



PRODUCT SHEET

Electrification X OT Companion

Master the OT inventory of your power systems, mitigate cyber risks effortlessly
[siemens.com/electrificationx](https://www.siemens.com/electrificationx)

SIEMENS

Contents

1		
Overview		3
2		
Features		4
Feature OT Asset Transparency		4
Feature Patch Management Level 1		8
Feature OT SIEM Integration		11
3		
Additional functions		12
4		
Subscription		14
5		
Prerequisites		15
6		
Ordering		17
7		
Product documentation		18
8		
Topology		19
9		
Customer support		20

Overview

Electrification X – OT Companion is a cloud-hosted, IoT-enabled application designed for operators of power systems in utilities, industries, and infrastructure. It provides comprehensive visibility and management capabilities across multi-vendor, multi-generation, and multi-technology Operational Technology (OT) environments, such as protection relays, substation automation systems, RTUs, networking devices and PCs.

The application combines inventory management, baseline version control, and vulnerability monitoring into a unified platform. Users can perform configuration comparisons, assess cyber risks and plan maintenance or mitigation actions directly within the system. OT Companion supports three operation modes: fully connected, air-gapped, and manual CSV-based operation, ensuring flexibility for all cybersecurity policies.

By using complementary data collectors from the SICAM 8 portfolio, customers can benefit from automatic device discovery and enumeration via OT protocols like IEC 61850, SNMP and a growing number of other protocols. If these gateways are connected to the cloud, real-time monitoring of device information is enabled.

Electrification X – OT Companion enables a closed-loop process for OT asset management and cybersecurity: from automated asset discovery and normalization, to contextual vulnerability detection, structured risk assessment aligned to industry best practices, and auditable mitigation workflows. This ensures that identified risks are consistently evaluated, prioritized, and transitioned into managed and traceable actions across the organization.

Benefits of OT Companion



Gain full transparency over your multi-vendor, multi-generation OT inventory, ensuring system integrity across all sites



Proactively monitor vulnerabilities and manage patches to mitigate risks, leveraging continuous updates from a central database covering Siemens and third-party products



Support alignment with IEC 62443 and NIST recommended practices to fulfill NIS2 and NERC CIP regulatory requirements



Reduce manual tasks with automated data collection and real-time updates, allowing teams to focus on meaningful work



Establish a structured, risk-based decision process for vulnerabilities by combining standardized scoring methods with asset-specific operational context.

Features

This chapter contains the packages, including features, that can be subscribed to within the feature set OT Companion.

Feature OT Asset Transparency

The base package provides the foundation for asset visibility and configuration management. It includes OT Inventory, Baseline Management, Product Catalog and Customization pages.

OT Inventory

The OT Inventory module establishes comprehensive asset visibility across substations, plants, and industrial networks within Electrification X – OT Companion. It consolidates all connected and discovered devices into a unified interface, presenting vendor-independent asset information including product identifiers, firmware versions, serial numbers, and installed subcomponents.

Asset Discovery and Data Integration

Automated discovery through SICAM GridEdge IoT gateways supports standard OT protocols (IEC 61850, SNMP) for reliable asset enumeration. The system accommodates diverse operational environments through:

- Continuous synchronization for connected networks
- Air-gapped ZIP imports for isolated environments
- Manual CSV uploads for brownfield or offline infrastructures

Operational Capabilities

Users can define power-system topologies manually or through automated processes, apply search and filter criteria to device inventories, and export data for integration with engineering, maintenance, or cybersecurity platforms. Asset-to-device relationships maintain full traceability between physical equipment and digital representations.

Foundation for Risk Management

By combining normalized asset data with contextual attributes—process criticality, network exposure, operating zone, and location hierarchy—the OT Inventory enables risk-based vulnerability prioritization and supports structured cybersecurity decision-making across the OT environment.

Baseline Management

Baseline Management provides structured configuration control and compliance capabilities within Electrification X – OT Companion. Aligned with NIST SP 800-128 principles, it enables organizations to define, document, and monitor approved configurations across OT environments.

