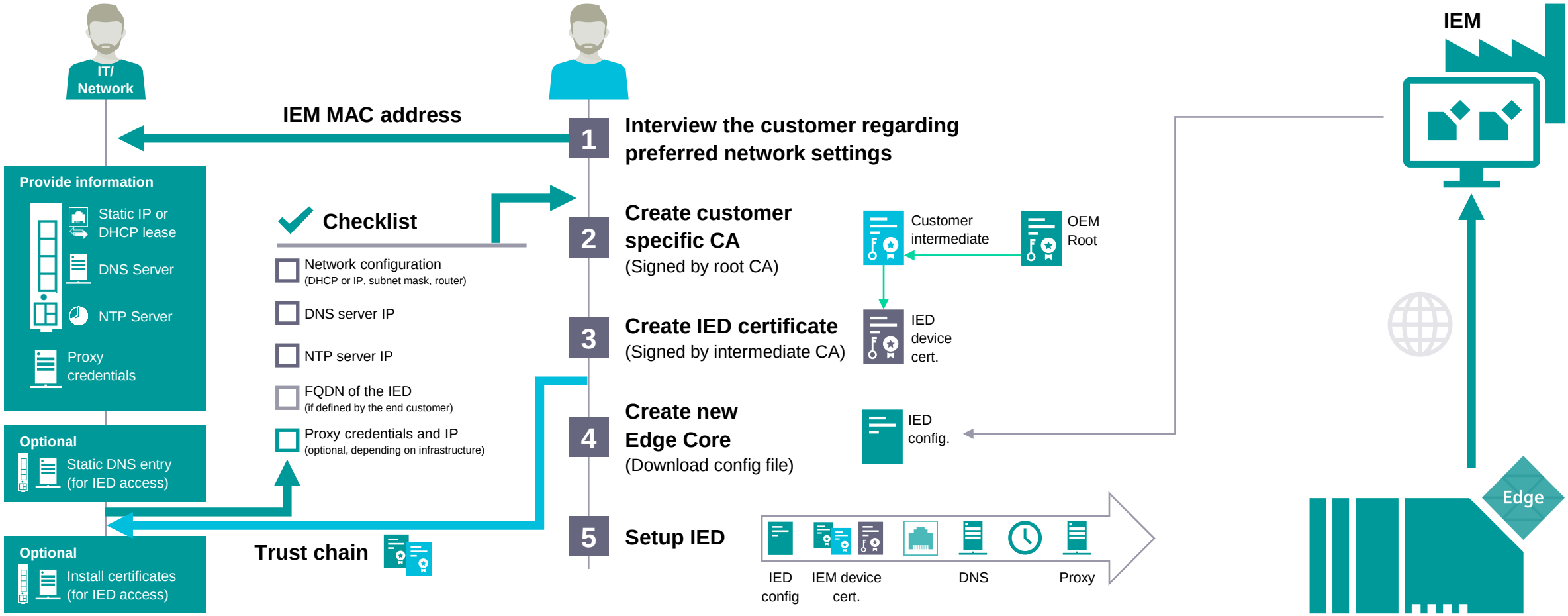


IEM activation defines URLs, certificates and proxy settings



SIEMENS

Plant Operator
Industrial Edge Device installation

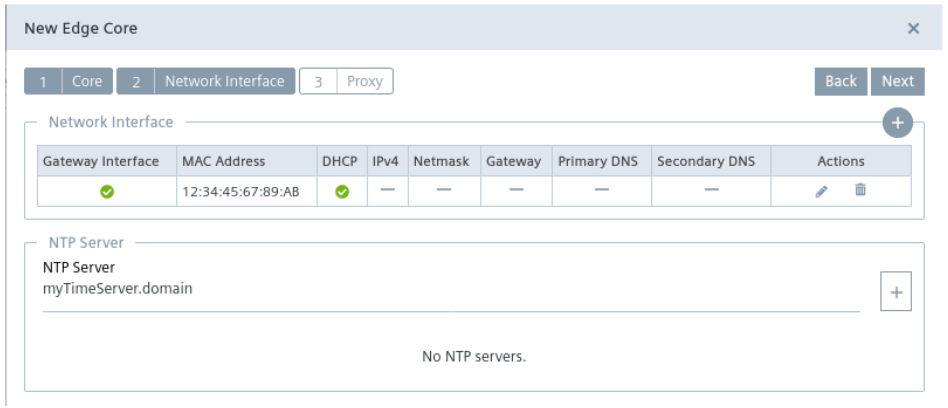


Please take notice: The workflow shown depends on the used infrastructure

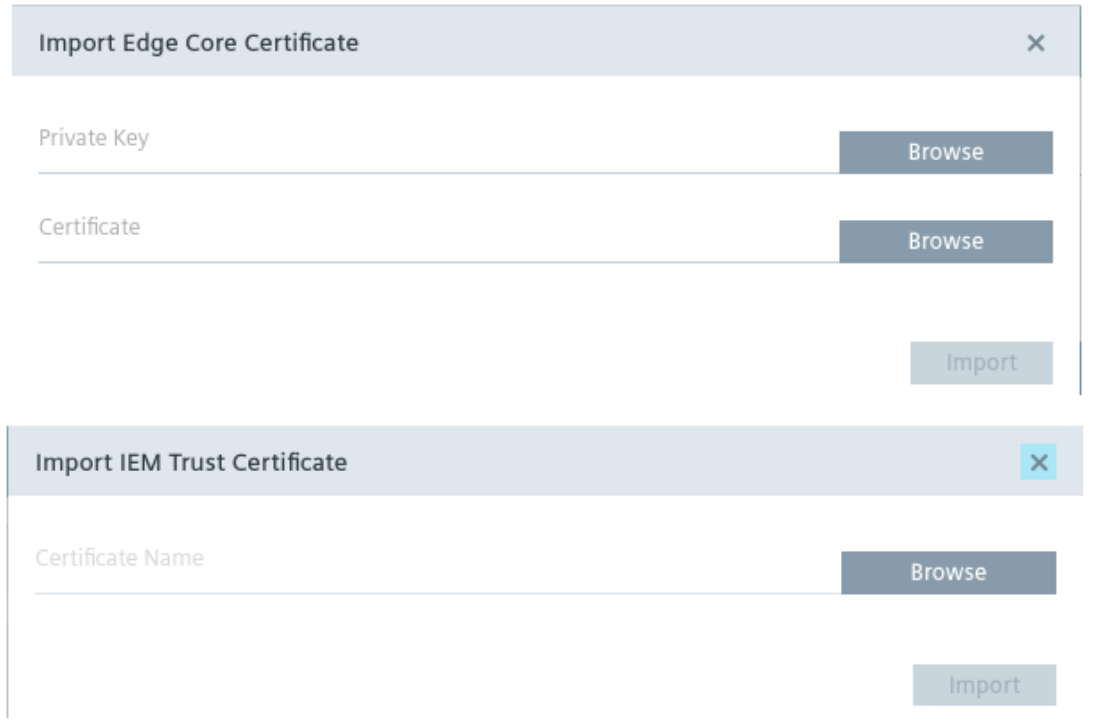
SIEMENS

Plant Operator
Industrial Edge Device installation dialogue

IP, DNS, NTP and Proxy settings are defined during creation in IEM



Certificates can be uploaded in the IED webserver



SIEMENS

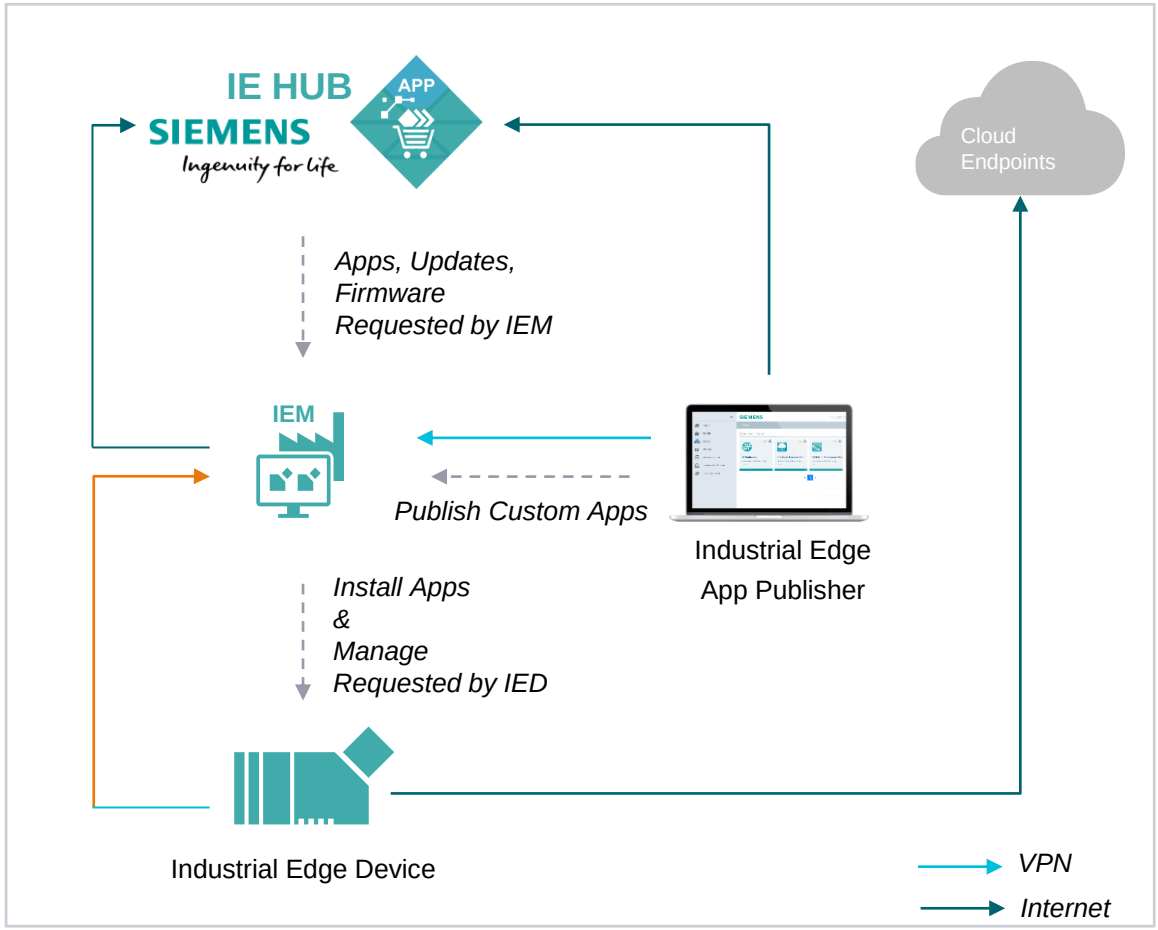
Data Flow – Internet and VPN

VPN : Virtual Private Network

Incase distributed IE use case
(Machine Builder / End Customer - Multiple Location)

Connection between Client, IED and IEM must be established through a VPN solution.

(e.g. SINEMA RC)

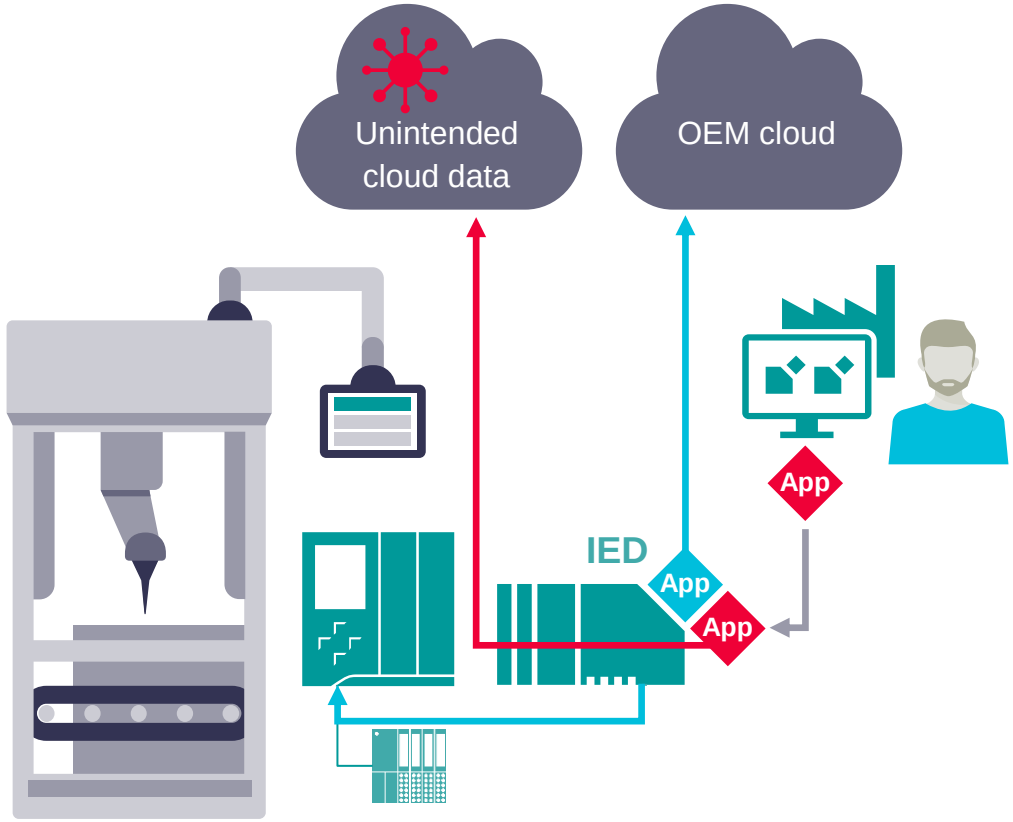


The connections are always initiated from lower level to higher level

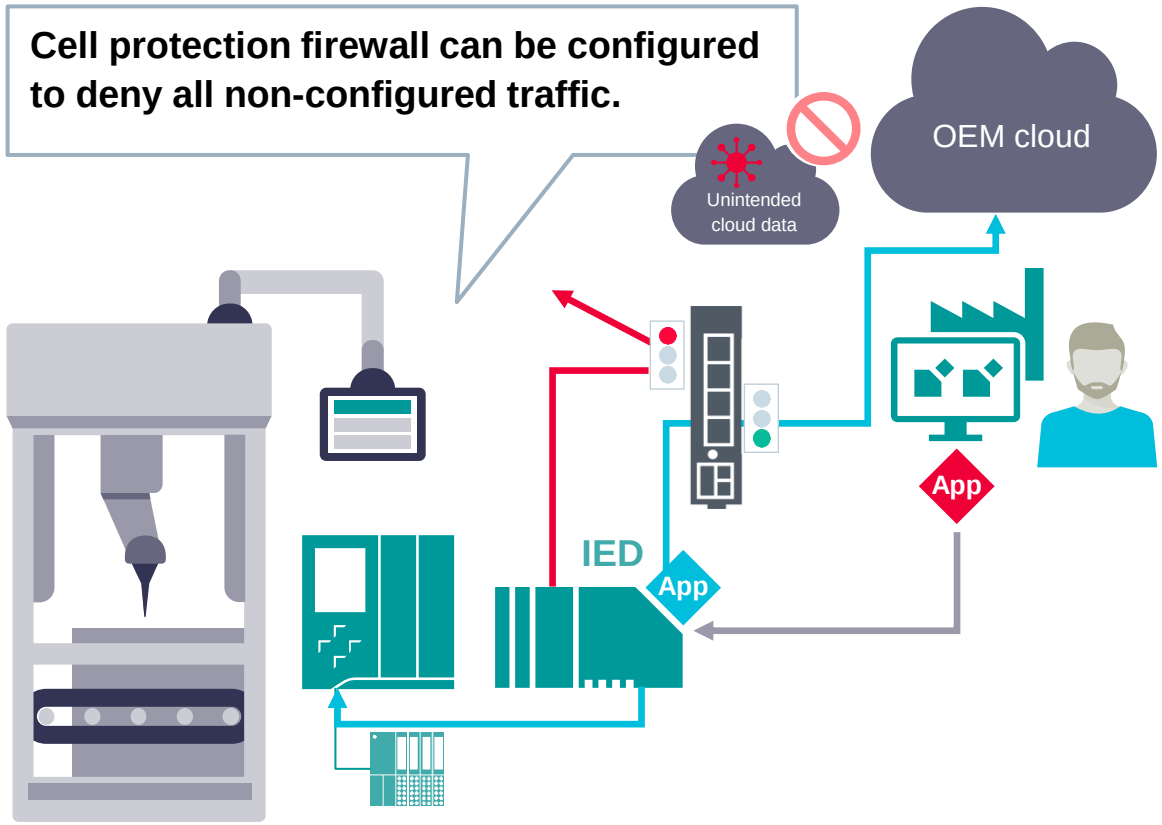
SIEMENS

Plant Operator

Network configuration – Apps might open connections



Challenge: Machine builder might install further apps with unintended communication services



Recommendation:
Use Cell Protection concept with firewalls

SIEMENS

Industrial Edge Security Capabilities

SIEMENS

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 and 2 factor authentication.
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 SOC2 and ISO27001.
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) is used within data centers to protect the endpoints.

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[1].
Full disk encryption	Encrypted rootfs and data partitions	All system partitions are encrypted and locked by crypto hardware[1].
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 ISO image does not provide root user login by default.
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.

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

Industrial Edge Device security

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.
SELinux	Enforcement of access control policies to the operating system resources	Industrial Edge defines and implements SELinux policies to enforce least privilege principle to apps and services. This provides an additional layer of system security.
No root user login	Prevents access to the administrative account	The Industrial Edge ISO images does not provide any possibility to login as root user.
Digital signatures for Industrial Edge software artifacts	Integrity and authenticity of the software artifacts	Digital 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 one-time token from the Industrial Edge Management backend.
Manufacturer device certificate	Hardware authenticity	The manufacturer device certificate provides a proof-of-origin of the Edge Device provisioned during the manufacturing process.

Network security

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.
Web interfaces	Common termination of TLS for all services	All web interfaces are secured through TLS 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.