Configuration Baselines

Each baseline represents a formally reviewed configuration snapshot for a system or Configuration Item (CI), serving as the reference point for changes, updates, and audits. Organizations can establish baselines for:

- Firmware and software versions
- Protection setting parameters for supported relays

Deviation Detection and Reporting

The system automatically identifies deviations between installed and approved configurations. Results can be filtered by station, product, or device type, and exported for compliance verification and reporting purposes.

Configuration Management

Configuration files (binary, CSV, JSON, TXT formats) are archived within the platform for backup and restoration. Protection setting templates can be created from existing relay configurations to standardize deployments and ensure validated operation across assets.

Workflow Integration

Detected deviations can be systematically reviewed and addressed through performance metrics (KPIs) and structured workflows, enabling organizations to evaluate risks, define mitigation strategies, and maintain auditable decision records.

These capabilities establish a trusted configuration baseline that supports change control, facilitates compliance audits, and strengthens cybersecurity resilience.

Product Catalog

The product catalog provides a centralized repository of all products and manufacturers within the OT environment. It is automatically populated from detected device identities, ensuring consistency across inventories and baselines. A wide range of Siemens products are pre-classified with standardized manufacturer, family, and model designations, enabling immediate operational visibility.

Product Information Management

Users can maintain comprehensive metadata for each product entry:

- Product lifecycle status
- Firmware and configuration variants
- Functional descriptions
- Documentation links and ordering details

The system allows for manual normalization of vendor naming conventions, ensuring consistent grouping of devices under unified manufacturer, family, and model designations.

Firmware and Software Component Tracking

The catalog includes firmware and software components as structured entities with associated lifecycle information:

- Release dates and version history
- Approval status
- Release documentation

This structure supports security-focussed and functional patch management and release control processes by adding product data to vulnerability monitoring, baselines, and operational workflows.

Obsolescence Management

Maintaining product lifecycle status enables proactive obsolescence management. Organizations can identify devices approaching end-of-life or end-of-support, plan technology refresh cycles before support discontinuation, and prioritize replacement investments based on operational criticality. This visibility reduces unplanned downtime risks and ensures continuity of vendor support for critical assets.

Operational Value

The product catalog enables accurate reporting, vulnerability monitoring, and lifecycle management. Organizations can make informed decisions on equipment modernization, support planning, and cybersecurity readiness based on current product information.

Service Maintenance Task

The service & maintenance task module in Electrification X – OT Companion provides an integrated workflow framework for documenting and managing all operational service activities across OT assets. It helps utilities and industrial operators structure their maintenance routines, ensure accountability, and maintain a verifiable digital record of field interventions.

Users can plan, assign, and track maintenance or inspection activities directly within the application. Each task captures relevant metadata such as responsible teams, task type, criticality, due date, status, and related documents or references (e.g., service reports, calibration records, or commissioning notes).

The workflow supports recurring maintenance cycles and facilitates the documentation of corrective, preventive, or condition-based actions.

Historic tasks are preserved in a central audit trail, providing full transparency of maintenance history for each asset. This traceability enhances operational planning, supports compliance with maintenance policies and safety standards, and enables organizations to demonstrate continuous equipment reliability and security adherence during audits or regulatory reviews.

OT Insights Dashboard

The OT Insights Dashboard in Electrification X – OT Companion transforms complex asset data into meaningful, actionable intelligence. It offers an analytical overview of key performance indicators (KPIs) and metrics related to asset inventory, configuration status, lifecycle, and baseline adherence.

Users can filter and slice data dynamically by partition, location, or product technology to focus on specific substations, regions, or domains. Predefined widgets visualize asset distribution by manufacturer, product technology, and operating state, while additional charts highlight baseline adherence, obsolescence status, and process criticality.

The dashboard empowers users to identify deviations or risks at a glance – for example, outdated firmware, undefined baselines, or phased-out equipment – and to correlate technical insights with operational priorities.

By combining asset transparency with intuitive analytics, OT Insights enables IT/OT managers and engineers to evaluate fleet health, monitor cybersecurity readiness, and report on compliance progress in a single, unified interface.

It serves as a strategic cockpit for data-driven decisions, supporting both day-to-day operations and long-term asset lifecycle optimization.

Two optional features can be added to the subscription on demand for the following use cases

Feature

Patch Management Level 1

The Patch Management Level 1 module provides proactive Vulnerability Monitoring and structured workflows for risk assessment and patch coordination. It enables operators to maintain a strong cybersecurity posture by continuously tracking relevant vendor advisories, evaluating impacts, and planning mitigation measures.

Vulnerability Monitoring

The integrated vulnerability view consolidates real-time notifications of newly disclosed CVEs, vendor advisories, and product-specific alerts. Each entry may include:

- CVSS scores and severity ratings
- Affected components and product versions
- Recommended mitigations
- References to CWE/CVE documentation
- Cross-links to potentially impacted devices in the organization's inventory

Environmental Risk Scoring

The system calculates environmental CVSS scores for each potentially affected device using customizable device risk profiles. These profiles incorporate contextual properties such as network exposure, process criticality, and operational environment. This contextualized scoring enables organizations to prioritize vulnerabilities based on actual risk to their specific infrastructure rather than relying solely on generic vendor severity ratings. This allows security and maintenance teams to assess exposure immediately and prioritize actions based on operational relevance.

Vulnerability Intelligence Service

Through the built-in watchlist, users subscribe to Siemens' Vulnerability Intelligence Service, which aggregates and validates data from global sources across multiple OEMs and product lines. The service provides (as of the publication of this document):

- 2,000+ monitored sources for comprehensive coverage
- 140,000+ notifications processed and validated
- 400,000+ components in the vulnerability database
- CVE completeness since 2021 for historical analysis
- EUVD completeness since 2025 for EU regulatory compliance

Organizations can request monitoring for additional products to ensure full coverage of their asset portfolio. Automated notifications are issued when new advisories are published, ensuring continuous awareness and timely response to emerging threats.

Watchlist configuration and product requests

Through the built-in Watchlist, users subscribe to Siemens' Vulnerability Intelligence Service, which aggregates and validates data from global sources – including NVDs, vendor PSIRTs, and research repositories – across multiple OEMs and product lines.

Organizations can request monitoring for additional products to ensure full coverage of their asset portfolio and receive automated notifications when new advisories are issued, ensuring continuous awareness and timely response to emerging threats.

Electrification X – OT Companion supports structured, guided risk assessment workflows aligned with industry-standard frameworks including CISA's Stakeholder-Specific Vulnerability Categorization (SSVC), NIST SP 800-40, and FIRST CVSS.

From Unmanaged to Managed Risk

The application guides users through a systematic process to transform unmanaged vulnerabilities into managed risks with documented organizational decisions.

Input foundation:

- Detailed OT inventory
- Vulnerability intelligence
- Industry frameworks

Guided Assessment Workflow:

1. **Risk overview:** Summary of vulnerability details and all affected devices across the inventory
2. **Organizational decision:** Guidance on general risk response approach—how to treat the vulnerability across the operated inventory
3. **Contextual risk:** Explanation of operational risks for the energy system operator, considering asset-specific factors:
 - Network exposure and segmentation
 - Process criticality and operational impact
 - Asset risk classification
 - Existing compensating controls
4. **Probability & Likelihood:** Consideration of exploitability in the given environment based on currently available information
5. **Mitigation measures:** Documentation of valid mitigation steps, workarounds and compensating controls

Response options at scale

Based on the assessment, operators can document one of four risk response strategies for affected devices:

- **Accept:** Risk accepted because probability of exploitation is less than effort for mitigation
- **Mitigate:** Risk mitigated by patch to specific firmware/software version
- **Transfer:** Risk transferred by stricter monitoring of device and perimeter (SIEM/SOC)
- **Avoid:** Risk avoided by turning off affected functionality, reconfiguration of perimeter, or replacement of device

Each decision creates an auditable record linking the vulnerability to specific devices, the chosen response strategy, and the documented rationale.