Data security

Component	Purpose	Description
User credentials	Privacy protection	All user credentials are stored salted and hashed.
IE Cloud Connector	Secured data transfer to the cloud provider	The Industrial Edge Cloud Connector provides secured communication channel with TLS, strong cipher suites and authentication.
Offline operations	Resilient operations without connectivity	The IEM and Edge Devices can be operated offline. Connection is only required for maintenance purposes, for example for updates or new app deployments and are fully controlled by the operator.
Digital signing of apps	Provide integrity and authenticity	Edge Apps provided by Siemens are signed by CMS (Cryptographic Message Syntax) schemes. Further Edge Apps signed by the Industrial Edge trust can be found in the Industrial Edge Ecosystem.
Reverse proxy user session	Central TLS termination for system and apps authentication	The system provides a reverse proxy for apps which is secured and linked to the user management. All security relevant aspects are handled centrally by the system. The user is authenticated through username and password by a central authentication service. The session is protected by an expiring session token.

Industrial Edge IEC62443 compliance

SIEMENS

IEC 62443 for Industrial Control Systems

7 Foundational Requirements

- **FR 1** – Identification and authentication control
- **FR 2** – Use control
- **FR 3** – System integrity
- **FR 4** – Data confidentiality
- **FR 5** – Restricted data flow
- **FR 6** – Timely response to events
- **FR 7** – Resource availability

Defines security requirements for industrial control systems

From IEC62443-3-3

SIEMENS

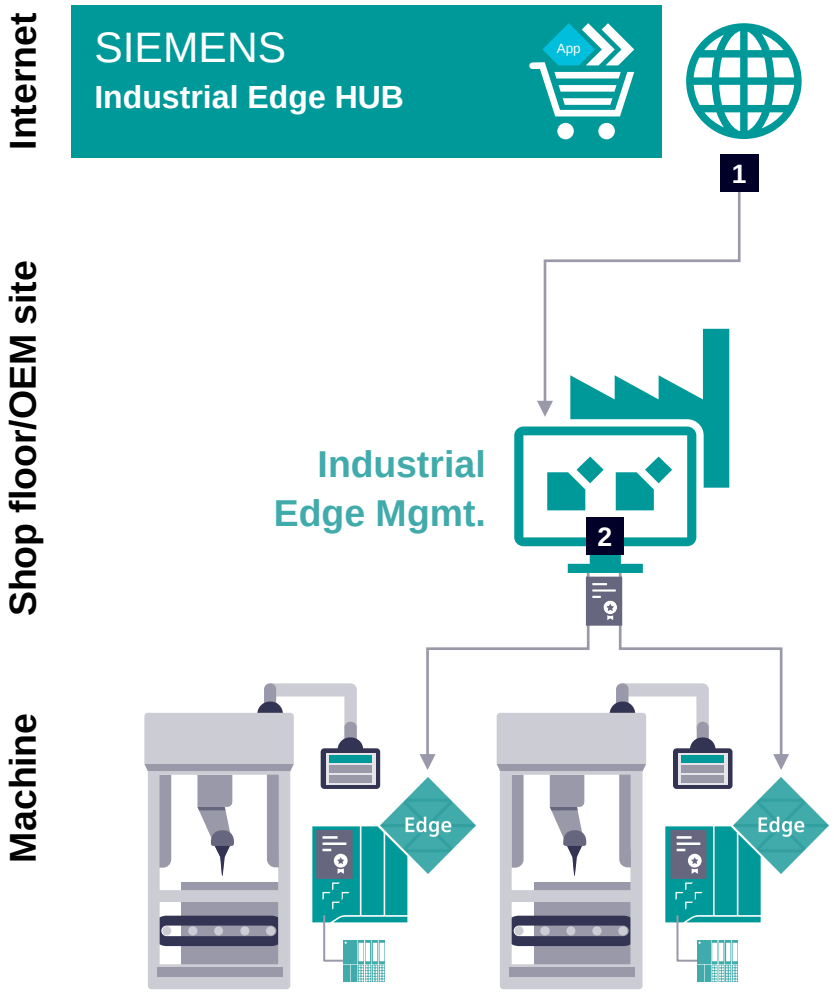
Supported Industrial Edge features contributing to IEC 62443

Fundamental Requirements	Supported Features with Industrial Edge
FR1 - Identification and Authentication Control	Multi-factor User Authentication, User Management
FR2 - Use Control	Management of Roles and Groups. Authentication Termination, Authorization Code. NTP Support
FR3 - System Integrity	IMA,TPM Support, SELinux, Measured Boot, System Updates from SIEMENS
FR4 - Data Confidentiality	System wide usage of Digital Certificates (PKI), TPM Support
FR5 - Restricted Data Flow	System wide usage of HTTPS, SSH. Proxy Support for IE components
FR6 - Timely Response to Events	Logs, Alarms and Warnings for Ecosystem and Applications
FR7 - Resource Availability	IE State Service(Backup and Restore)

Industrial Edge Certificate Handling

SIEMENS

Certificate Handling
Overview

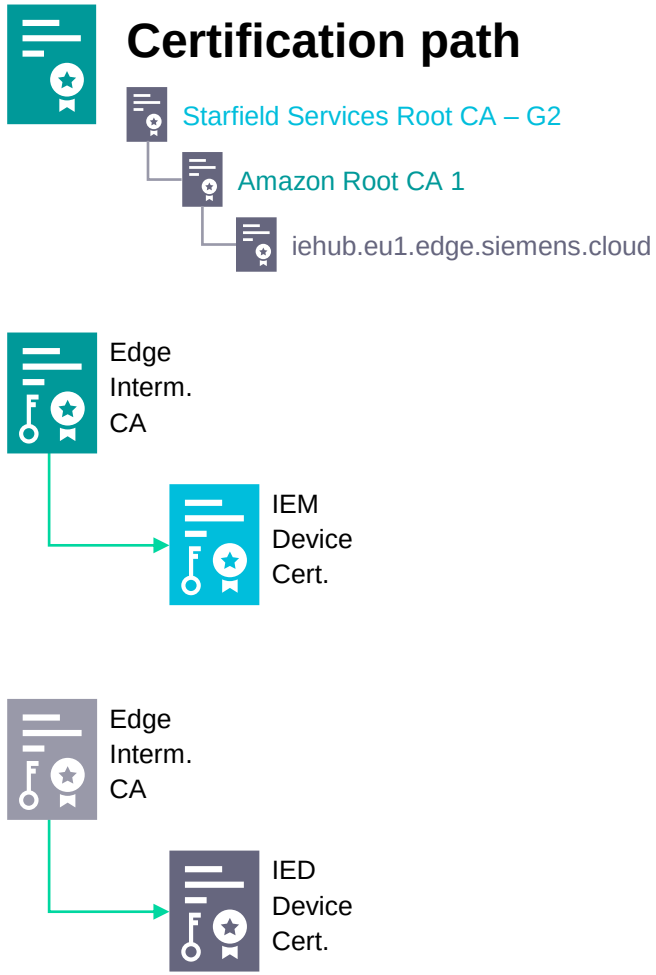


IE HUB
- Certificate generated by Amazon CA
- Strong Ciphers

IE Management
Own managed certificates

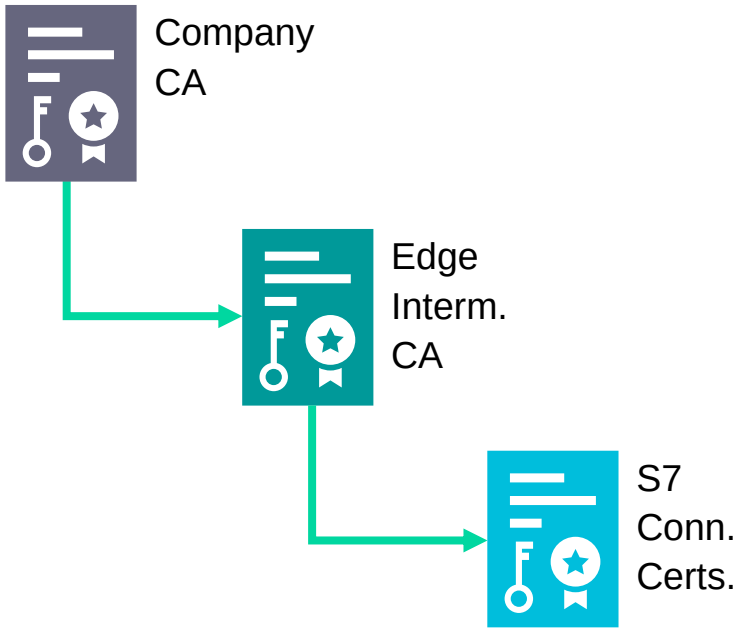
IE Device
- Own managed certificates
- Certificates are used by the devices as a proof of identity