Compliance and Governance Value

This structured workflow ensures:

- **Traceability:** Complete audit trail of risk decisions, rationale, and mitigation actions
- **Consistency:** Organization-wide standards for vulnerability response across distributed sites
- **Scalability:** Systematic approach to managing vulnerabilities affecting hundreds of devices
- **Compliance:** Alignment with internal policies, industry standards and regulatory requirements (NIS2, NERC CIP, IEC 62443, NIST CSF)

The documented decision process provides governance teams with evidence of due diligence during audits and demonstrates systematic vulnerability management practices required by modern cybersecurity regulations.

OT Risk Dashboard

The OT risk dashboard in Electrification X – OT Companion provides a unified analytical view of cybersecurity-related metrics and trends across the entire OT environment. It translates large volumes of vulnerability data into clear, actionable insights, supporting proactive Risk Management and compliance reporting.

Users can filter and analyze data dynamically by partition, location, or technology domain to focus on specific substations, product families, or operational areas. The dashboard visualizes vulnerability coverage, base-score distributions (CVSS), affected products, and the number of devices potentially exposed within each site. Additional charts illustrate vulnerability trends by region and priority, helping teams identify where the highest cyber-risk concentrations exist and whether mitigation measures are improving over time.

By combining real-time vulnerability intelligence with contextual asset data, the OT risk dashboard enables operators to prioritize remediation efforts based on actual impact rather than generic severity scores. It also provides management with the KPIs needed to demonstrate compliance progress and to benchmark the organization's cybersecurity posture. In essence, it transforms vulnerability monitoring into a transparent, measurable, and continuously improving part of daily OT operations.

Value for compliance and Risk Management

This module supports regulatory compliance requirements (NIS2, NERC CIP and similar) by providing documented evidence of vulnerability tracking, risk assessment, and remediation planning—essential for audits and security governance frameworks

Feature

OT SIEM Integration

The OT SIEM Integration module provides interoperability with Siemens' SIEM as a service, a managed service delivered by Siemens Electrification & Automation.

Unified Asset and Security Monitoring

This integration bridges asset visibility and real-time cybersecurity monitoring, providing operators and SOC teams with a unified perspective on operational threats. The system enriches SIEM-based alerts with:

- Asset context and inventory data
- Configuration details
- Known vulnerabilities and risk profiles

This enrichment enables more effective threat prioritization and coordinated response between IT and OT teams, transforming generic security alerts into actionable intelligence grounded in operational context.

SIEM Alerts

OT Companion visualizes security alerts that have been detected and correlated by Siemens' SIEM through log collectors deployed across the customer's infrastructure. Alerts are displayed in a dedicated overview, enabling immediate assessment of affected locations, assets, or device types.

By correlating event data with the OT inventory and known vulnerability information, the system helps users understand which assets are impacted and how critical each incident may be within the operational context.

This integration accelerates incident triage and root-cause analysis, supports compliance with cybersecurity frameworks such as IEC 62443, and enables a more coordinated response between IT security operations and OT engineering teams.

Ultimately, it transforms OT Companion into a collaborative monitoring cockpit that unites asset intelligence, vulnerability context, and threat detection in one ecosystem.

Additional functions

Dashboard Widgets

The Dashboard widgets in Electrification X – OT Companion provide users with a customizable, at-a-glance view of key performance indicators (KPIs) that summarize the operational and cybersecurity health of their OT environments. These analytic widgets can be added to the central Electrification X dashboard, enabling managers and engineers to continuously monitor configuration compliance, vulnerability coverage, and overall fleet readiness across all locations.