Certification path



SIEMENS

Certificate Handling
Edge Device

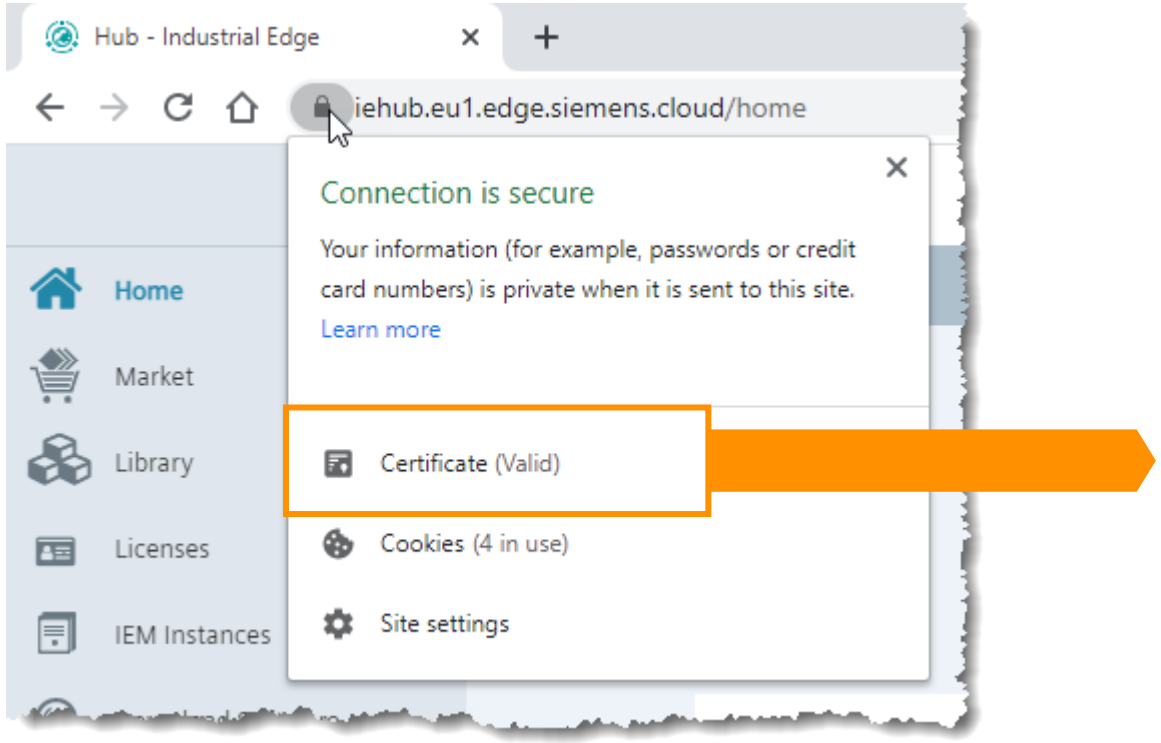


SIMATIC S7 Connector App
Using signed OPC UA
data source

OPC UA Server

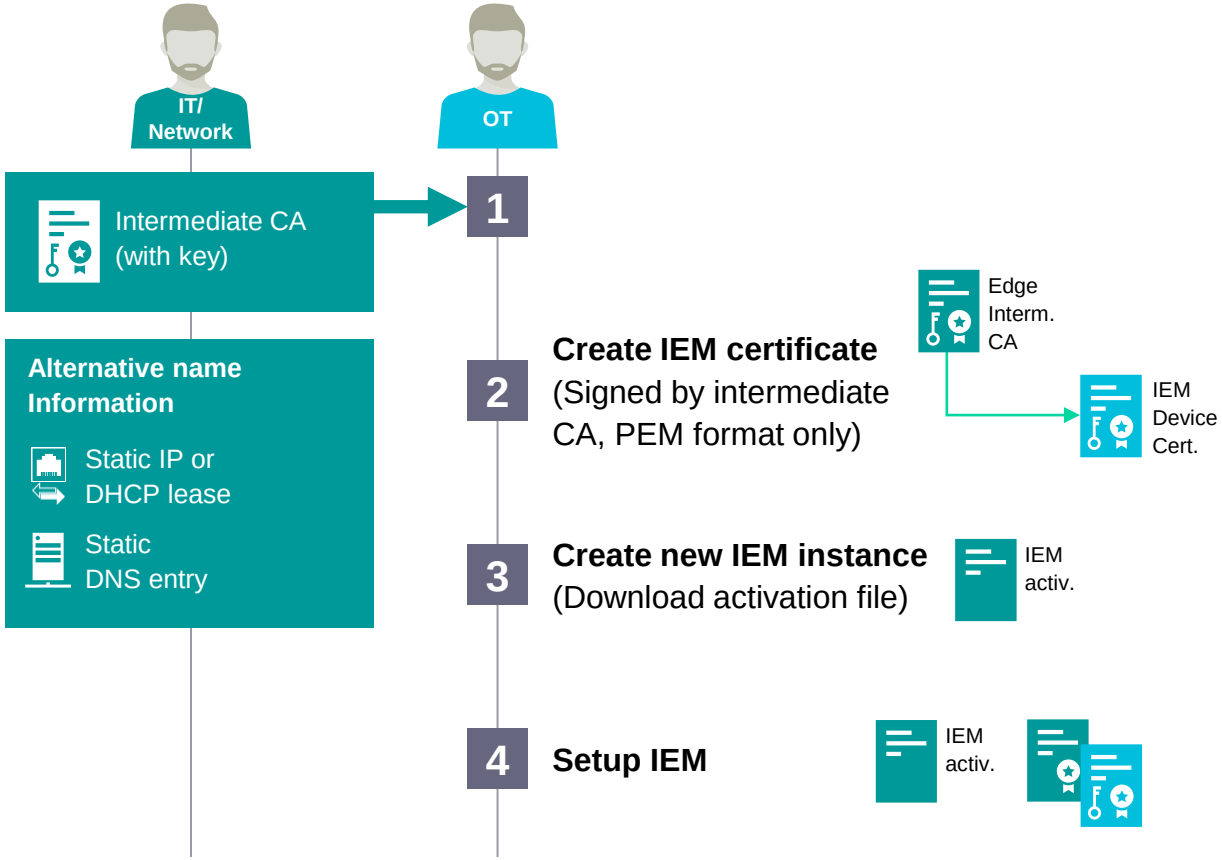
SIEMENS

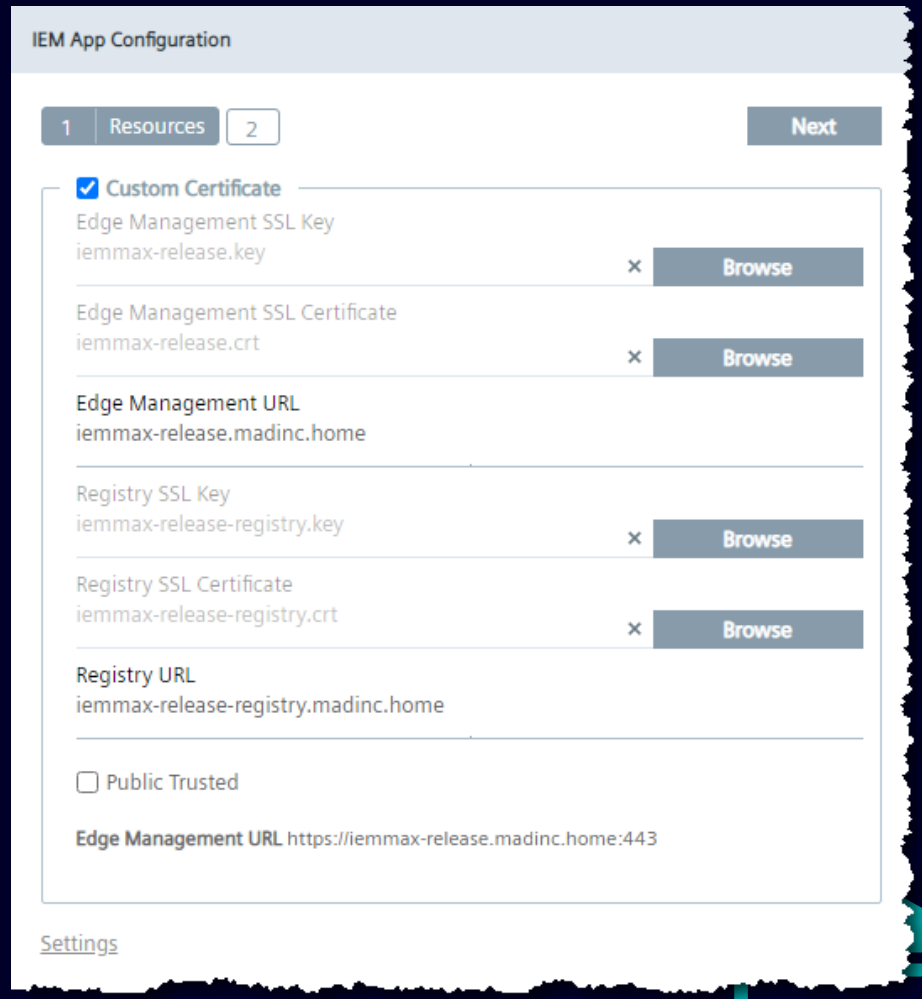
Certificate Handling
Industrial Edge Hub



SIEMENS

Certificate Handling
Industrial Edge Management





IEM activation defines URLs, certificates and proxy settings

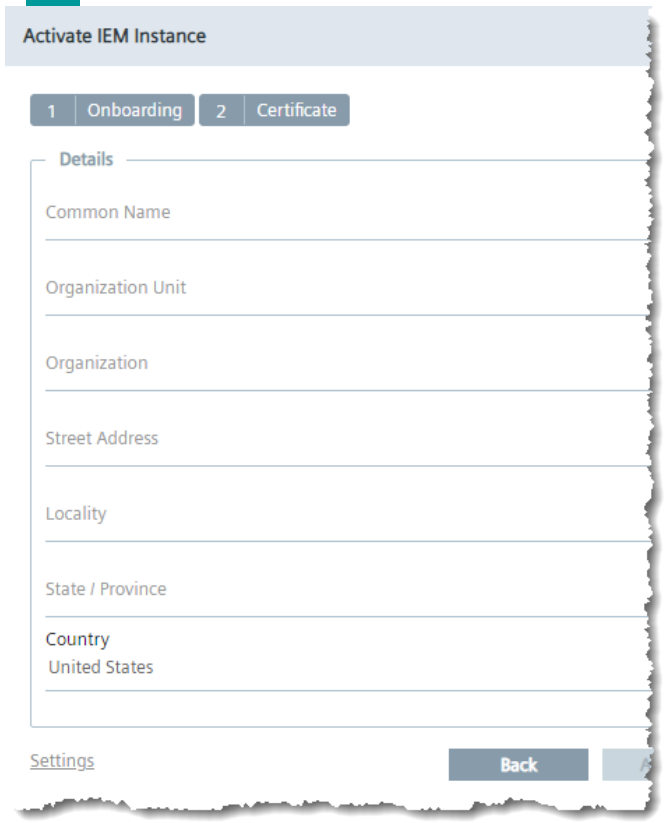
IEM

Please take notice: The workflow shown depends on the used infrastructure

SIEMENS

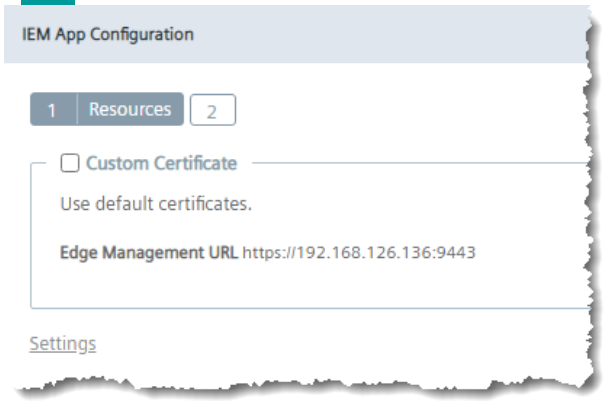
Industrial Edge Management installation
Step-by-Step guidance

1



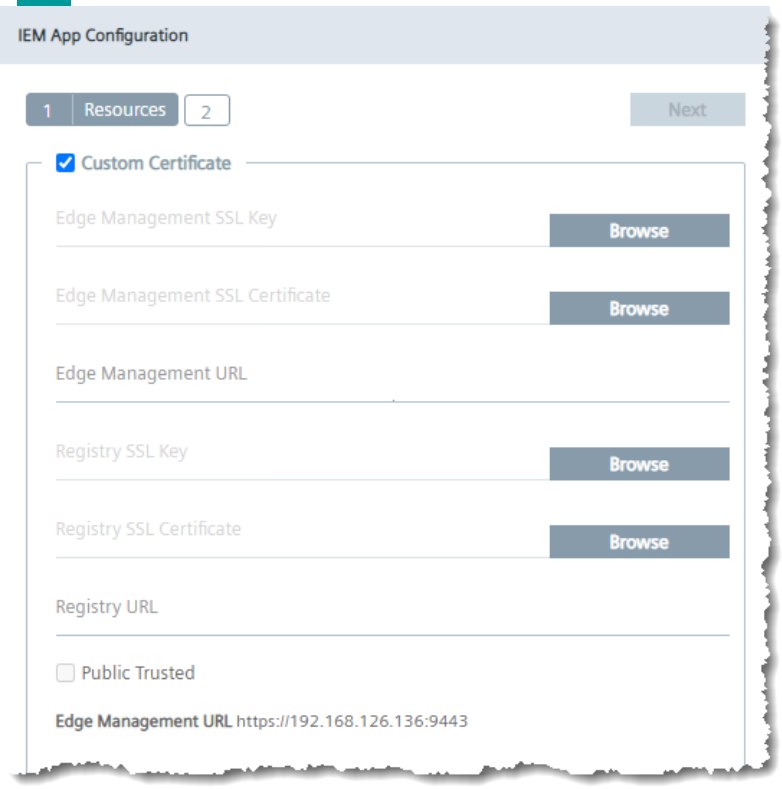
IEM internal root and intermediate CA are generated