- The Baseline Adherence Widget displays how well the installed software and firmware versions of devices align with defined baseline versions. A central percentage indicates the share of components in compliance, while visual color indicators highlight deviations or undefined baselines. Thresholds for acceptable adherence can be tailored using the KPI Limits feature, and the widget automatically reflects any updates made in Baseline Management.
- The Vulnerability Monitored Inventory Widget visualizes what portion of device components are actively monitored for security vulnerabilities. It derives data from the configured Watchlist, showing total monitored products and compliance ratios, with KPI-based color thresholds signaling areas that require attention. Together, these widgets turn complex data into intuitive insights for continuous improvement and governance reporting.

Notifications and Alarms

The Notifications and alarms feature in Electrification X – OT Companion ensures that users remain informed about critical cybersecurity and maintenance events without the need for constant manual monitoring. It acts as an intelligent alerting layer that keeps IT/OT managers, engineers, and security officers continuously up to date on system changes and emerging risks.

Users can activate daily email notifications summarizing new or modified vulnerabilities, pending or assigned workflow tasks, and relevant end-of-life product alerts. These concise reports provide immediate situational awareness, allowing teams to prioritize actions and coordinate responses efficiently.

Within the application, a central alarm list consolidates all real-time alerts, including newly published vulnerabilities affecting monitored assets and upcoming product obsolescence within the next six months. Each event entry provides direct links to the affected devices or components for rapid investigation.

By combining automation with transparency, Notifications and Alarms transform OT Companion into a proactive monitoring assistant, ensuring that critical updates never go unnoticed and that operational and cybersecurity readiness remain continuously maintained.

Supported Use Cases

Electrification X – OT Companion supports a wide range of operational and cybersecurity use cases across OT environments, including:

- Risk-based vulnerability prioritization using asset-specific environmental context
- Structured and auditable risk assessment aligned to industry best practices (CISA's SSVC and NIST CP 800-40r4)
- Centralized asset inventory and lifecycle management across multi-vendor environments
- Baseline definition and deviation tracking for firmware, software, and protection settings
- Backup and archiving of configuration files
- Documentation and governance of mitigation actions and maintenance workflows
- Cybersecurity management in online-connected, air-gapped and hybrid OT environments
- Integration of SIEM-based alerts to correlate anomalies with asset context and vulnerability exposures

These use cases enable organizations to improve operational efficiency, strengthen cybersecurity posture, and support compliance with regulatory and internal requirements.

Subscription

Standard subscription plan	Electrification X - OT Companion
Subscription metric	<ul style="list-style-type: none"> Feature OT Asset Transparency: per asset linked with an OT device (counted regardless of connection mode: Cloud-Connected, Air-Gapped, or Manual CSV) Feature Patch Management Level 1: per typical subscribed in the Watchlist for vulnerability monitoring Feature OT SIEM Integration: one system connection per tenant
Subscription term	Annually, auto-renewal
Billing term	Annually, payment in advance
Upscale	Effective immediately, pro-rated billing
Downscale/Cancellation	Effective with end of subscription term
Connected devices	To be purchased separately
Permitted Users	Unlimited, Extended Use

The Electrification X OT Companion feature set subscription plan is the regular, scalable offering for this cloud service. The subscription term is twelve (12) months with automatic renewal; the cloud service fee is paid in advance. The subscription plan can be upscaled at any time and cloud service fees for upscales are calculated on a pro-rated basis. The customer can also scale down the cloud service effective with the end of the current subscription term. The subscription fee will be adjusted for the upcoming billing term. The cloud service can be cancelled any time, effective with the end of the current subscription term.

The subscription plan can be purchased in feature packages:

- OT Asset Transparency (Base Package) - per asset in the topology structure that is linked with an OT device for the package OT Asset Transparency.

The core package can be topped with additional packages

- Patch Management Level 1 - per a specific typical that is subscribed for security vulnerabilities in the watchlist
- OT SIEM Integration – valid for integrating one particular environment per tenant

Extended Use entitles the customer to authorize its affiliates and third parties to access and use the cloud services in accordance with the rights set out in the Terms and Conditions.

Prerequisites

Electrification X tenant

The Electrification feature set is operated on an Electrification X tenant. Therefore, a tenant with an Electrification X Base Package is required. The Electrification X Base Package has a subscription term of 12 month and must be purchased together with the OT Companion feature set and at least the OT Asset Transparency package. To enable the functions Tasks and Vulnerabilities the additional, optional package Patch Management is required if not otherwise already available and in operation.

Supported connected devices

SICAM 8-based gateway solutions—including physical devices such as CP-8031, CP-8050, and SIMATIC IPC227E, as well as virtualized deployments—enable automated data collection, normalization, and continuous synchronization of OT asset information. These gateways significantly reduce manual effort, improve data quality, and enable scalable deployment across distributed OT environments.

Device compatibility and requirements

The cloud service is compatible with commercially available connected devices from Siemens running either the SICAM A8000 or SICAM S8000 automation platform. Virtual machines are also supported; refer to SICAM S8000 manuals for up-to-date compatibility information.

Discoverable OT devices

To enable automatic discovery of OT device information, one of the following must be configured:

- **IEC 61850-enabled devices:** One additional IEC 61850 client connection must be available in IEC 61850-server enabled protection, substation automation, and control products such as protection relays, power quality and fault recorders, or remote terminal units
- **SNMP-enabled devices:** SNMPv1, SNMPv2c, or SNMPv3 must be available and activated for read access on networking-enabled OT equipment such as routers, switches, RTUs, and PCs
- Additional options are made available over time, please refer to SICAM 8 GridEdge Device Group for up-to-date information

Deployment responsibilities

Connected devices must be purchased and installed on premises at a site specified by the customer as agreed between the customer and Siemens. The customer is responsible for installing the connected device and any associated costs to perform the cloud service in accordance with the related documentation for the Connected Device.

For order information, customers may contact their local sales representative.

This prerequisite is not necessary, if Electrification X - OT Companion is used without automated device discovery by importing inventory records based on file imports.

Web browser and viewing devices

Google Chrome and Microsoft Edge browsers have been tested and are recommended to be used to access the cloud service. Other modern standard web browsers will likely be compatible. A screen resolution of 1920 x 1080 pixels or higher is recommended for best user experience.

Internet Connection

The bandwidth of customer's internet connection determines the performance of the cloud service.

Ordering

Ordering process for the subscription

To order the cloud service for the first time, customer must request a quote from its Siemens sales representative. Depending on the offering either with services, then customer will receive a link to his tenant, or without services, then the customer will receive a link to the shopping cart. In this case customer needs to (i) choose the payment options and (ii) accept the Terms and Conditions to start using the cloud service. The "Terms and Conditions" consist of the "Supplemental Terms Electrification & Automation", the Base Terms and the General Software and Cloud Supplemental Terms, the Acceptable Use Policy, the Siemens Data Processing Terms, this Product and Service Data Sheet and any other Supplemental Terms which may be referenced in either of the mentioned documents. Customer may upgrade, downgrade, and cancel the cloud services directly in the subscription manager store <https://subscribe.siemens.com>.

Ordering connected devices

To order connected devices the customers may request a quote from their Siemens sales representative.

Connected device

Devices running either the SICAM A8000 or SICAM S8000 automation platform are supported, this includes SICAM CP-8031/CP-8050, SIMATIC IPC227E and other physical devices. Virtual machines are supported as well, see SICAM S8000 manuals for up-to-date information.

Ordering

For order information, customers may contact their local sales representative.