2



After first sign-in use default certificates or …

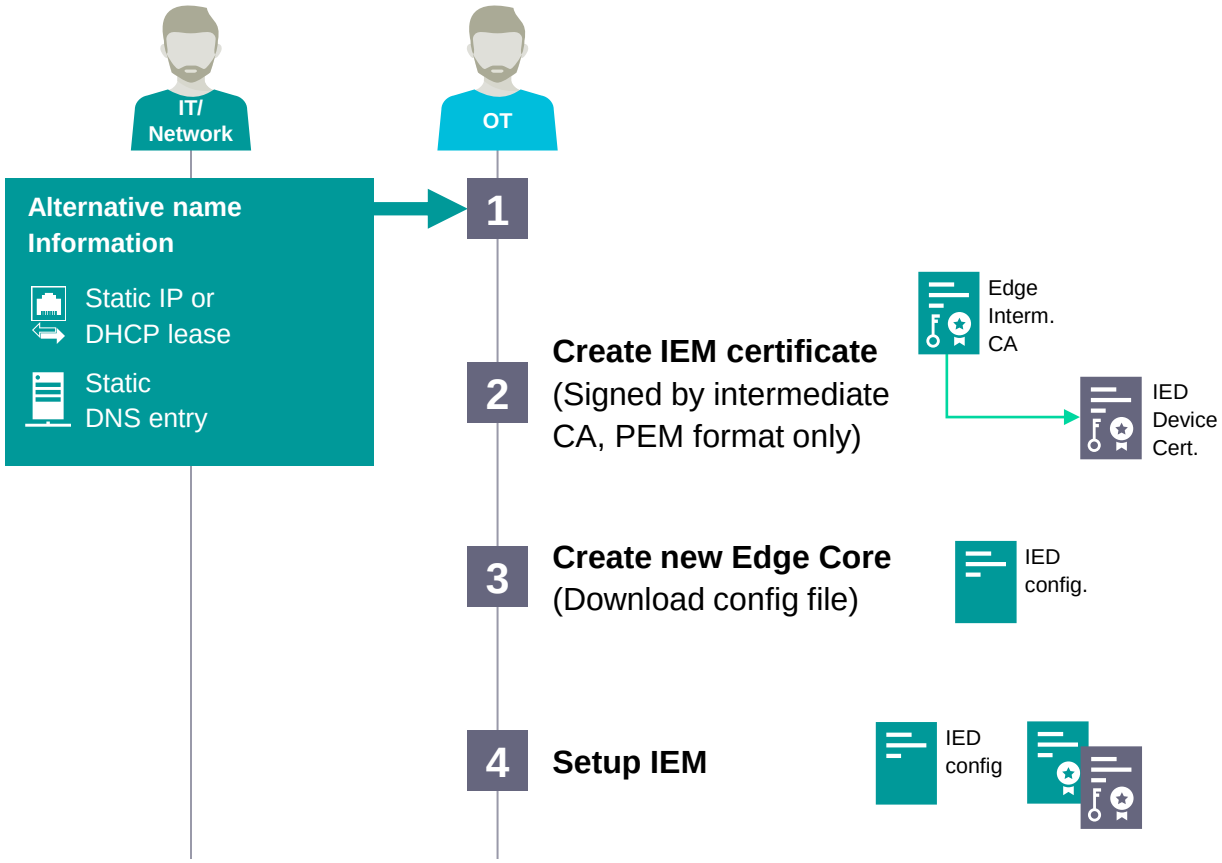
3



Set up custom certificates

SIEMENS

Certificates
Edge Device

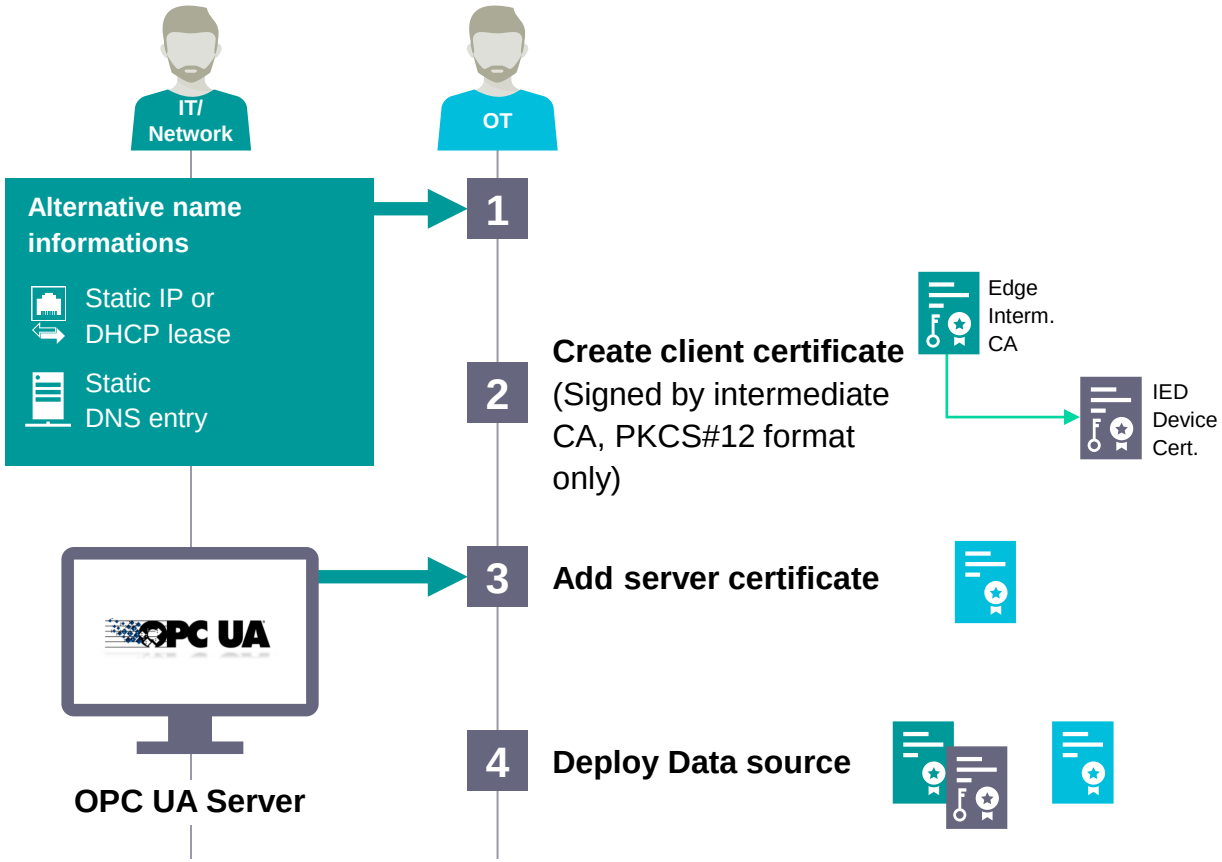


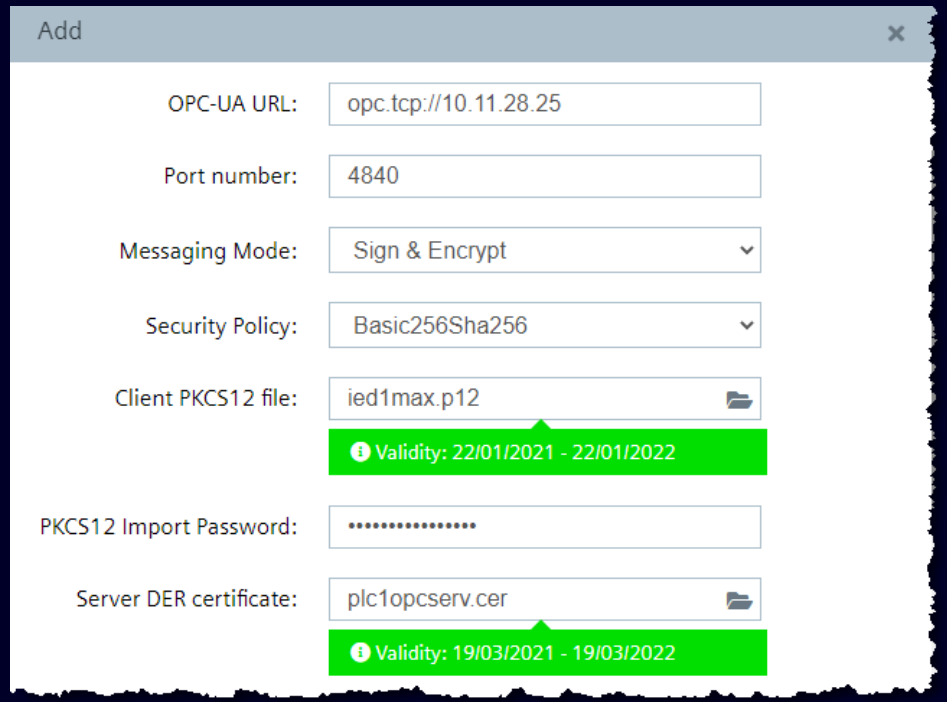
Certificates can be uploaded in the IED webserver

Please take notice: The workflow shown depends on the used infrastructure

SIEMENS

Certificates
SIMATIC S7 Connector



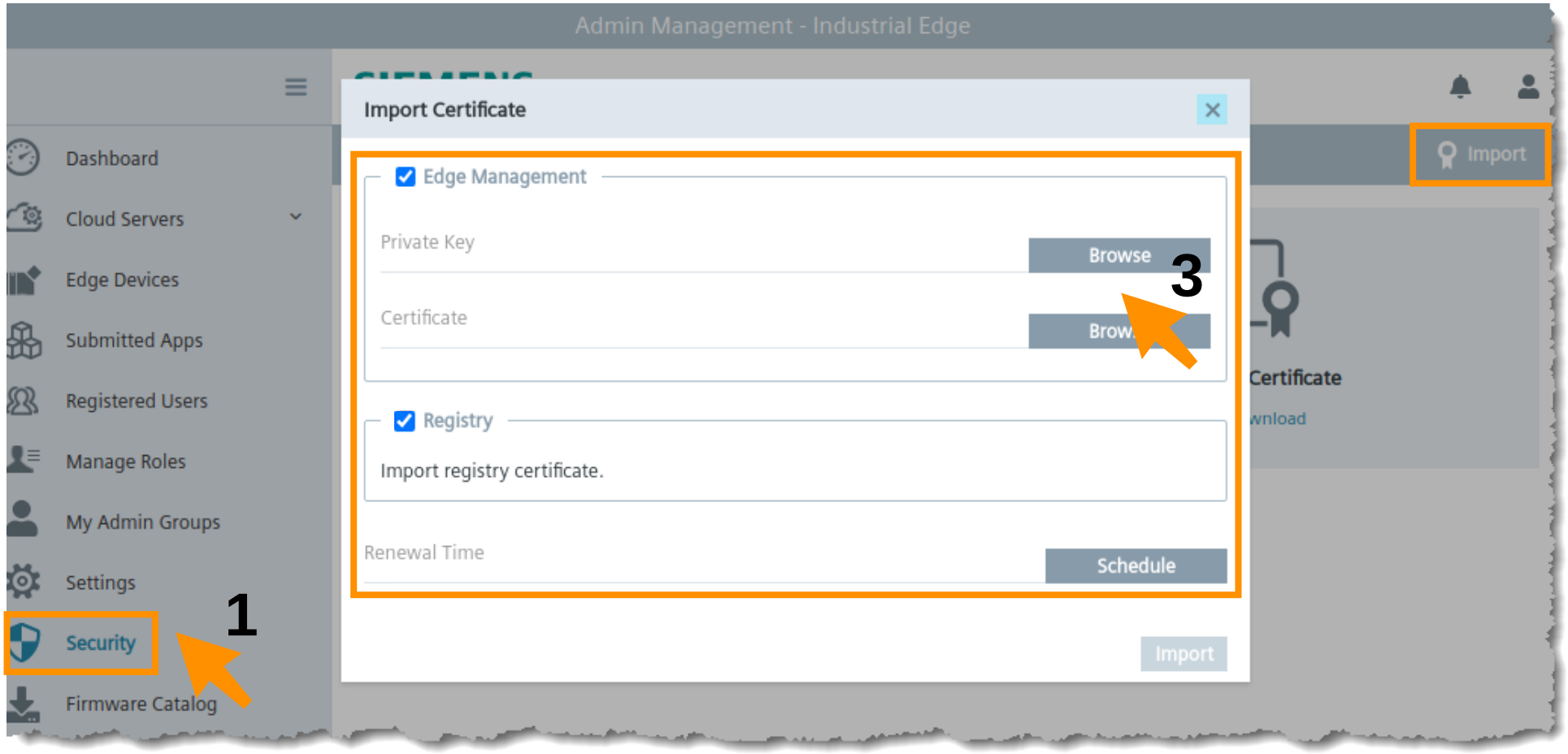


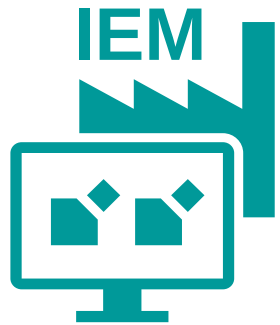
Certificates can be added during setup of data source

Please take notice: The workflow shown depends on the used infrastructure

SIEMENS

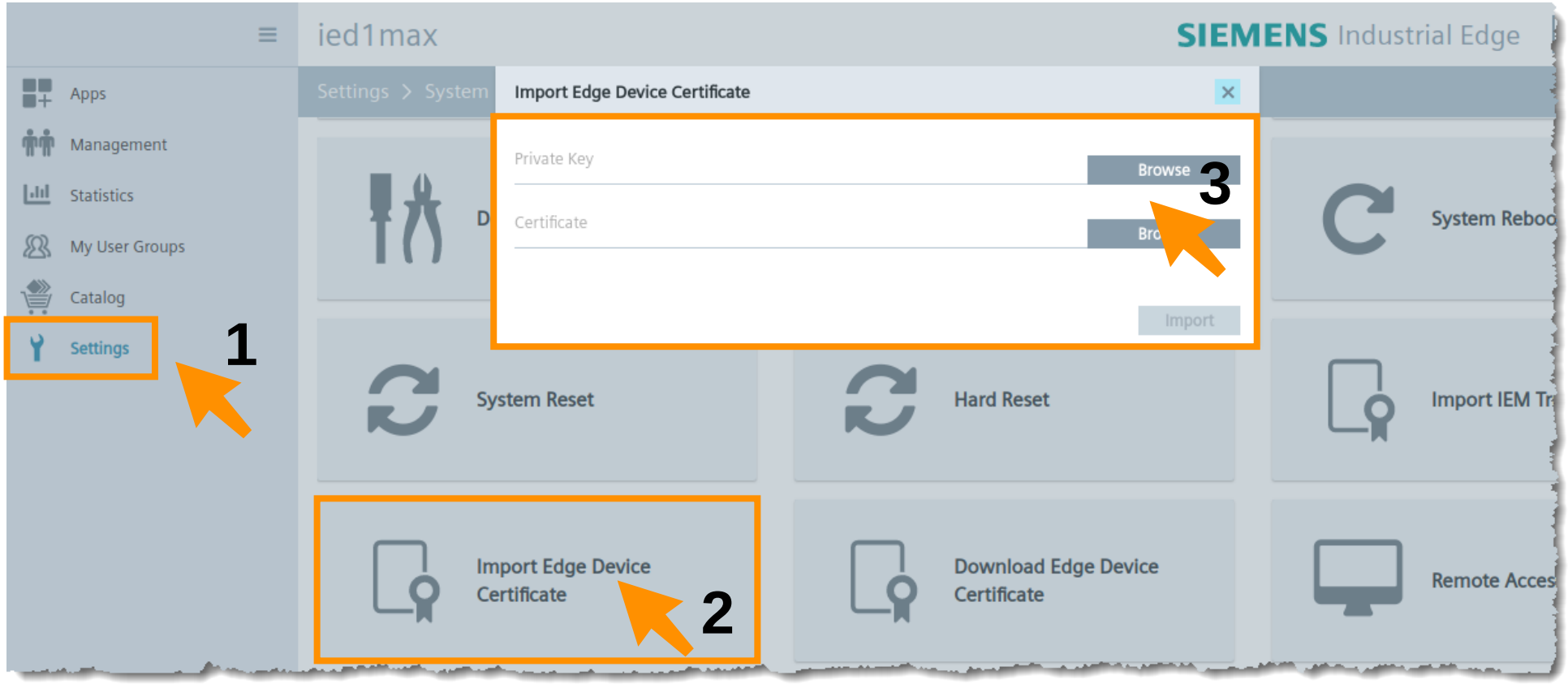
Industrial Edge Management
How to change certificates afterwards





SIEMENS

Industrial Edge Device
How to change certificates afterwards

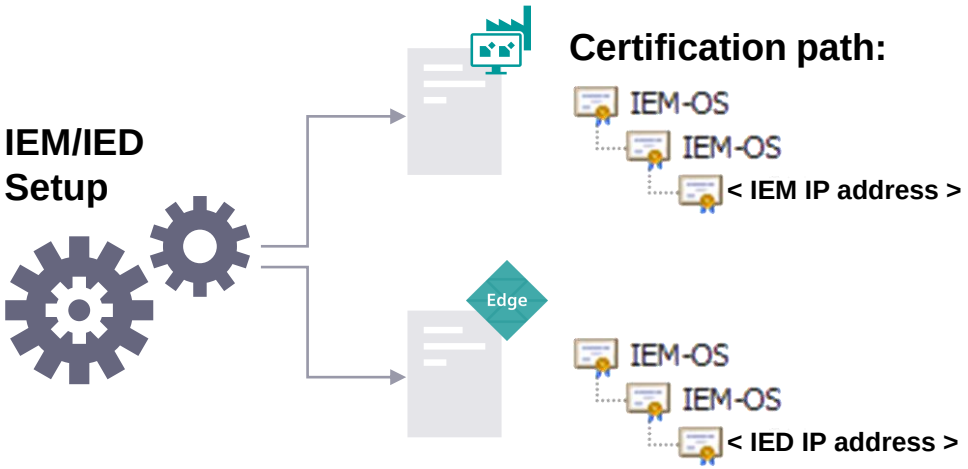


IED Edge

SIEMENS

Certificate management
Challenges due to internet-based connectivity

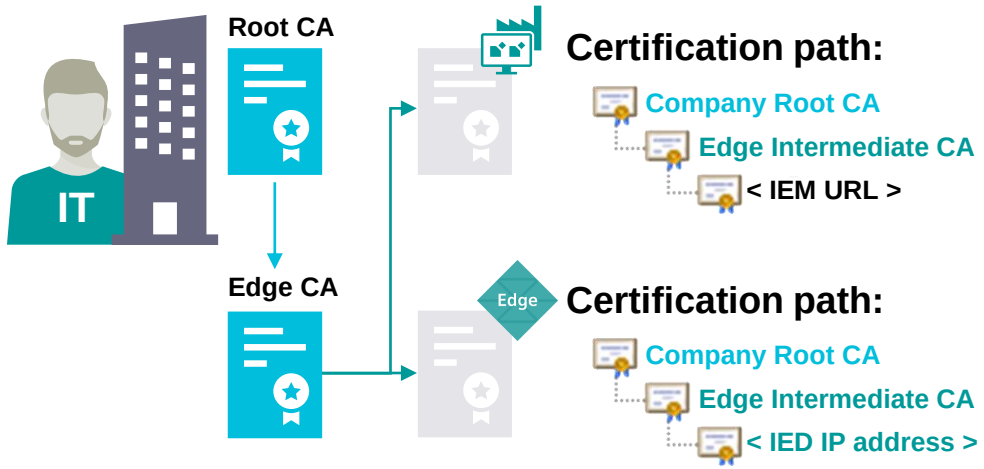
Use of default certificates



Create certificate generically during setup

- \+ Easy setup
- − No further proof of identity
- − IEM CA needs to be integrated in IT infrastructure

Use certificates signed by PKI



Create certificates with a Public Key Infrastructure (PKI)

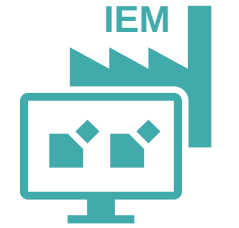
- − More complex setup
- \+ Proves that the device belongs to the company
- \+ No further distribution of IEM Root CA required

SIEMENS

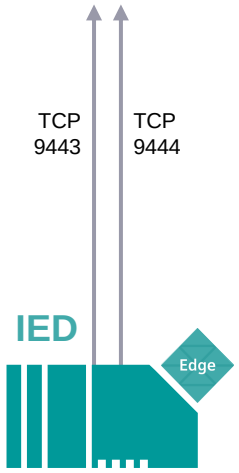
Industrial Edge Ports and connections

SIEMENS

Industrial Edge Management Application
Two different ways of setup



“Out-of-the-box” configuration

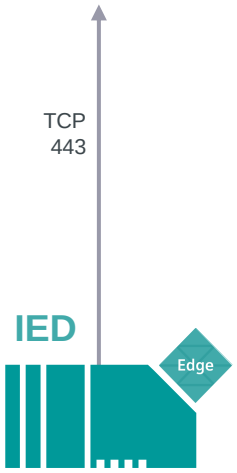


- 2 outgoing TCP connections
  (must be configured in cell protection firewall)
- Automatic (self signed) certificate management
  (automatic renewal before expiration)
- No integration in customers PKI infrastructure
  (no central management for revocation)
- TCP/IP based communication
  (less flexibility but easy setup)

Small networks without centralized administration

IP based

Advanced configuration used in this use case



- 1 outgoing TCP (HTTPS) connection
  (already allowed by most firewall policies)
- No automatic certificate management
- Integration in customers PKI infrastructure
  (Customer can use custom certificates created by their own PKI)
- DNS based communication
  (more flexibility but advanced setup, need of DNS servers)

Larger networks with centralized administration

DNS based

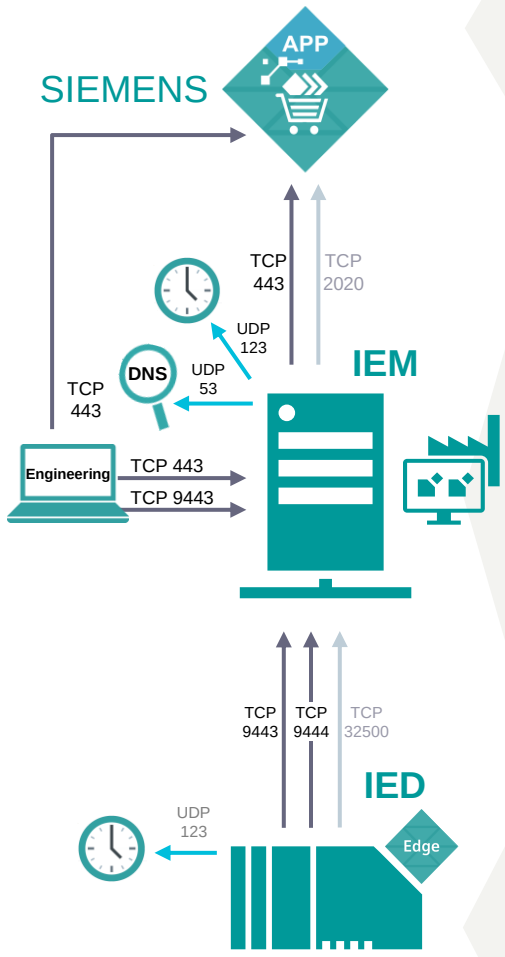
SIEMENS

IP based IEM addressing
(Out-of-the-box configuration)

Internet

Shop floor

Machine



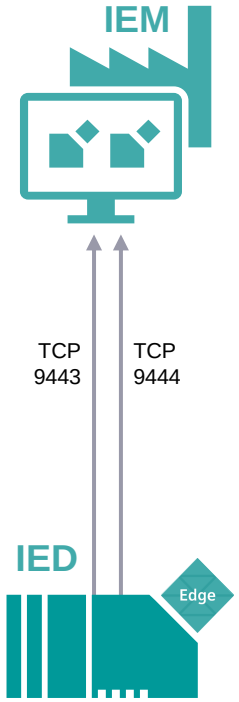
Dst. Port	Source	Destination	Mandatory	Description
TCP 443	Engineering	iehub.eu1.edge.siemens.cloud	Recomm.	HTTPS access (Engineering ➔ HUB)
TCP 443	IEM	portal.eu1.edge.siemens.cloud portal-hub.eu1.edge.siemens.cloud portalhub.eu1.edge.siemens.cloud portal-relay.eu1.edge.siemens.cloud portalauth.eu1.edge.siemens.cloud artifacts.eu1.edge.siemens.cloud oss.eu1.edge.siemens.cloud applications.eu1.edge.siemens.cloud	Yes	HTTPS access (IEM ➔ HUB)
TCP 2020	IEM	portal-relay.eu1.edge.siemens.cloud	No	Siemens remote support (IEM ➔ HUB)

Dst. Port	Source	Destination	Mandatory	Description
TCP 443	Engineering	IEM	Yes	Configuration (OS UI)
TCP 9443	Engineering	IEM	Yes	Configuration (Mgmt. UI)
TCP/ UDP 53	IEM	DNS Server	Yes	Domain Name Resolution
UDP 123	IEM	NTP Server	Yes.	NTP Time Synchronization
TCP 443	IEM	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	Yes	HTTPS access (IEM ➔ HUB)
TCP 9443	IED	IEM	Yes	Edge device access
TCP 9444	IED	IEM	Yes	Edge device access
TCP 32500	IED	IEM	No	SSH Tunnel (IED ➔ IEM)
TCP 2020	IEM	portal-relay.eu1.edge.siemens.cloud	No	Siemens remote support (IEM ➔ HUB)

Dst. Port	Source	Destination	Mandatory	Description
TCP 443	Engineering	IED	Yes	Configuration access (Device UI)
UDP 123	IED	NTP Server	Yes	NTP Time Synchronization
TCP 9443	IED	IEM	Yes	HTTPS access (IED ➔ IEM)
TCP 9444	IED	IEM	Yes	HTTPS access (IED ➔ IEM)
TCP 32500	IED	IEM	No	SSH Tunnel (IED ➔ IEM)

SIEMENS

Industrial Edge Management Application
Two different ways of setup

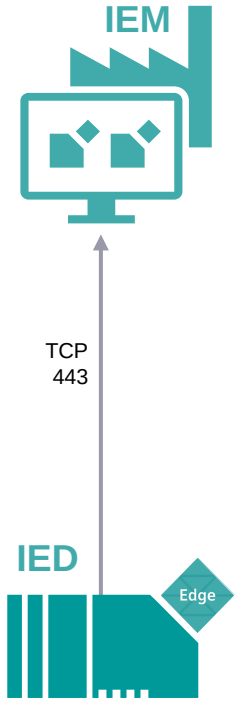


“Out-of-the-box” configuration

- 2 outgoing TCP connections
  (must be configured in cell protection firewall)
- Automatic certificate management
  (automatic renewal before expiration)
- No integration in customers PKI infrastructure
  (no central management for revocation)
- TCP/IP based communication
  (less flexibility but easy setup)

Small networks without centralized administration

IP based



Advanced configuration used in this use case

- 1 outgoing TCP (HTTPS) connection
  (already allowed by most firewall policies)
- No automatic certificate management
- Integration in customers PKI infrastructure
  (Customer can use custom certificates created by their own PKI)
- URL based communication
  (more flexibility but advanced setup, need of DNS servers)

Larger networks with centralized administration

DNS based

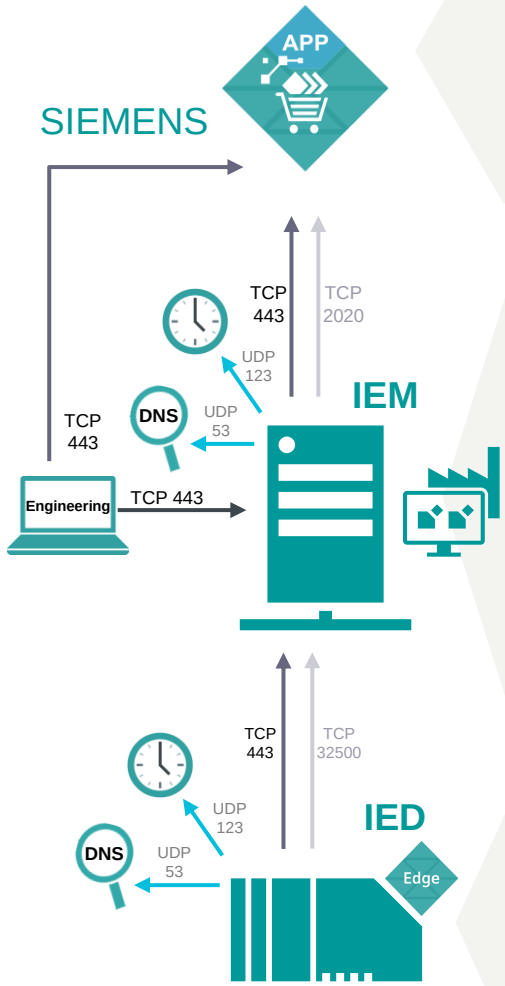
SIEMENS

DNS based IEM addressing

Internet

Shop floor

Machine



Dst. Port	Source	Destination	Mandatory	Description
TCP 443	Engineering	iehub.eu1.edge.siemens.cloud	Recomm.	HTTPS access (Engineering ➔ HUB)
TCP 443	IEM	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	Yes	HTTPS access (IEM ➔ HUB)
TCP 2020	IEM	portal-relay.eu1.edge.siemens.cloud	No	Siemens remote support (IEM ➔ HUB)

Dst. Port	Source	Destination	Mandatory	Description
TCP 443	Engineering	*[Edge Management URL as configured in IEM]*	Yes	Configuration (Mgmt. UI/OS UI)
UDP 53	IEM	DNS Server	Yes	Domain Name Resolution
UDP 123	IEM	NTP Server	Yes	NTP Time Synchronization
TCP 443	IEM	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	Yes	HTTPS access (IEM ➔ HUB)
TCP 443	IED	*[Edge Management URL as configured in IEM]* *[Registry URL as configured in IEM]*	Yes	Edge device access
TCP 32500	IED	IEM	No	SSH Tunnel (IED ➔ IEM)
TCP 2020	IEM	portal-relay.eu1.edge.siemens.cloud	No	Siemens remote support (IEM ➔ HUB)

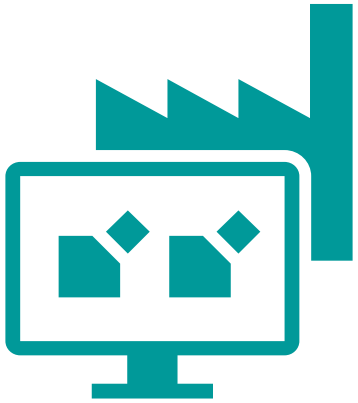
Dst. Port	Source	Destination	Mandatory	Description
TCP 443	Engineering	IED	Yes	Configuration access (Device UI)
UDP 53	IED	DNS Server	Yes	Domain Name Resolution
UDP 123	IED	NTP Server	Yes	NTP Time Synchronization
TCP 443	IED	*[Edge Management URL as configured in IEM]* *[Registry URL as configured in IEM]*	Yes	HTTPS access (IED ➔ IEM)
TCP 32500	IED	IEM	No	SSH Tunnel (IED ➔ IEM)

SIEMENS

Further Information

SIEMENS

Industrial Edge
Security related application examples



109779989 – Industrial Edge Management – **Getting Started**

109780393 – Industrial Edge Management – **Operation**

109781002 – Industrial Edge Management –
Security overview and requirements

Contact

siemens.com/industrial-edge

SIEMENS