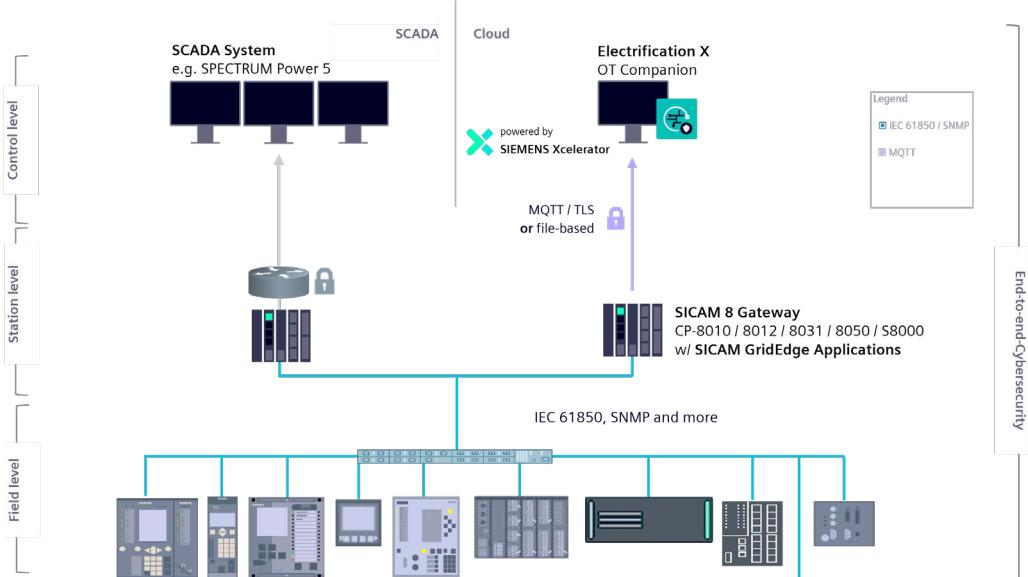
Product documentation

Technical documents	Document ID	Document ID German	Document ID English
Building X – Accounts User Guide	A6V12050070		
Building X – Devices User Guide	A6V12050067		
Electrification X – Base Package Operating Manual		E50417-H7500-C200-A2	E50417-H7540-C200-A2
Electrification X – Engineering Guide		E50417-H7500-C203-A2	E50417-H7540-C203-A2
Electrification X – Security Manual		E50417-H7500-C204-A2	E50417-H7540-C204-A2
Electrification X – OT Companion User Manual		E50417-H7500-C211-A5	E50417-H7540-C211-A5
SICAM GridEdge – IoT Monitoring			50417-H7640-C642-A8
SICAM 8 Applications – Communication			DC8-134-2
SICAM GridEdge – SIPROTEC 4 Client			E50417-H7640-C646-A2
SICAM GridEdge – 3rd Party Connector-01			E50417-H7640-C647-A3
SICAM GridEdge – 3rd Party Connector-02			50417-H7640-C648-A1

[↗ Technical documents can be downloaded here](#)

Topology

End-to-end cybersecurity



Data communication between the Connected devices and the cloud service

Key benefits



Instantly see all OT assets across sites, vendors, and generations in one central view



Get early warnings and actionable insights to reduce risks and increase resilience



Generate reports and prove compliance with just a few clicks



Compare, track, and update firmware/ software versions across all critical assets



Benefit from security insights on 400,000+ OT/IT components for rapid vulnerability insights

Customer support

Siemens offers helpdesk support.

Customer may contact its local Siemens representative for support requests.

<https://isp.portal.siemens.com/>

Email: support.ea.si@siemens.com

Germany / Austria / United Kingdom Phone: +49 9131 1743072

China Phone: +86 400 150 6060

Brazil Phone: +55 0800 011 9484

India Phone: +91 1 800 266 7480

Published by
Siemens AG
Smart Infrastructure
Electrification & Automation
Mozartstrasse 31c
91052 Erlangen, Germany

For the U.S.
published by
Siemens Industry Inc.
3617 Parkway Lane
Peachtree Corners, GA 30092
United States

© Siemens 2026

Subject to changes and errors. The information given in this document only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract.