

SIMATIC NET

Industrial Ethernet Security SINEC Security Monitor V4.9.1

Operating Instructions

Preface	1
Security recommendations	2
Function and structure	3
Planning deployment	4
Installation	5
Commissioning	6
Preparing, adding, and managing data sources	7
Operator control	8
Maintenance	9
Decommissioning, dismantling, and disposal	10
Listing SSMCTL Commands	11
Security Forwarding Data Format	A

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 Aktiengesellschaft. 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.

Table of contents

- 1 **Preface 9**
- 2 **Security recommendations..... 15**
 - 2.1 Security recommendations..... 15
 - 2.2 Security functions 18
 - 2.3 Intended operational environment 19
 - 2.4 Communication ports 21
 - 2.5 Ciphers used 25
- 3 **Function and structure 43**
 - 3.1 Function overview 43
 - 3.2 Components and licenses..... 44
 - 3.2.1 SSM Server 45
 - 3.2.2 SSM Intelligence Database 48
 - 3.2.3 SSM Sensor (optional) 48
 - 3.2.4 SSM Agent (optional) 49
 - 3.3 Working modes..... 49
- 4 **Planning deployment 51**
 - 4.1 Planning usage of SINEC Security Monitor Server and Sensor 51
 - 4.2 Planning data sources for network traffic capture..... 51
 - 4.3 Network bandwidth usage for traffic between Server and Sensor 52
 - 4.4 Supported Microsoft Windows versions for vulnerabilities association 52
 - 4.5 Supported network scenarios 53
 - 4.5.1 SSM Server interfaces 53
 - 4.5.2 SSM Sensor interfaces 53
 - 4.5.3 Overview of supported network scenarios 54
 - 4.5.4 Communication between SSM Server and SSM Sensor 56
 - 4.5.5 Communication between SSM Agent and SSM Server or SSM Sensor 59
 - 4.5.6 Agentless communication with the SSM Server 62
 - 4.5.7 No Agent communication with the SSM Server 64
 - 4.5.8 Access to the WBM..... 67
 - 4.5.9 SSM Server diagnostics communication..... 68
 - 4.5.10 SSM Sensor diagnostics communication 69
- 5 **Installation..... 71**
 - 5.1 Hardware requirements and recommendations 71
 - 5.1.1 Hardware requirements and recommendations for SSM Server 71
 - 5.1.2 Hardware requirements and recommendation for SSM Sensor 73
 - 5.1.3 Hardware requirements for SSM Server on Virtualization Platforms 74
 - 5.2 Hardware preparation 75

5.3	Installation of software	78
5.3.1	Open firewall ports.....	78
5.3.2	Standard accounts	79
5.3.3	Software packages.....	80
5.3.4	SHA256 checksums	82
5.3.5	Verifying signatures of signed installation files.....	82
5.3.6	Preparing the USB flash drives	83
5.3.6.1	Software packages and applications needed.....	83
5.3.6.2	Preparing USB flash drive A	84
5.3.6.3	Preparing USB flash drive B.....	85
5.3.7	Installing the SSM Server software on a physical hardware.....	87
5.3.7.1	Software packages and applications needed.....	87
5.3.7.2	Installing the operating system	88
5.3.7.3	Installation precheck of the disk (optional)	89
5.3.7.4	Configuring the SINEC Security Monitor Server	89
5.3.7.5	Logging in to the SINEC Security Monitor System.....	91
5.3.7.6	Requesting a SINEC Security Monitor license for the SINEC Security Monitor Server	91
5.3.7.7	Verifying the installation status of SINEC Security Monitor Server.....	92
5.3.7.8	Adding the internal SSM Sensor	93
5.3.7.9	Configuring the system time	93
5.3.7.10	Finding the SINEC Security Monitor version number	94
5.3.8	Installing the SSM Server software in a virtual environment (ESXi)	95
5.3.8.1	Software requirements for SSM Server on Virtualization Platforms	95
5.3.8.2	VMware with TPM	95
5.3.8.3	WMware without vTPM	104
5.3.9	Installing the SINEC Security Monitor Sensor	108
5.3.9.1	Software packages and applications needed	108
5.3.9.2	Installing the operating system on the SINEC Security Monitor Sensor.....	109
5.3.9.3	Installation precheck of the disk (optional)	110
5.3.9.4	Configuring the SINEC Security Monitor Sensor.....	110
5.3.9.5	Setting the system time of the SSM Sensor	112
5.3.9.6	Requesting a SINEC Security Monitor license for the SINEC Security Monitor Sensor	112
5.3.9.7	Adding Sensors	113
5.3.9.8	Verifying the status of SINEC Security Monitor Sensor services	115
6	Commissioning	117
6.1	Initial system configuration	117
6.1.1	Creating user account	117
6.1.2	Updating the SINEC Security Monitor Intelligence Databases.....	119
6.2	System parameters configuration	121
6.2.1	Configuring network settings	121
6.2.2	Restricting access control	122
6.2.3	Configuring system backups	122
6.2.4	Preparing a remote Linux server for backups.....	124
6.2.5	Setting up email notifications	130
6.2.6	Configuring general log settings.....	131
6.2.7	Configuring asset types and zones.....	132
6.2.7.1	Setting asset types	133
6.2.7.2	Setting asset zones	133
6.2.8	Managing correlation rules	134
6.2.8.1	Configuring anomaly baselines.....	136

6.2.8.2	Upgrading or downgrading security events.....	140
6.2.9	Configuring security reports	141
6.2.10	Configuring system notifications.....	142
6.3	Setting the SINEC Security Monitor working mode.....	143
6.4	Certificate management.....	145
6.4.1	Overview	145
6.4.2	Managing certificates.....	146
6.5	Third-party system integration	148
6.5.1	Configuring security log forwarding to third-party systems.....	148
7	Preparing, adding, and managing data sources.....	149
7.1	SINEC Security Monitor Sensor	149
7.1.1	Adding Sensors.....	149
7.1.2	Managing Sensors	150
7.1.3	Editing a Sensor.....	152
7.2	SINEC Security Monitor Agent	156
7.2.1	Installing the SINEC Security Monitor Agent on a Microsoft Windows-based asset.....	156
7.2.2	Enabling and Configuring USB Event Logging on Windows Devices	157
7.2.3	Adding a data source in agent mode	158
7.2.4	Verifying a SINEC Security Monitor Agent after installation	160
7.3	Agentless security log collection.....	160
7.3.1	Preparing and adding a Microsoft Windows computer for agentless security log collection...	160
7.3.1.1	Configuring WinRM	162
7.3.1.2	Configuring Remote WMI	167
7.4	No agent data sources	174
7.4.1	Adding a data source in no agent mode	174
7.4.2	Configuring an endpoint for syslog data collection.....	176
7.4.3	Preparing Linux systems for log data forwarding.....	178
7.5	Managing log data sources	178
8	Operator control	181
8.1	Monitoring the security situation.....	181
8.2	Accessing the SINEC Security Monitor Server	182
8.3	Typical usage scenarios	183
8.3.1	Analyzing security events.....	183
8.3.2	Monitoring operations in all six dimensions.....	184
8.3.2.1	Getting an overview on security statistics	185
8.3.2.2	Asset dimension	186
8.3.2.3	Network dimension.....	187
8.3.2.4	Vulnerability dimension	189
8.3.2.5	Application dimension	189
8.3.2.6	User account dimension.....	190
8.3.2.7	Operation and maintenance dimension.....	190
8.3.3	Managing the use of USB storage devices in an OT environment.....	192
8.3.4	Detecting intrusion threats.....	193
8.3.5	Monitoring malware threats.....	194
8.4	Security monitoring operation	195

8.4.1	Managing asset monitoring.....	195
8.4.1.1	Assets dashboard	195
8.4.1.2	Monitoring assets	196
8.4.1.3	Maintaining assets	197
8.4.1.4	Monitoring asset vulnerabilities.....	198
8.4.2	Monitoring asset user accounts	199
8.4.3	Monitoring applications	200
8.4.4	Central security log management.....	201
8.4.5	Generating a security monitoring report.....	202
8.4.5.1	Downloading the security report	202
8.5	Handling security events	203
8.5.1	Monitoring risks.....	203
8.5.2	Monitoring and responding to security events	204
8.5.3	Analyzing security event trends.....	207
9	Maintenance	209
9.1	Diagnostics	209
9.1.1	Diagnostics tools.....	209
9.1.1.1	Diagnostics page.....	209
9.1.1.2	Security self-monitoring	210
9.1.1.3	OPC UA interface	210
9.1.1.4	Packet capture	218
9.1.1.5	Audit Log.....	218
9.1.2	Fault messages	219
9.1.3	Troubleshooting.....	219
9.1.3.1	SINEC Security Monitor Server problems.....	219
9.1.3.2	Security monitoring problems	220
9.2	Corrective maintenance	221
9.2.1	Software maintenance	221
9.2.1.1	Log data diagnosis	221
9.3	Preventive maintenance	222
9.3.1	Reinstalling the SINEC Security Monitor Server	222
9.3.1.1	Backup configuration settings	222
9.3.2	Reinstalling the SINEC Security Monitor Sensor.....	223
9.3.3	Reinstalling the SINEC Security Monitor Agent.....	223
9.3.3.1	Uninstalling the SINEC Security Monitor Agent	223
9.3.4	Checking for system updates.....	223
9.3.5	Rebooting the SINEC Security Monitor System	224
9.3.6	Updating the vulnerability library and correlation rules	225
9.3.7	Managing backups.....	225
9.3.8	Using the test mode.....	226
9.3.9	Checking system alarms.....	227
9.3.10	SINEC Security Monitor Agent remote update	228
9.4	Updating system components	230
9.4.1	Overview of the upgrade process	230
9.4.2	SSM Server software update.....	233
9.4.3	SSM Sensor software upgrade	237
9.4.4	SSM Agent update	240
9.4.5	Checking data sources	241
9.4.5.1	Checking Agentless log collection after the migration.....	241

9.4.6	Updating the SSM Intelligence Database.....	242
9.4.6.1	Updating the SSM Intelligence Database.....	242
10	Decommissioning, dismantling, and disposal	243
11	Listing SSMCTL Commands.....	245
A	Security Forwarding Data Format.....	247
A.1	Security Forwarding Data Format	247
	Index	259

Preface

Validity

The information in this document applies to SINEC Security Monitor in the following version:

- V4.9.1

Required experience

To configure and operate the product described in this document, knowledge of the following products, systems and technologies is required:

- SINEC Security Monitor
Read this manual for more information
- Network security
Understanding the impact of security software on network operations
- Basic knowledge of Linux administration

Purpose of this documentation

This document contains all the information required for installation, commissioning, operation and maintenance.

Current manual edition and further information on the Internet

You will find the current version of this manual on the Internet pages of Siemens Industry Online Support:

Link: (<https://support.industry.siemens.com/cs/us/en/ps/29526/man>)

On this page, you will also find additional information e.g. product notices, FAQs etc.

The manual can also be found in DI SW Support Center (<https://support.sw.siemens.com/en-US/>) after purchase. There you can also download software updates as well as updates for the underlying Intelligence database.

Notes on this document

Cross-references

In this manual, there are often cross-references to other sections.

To return to the initial page after jumping to a cross-reference, some PDF readers support the command <Alt>+<left arrow>.

Search

To show all places where a term was found in a list, some PDF readers support the command <Ctrl>+<Shift>+<F>.

Terms

- Allow list
Also known as whitelist. Entries on this list will be displayed as events, when detected.
- Asset
Device in the OT environment
- Communication links
Network traffic caused by applications on different assets communicating with each other
- Deny list
Also known as blacklist. Entries on this list will raise an alert, when detected.
- Device
This term refers to all devices supported by SINEC Security Monitor in the network.
If the devices differ in the particular context, the product name or type will be used.
- Endpoint
Device connected to a network
- Firewall
Security module with firewall
- Network TAP
A network TAP (Test Access Point) is an external monitoring device which collects the traffic data between two monitoring points.
- Sensor
Device for collection and analysis of network traffic
- Server
Central component of SINEC Security Monitor (server hardware with installed SINEC Security Monitor software)
- Suricata
Open source network analysis and threat detection software. <https://suricata.io/> (<https://suricata.io/>)

Abbreviations

- ATT&
Adversarial Tactics, Techniques, and Common Knowledge
- CA
Certification Authority
- DNS
Domain Name System
- DoS
Denial of Service
- HMI
Human-Machine Interface

- IDS
Intrusion Detection System
- iLO
Integrated Lights-Out
- IPC
Industry-grade PC
- IT
Information Technology
- LAN
Local Area Network
- NIC
Network Interface Card
- NTP
Network Time Protocol (protocol for time synchronization between computers)
- O&M
Operation and Maintenance
- OT
Operational Technology
- PKI
Public Key Infrastructure
- PLC
Programmable Logic Controller
- RDP
Remote Desktop Protocol
- SIEM
Security Information and Event Management
- SSM
SINEC Security Monitor
- TAP
Terminal Access Point
- TLS
Transport Layer Security
- TTP
Tactics, Techniques and Procedures
- USB
Universal Serial Bus
- VLAN
Virtual Local Area Network
- VM
Virtual Machine
- WBM
Web Based Management, web interface of the SINEC Security Monitor Server software

- WLAN
Wireless Local Area Network
- WMI
Windows Management Instrumentation

License conditions

Note

Open source software

The product contains open source software. Read the license conditions for open source software carefully before using the product.

You will find license conditions in the following document on the supplied data medium:

- OSS_SINEC-Security-Monitor_99.pdf

Siemens provides products and solutions with industrial cybersecurity 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 cybersecurity 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 cybersecurity measures that may be implemented, please visit
<https://www.siemens.com/cybersecurity-industry>.

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 Cybersecurity RSS Feed under
<https://new.siemens.com/cert>.

Note on firmware/software support

Check regularly for new firmware/software versions or security updates and apply them. After the release of a new version, previous versions are no longer supported and are not maintained.

Decommissioning

Note that personal data such as addresses or passwords might be saved on the computer on which the software is installed.

Decommission the device properly to prevent unauthorized persons from accessing confidential data.

For decommissioning, delete all data from the device. Refer to chapter Decommissioning, dismantling, and disposal (Page 243).

SIMATIC NET glossary

The SIMATIC NET glossary describes terms that may be used in this document.

You will find the SIMATIC NET glossary in the Siemens Industry Online Support at the following address:

Link: (<https://support.industry.siemens.com/cs/ww/en/view/50305045>)

Training, Service & Support

You will find information on training, service and support in the multilanguage document "DC_support_99.pdf" on the Internet pages of Siemens Industry Online Support:

Link: (<https://support.industry.siemens.com/cs/ww/en/view/38652101>)

Security recommendations

2.1 Security recommendations

General information

- Ensure that regular checks are in place to make sure that the system meets the following recommendations and your internal organization's security guidelines.
- Evaluate plant security holistically. Siemens recommendations like Defense-in-Depth and cell protection concept can support you in this regard.
- Check regularly for news on the Siemens Internet pages.
You can find information on Industrial Security here:
Link: (<https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity.html>)
You can find a selection of documentation on the topic of network security here:
Link: (<https://support.industry.siemens.com/cs/ww/en/view/92651441>)
- Keep all SINEC Security Monitor components (SSM Server, SSM Sensors, SSM Agents, SSM Intelligence Database) up to date. Make sure that all components of the SSM intelligence database are up to date and uploaded to the system. Check regularly for security updates and apply them.
Refer to chapter Checking for system updates (Page 223).
- Keep the operating system of all assets up to date. Check regularly for security updates and apply them.
Refer to chapter Checking for system updates (Page 223).
- Install and run antivirus software on your devices.
- Connections over unsecured network areas must be protected by security mechanisms such as VPN.
- SINEC Security Monitor is only intended for connections with trusted networks and should not be connected directly with networks such as the Internet. If a connection to the Internet is required, ensure suitable protection of the system.
- Check authenticity and integrity of files before importing them into SINEC Security Monitor as described in chapter SHA256 checksums (Page 82)
- The integrity of the SINEC Security Monitor installation files can be verified with SHA-256 Secure Hash Algorithm comparing the sha256 of the ISO with the one provided using the following commands:
 - Windows: `certutil -hashfile <file> SHA256`
 - Linux: `sha256sum <file>`
- When decommissioning a SINEC Security Monitor Server or Sensor, delete all files on the hard drive and perform formatting measures with a suitable tool of your choice following the same procedure as for a Linux client decommissioning.

2.1 Security recommendations

- Restrict physical access to all USB interfaces, e.g. by installing the computers locked cabinet or server room with protocolled access and apply principle of least privilege.
- Enable remote access only for authorized personnel and using multi-factor authentication.
- You can find information regarding product innovations, new software versions and security incidents at:
Link (<https://new.siemens.com/global/en/products/services/cert.html?s=SINEC%20Security%20Monitor>)

Recommendations for using the SINEC Security Monitor server

- Always click on the "Log out" button in the Web interface when you have finished working with SINEC Security Monitor.
- Restrict access to SINEC Security Monitor to qualified and authorized personnel and ensure that access rights are updated regularly.
- Use the user and role administration of SINEC Security Monitor to configure the rights of the users according to their authorizations following the principle of least privilege.

Security Advisories

If Siemens detects and eliminates security incidents in the product, a Security Advisory will be published. Respective documents for SINEC Security Monitor can be found at the following site of the Siemens AG:

Link: (<https://new.siemens.com/global/en/products/services/cert.html?s=SINEC%20Security%20Inspector>)

Users, roles and passwords

General recommendations

- Define rules for use of the software.
- Define rules for the creation of passwords.
- Regularly update passwords and keys to increase security.
- Change the user name and default password for a user before you use the software.
- Only use strong passwords. Avoid weak passwords for example "password1", "123456789", "abcdefgh".
- Make sure that all passwords are protected and inaccessible to unauthorized persons.
- Do not use the same password for different users and systems or after it has expired.

Recommendations specific to SINEC Security Monitor

- Create users and roles that are tailored to the scope of authorization required by each user and apply principle of least privilege.
- Use the "super admin role" only when necessary.
- Disable the preset "admin" user after you have created new users with corresponding rights.

User accounts

- Each user must have their own user account. Sharing of user accounts between users is not recommended.
- The user must change the initial password when they log in for the first time.
- A secure password must:
 - Have a length of 8–32 characters.
 - Have at least one of each of the following characters: uppercase letter, lowercase letter, number, special character.
- Each user account must have a role assigned in accordance with their responsibilities on the SINEC Security Monitor System. Applying the principle of least privilege is recommended.
- Adjust access rights for the predefined roles so they match your required rights and restrictions.
- To restrict access to only certain pages combined with read-only permissions, define a new role with respective access rights to the required pages and create a user account in read-only mode with the restricted role assigned.

Certificates

- All connections between SINEC Security Monitor and its interface partners require secure communication based on authentication via certificates.

Secure and non-secure protocols

- Only activate protocols you require for monitoring and administration of the devices.
- If possible, use the most secure variants of protocols, e.g. SNMPv3.
- Some protocols offer both a secure and a non-secure version for communication.
- Only activate protocols that you require to use the system.
- Select the option that is suitable for the planned operating environment. If you use non-secure protocols or services, operate them only within a protected network area.
- Use secure protocols when access is not prevented by physical protection measures.

Restrict and supervise access to hardware

- Electronic devices with an openable housing, which are used for SINEC Security Monitor Servers and SINEC Security Monitor Sensors, must be placed into locked cabinets with door supervision.

2.2 Security functions

User accounts

- Restriction of possible passwords to "strong" passwords with 8-32 characters that contain at least one uppercase letter, lowercase letter, digit & special character.
- Passwords need to be changed on first login.
- Automatic logout of the user from the WBM when not in use for 30 minutes.
- Highly customizable user roles to realize principle of least privilege
- Read-only mode possible
- Access to each Web page can be restricted.
- User can add customized user roles.

Self-monitoring of the system

- OPC UA diagnostic model
- Audit log for system and security logs
- List views for system and security event notifications
- Diagnostics page of the WBM
- Data source diagnostics

Software

- Regular updates for the SINEC Security Monitor Intelligence Database (vulnerabilities, correlation rules and threat intelligence) are provided in regular frequency (typically in a 3 month timeframe).
- Siemens CERT measure plan
- System hardening as part of the installation process

Communication

- Wireguard VPN tool for encrypted communication between SINEC Security Monitor Server, SINEC Security Monitor Sensor
- HTTPS (Hypertext Transfer Protocol Secure): Encrypted communication between operator and WBM
- Only configured data sources communicate with SINEC Security Monitor Server. This includes devices that forward log data via syslog, agents or PCs that are configured for agentless monitoring or input from SINEC Security Monitor Sensors (security events and logs generated by the Sensor based on analysis of mirrored traffic).
- Certificates implemented in SINEC Security Monitor:
 - Communication over TLS protocol with authentication certificates
 - CA certificate

Hardening

- The system is designed to avoid security pitfalls during installation and operation wherever possible
- The installation procedure includes system hardening

Hardware

- Instructions and tools for secure decommissioning

2.3 Intended operational environment

General use of anomaly detection and recommendations are stated in the concept for discrete manufacturing.

Link: (<https://support.industry.siemens.com/cs/ww/en/view/109802750>)

SINEC Security Monitor placed in the operational environment

SINEC Security Monitor is the anomaly detection system provided by Siemens. The picture below shows how SINEC Security Monitor can be integrated in an OT environment with multiple factory segments.

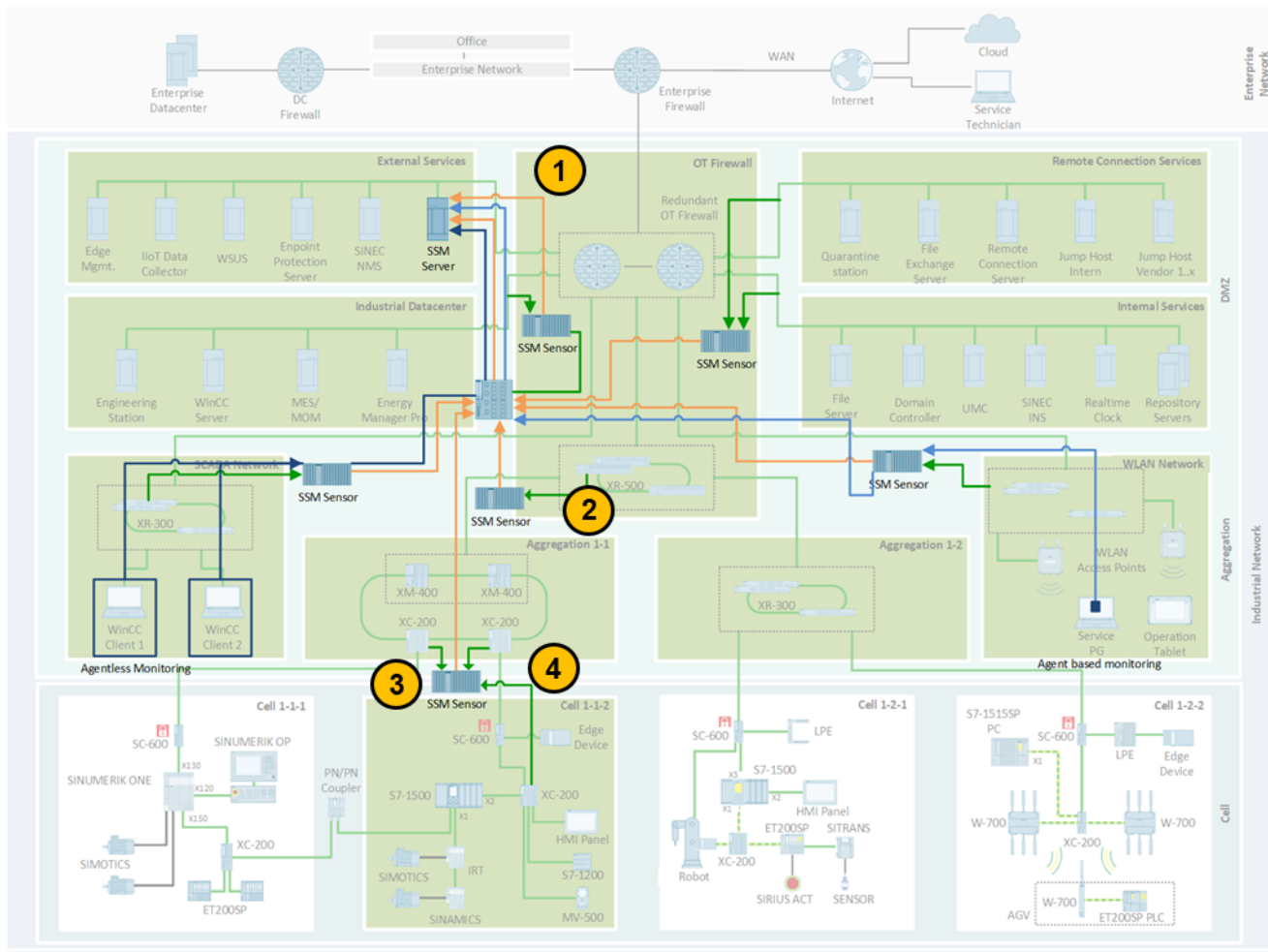
Each relevant segment that should be monitored has to have at least one SINEC Security Monitor Sensor which is connected to the mirror port of a network switch in this segment and analyzes the mirrored network traffic.

The sensor also collects logs from switches and syslogs e.g. from firewalls. The SINEC Security Monitor Sensors send pre-processed collected data to the SINEC Security Monitor Server via a secured "Wireguard" tunnel for further analysis and correlation. In addition, PCs can be monitored using agent-based and agentless monitoring.

In (2), a Microsoft Windows endpoint, e.g. a PC passes on collected logs "agentless" via WMI protocol to the SINEC Security Monitor Sensor. These logs might contain information about installed applications, newly created user accounts, USB usage, etc. In (3) a Microsoft Windows endpoint with the SINEC Security Agent software installed sends collected logs to the SINEC Security Monitor Sensor.

In this scenario, the central aggregation point called SINEC Security Monitor Server is placed in a specific network segment for external services (4).

2.3 Intended operational environment



Item

Description

Green lines

Mirrored network traffic

Orange lines

Monitoring data (Sensor Server Communication)

Dark blue lines

Agent communication

Light blue lines

Agentless communication

Figure 2-1 Integration of SINEC Security Monitor into an OT environment

General approach

The figure highlights the central anomaly detection server placed in the external services network in the Industrial Demilitarized zone (DMZ) as well as the anomaly detection sensors connected in different parts of the automation network. Via a separate network, data from the sensors is transmitted to the central server. As shown in the figure above there are different places where anomaly detection might be implemented:

1. Analyze data traffic via the switches in the DMZ networks
2. Analyze northbound/vertical traffic in automation network, sensors only connected to the central aggregation switches

3. Analyze horizontal communication (machine-to-machine) as well as vertical communication. This requires the use of distributed sensors in all network segments that should be monitored e.g. switches in production cells.
4. Get asset inventory of machines by use of anomaly detection and analyze machine internal communication (in addition to northbound and machine-to-machine communication)

2.4 Communication ports

The following tables provide an overview of the ports used.

- **Protocol / Function**
Supported protocols and functions
- **Protocol / Port number**
Protocol of the transport layer and assigned port number
- **Port status**
 - Closed
The port is closed by default.
 - Open
The port is always open and cannot be closed.
 - Open after configuration
The port is open if it has been configured.
 - Open with login
The port is opening at login to the service.
- **Authentication**
Specifies whether the protocol authenticates the communication partner during access.
- **Encryption**
Specifies whether the transfer is encrypted.

Table 2-1 Ports of the Server

Protocol / Function	Protocol / Port number	Port status	Authentication	Encryption
Gateway Service	TCP / 8443	Open with login	Yes	Yes
Wireguard Service	UDP / 5046	Open with login	Yes	Yes
Collector Service	TCP / 9000	Open with login	Yes	Yes
Syslog-ng Service	TCP / 514	Open after configuration	Yes	Yes
Syslog-ng Service	UDP / 514	Open after configuration	No	No
Logstash Service	TCP / 5046	Open	Yes	Yes
DNS Client	UDP / 53	Closed	No	No
SMTP Client	TCP / 25	Closed	Yes	No
NTP Client	UDP / 123	Closed	No	No

2.4 Communication ports

Protocol / Function	Protocol / Port number	Port status	Authentication	Encryption
Syslog Client	TCP / 514	Closed	No	No
Syslog Client	UDP / 514	Closed	No	No
OPC UA Service	TCP / 4840	Open with login	Yes	No
Syslog-ng Service	TCP / 6514	Open after configuration	Yes	Yes
Syslog-ng Service	UDP / 6514	Open after configuration	No	No

Table 2-2 Ports of the Sensor

Protocol / Function	Protocol / Port number	Port status	Authentication	Encryption
Syslog-ng Service	UDP / 514	Open	No	No
Syslog-ng Service	TCP / 514	Open	Yes	Yes
Syslog-ng Service	UDP / 6514	Open	No	No
Syslog-ng Service	TCP / 6514	Open	Yes	Yes
SNMP Client	UDP / 161	Closed	Version 1: No Version 3: Yes	No
S7comm Client	TCP / 102	Closed	No	No
WMI Client	TCP / 135	Closed	Yes	Yes
DNS Client	TCP / 53	Closed	No	No
NetBIOS Client	UDP / 137	Closed	No	No
Wireguard Client	UDP / 9000	Open	Yes	Yes
OPC UA Service	TCP / 4840	Open with login	Yes	No
NTP Client	UDP / 123	Closed	No	No
WinRM Client	HTTPS / 5986	Closed	Yes	Yes

Table 2-3 Ports of the Agent

Protocol / Function	Protocol / Port number	Port status	Authentication	Encryption
HTTPS Client	TCP / 9000	Open	Yes	Yes
BEATS Client	TCP / 5046	Open	Yes	Yes
WMI Service	TCP / 135	Open	Yes	No
WinRM Service	TCP / 5986	Open	Yes	Yes

The following tables provide information about traffic direction and port usage:

Table 2-4 Service ports used by the SINEC Security Monitor Server (standard)

Service	Port	Direction	From / to	Protocol	Usage
Gateway Service	8443	In-bound	Web browser of clients	TCP	Access SSM Web UI via HTTPS
NTP Service	123	Out-bound	NTP clients of the SINEC Security Monitor Server / third-party NTP server	UDP	Sync time with specific NTP server

Service	Port	Direction	From / to	Protocol	Usage
Wireguard Service	5046	In-bound	Wireguard client in the SINEC Security Monitor Sensor / Wireguard server in the SINEC Security Monitor Server	UDP	Communication between SINEC Security Monitor Server and SINEC Security Monitor Sensor
Collector Service	9000	In-bound	SINEC Security Monitor Agent / SINEC Security Monitor Server SINEC Security Monitor Sensor / SINEC Security Monitor Server	TCP	Direct registration communication of the SINEC Security Monitor Agent with the SINEC Security Monitor Server SINEC Security Monitor Sensor license activation SINEC Security Monitor Sensor certificate distribution
Logstash Service	5046	In-bound	SINEC Security Monitor Agent / logstash	TCP	Direct forwarding of Microsoft Windows logs to the SINEC Security Monitor Server
Gateway Service	-	Out-bound	SINEC Security Monitor Server / backup server	TCP	The SINEC Security Monitor System backs up raw logs, security data and system configuration to a remote backup server. This port is available only if a backup server is configured.
Logstash Service	-	Out-bound	SINEC Security Monitor Server / third-party syslog server	TCP	Transit of raw logs or security events to a third-party syslog server
Logstash Service	-	Out-bound	SINEC Security Monitor Server / third-party syslog server	UDP	Transit of raw logs or security events to a third-party syslog server
Gateway Service	-	Out-bound	SINEC Security Monitor Server / email server	TCP	Security event or system alarm notifications via email service
Zeek Service	-	In-bound	Mirror port	-	Mirror network traffic from switch to Zeek service
Suricata Service	-	In-bound	Mirror port	-	Mirror network traffic from switch to Suricata service
OPC UA Service	4840	In-bound	Diagnostics API / OPC UA server	TCP	The SINEC Security Monitor application calls the diagnostics API to read and write data to an OPC UA server

Table 2-5 Customizable service ports used by the SINEC Security Monitor Server

Service	Port	Direction	From / to	Protocol	Usage
Syslog-ng	514	In-bound	Endpoints / SINEC Security Monitor Server	TCP/UDP	SINEC Security Monitor Server receives syslog files from endpoints
Syslog-ng	6514	In-bound	Endpoints / SINEC Security Monitor Server	TCP/UDP	SINEC Security Monitor Server receives syslog files from endpoints

Any additional ports added and enabled by the user.

2.4 Communication ports

Table 2-6 Service ports used by the SINEC Security Monitor Sensor

Service	Port	Direction	From / to	Protocol	Usage
NTP Service	123	Out-bound	NTP clients of the SINEC Security Monitor Sensor / third-party NTP server	UDP	Sync time with specific NTP server
Wireguard Service	5046	Out-bound	Wireguard Service in the SINEC Security Monitor System	TCP/UDP	SINEC Security Monitor Sensor license activation and SINEC Security Monitor Sensor certificate distribution Communication between the SINEC Security Monitor System and SINEC Security Monitor Sensor
Zeek Service	-	In-bound	Mirror port	-	Mirror network traffic from switch to Zeek service
Suricata Service	-	In-bound	Mirror port	-	Mirror network traffic from switch to Suricata service
Prober Service	-	Out-bound	Siemens PLC	S7comm	Probing Siemens PLC
Prober Service	-	Out-bound	Assets supporting PN-DCP	PN-DCP	Probing assets that support PN-DCP
Prober Service	-	Out-bound	Assets supporting SNMP	SNMP	Probing assets that support SNMP
Prober Service	-	Out-bound	Assets supporting ICMP	ICMP	Probing assets that support ICMP
WMI Service	135	Out-bound	SINEC Security Monitor Sensor / clients	TCP	Collection of Microsoft Windows system information, account information and application information
WinRM Service	5986	Out-bound	SINEC Security Monitor Sensor / clients	TCP	Collection of Microsoft Windows system information, account information and application information
OPC UA Service	4840	In-bound	Diagnostics API / OPC UA server	TCP	The SINEC Security Monitor application calls the diagnostics API to read and write data to an OPC UA server
Syslog-ng	514	In-bound	Endpoints / SINEC Security Monitor Sensor	TCP/UDP	SINEC Security Monitor Sensor receives syslog files from endpoints
Syslog-ng	6514	In-bound	Endpoints / SINEC Security Monitor Sensor	TCP/UDP	SINEC Security Monitor Sensor receives syslog files from endpoints

Table 2-7 Service ports used by the SINEC Security Monitor Agent

Service	Port	Direction	From / to	Protocol	Usage
LogAgent Service	9000	Out-bound	SINEC Security Monitor Sensor / SINEC Security Monitor System	TCP	The SINEC Security Monitor Agent sends registration and heartbeat requests to the SINEC Security Monitor Sensor or SINEC Security Monitor System
Beats Service	5046	Out-bound	SINEC Security Monitor Sensor / SINEC Security Monitor System	TCP	The SINEC Security Monitor Agent sends acquired data from endpoints to the SINEC Security Monitor Sensor or SINEC Security Monitor System

Service	Port	Direction	From / to	Protocol	Usage
WMI Service	135	In-bound	SINEC Security Monitor Sensor / SINEC Security Monitor Agent	TCP	Log collection of Microsoft Windows clients through WMI service
WinRM Service	5986	In-bound	SINEC Security Monitor Sensor / clients	TCP	Log collection of Microsoft Windows clients through WinRM service

2.5 Ciphers used

The following data is specified in the tables:

- **Category**
Authentication/encryption method, protocol version or cipher suite
- **Name**
Name of the category according to IANA
You can find an overview of the TLS parameters and cipher suites on the following page:
Link: (<https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml#tls-parameters-4>)
- **Value (hex)**
Value (hexadecimal) of the suite according to IANA
- **Enabled by default**
Parameters are Y (Yes) and N (No)
- **Security grade**
Refer to table "Security grades to rate cryptographic algorithms" in chapter Preparing and adding a Microsoft Windows computer for agentless security log collection (Page 160)
- **SSL/TLS protocols**
The mapping of protocol versions to security grades is as follows:

Table 2-8 Supported TLS protocol versions

Security grade	Protocol version	Comments
5	TLSv1.3	Current best practice
5	TLSv1.2	Previous best practice, supported by majority of web servers

Server

Table 2-9 HTTPS (TCP / 8443) Server

Category	Name	Value (hex)	Enabled by default	Security grade
Cipher suite	TLS_ECDHE_ECD-SA_WITH_AES_256_GCM_SHA384	0xc02c	Y	5
Cipher suite	TLS_ECDHE_ECDSA_WITH_CHA20_POLY1305_SHA256	0xc030	Y	5

2.5 Ciphers used

Category	Name	Value (hex)	Enabled by default	Security grade
Cipher suite	TLS_AES_256_GCM_SHA384	0x1302	Y	5
Cipher suite	TLS_CHACHA20_POLY1305_SHA256	0x1303	Y	5
Cipher suite	TLS_AES_128_GCM_SHA256	0x1301	Y	5
Cipher suite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	0xc030	Y	5
Cipher suite	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	0xcca8	Y	5
Cipher suite	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	0xc02f	Y	5
Cipher suite	TLS_AES_256_GCM_SHA384	0x1302	Y	5
Cipher suite	TLS_CHACHA20_POLY1305_SHA256	0x1303	Y	5
Cipher suite	TLS_AES_128_GCM_SHA256	0x1301	Y	5
Key exchange	ECDH >= 250 Bit	.	Y	5
Key exchange	DH, RSA >= 3000 Bit	.	Y	5
Named group	secp256r1 (prime256v1)	0x0017	Y	5
Named group	secp384r1	0x0018	Y	5
Named group	secp521r1	0x0019	Y	5
Named group	X25519	0x001d	Y	5
Named group	X448	0x001e	Y	5
Named group	ffdhe3072	0x0101	Y	5
Named group	-	0x0102	Y	0
Named group	-	0x0103	Y	0
Named group	-	0x0104	Y	0
Named group	secp256r1 (prime256v1)	0x0017	Y	5
Named group	secp384r1	0x0018	Y	5
Named group	secp521r1	0x0019	Y	5
Named group	X25519	0x001d	Y	5
Named group	X448	0x001e	Y	5
Named group	ffdhe3072	0x0101	Y	5
Named group	-	0x0102	Y	0
Named group	-	0x0103	Y	0
Named group	-	0x0104	Y	0
Protocol version	TLSv1.2	.	Y	5
Protocol version	TLSv1.3	.	Y	5
Protocol version	TLSv1.2	.	Y	5
Protocol version	TLSv1.3	.	Y	5
Signature	sha256+ecdsa	0x0403	Y	5
Signature	sha384+ecdsa	0x0503	Y	5
Signature	sha256+rsa	0x0401	Y	5
Signature	sha384+rsa	0x0501	Y	5
Signature	sha512+rsa	0x0601	Y	5
Signature	sha256+rsaepss	0x0804	Y	5
Signature	sha384+rsaepss	0x0805	Y	5
Signature	sha512+rsaepss	0x0806	Y	5

Logstash for Beats (TCP / 5046) Server

Category	Name	Value (hex)	Enabled by default	Security grade
Cipher suite	TLS_ECDHE_ECD-SA_WITH_AES_256_GCM_SHA384	0xc02c	Y	5
Cipher suite	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	0xc0a9	Y	5
Cipher suite	TLS_ECDHE_ECD-SA_WITH_AES_128_GCM_SHA256	0xc02b	Y	5
Cipher suite	TLS_AES_256_GCM_SHA384	0x1302	Y	5
Cipher suite	TLS_CHACHA20_POLY1305_SHA256	0x1303	Y	5
Cipher suite	TLS_AES_128_GCM_SHA256	0x1301	Y	5
Cipher suite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	0xc030	Y	5
Cipher suite	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	0xc02f	Y	5
Cipher suite	TLS_AES_256_GCM_SHA384	0x1302	Y	5
Cipher suite	TLS_CHACHA20_POLY1305_SHA256	0x1303	Y	5
Cipher suite	TLS_AES_128_GCM_SHA256	0x1301	Y	5
Key exchange	ECDH >= 250 Bit	.	Y	5
Key exchange	DH, RSA >= 3000 Bit	.	Y	5
Named group	secp256r1 (prime256v1)	0x0017	Y	5
Named group	secp384r1	0x0018	Y	5
Named group	secp521r1	0x0019	Y	5
Named group	X25519	0x001d	Y	5
Named group	X448	0x001e	Y	5
Named group	ffdhe3072	0x0101	Y	5
Named group	-	0x0102	Y	0
Named group	-	0x0103	Y	0
Named group	-	0x0104	Y	0
Named group	secp256r1 (prime256v1)	0x0017	Y	5
Named group	secp384r1	0x0018	Y	5
Named group	secp521r1	0x0019	Y	5
Named group	X25519	0x001d	Y	5
Named group	X448	0x001e	Y	5
Named group	ffdhe3072	0x0101	Y	5
Named group	-	0x0102	Y	0
Named group	-	0x0103	Y	0
Named group	-	0x0104	Y	0
Protocol version	TLSv1.2	.	Y	5
Protocol version	TLSv1.3	.	Y	5
Protocol version	TLSv1.2	.	Y	5
Protocol version	TLSv1.3	.	Y	5
Signature	sha256+ecdsa	0x0403	Y	5

2.5 Ciphers used

Category	Name	Value (hex)	Enabled by default	Security grade
Signature	sha384+ecdsa	0x0503	Y	5
Signature	sha256+rsa	0x0401	Y	5
Signature	sha384+rsa	0x0501	Y	5
Signature	sha512+rsa	0x0601	Y	5
Signature	sha256+rsaepss	0x0804	Y	5
Signature	sha384+rsaepss	0x0805	Y	5
Signature	sha512+rsaepss	0x0806	Y	5

Table 2-10 Syslog-ng (TCP / 6514) Server

Category	Name	Value (hex)	Enabled by default	Security grade
Cipher suite	TLS_ECDHE_ECD-SA_WITH_AES_256_GCM_SHA384	0xc02c	Y	5
Cipher suite	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	0xc0a9	Y	5
Cipher suite	TLS_ECDHE_ECD-SA_WITH_AES_128_GCM_SHA256	0xc02b	Y	5
Cipher suite	TLS_AES_256_GCM_SHA384	0x1302	Y	5
Cipher suite	TLS_CHACHA20_POLY1305_SHA256	0x1303	Y	5
Cipher suite	TLS_AES_128_GCM_SHA256	0x1301	Y	5
Cipher suite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	0xc030	Y	5
Cipher suite	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	0x009f	Y	5
Cipher suite	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	0xc02f	Y	5
Cipher suite	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	0x009e	Y	5
Cipher suite	TLS_AES_256_GCM_SHA384	0x1302	Y	5
Cipher suite	TLS_CHACHA20_POLY1305_SHA256	0x1303	Y	5
Cipher suite	TLS_AES_128_GCM_SHA256	0x1301	Y	5
Key exchange	ECDH >= 250 Bit	.	Y	5
Key exchange	DH, RSA >= 3000 Bit	.	Y	5
Named group	secp256r1 (prime256v1)	0x0017	Y	5
Named group	secp384r1	0x0018	Y	5
Named group	secp521r1	0x0019	Y	5
Named group	secp256r1 (prime256v1)	0x0017	Y	5
Named group	secp384r1	0x0018	Y	5
Named group	secp521r1	0x0019	Y	5
Named group	X25519	0x001d	Y	5
Named group	X448	0x001e	Y	5
Protocol version	TLSv1.2	.	Y	5
Protocol version	TLSv1.3	.	Y	5
Protocol version	TLSv1.2	.	Y	5
Protocol version	TLSv1.3	.	Y	5

Category	Name	Value (hex)	Enabled by default	Security grade
Signature	sha256+ecdsa	0x0403	Y	5
Signature	sha256+ecdsa	0x0403	Y	5
Signature	sha384+ecdsa	0x0503	Y	5
Signature	sha512+ecdsa	0x0603	Y	5
Signature	sha384+ecdsa	0x0503	Y	5
Signature	sha256+rsa	0x0401	Y	5
Signature	sha256+rsa	0x0401	Y	5
Signature	sha384+rsa	0x0501	Y	5
Signature	sha512+rsa	0x0601	Y	5
Signature	sha256+rsaepss	0x0804	Y	5
Signature	sha384+rsaepss	0x0805	Y	5
Signature	sha512+rsaepss	0x0806	Y	5
Signature	sha256+rsaepss	0x0804	Y	5
Signature	sha384+rsaepss	0x0805	Y	5
Signature	sha512+rsaepss	0x0806	Y	5

Table 2-11 Logstash for Syslog-ng (TCP / 8514) Server

Category	Name	Value (hex)	Enabled by default	Security grade
Cipher suite	TLS_ECDHE_ECD-SA_WITH_AES_256_GCM_SHA384	0xc02c	Y	5
Cipher suite	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	0xc0a9	Y	5
Cipher suite	TLS_ECDHE_ECD-SA_WITH_AES_128_GCM_SHA256	0xc02b	Y	5
Cipher suite	TLS_AES_256_GCM_SHA384	0x1302	Y	5
Cipher suite	TLS_CHACHA20_POLY1305_SHA256	0x1303	Y	5
Cipher suite	TLS_AES_128_GCM_SHA256	0x1301	Y	5
Cipher suite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	0xc030	Y	5
Cipher suite	TLS_AES_256_GCM_SHA384	0x1302	Y	5
Cipher suite	TLS_CHACHA20_POLY1305_SHA256	0x1303	Y	5
Cipher suite	TLS_AES_128_GCM_SHA256	0x1301	Y	5
Key exchange	ECDH >= 250 Bit	.	Y	5
Key exchange	DH, RSA >= 3000 Bit	.	Y	5
Named group	secp256r1 (prime256v1)	0x0017	Y	5
Named group	secp384r1	0x0018	Y	5
Named group	secp521r1	0x0019	Y	5
Named group	X25519	0x001d	Y	5
Named group	X448	0x001e	Y	5
Named group	ffdhe3072	0x0101	Y	5
Named group	-	0x0102	Y	0

2.5 Ciphers used

Category	Name	Value (hex)	Enabled by default	Security grade
Named group	-	0x0103	Y	0
Named group	-	0x0104	Y	0
Named group	secp256r1 (prime256v1)	0x0017	Y	5
Named group	secp384r1	0x0018	Y	5
Named group	secp521r1	0x0019	Y	5
Named group	X25519	0x001d	Y	5
Named group	X448	0x001e	Y	5
Named group	ffdhe3072	0x0101	Y	5
Named group	-	0x0102	Y	0
Named group	-	0x0103	Y	0
Named group	-	0x0104	Y	0
Protocol version	TLSv1.2	.	Y	5
Protocol version	TLSv1.3	.	Y	5
Protocol version	TLSv1.2	.	Y	5
Protocol version	TLSv1.3	.	Y	5
Signature	sha256+ecdsa	0x0403	Y	5
Signature	sha384+ecdsa	0x0503	Y	5
Signature	sha256+rsa	0x0401	Y	5
Signature	sha384+rsa	0x0501	Y	5
Signature	sha512+rsa	0x0601	Y	5
Signature	sha256+rsaepss	0x0804	Y	5
Signature	sha384+rsaepss	0x0805	Y	5
Signature	sha512+rsaepss	0x0806	Y	5

Table 2-12 Collector Service (TCP / 9000) Server

Category	Name	Value (hex)	Enabled by default	Security grade
Cipher suite	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	0xc02c	Y	5
Cipher suite	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	0xcca9	Y	5
Cipher suite	TLS_AES_256_GCM_SHA384	0x1302	Y	5
Cipher suite	TLS_CHACHA20_POLY1305_SHA256	0x1303	Y	5
Cipher suite	TLS_AES_128_GCM_SHA256	0x1301	Y	5
Cipher suite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	0xc030	Y	5
Cipher suite	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	0xcca8	Y	5
Cipher suite	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	0xc02f	Y	5
Cipher suite	TLS_AES_256_GCM_SHA384	0x1302	Y	5
Cipher suite	TLS_CHACHA20_POLY1305_SHA256	0x1303	Y	5
Cipher suite	TLS_AES_128_GCM_SHA256	0x1301	Y	5

Category	Name	Value (hex)	Enabled by default	Security grade
Key exchange	ECDH >= 250 Bit	.	Y	5
Key exchange	DH, RSA >= 3000 Bit	.	Y	5
Named group	secp256r1 (prime256v1)	0x0017	Y	5
Named group	secp384r1	0x0018	Y	5
Named group	secp521r1	0x0019	Y	5
Named group	X25519	0x001d	Y	5
Named group	X448	0x001e	Y	5
Named group	ffdhe3072	0x0101	Y	5
Named group	-	0x0102	Y	0
Named group	-	0x0103	Y	0
Named group	-	0x0104	Y	0
Named group	secp256r1 (prime256v1)	0x0017	Y	5
Named group	secp384r1	0x0018	Y	5
Named group	secp521r1	0x0019	Y	5
Named group	X25519	0x001d	Y	5
Named group	X448	0x001e	Y	5
Named group	ffdhe3072	0x0101	Y	5
Named group	-	0x0102	Y	0
Named group	-	0x0103	Y	0
Named group	-	0x0104	Y	0
Protocol version	TLSv1.2	.	Y	5
Protocol version	TLSv1.3	.	Y	5
Protocol version	TLSv1.2	.	Y	5
Protocol version	TLSv1.3	.	Y	5
Signature	sha256+ecdsa	0x0403	Y	5
Signature	sha384+ecdsa	0x0503	Y	5
Signature	sha384+ecdsa	0x0503	Y	5
Signature	sha256+rsa	0x0401	Y	5
Signature	sha256+rsa	0x0401	Y	5
Signature	sha384+rsa	0x0501	Y	5
Signature	sha512+rsa	0x0601	Y	5
Signature	sha256+rsaepss	0x0804	Y	5
Signature	sha384+rsaepss	0x0805	Y	5
Signature	sha512+rsaepss	0x0806	Y	5
Signature	sha256+rsaepss	0x0804	Y	5
Signature	sha384+rsaepss	0x0805	Y	5
Signature	sha512+rsaepss	0x0806	Y	5

2.5 Ciphers used

Table 2-13 Logforwarding (TCP / 6514) Client

Category	Name	Value (hex)	Enabled by default	Security grade
Cipher suite	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	0x00a2	Y	n/a
Cipher suite	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	0xc027	Y	n/a
Cipher suite	TLS_ECDHE_ECD- SA_WITH_AES_128_CBC_SHA256	0xc023	Y	n/a
Cipher suite	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	0xc013	Y	n/a
Cipher suite	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	0xc009	Y	n/a
Cipher suite	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	0xc028	Y	n/a
Cipher suite	TLS_ECDHE_ECD- SA_WITH_AES_256_CBC_SHA384	0xc024	Y	n/a
Cipher suite	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	0xc014	Y	n/a
Cipher suite	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	0xc00a	Y	n/a
Cipher suite	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	0x0067	Y	n/a
Cipher suite	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	0x0033	Y	n/a
Cipher suite	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	0x0040	Y	n/a
Cipher suite	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	0x006b	Y	n/a
Cipher suite	TLS_DHE_DSS_WITH_AES_256_CBC_SHA	0x0038	Y	n/a
Cipher suite	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	0x0039	Y	n/a
Cipher suite	TLS_RSA_WITH_AES_128_GCM_SHA256	0x009c	Y	n/a
Cipher suite	TLS_RSA_WITH_AES_256_GCM_SHA384	0x009d	Y	n/a
Cipher suite	TLS_RSA_WITH_AES_128_CBC_SHA256	0x003c	Y	n/a
Cipher suite	TLS_RSA_WITH_AES_256_CBC_SHA256	0x003d	Y	n/a
Cipher suite	TLS_RSA_WITH_AES_128_CBC_SHA	0x002f	Y	n/a
Cipher suite	TLS_RSA_WITH_AES_256_CBC_SHA	0x0035	Y	n/a
Cipher suite	TLS_AES_256_GCM_SHA384	0x1302	Y	n/a
Cipher suite	TLS_AES_128_GCM_SHA256	0x1301	Y	n/a
Cipher suite	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	0x009f	Y	n/a
Cipher suite	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384	0x00a3	Y	n/a
Cipher suite	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	0x006a	Y	n/a
Cipher suite	TLS_ECDH_ECD- SA_WITH_AES_256_GCM_SHA384	0xc02e	Y	n/a
Cipher suite	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384	0xc032	Y	n/a
Cipher suite	TLS_ECDH_ECD- SA_WITH_AES_128_GCM_SHA256	0xc02d	Y	n/a
Cipher suite	TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256	0xc031	Y	n/a
Cipher suite	TLS_ECDH_ECD- SA_WITH_AES_256_CBC_SHA384	0xc026	Y	n/a
Cipher suite	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384	0xc02a	Y	n/a
Cipher suite	TLS_ECDH_ECD- SA_WITH_AES_128_CBC_SHA256	0xc025	Y	n/a
Cipher suite	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256	0xc029	Y	n/a

Category	Name	Value (hex)	Enabled by default	Security grade
Cipher suite	TLS_DHE_DSS_WITH_AES_128_CBC_SHA	0x0032	Y	n/a
Cipher suite	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	0xc005	Y	n/a
Cipher suite	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	0xc00f	Y	n/a
Cipher suite	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	0xc004	Y	n/a
Cipher suite	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	0xc00e	Y	n/a
Named group	X25519	0x001d	Y	n/a
Named group	secp256r1 (prime256v1)	0x0017	Y	n/a
Named group	secp384r1	0x0018	Y	n/a
Named group	secp521r1	0x0019	Y	n/a
Named group	X448	0x001e	Y	n/a
Named group	ffdhe2048	0x0100	Y	n/a
Named group	ffdhe3072	0x0101	Y	n/a
Named group	.	0x0102	Y	n/a
Named group	.	0x0103	Y	n/a
Named group	.	0x0104	Y	n/a
Protocol version	TLSv1.3	–	Y	n/a
Protocol version	TLSv1.2	–	Y	n/a
Signature	sha256+ecdsa	0x0403	Y	n/a
Signature	sha384+ecdsa	0x0503	Y	n/a
Signature	sha512+ecdsa	0x0603	Y	n/a
Signature	ed25519	0x0807	Y	n/a
Signature	ed448	0x0808	Y	n/a
Signature	sha256+rsaepss	0x0804	Y	n/a
Signature	sha384+rsaepss	0x0805	Y	n/a
Signature	sha512+rsaepss	0x0806	Y	n/a
Signature	sha256+rsapss	0x0809	Y	n/a
Signature	sha384+rsapss	0x080a	Y	n/a
Signature	sha512+rsapss	0x080b	Y	n/a
Signature	sha256+rsa	0x0401	Y	n/a
Signature	sha384+rsa	0x0501	Y	n/a
Signature	sha512+rsa	0x0601	Y	n/a
Signature	sha256+dsa	0x0402	Y	n/a
Signature	sha224+ecdsa	0x0303	Y	n/a
Signature	sha224+rsa	0x0301	Y	n/a
Signature	sha224+dsa	0x0302	Y	n/a
Signature	sha1+ecdsa	0x0203	Y	n/a
Signature	sha1+rsa	0x0201	Y	n/a
Signature	sha1+dsa	0x0202	Y	n/a

2.5 Ciphers used

Table 2-14 SMTP (TCP / 25) Client

Category	Name	Value (hex)	Enabled by default	Security grade
Cipher suite	TLS_ECDHE_ECD-SA_WITH_AES_256_GCM_SHA384	0xc02c	Y	5
Cipher suite	TLS_ECDHE_ECD-SA_WITH_AES_128_GCM_SHA256	0xc02b	Y	5
Cipher suite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	0xc030	Y	5
Cipher suite	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	0x009f	Y	5
Cipher suite	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384	0x00a3	Y	5
Cipher suite	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	0xc02f	Y	5
Cipher suite	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	0x009e	Y	5
Cipher suite	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	0x00a2	Y	5
Cipher suite	TLS_AES_256_GCM_SHA384	0x1302	Y	5
Cipher suite	TLS_AES_128_GCM_SHA256	0x1301	Y	5
Cipher suite	TLS_CHACHA20_POLY1305_SHA256	0x1303	Y	5
Named group	X25519	0x001d	Y	5
Named group	secp256r1 (prime256v1)	0x0017	Y	5
Named group	secp384r1	0x0018	Y	5
Named group	secp521r1	0x0019	Y	5
Named group	X448	0x001e	Y	5
Named group	ffdhe3072	0x0101	Y	5
Named group	-	0x0102	Y	0
Named group	-	0x0103	Y	0
Named group	-	0x0104	Y	0
Protocol version	TLSv1.3	.	Y	5
Protocol version	TLSv1.2	.	Y	5
Signature	sha256+ecdsa	0x0403	Y	5
Signature	sha384+ecdsa	0x0503	Y	5
Signature	sha512+ecdsa	0x0603	Y	5
Signature	ed25519	0x0807	Y	5
Signature	ed448	0x0808	Y	5
Signature	sha256+rsaepss	0x0804	Y	5
Signature	sha384+rsaepss	0x0805	Y	5
Signature	sha512+rsaepss	0x0806	Y	5
Signature	sha256+rsapss	0x0809	Y	5
Signature	sha384+rsapss	0x080a	Y	5
Signature	sha512+rsapss	0x080b	Y	5
Signature	sha256+rsa	0x0401	Y	5
Signature	sha384+rsa	0x0501	Y	5
Signature	sha512+rsa	0x0601	Y	5
Signature	sha256+dsa	0x0402	Y	5

Table 2-15 SSH (TCP / 22) Server

Category	Name	Value (hex)	Enabled by default	Security grade
Ciphers for encryption (enc)	aes128-ctr	n/a	Y	4
Ciphers for encryption (enc)	aes192-ctr	n/a	Y	4
Ciphers for encryption (enc)	aes256-ctr	n/a	Y	4
Host key (key)	ecdsa-sha2-nistp256	n/a	Y	4
Host key (key)	ssh-ed25519	n/a	Y	4
Key exchange (kex)	curve25519-sha256	n/a	Y	4
Key exchange (kex)	ecdh-sha2-nistp256	n/a	Y	4
Key exchange (kex)	ecdh-sha2-nistp384	n/a	Y	4
Key exchange (kex)	ecdh-sha2-nistp521	n/a	Y	4
Key length	ECDH >= 250 Bit	n/a	Y	5
MAC	umac-128-etm@openssh.com	n/a	Y	4
MAC	hmac-sha2-256-etm@openssh.com	n/a	Y	4
MAC	hmac-sha2-512-etm@openssh.com	n/a	Y	4
Protocol version	SSHv2.0	n/a	Y	5

Table 2-16 SSH (TCP / 2222) Client

Category	Name	Value (hex)	Enabled by default	Security grade
Ciphers for encryption (enc)	aes128-ctr	n/a	Y	4
Ciphers for encryption (enc)	aes192-ctr	n/a	Y	4
Ciphers for encryption (enc)	aes256-ctr	n/a	Y	4
Host key (key)	ecdsa-sha2-nistp256-cert-v01@openssh.com	n/a	Y	4
Host key (key)	ecdsa-sha2-nistp384-cert-v01@openssh.com	n/a	Y	4
Host key (key)	ecdsa-sha2-nistp521-cert-v01@openssh.com	n/a	Y	4
Host key (key)	-	n/a	Y	0
Host key (key)	ssh-ed25519-cert-v01@openssh.com	n/a	Y	4
Host key (key)	ecdsa-sha2-nistp256	n/a	Y	4
Host key (key)	ecdsa-sha2-nistp384	n/a	Y	4
Host key (key)	ecdsa-sha2-nistp521	n/a	Y	4
Host key (key)	-	n/a	Y	0
Host key (key)	ssh-ed25519	n/a	Y	4
Host key (key)	-	n/a	Y	0

2.5 Ciphers used

Category	Name	Value (hex)	Enabled by default	Security grade
Host key (key)	-	n/a	Y	0
Key exchange (kex)	curve25519-sha256	n/a	Y	4
Key exchange (kex)	ecdh-sha2-nistp256	n/a	Y	4
Key exchange (kex)	ecdh-sha2-nistp384	n/a	Y	4
Key exchange (kex)	ecdh-sha2-nistp521	n/a	Y	4
Key length	ECDH >= 250 Bit	n/a	Y	5
MAC	umac-128-etm@openssh.com	n/a	Y	4
MAC	hmac-sha2-256-etm@openssh.com	n/a	Y	4
MAC	hmac-sha2-512-etm@openssh.com	n/a	Y	4
Protocol version	SSHv2.0	n/a	Y	5

Table 2-17 SNMP Client

Category	Name	Value (hex)	Enabled by default	Security grade
Authentication	HMAC-MD5-96	n/a	Y	0
Authentication	HMAC-SHA-96	n/a	Y	3
Encryption	des-cbc	n/a	Y	3

Sensor

Table 2-18 WinRMBeat (HTTPS / 5986) Client

Category	Name	Value (hex)	Enabled by default	Security grade
Cipher suite	TLS_ECDHE_ECD-SA_WITH_AES_128_GCM_SHA256	0xc02b	Y	5
Cipher suite	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	0xc02f	Y	5
Cipher suite	TLS_ECDHE_ECD-SA_WITH_AES_256_GCM_SHA384	0xc02c	Y	5
Cipher suite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	0xc030	Y	5
Cipher suite	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	0xcca9	Y	5
Cipher suite	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	0xcca8	Y	5
Cipher suite	TLS_AES_128_GCM_SHA256	0x1301	Y	5
Cipher suite	TLS_AES_256_GCM_SHA384	0x1302	Y	5
Cipher suite	TLS_CHACHA20_POLY1305_SHA256	0x1303	Y	5
Named group	X25519	0x001d	Y	5
Named group	secp256r1 (prime256v1)	0x0017	Y	5
Named group	secp384r1	0x0018	Y	5

Category	Name	Value (hex)	Enabled by default	Security grade
Named group	secp521r1	0x0019	Y	5
Protocol version	TLSv1.2	-	Y	5
Protocol version	TLSv1.3	-	Y	5
Signature	sha256+rsaepss	0x0804	Y	5
Signature	sha256+ecdsa	0x0403	Y	5
Signature	ed25519	0x0807	Y	5
Signature	sha384+rsaepss	0x0805	Y	5
Signature	sha512+rsaepss	0x0806	Y	5
Signature	sha256+rsa	0x0401	Y	5
Signature	sha384+rsa	0x0501	Y	5
Signature	sha512+rsa	0x0601	Y	5
Signature	sha384+ecdsa	0x0503	Y	5
Signature	sha512+ecdsa	0x0603	Y	5
Signature	sha1+rsa	0x0201	Y	1
Signature	sha1+ecdsa	0x0203	Y	1

Table 2-19 SSH Server

Category	Name	Value (hex)	Enabled by default	Security grade
Ciphers for encryption (enc)	aes128-ctr	n/a	Y	4
Ciphers for encryption (enc)	aes192-ctr	n/a	Y	4
Ciphers for encryption (enc)	aes256-ctr	n/a	Y	4
Host key (key)	ecdsa-sha2-nistp256	n/a	Y	4
Host key (key)	ssh-ed25519	n/a	Y	4
Key exchange (kex)	curve25519-sha256	n/a	Y	4
Key exchange (kex)	ecdh-sha2-nistp256	n/a	Y	4
Key exchange (kex)	ecdh-sha2-nistp384	n/a	Y	4
Key exchange (kex)	ecdh-sha2-nistp521	n/a	Y	4
Key length	ECDH >= 250 Bit	n/a	Y	5
MAC	umac-128-etm@openssh.com	n/a	Y	4
MAC	hmac-sha2-256-etm@openssh.com	n/a	Y	4
MAC	hmac-sha2-512-etm@openssh.com	n/a	Y	4
Protocol version	SSHv2.0	n/a	Y	5

2.5 Ciphers used

Table 2-20 SSH Client

Category	Name	Value (hex)	Enabled by default	Security grade
Ciphers for encryption (enc)	aes128-ctr	n/a	Y	4
Ciphers for encryption (enc)	aes192-ctr	n/a	Y	4
Ciphers for encryption (enc)	aes256-ctr	n/a	Y	4
Host key (key)	ecdsa-sha2-nistp256-cert-v01@openssh.com	n/a	Y	4
Host key (key)	ecdsa-sha2-nistp384-cert-v01@openssh.com	n/a	Y	4
Host key (key)	ecdsa-sha2-nistp521-cert-v01@openssh.com	n/a	Y	4
Host key (key)	sk-ecdsa-sha2-nistp256-cert-v01@openssh.com	n/a	Y	4
Host key (key)	ssh-ed25519-cert-v01@openssh.com	n/a	Y	4
Host key (key)	sk-ssh-ed25519-cert-v01@openssh.com	n/a	Y	4
Host key (key)	ecdsa-sha2-nistp256	n/a	Y	4
Host key (key)	ecdsa-sha2-nistp384	n/a	Y	4
Host key (key)	ecdsa-sha2-nistp521	n/a	Y	4
Host key (key)	sk-ecdsa-sha2-nistp256@openssh.com	n/a	Y	4
Host key (key)	ssh-ed25519	n/a	Y	4
Host key (key)	sk-ssh-ed25519@openssh.com	n/a	Y	4
Key exchange (kex)	curve25519-sha256	n/a	Y	4
Key exchange (kex)	ecdh-sha2-nistp256	n/a	Y	4
Key exchange (kex)	ecdh-sha2-nistp384	n/a	Y	4
Key exchange (kex)	ecdh-sha2-nistp521	n/a	Y	4
Key length	ECDH >= 250 Bit	n/a	Y	5
MAC	umac-128-etm@openssh.com	n/a	Y	4
MAC	hmac-sha2-256-etm@openssh.com	n/a	Y	4
Protocol version	SSHv2.0	n/a	Y	5

Agent

Table 2-21 BEATS (TCP / 5046) Client

Category	Name	Value (hex)	Enabled by default	Security grade
Cipher suite	TLS_ECDHE_ECD-SA_WITH_AES_128_GCM_SHA256	0xc02b	Y	5
Cipher suite	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	0xc02f	Y	5
Cipher suite	TLS_ECDHE_ECD-SA_WITH_AES_256_GCM_SHA384	0xc02c	Y	5
Cipher suite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	0xc030	Y	5

Category	Name	Value (hex)	Enabled by default	Security grade
Cipher suite	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	0xcca9	Y	5
Cipher suite	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	0xcca8	Y	5
Cipher suite	TLS_AES_128_GCM_SHA256	0x1301	Y	5
Cipher suite	TLS_AES_256_GCM_SHA384	0x1302	Y	5
Cipher suite	TLS_CHACHA20_POLY1305_SHA256	0x1303	Y	5
Named group	X25519	0x001d	Y	5
Named group	secp256r1 (prime256v1)	0x0017	Y	5
Named group	secp384r1	0x0018	Y	5
Named group	secp521r1	0x0019	Y	5
Protocol version	TLSv1.2	.	Y	5
Protocol version	TLSv1.3	.	Y	5
Signature	sha256+rsaepss	0x0804	Y	5
Signature	sha256+ecdsa	0x0403	Y	5
Signature	ed25519	0x0807	Y	5
Signature	sha384+rsaepss	0x0805	Y	5
Signature	sha512+rsaepss	0x0806	Y	5
Signature	sha256+rsa	0x0401	Y	5
Signature	sha384+rsa	0x0501	Y	5
Signature	sha512+rsa	0x0601	Y	5
Signature	sha1+rsa	0x0201	Y	1
Signature	sha1+ecdsa	0x0203	Y	1

Table 2-22 HTTPS (TCP / 9000) Client

Category	Name	Value (hex)	Enabled by default	Security grade
Cipher suite	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	0xC02B	Y	5
Cipher suite	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	0xC02F	Y	5
Cipher suite	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	0xC02C	Y	5
Cipher suite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	0xC030	Y	5
Cipher suite	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	0xCCA9	Y	5
Cipher suite	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	0xCCA8	Y	5
Cipher suite	TLS_AES_128_GCM_SHA256	0x1301	Y	5
Cipher suite	TLS_AES_256_GCM_SHA384	0x1302	Y	5
Cipher suite	TLS_CHACHA20_POLY1305_SHA256	0x1303	Y	5
Named group	X25519	0x001d	Y	5
Named group	secp256r1 (prime256v1)	0x0017	Y	5

2.5 Ciphers used

Category	Name	Value (hex)	Enabled by default	Security grade
Named group	secp384r1	0x0018	Y	5
Named group	secp521r1	0x0019	Y	5
Protocol version	TLSv1.2	.	Y	5
Protocol version	TLSv1.3	.	Y	5
Signature	sha256+rsaepss	0x0804	Y	5
Signature	sha256+ecdsa	0x0403	Y	5
Signature	ed25519	0x0807	Y	5
Signature	sha384+rsaepss	0x0805	Y	5
Signature	sha512+rsaepss	0x0806	Y	5
Signature	sha256+rsa	0x0401	Y	5
Signature	sha384+rsa	0x0501	Y	5
Signature	sha512+rsa	0x0601	Y	5
Signature	sha384+ecdsa	0x0503	Y	5
Signature	sha512+ecdsa	0x0603	Y	5
Signature	sha1+rsa	0x0201	Y	1
Signature	sha1+ecdsa	0x0203	Y	1

Table 2-23 Update Agent (TCP / 9000) Client

Category	Name	Value (hex)	Enabled by default	Security grade
Cipher suite	TLS_ECDHE_ECD-SA_WITH_AES_128_GCM_SHA256	0xC02B	Y	5
Cipher suite	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	0xC02F	Y	5
Cipher suite	TLS_ECDHE_ECD-SA_WITH_AES_256_GCM_SHA384	0xC02C	Y	5
Cipher suite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	0xC030	Y	5
Cipher suite	TLS_ECDHE_ECDSA_WITH_CHA-CHA20_POLY1305_SHA256	0xCCA9	Y	5
Cipher suite	TLS_ECDHE_RSA_WITH_CHA-CHA20_POLY1305_SHA256	0xCCA8	Y	5
Cipher suite	TLS_AES_128_GCM_SHA256	0x1301	Y	5
Cipher suite	TLS_AES_256_GCM_SHA384	0x1302	Y	5
Cipher suite	TLS_CHACHA20_POLY1305_SHA256	0x1303	Y	5
Named group	X25519	0x001d	Y	5
Named group	secp256r1 (prime256v1)	0x0017	Y	5
Named group	secp384r1	0x0018	Y	5
Named group	secp521r1	0x0019	Y	5
Protocol version	TLSv1.2	.	Y	5
Protocol version	TLSv1.3	.	Y	5
Signature	sha256+rsaepss	0x0804	Y	5
Signature	sha256+ecdsa	0x0403	Y	5

Category	Name	Value (hex)	Enabled by default	Security grade
Signature	ed25519	0x0807	Y	5
Signature	sha384+rsaepss	0x0805	Y	5
Signature	sha512+rsaepss	0x0806	Y	5
Signature	sha256+rsa	0x0401	Y	5
Signature	sha384+rsa	0x0501	Y	5
Signature	sha512+rsa	0x0601	Y	5
Signature	sha384+ecdsa	0x0503	Y	5
Signature	sha512+ecdsa	0x0603	Y	5
Signature	sha1+rsa	0x0201	Y	1
Signature	sha1+ecdsa	0x0203	Y	1

Table 2-24 Agentless log collection WinRM (TCP / 5986)

Category	Name	Value (hex)	Enabled by default	Security grade
Cipher suite	TLS_RSA_WITH_AES_128_CBC_SHA	n/a	n/a	1
Cipher suite	TLS_RSA_WITH_AES_256_CBC_SHA	n/a	n/a	1
Cipher suite	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	n/a	n/a	1
Cipher suite	TLS_RSA_WITH_3DES_EDE_CBC_SHA	n/a	n/a	1
Cipher suite	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	n/a	n/a	2
Cipher suite	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	n/a	n/a	2
Cipher suite	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	n/a	n/a	2
Cipher suite	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	n/a	n/a	2
Cipher suite	TLS_RSA_WITH_AES_128_GCM_SHA256	n/a	n/a	3
Cipher suite	TLS_RSA_WITH_AES_256_GCM_SHA384	n/a	n/a	3
Cipher suite	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	n/a	n/a	4
Cipher suite	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	n/a	n/a	4
Cipher suite	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	n/a	n/a	4
Cipher suite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	n/a	n/a	4
Cipher suite	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	n/a	n/a	4
Cipher suite	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	n/a	n/a	4
Cipher suite	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	n/a	n/a	5
Cipher suite	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	n/a	n/a	5
Cipher suite	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	n/a	n/a	5
Cipher suite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	n/a	n/a	5

2.5 Ciphers used

Category	Name	Value (hex)	Enabled by default	Security grade
Cipher suite	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	n/a	n/a	5
Cipher suite	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	n/a	n/a	5

Function and structure

3.1 Function overview

SINEC Security Monitor is a security monitoring solution for industrial Operational Technology (OT) environments.

Overview

The main functions of SINEC Security Monitor are:

- Security log management
- Network traffic security analysis.

The software components of the SINEC Security Monitor system run on CoreShield S2L2 Linux servers and IPCs (industry-grade PCs), which act as SINEC Security Monitor servers and SINEC Security Monitor sensors respectively. Additionally, a Microsoft Windows application, the SINEC Security Monitor Agent may be installed on suitable OT assets throughout the network.

A comprehensive web-based user interface serves all users, for example system administrators and security administrators, as the base for information and control.

Functions

SINEC Security Monitor combines the functionality of a SIEM (Security Information and Event Management) system and an IDS (Intrusion Detection System) with further security monitoring features.

- Visualization of the current OT security situation and operational risks
- Scalable system adjusted to the size of the OT environment
- Alerts for security administrators so that they can promptly deal with malware, anomalies, intruders and other threats
- The entire SINEC Security Monitor system collects network traffic and security logs in the OT network and monitors and analyzes the assets and their abnormal behaviors
- Detection of all assets in the OT network and discovery of the OT network topology

Generated security events can additionally be sent to third-party SIEM solutions using Syslog (via TLS).

3.2 Components and licenses

The system consists of:

- SINEC Security Monitor Server hardware and SINEC Security Monitor Server software
- SINEC Security Monitor Sensor hardware and Sensor software (optional, requires separate add-on)
- SINEC Security Monitor Intelligence Database
- SINEC Security Monitor Agent, a Microsoft Windows software program suite (optional, requires separate add-on)
- SINEC Security Monitor Agentless configuration suite for security log collection for PCs (optional, requires separate add-on)

SINEC Security Monitor Licenses are available as a yearly subscription. Choose the size of your license package depending on the number of assets you want to monitor with SINEC Security Monitor.

License name	Size (number of assets)
SINEC Security Monitor XS	100
SINEC Security Monitor S	500
SINEC Security Monitor M	1,000
SINEC Security Monitor L	3,000

If the maximum supported asset limit is exceeded, the SINEC Security Monitor software will show a notification in the WBM. Please note that if the asset limit is exceeded for a longer timeframe, the functionalities of the software might be reduced.

Upgrade to another license size

With an upgrade package, you can switch to a higher license size. Your subscription will continue and the upgrade package will only be charged for the remaining months of your subscription.

Add-ons

Gathering data from Windows PCs or from distributed SSM Sensors is only possible with the corresponding add-on.

Add-on name	Description	Number of assets / supported data sources
PC Agent Add-On	Add-on that allows integration of data from Windows PCs by installing agents.	Unlimited
Distributed sensor Add-On	Add-on that allows integration of data from distributed sensors by installing sensor software on e.g. IPCs.	Unlimited

Requesting a SINEC Security Monitor Server license:

See chapter Requesting a SINEC Security Monitor license for the SINEC Security Monitor Server (Page 91)

See chapter Requesting a SINEC Security Monitor license for the SINEC Security Monitor Sensor (Page 112)

3.2.1 SSM Server

User interface

Operators and administrators can access the system using the web-based user interface.

The web-based user interface will be called WBM (web based management) from this point.

SINEC Security Monitor Server functions

SINEC Security Monitor Server provides:

- Asset management
- Vulnerability management
- Network topology/network load
- Log collection, aggregation and forwarding
- Internal audit log
- Security event and risk management
- Smart correlation and allow-list-based analysis
- Security visualization for local OT admin
- Sending security events to third-party SIEM system

Recommended hardware

For the recommended hardware, refer to chapter Hardware requirements and recommendations for SSM Server (Page 71).

3.2 Components and licenses

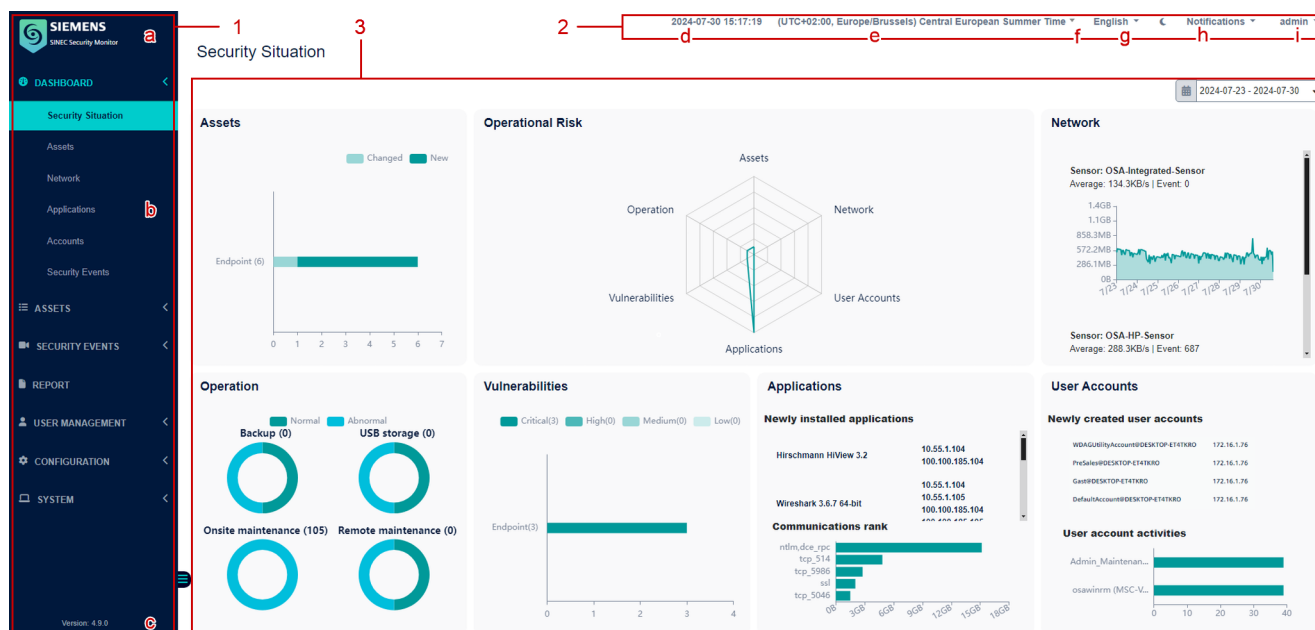


Figure 3-1 Structure of the WBM

Item	Function
1	Navigation bar
	a) Logo and product name
	b) Menu
	c) SINEC Security Monitor version
2	Title bar
	d) Date and time in the selected time zone
	e) Selected time zone
	f) Language (English, Deutsch, Chinese 中文)
	g) Dark mode and light mode
	h) Notification
	i) Username (Change password, Logout)
3	Display of the currently selected section
	Menu icon for toggling the navigation bar

Table 3-1 Structure of the main menu

Menu item	Purpose
Dashboard	Charts, diagrams, and lists give a full overview of all dimensions of the OT environment.
Assets	Shows detailed information on all assets in the OT environment.
Security Events	Shows detailed information on security events.
Report	Reports offer detailed information on the overall situation of the OT environment within a specific period. Reports can be downloaded, exported, or scheduled to be sent by email.

User Management	Define user roles and add users.
Configuration	Configure the SINEC Security Monitor System.
System	Control the SINEC Security Monitor System.

Operating the WBM

Special functions appear on many pages of the WBM to prioritize information displayed in lists and diagrams.

- **Mouseover**
Use the mouseover on graphical elements without clicking to reveal more information. For example: full names of abbreviated labels, number and percentages and detailed charts. Text abbreviated with "..." can be fully displayed either by mouseover or mouse click.
- **Searching lists**
The search bar can be used to find information in lists.
- **Advanced search**
Larger lists also have an option for an advanced search, where multiple criteria can be chosen for selection. When available, it is accessed by clicking on the "Basic Search" button.
- **Sorting tables**
Use the arrow controls to sort the information shown in the tables.
- **Items per page**
To manage the display of large lists with many items, 10, 25, 50 or 100 items per page can be selected. The arrow buttons < and > are used to navigate the pages.
- **Calendar**
Lists are provided with a calendar to select a specific period for a list.
- **Filter**
A filter can be used to refine a search or to select desired items.
- **Columns**
Select and deselect columns for a customized view.
- **Action buttons**
Action buttons appear on lists in the "Actions" column. They allow you to show details, edit and delete entries in the list and more.

Button (example)	Description
	Shows details for the selected entry
	Opens the edit window of the selected entry
	Deletes the selected entry from the list

- **Notifications**

Notifications via email, pop-up window or sound alarm can be configured for specific system event notifications and security event notifications.

Refer to chapter Configuring system notifications (Page 142).

3.2.2 SSM Intelligence Database

SINEC Security Monitor Intelligence Database

This database comprises:

- SINEC Security Monitor Correlation Rules Library
The library includes customized security event detection rules that are based on user requirements.
For example, S7comm: Firmware upgrade, upload PLC configuration, download PLC configuration, USB plugin and more.
- SINEC Security Monitor Vulnerabilities Library
The library currently covers more than 180,000 CVSS 2.0 and CVSS 3.1 rated vulnerabilities.
- SINEC Security Monitor Threat Intelligence Library
The Threat Intelligence Library includes security event rules that originate from ET Pro® (developed by the 3rd party commercial corporation Proof Point).
The library covers more than 40 different categories of security event detection rules for malware command and control, credential phishing, DDoS, botnets, network anomalies, exploits, vulnerabilities and more.

Updates will be regularly provided.

3.2.3 SSM Sensor (optional)

SINEC Security Monitor Sensor functions

The SINEC Security Monitor Sensor provides:

- Asset discovery
- Intrusion detection
- Anomaly detection
- Malware traffic detection
- Deep packet inspection of network traffic
- Industrial control protocol analysis

Recommended hardware

For the recommended hardware, refer to chapter Hardware requirements and recommendations for SSM Server (Page 71).

3.2.4 SSM Agent (optional)

Security log collection modes

There are three main log collection modes available:

- **Agent mode**
Log collection using the SINEC Security Monitor Agent on Microsoft Windows clients
Collected data are for example: Application logs, security logs, system logs, user accounts data, installed program data in Microsoft Windows and patch information.
- **Agentless mode**
Log collection from Microsoft Windows clients using the tools RemoteWMI (hmibeat) or WinRM (winrmbeat) from the SINEC Security Monitor Agentless configuration suite
Collected data are for example: Application logs, security logs, system logs, user accounts data, installed program data in Microsoft Windows and patch information.
- **No Agent mode**
Log collection via Syslog from endpoints, like Linux devices, firewalls, routers and other systems
The Syslog data are actively forwarded by the syslog clients to the SSM Server directly or via the SSM Sensor.

SINEC Security Monitor Agent

The SINEC Security Monitor Agent is a Microsoft Windows software service which runs on workstations within the production site.

The SINEC Security Monitor Agent provides:

- Security log and information collection

SINEC Security Monitor Agentless packages

Suite of PowerShell scripts to facilitate the installation of secure log collection from Microsoft Windows clients. During the installation, one Windows workstation becomes a dedicated certificate authority (CA) to ensure secure communication.

3.3 Working modes

The system has two working modes:

- **Learning mode**
In learning mode, everything detected by the SINEC Security Monitor System (IP addresses, communication links, applications, user accounts and USB devices) is added to allow lists (whitelisting) and no security events will be generated.
- **Operational mode**
Every change in the environment causes a security event that needs to be evaluated either directly in SINEC Security Monitor or needs to be sent to a 3rd party SIEM system. Depending on this evaluation by a qualified expert, a possible resulting action could be to add the event or underlying event to the "allow lists" or to start appropriate countermeasures.

3.3 Working modes

Recommendations for "Learning mode"

It is recommended to activate learning mode after the SINEC Security Monitor System's installation. In learning mode, detected IP addresses, communication links, applications, user accounts and USB devices are automatically added to allow lists (also referred to as whitelisting or baselining). The respective security events will not be recorded and the system will not generate security events for devices on the allow list.

Switching to "Operational mode"

A suitable timeframe has to be defined by the users. A learning time of at least two weeks is recommended. After this time the system needs to be switched to operational mode manually.

Planning deployment

4.1 Planning usage of SINEC Security Monitor Server and Sensor

Installing SINEC Security Monitor Server and SINEC Security Monitor Sensor on the same device

SINEC Security Monitor is installed only on the SINEC Security Monitor Server (Dell / HPE server).

Software installation on the Security Monitor Server involves:

- SINEC Security Monitor Server software package installation
- SINEC Security Monitor Server configuration

Installing Security Monitor Server and Security Monitor Sensor(s) on separate devices (only possible with the optional "Distributed sensor Add-On")

Security Monitor is installed on at least two separate devices, Security Monitor Server (Dell / HPE server) with virtual Security Monitor Sensor and one or more distributed Security Monitor Sensor(s) (SIMATIC IPC or HPE server).

Software installation on the SINEC Security Monitor Server involves:

- SINEC Security Monitor Server software package installation
- SINEC Security Monitor Server configuration

Software installation on the SINEC Security Monitor Sensor involves:

- SINEC Security Monitor Sensor software package installation
- SINEC Security Monitor Sensor configuration

4.2 Planning data sources for network traffic capture

When planning the data sources for network capture data, there are different possibilities for data acquisition.

- The network traffic data can be acquired from mirror ports of network switches. We advise using this option.
- The network traffic data can also be acquired using network TAPs.
- No direct link from the capture point (e.g., the TAP) to the SINEC Security Monitor Sensor is possible and the captured data must be routed through the LAN.

4.3 Network bandwidth usage for traffic between Server and Sensor

The network bandwidth usage has been determined for variable network speeds between SSM Server and SSM Sensor and fixed syslog volumes.

- H1 port of the SSM Server:
Network communication port and user access port that is used to communicate with the SSM Sensor and to receive syslog traffic.
- H1 port of the SSM Sensor:
Network communication port that is used to communicate with the SSM Server and to receive syslog traffic.
- M port:
Network mirror port that reveals the monitored traffic bandwidth.

Table 4-1 Network bandwidth usage for traffic between Server and Sensor

Monitor traffic (Mbit/s) (M port)	Monitor syslog (log/s) (H1 port)	Network bandwidth (kByte/s) (H1 port)	
		Server	Sensor
10	500	632.13	1214.19
20	500	713.53	2427.42
30	500	711.78	3633.61
40	500	722.84	4840.80
50	500	767.11	6045.74
60	500	780.18	7261.45
70	500	788.89	8429.37
80	500	824.51	9639.93
90	500	864.37	10826.41
100	500	893.65	12036.14
200	500	1134.12	23846.83
300	500	1311.12	35587.85
400	500	1306.16	44554.55
500	500	1350.00	51802.98
1000	500	1489.91	68835.29

4.4 Supported Microsoft Windows versions for vulnerabilities association

Table 4-2 Supported Microsoft Windows versions for vulnerabilities association

Operating system	Build version
Windows10 Pro	10.0.19044
Windows10 Home	10.0.19044
Windows10 Pro	10.0.19042
Windows10 Pro	10.0.19041
Windows10 Pro	10.0.18363

Operating system	Build version
Windows10 Enterprise TSC	10.0.17763
Windows10 Enterprise	10.0.14393
Windows10 Enterprise	10.0.10586
Windows Server 2012 R2	6.3.9600
Windows Server 2016	10.0.14393

4.5 Supported network scenarios

4.5.1 SSM Server interfaces

The SSM Server supports the configuration of four network interface cards (NIC). A main network interface, two additional interfaces for service purposes and an interface to monitor network traffic.

Note: All IP addresses in this chapter are just examples.

- The H1 port (main NIC), H2 port and H3 port can all take on the role of access to the WBM, diagnostics communication, and connection to the SSM Sensor, SSM Agent, No Agent, and Agentless data sources.
- The M port is used to monitor network traffic.

During the SSM Server installation process, you can configure the IP addresses of the main and other NICs to match your actual network environment.

Table 4-3 SSM Server interfaces

Interface	Description
H1	Main NIC Communication with data sources (Sensor/Agent/Agentless/No Agent)
H2	Access to the WBM
H3	Communication with diagnostics tools
M	Network traffic mirror port

4.5.2 SSM Sensor interfaces

The SSM Sensor supports the configuration of three NICs. A main network interface, a additional interface for service purposes and an interface to monitor network traffic.

- The H1 port (main NIC) and H2 port can both take on the role of communication with the SSM Server's H1 port, data/diagnostics communication and connection to the SSM Agent, No Agent, and Agentless data sources.
- The M port is used to monitor network traffic.

During the SSM Server installation process, you can configure the IP addresses of the main and other NICs to match your actual network environment.

Table 4-4 SSM Sensor interfaces

Interface	Description
H1	Main NIC Communication with the SSM Server
H2	Communication with data sources (Agent/No Agent/Agentless) and diagnostics tools
M	Network traffic mirror port

4.5.3 Overview of supported network scenarios

Note

- Definition of the main NIC of the SSM Server:
Network interface card that establishes data connection between the virtual SSM Sensor and the SSM Server internal service.
 - Definition of the main NIC of the SSM Sensor:
During the configuration of the SSM Sensor, the network adapter that connects the SSM Sensor to the SSM Server is called the main NIC.
 - For both devices, SSM Server and SSM Sensor, there is no special functional difference between the main NIC and the other NICs.
-

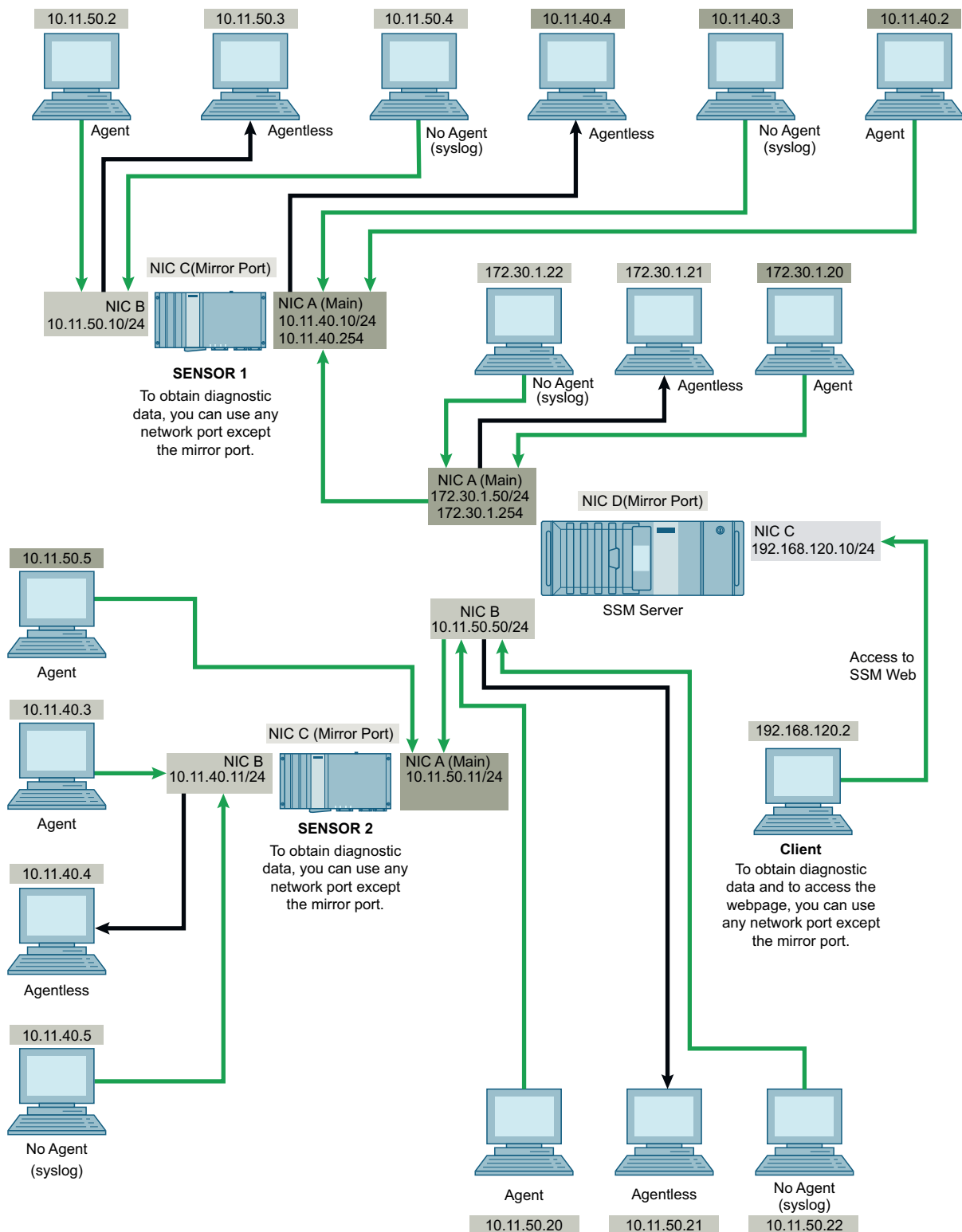


Figure 4-1 Network scenarios overview

4.5.4 Communication between SSM Server and SSM Sensor

During the installation process of the SSM Sensor, four scenarios could be considered when you configure the IP address of the SSM Sensor host.

For more information on the configuration of the SSM Sensor, refer to chapter Configuring the SINEC Security Monitor Sensor (Page 110).

Sensor scenario 1

SSM Server and SSM Sensor have each one NIC.

The IP addresses of the main NIC of the SSM Server and the main NIC of the SSM Sensor are in different network segments. You can configure the main NIC of the SSM Sensor to connect to the main NIC of the SSM Server via Firewall/Router.

Table 4-5 Sensor scenario 1, addressing example

NIC name	IP address
SSM Server NIC A – main NIC	IP address: 172.30.1.50/24 Gateway: 172.30.1.254
SSM Sensor NIC A – main NIC	IP address: 10.11.40.10/24 Gateway: 10.11.40.254

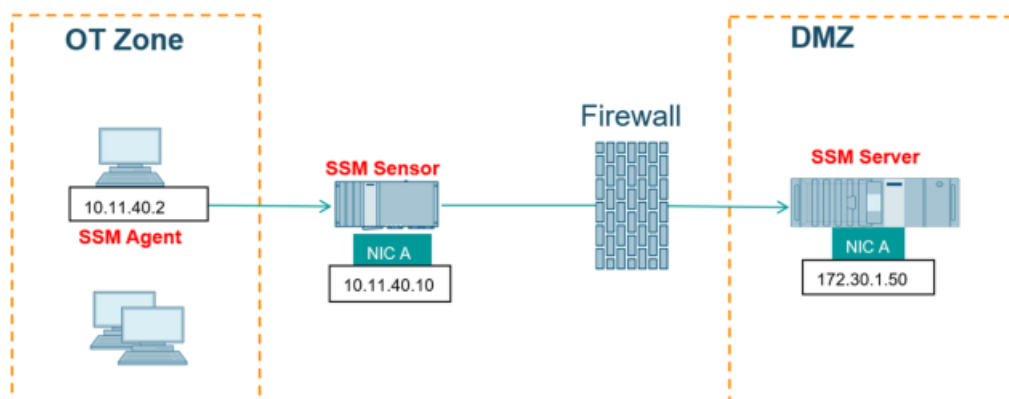


Figure 4-2 Sensor Scenario 1

Sensor scenario 2

The SSM Server has one NIC and the SSM Sensor has two NICs to communicate with an SSM Agent and the SSM Server.

The IP addresses of NIC B of the SSM Sensor and the main NIC of the SSM Server are in the same network segment. You can configure NIC B of the SSM Sensor to connect directly to the main NIC of the SSM Server.

Table 4-6 Sensor scenario 2, addressing example

NIC name	IP address
SSM Server NIC A – main NIC	10.11.50.50/24
SSM Sensor NIC A	10.11.40.10/24
SSM Sensor NIC B – main NIC	10.11.50.11/24

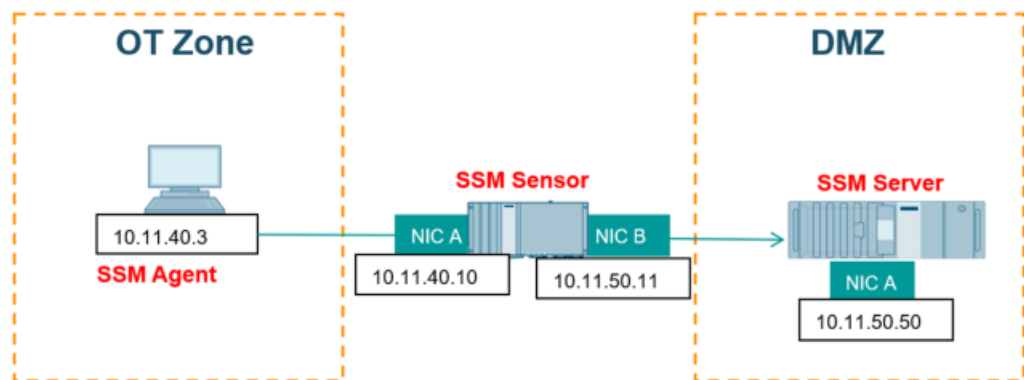


Figure 4-3 Sensor Scenario 2

Sensor scenario 3

The SSM Server has one NIC, the SSM Sensor has multiple NICs (up to 3) to communicate with SSM Agents and the SSM Server.

The IP addresses of NIC B of the SSM Sensor and the main NIC of the SSM Server are in the same network segment. You can configure NIC B of the SSM Sensor to connect directly to the main NIC of the SSM Server.

Table 4-7 Sensor scenario 3, addressing example

NIC name	IP address
SSM Server NIC A – main NIC	10.11.50.50/24
SSM Sensor NIC A	10.11.40.10/24
SSM Sensor NIC B – main NIC	10.11.50.11/24
SSM Sensor NIC C	172.30.1.100

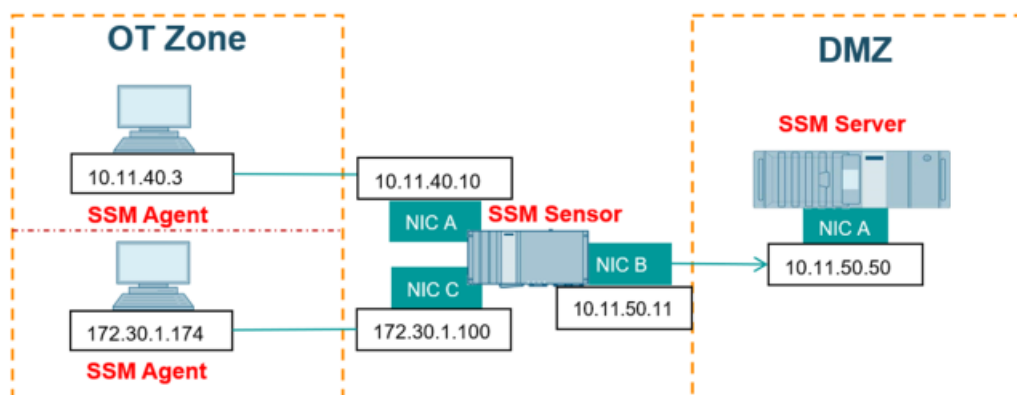


Figure 4-4 Sensor Scenario 3

Sensor scenario 4

The SSM Server has three NICs, the SSM Sensor has two NICs to communicate with SSM Agents and the SSM Server.

The IP addresses of the main NIC of the SSM Sensor and NIC B of the SSM Server are in the same network segment. You can configure the main NIC of the SSM Sensor to connect directly to NIC B of the SSM Server.

Table 4-8 Sensor scenario 4, addressing example

NIC name	IP address
SSM Server NIC A – main NIC	172.30.1.50/24
SSM Server NIC B	10.11.50.50/24
SSM Server NIC C	192.168.120.10/24
SSM Sensor NIC A – main NIC	10.11.50.11/24
SSM Sensor NIC B	10.11.40.11/24

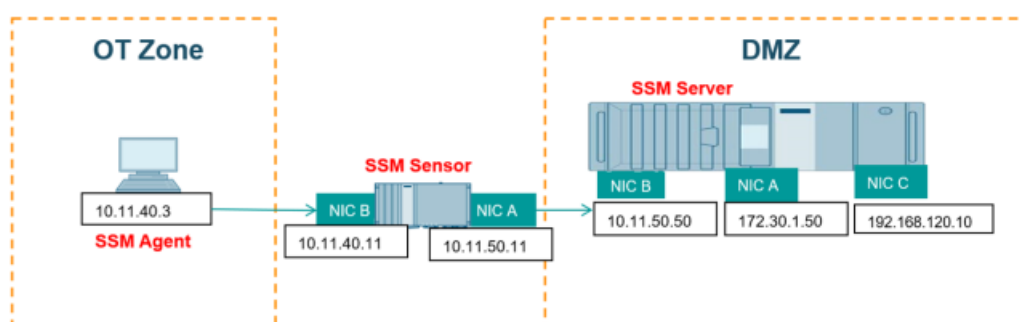


Figure 4-5 Sensor Scenario 4

4.5.5 Communication between SSM Agent and SSM Server or SSM Sensor

During the installation process of the SSM Agent, four scenarios could be considered when you configure the IP address of the current host.

Agent scenario 1.1 and 1.2

The SSM Server has only one NIC.

Agent scenario 1.1: The corresponding firewall policies are enabled between the SSM Agent and the SSM Server (in this example: Agent 1.1).

Agent scenario 1.2: The IP addresses of the SSM Agent and the main NIC of the SSM Server are in the same network segment (in this example: Agent 1.2).

The SSM Agent forwards its data directly to the SSM Server.

Table 4-9 Agent scenario 1.1 and 1.2, addressing example

NIC/Host name	IP address
SSM Server NIC A – main NIC	IP address: 172.30.1.50/24 Gateway: 172.30.1.254
SSM Agent host 1.1	192.168.1.12
SSM Agent host 1.2	172.30.1.20

When installing the SSM Agent, you must enter a destination IP address.

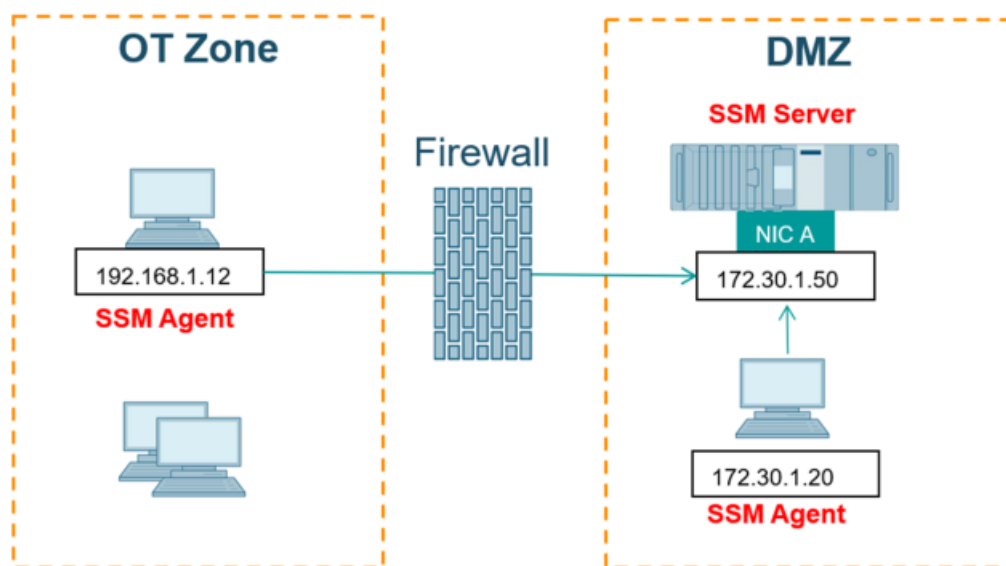


Figure 4-6 Agent Scenario 1.1 (left) and 1.2 (right)

In "Agent scenario 1.1" and "Agent scenario 1.2", the destination IP address is the SSM Server's main NIC IP address.

Agent scenario 2

The SSM Server and the SSM Sensor have only one NIC.

The SSM Agent and the SSM Server are in different network segments and separated by firewall policies. You can use the SSM Sensor that is deployed on the SSM Agent side for data transmission.

Firewall policies between the SSM Sensor to the SSM Server could be enabled. The data of the SSM Agent is forwarded to the SSM Server by the SSM Sensor.

Table 4-10 Agent scenario 2, addressing example

NIC/Host name	IP address
SSM Server NIC A – main NIC	IP address: 172.30.1.50/24 Gateway: 172.30.1.254
SSM Sensor NIC A – main NIC	IP address: 10.11.40.10/24 Gateway: 10.11.40.254
SSM Agent Host	10.11.40.2

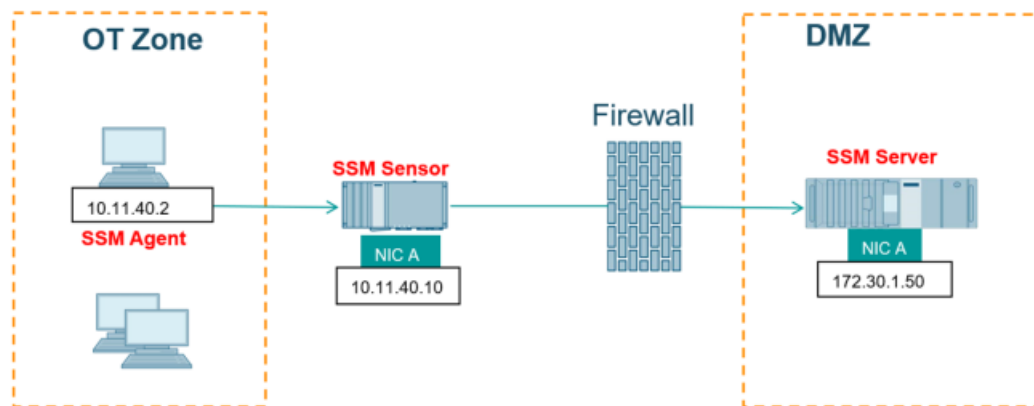


Figure 4-7 Agent Scenario 2

When installing the SSM Agent, you must enter a destination IP address.

In "Agent scenario 2", the destination IP address is the SSM Sensor's main NIC IP address.

Agent scenario 3

The SSM Server has one NIC and the SSM Sensor has two NICs.

- The IP addresses of the SSM Agent host and the main NIC of the SSM Sensor are in the same network segment. You can use the SSM Sensor for data transmission.
- Data that is sent by the SSM Agent in the OT zone is received by the main NIC of the SSM Sensor and forwarded to the SSM Server using iptables.
- The SSM Sensor's NIC B is responsible for data transmission to the SSM Server. Data is forwarded to the SSM Server through routing rules.

Table 4-11 Agent scenario 3, addressing example

NIC/Host name	IP address
SSM Server NIC A – main NIC	10.11.50.50/24
SSM Sensor NIC A – main NIC	10.11.40.10/24

NIC/Host name	IP address
SSM Sensor NIC B	10.11.50.11/24
SSM Agent host	10.11.40.3

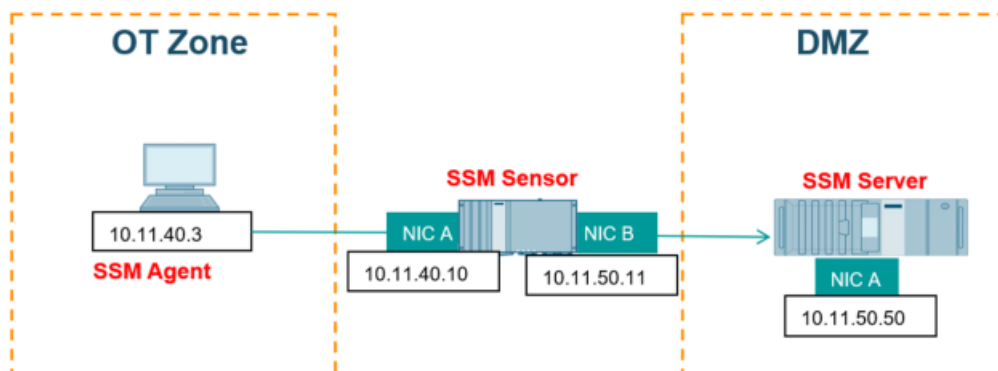


Figure 4-8 Agent Scenario 3

When installing the SSM Agent, you must enter a destination IP address.

In "Agent scenario 3", the destination IP address is the SSM Sensor's main NIC IP address.

Agent scenario 4

The SSM Server has three NICs.

The IP addresses of the SSM Agent and NIC A of the SSM Server are in the same network segment. The SSM Agent forwards its data directly to the SSM Server.

Table 4-12 Agent scenario 4, addressing example

NIC/Host name	IP address
SSM Server NIC A – main NIC	10.11.50.50/24
SSM Server NIC B	172.30.1.50/24
SSM Server NIC C	192.168.120.10/24
SSM Agent host	10.11.50.20

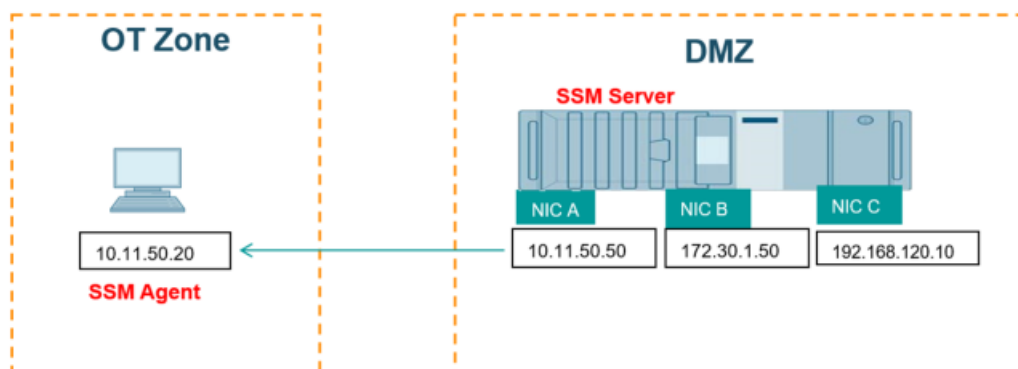


Figure 4-9 Agent Scenario 4

When installing the SSM Agent, you must enter a destination IP address.

In "Agent scenario 4", the destination IP address is the IP address of NIC A of the SSM Server.

4.5.6 Agentless communication with the SSM Server

The SSM Agentless Configuration Suite is a software package that supports security log collection and remote data acquisition from Microsoft Windows Clients.

For instructions on preparing Agentless data sources, refer to chapter Agentless security log collection (Page 160).

Agentless scenario 1

The IP addresses of the main NIC of the SSM Server and Agentless Microsoft Windows client are in the same network segment.

Table 4-13 Agentless scenario 1, addressing example

NIC/Host name	IP address
SSM Server NIC A – main NIC	172.30.1.50/24
SSM Server NIC B	10.11.50.50/24
SSM Server NIC C	192.168.120.10/24
Agentless Microsoft Windows client	172.30.1.21

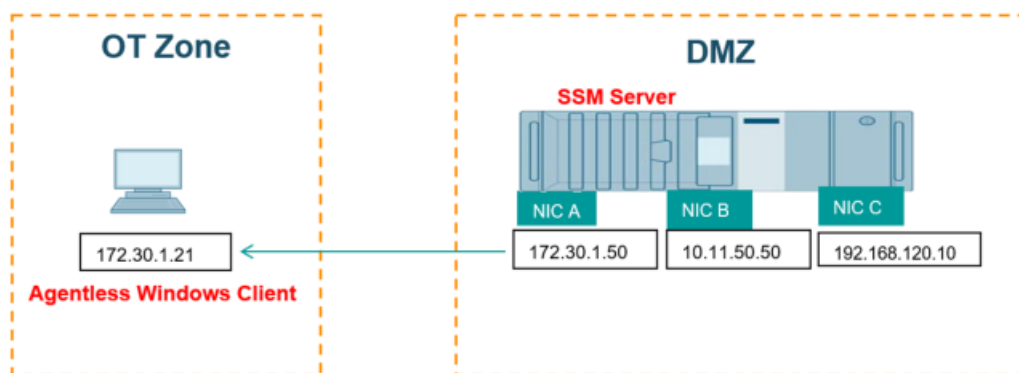


Figure 4-10 Agentless Scenario 1

When adding remote agentless nodes on the WBM, select the IP address of the main NIC of the SSM Server for the Destination field on the "Configuration" > "Sensor" > "Add" page.

Agentless scenario 2

The IP addresses of NIC B of the SSM Sensor and the Agentless Microsoft Windows client are in the same network segment.

Table 4-14 Agentless scenario 2, addressing example

NIC/Host name	IP address
SSM Server NIC A – main NIC	IP address: 172.30.1.50/24 Gateway: 172.30.1.254
SSM Server NIC B	10.11.40.50/24
SSM Server NIC C	192.168.120.10/24
SSM Sensor NIC A – main NIC	IP address: 10.11.40.10/24 Gateway: 10.11.40.254
SSM Sensor NIC B	10.11.50.10/24
Agentless Microsoft Windows client	10.11.50.3

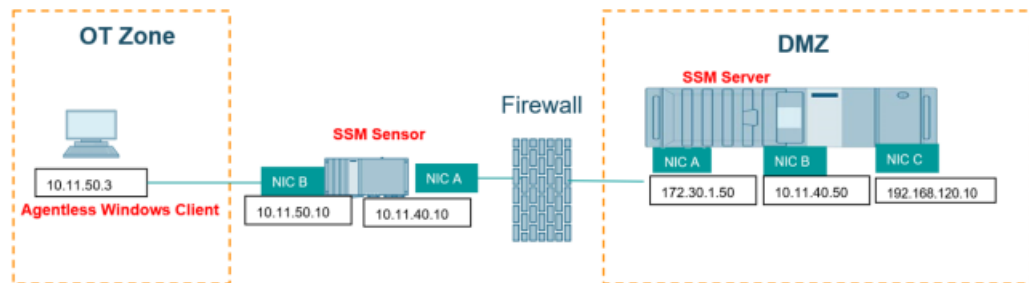


Figure 4-11 Agentless Scenario 2

When adding remote agentless nodes on the WBM, select the IP address of NIC B of the SSM Sensor for the Destination field on the "Configuration" > "Sensor" > "Add" page.

Agentless scenario 3

The IP addresses of the main NIC the SSM Sensor and the Agentless Microsoft Windows client are in the same network segment.

Table 4-15 Agentless scenario 3, addressing example

NIC/Host name	IP address
SSM Server NIC A – main NIC	IP address: 172.30.1.50/24 Gateway: 172.30.1.254
SSM Server NIC B	10.11.50.50/24
SSM Server NIC C	192.168.120.10/24
SSM Sensor NIC A	10.11.40.10/24
SSM Sensor NIC B – main NIC	IP address: 10.11.50.10/24 Gateway: 10.11.50.254
Agentless Microsoft Windows client	10.11.40.4

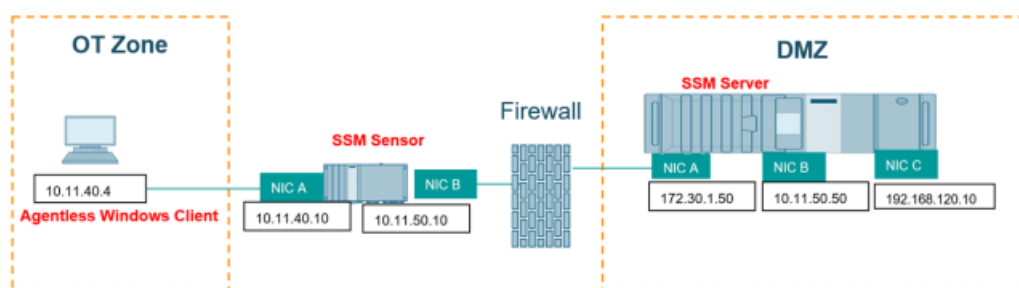


Figure 4-12 Agentless Scenario 3

When adding remote agentless nodes on the WBM, select the IP address of the main NIC of the SSM Sensor for the Destination field on the "Configuration" > "Sensor" > "Add" page.

Agentless scenario 4

The SSM Server has three NICs. The IP addresses of NIC B of the SSM Server and the Agentless Microsoft Windows client are in the same network segment.

Table 4-16 Agentless scenario 4, addressing example

NIC/Host name	IP address
SSM Server NIC A – main NIC	172.30.1.50/24
SSM Server NIC B	10.11.50.50/24
SSM Server NIC C	192.168.120.10/24
Agentless Microsoft Windows client	10.11.50.21

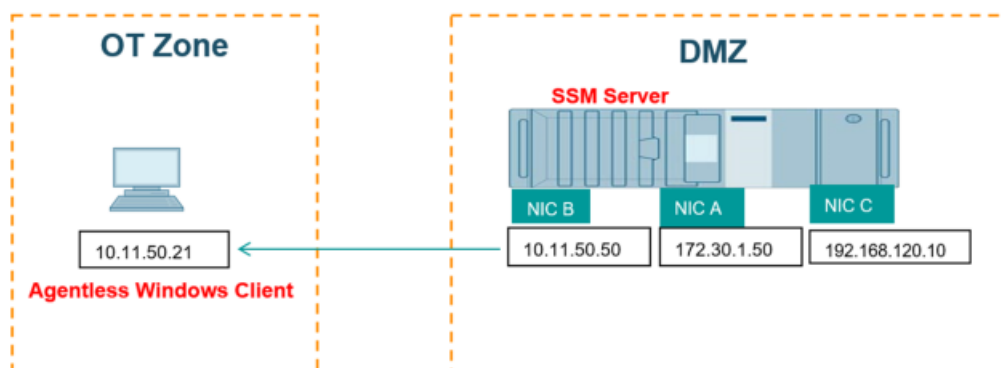


Figure 4-13 Agentless Scenario 4

When adding remote agentless nodes on the WBM, select the IP address of the NIC B of the SSM Server for the Destination field on the "Configuration" > "Sensor" > "Add" page.

4.5.7 No Agent communication with the SSM Server

Syslog data is actively forwarded by syslog clients to the SSM Server.

For configuration instructions, refer to chapter Configuring an endpoint for syslog data collection (Page 176).

No agent scenario 1

The IP addresses of the main NIC of the SSM Server and the No Agent syslog client are in the same network segment.

Table 4-17 No agent scenario 1

NIC/Host name	IP address
SSM Server NIC A – main NIC	172.30.1.50/24
SSM Server NIC B	10.11.50.50/24
SSM Server NIC C	192.168.120.10/24
No Agent syslog client	172.30.1.22

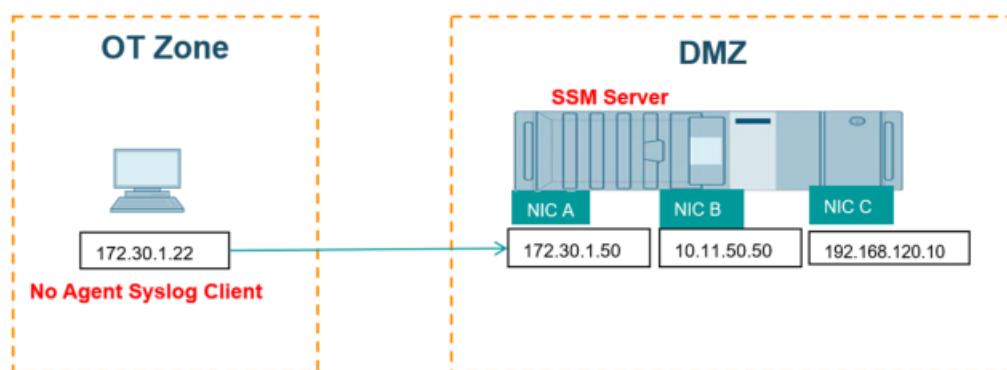


Figure 4-14 No Agent Scenario 1

When adding the No Agent data source to the WBM, select the IP address of the main NIC of the SSM Server for the "Destination" field.

No agent scenario 2

The IP addresses of NIC B of the SSM Sensor and the No Agent syslog client are in the same network segment.

Table 4-18 No agent scenario 2

NIC/Host name	IP address
SSM Server NIC A – main NIC	172.30.1.50/24
SSM Server NIC B	10.11.50.50/24
SSM Server NIC C	192.168.120.10/24
SSM Sensor NIC A – main NIC	10.11.50.10/24
SSM Sensor NIC B	10.11.40.10/24
No Agent syslog client	10.11.40.5

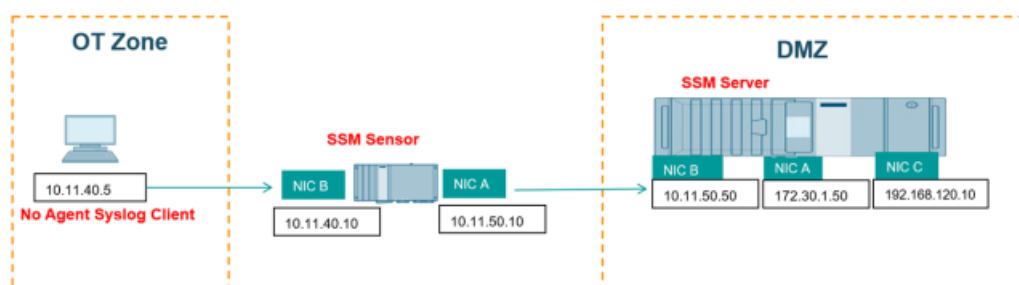


Figure 4-15 No Agent Scenario 2

When adding the No Agent data source to the WBM, select the IP address of NIC B of the SSM Sensor for the "Destination" field.

No agent scenario 3

The IP addresses of the main NIC of the SSM Sensor and the No Agent syslog client are in the same network segment.

Table 4-19 No agent scenario 3

NIC/Host name	IP address
SSM Server NIC A – main NIC	IP address: 172.30.1.50/24 Gateway: 172.30.1.254
SSM Server NIC B	10.11.50.50/24
SSM Server NIC C	192.168.120.10/24
SSM Sensor NIC A	10.11.40.10/24
SSM Sensor NIC B - main NIC	IP address: 10.11.50.10/24 Gateway: 10.11.50.254
No Agent syslog client	10.11.40.5

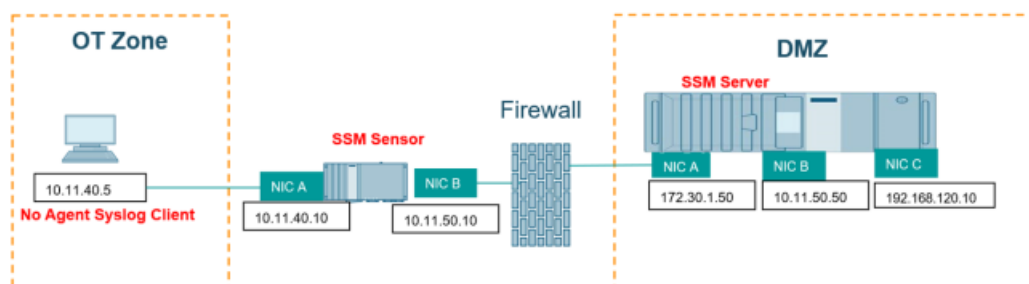


Figure 4-16 No Agent Scenario 3

When adding the No Agent data source to the WBM, select the IP address of the main NIC of the SSM Sensor for the "Destination" field.

No agent scenario 4

The IP addresses of NIC B of the SSM Server and the No Agent syslog client are in the same network segment.

Table 4-20 No agent scenario 4

NIC name	IP address
SSM Server NIC A – main NIC	172.30.1.50/24
SSM Server NIC B	10.11.50.50/24
SSM Server NIC C	192.168.120.10/24
No Agent syslog clients	10.11.50.22

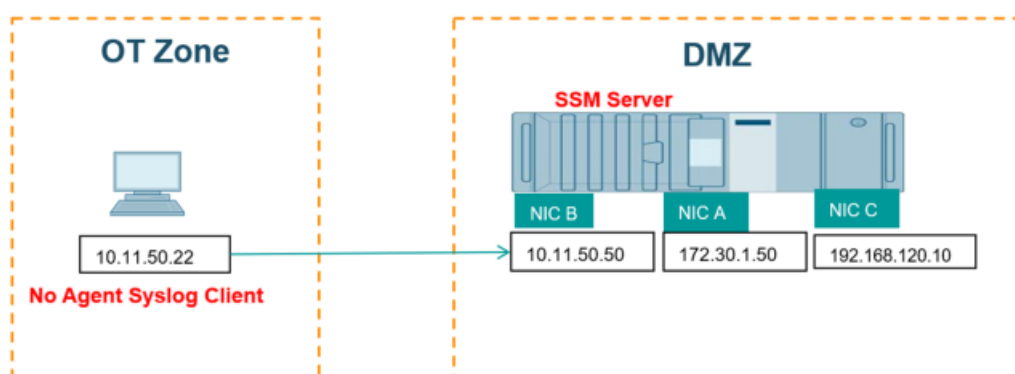


Figure 4-17 No Agent Scenario 4

When adding the No Agent data source to the WBM, select the IP address of NIC B of the SSM Server for the "Destination" field.

4.5.8 Access to the WBM

During the SSM Server installation process, the IP addresses of the SSM Server's NICs can be configured for access to the WBM.

Table 4-21 Access to the WBM

NIC name	IP address
SSM Server NIC A – main NIC	172.30.1.50/24
SSM Server NIC B	10.11.50.50/24
SSM Server NIC C	192.168.120.10/24

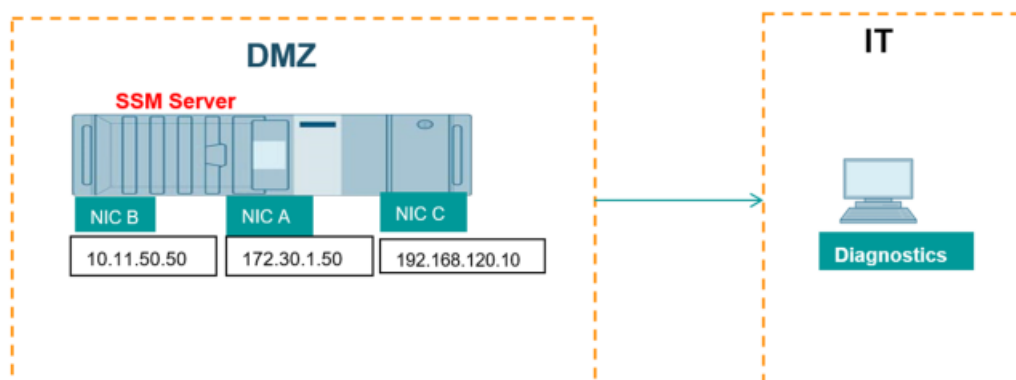


Figure 4-18 Access to the WBM

4.5.9 SSM Server diagnostics communication

During the SSM Server's installation process, the IP addresses of the SSM Server's NICs can be configured for access to the SSM Server's diagnostics communication.

Table 4-22 Access to the SSM Server's diagnostics communication

NIC name	IP address
SSM Server NIC A – main NIC	172.30.1.50/24
SSM Server NIC B	10.11.50.50/24
SSM Server NIC C	192.168.120.10/24

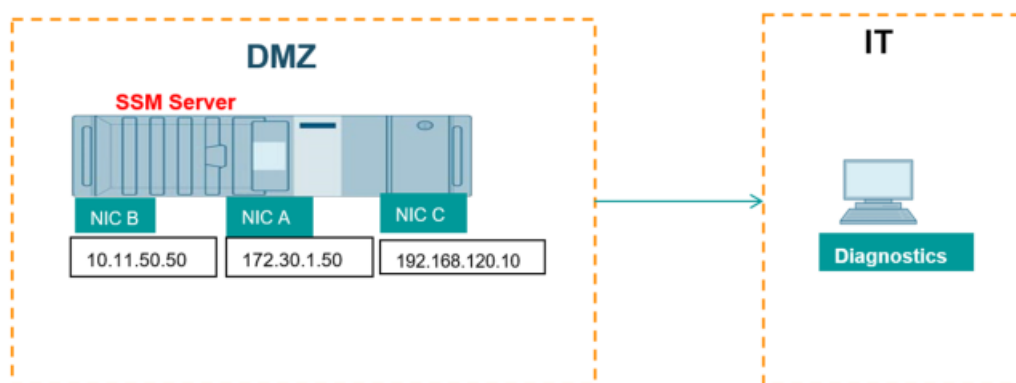


Figure 4-19 Server Diagnostics Communication

4.5.10 SSM Sensor diagnostics communication

During the SSM Sensor's installation process, the IP addresses of the SSM Sensor's NICs can be configured for access to the SSM Sensor's diagnostics communication.

Table 4-23 Access to the SSM Sensor's diagnostics communication

NIC name	IP address
SSM NIC A – main NIC	10.11.50.10/24
SSM Server NIC B	10.11.40.11/24

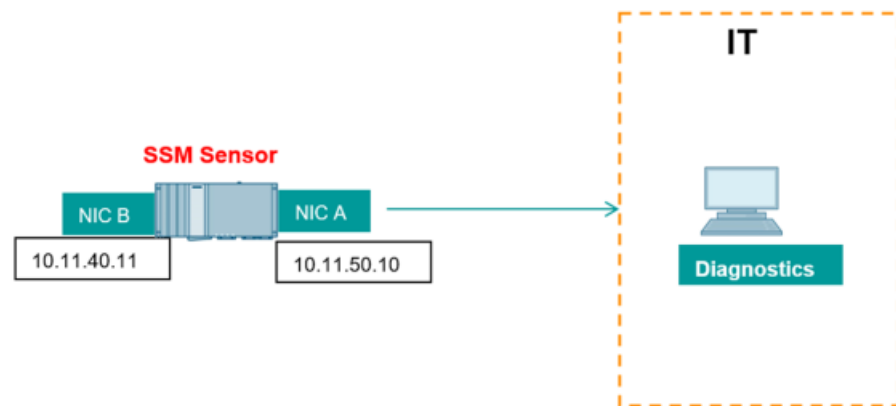


Figure 4-20 Sensor Diagnostics Communication

Installation

5.1 Hardware requirements and recommendations

5.1.1 Hardware requirements and recommendations for SSM Server

SINEC Security Monitor Server recommended hardware

Note

SINEC Security Monitor has been thoroughly tested in accordance with these recommendations. Should hardware other than that recommended be used for SINEC Security Monitor, performance and stress testing has to be performed by the customer.

- Dell R450 Server
Estimation of supported amount of assets for this configuration: Up to 6,000 assets with typical network traffic. This value highly depends on the network topology and network traffic in your application. For higher amount of assets, larger hardware configuration or multiple servers need to be considered.

Table 5-1 SSM Server recommendations - Dell R450

Quantity	Component
1	PowerEdge R450 Motherboard with Broadcom 5720 Dual Port 1Gb On-Board LOM
2	Intel Xeon Silver 4314 2.4 GHz, 16C/32T, 10.4 GT/s, 24 MB cache, Turbo, HT (135W) DDR4-2666
1	iDRAC Group Manager, Disabled
1	iDRAC Group Manager, Disabled
1	Standard Bezel
1	Riser Config 1, 2x16LP
1	PowerEdge R450 x4, x10 Long Drive Shipping Material
1	No Quick Sync
1	Performance Optimized
1	3200MT/s RDIMMs
12	16GB RDIMM, 3200MT/s, Dual Rank
1	iDRAC9, Enterprise 15G
4	4TB 7.2K RPM NLSAS ISE 12Gbps 512n 3.5in Hard Drive
1	PERC H745 Controller, Front
2	Heatsink for CPU less or equal 165W
1	No Internal Optical Drive
1	Dual, Hot-plug, Power Supply Redundant (1+1), 800W, Mixed Mode, NAF
1	Trusted Platform Module 2.0

5.1 Hardware requirements and recommendations

Quantity	Component
2	Jumper Cord - C13/C14, 2M, 250V, 10A
1	Intel i350 Quad Port 1GbE BASE-T, OCP NIC 3.0
1	No Systems Documentation, No OpenManage DVD Kit
1	Front PERC Mechanical Parts, front load
1	A11 drop-in/stab-in Combo Rails Without Cable Management Arm
1	Cable Management Arm
1	Unconfigured RAID

- HPE ProLiant DL380

Table 5-2 SINEC Security Monitor Server recommendations - HPE ProLiant DL380

Quantity	Component
2	Intel Xeon Silver 4314 2.4 GHz The processor mainly determines the operating speed of the programs. A high-performance processor is more suitable for larger installations.
12	RAM: DDR4, 16 GB DIMM, 2933 MT/s The larger the main memory capacity, the higher the operating speed of the system. Larger installations will generally also require a larger memory capacity.
2	System disks: 960 GB SSD (RAID1)
4	Data disks: 2 TB SSD (RAID5) The storage capacity determines the volume of original data that the SINEC Security Monitor Server can store permanently.
2	500 W hot-plug power supply
1 (minimum)	1 Gigabit, 4-port network adapter For management, user interface and to receive data from SINEC Security Monitor Sensors.
1	iLO Enterprise (remote server management)
1	Security: TPM 2.0

VMware hardware requirements

For the VMware solution, refer to chapter Hardware requirements for SSM Server on Virtualization Platforms (Page 74).

5.1.2 Hardware requirements and recommendation for SSM Sensor

SINEC Security Monitor Sensor recommended hardware

Note

SINEC Security Monitor has been thoroughly tested in accordance with these recommendations. Should hardware other than that recommended be used for SINEC Security Monitor, performance and stress testing has to be performed by the customer.

- SIMATIC IPC 427E



Figure 5-1 SIMATIC IPC 427E

Table 5-3 SINEC Security Monitor Sensor recommendations instead of components - IPC 427E

Quantity	Component
1	Intel i5-6442EQ The processor is the main determinant of the operating speed of the programs. A high-performance processor is more suitable for high traffic volume.
2	8 GB memory The main memory capacity also contributes to the speed of the system. A higher memory capacity is recommended for high traffic volume.
1	480 GB SSD The SINEC Security Monitor Sensor does not permanently store collected data.
3	Gigabit Ethernet (IE/PN) (Intel Ethernet i350 QP 1 Gb server adapter) Purpose: • Management • Data collection from SINEC Security Monitor Agent • Mirror port connection
1	10 Gigabit 2-port BASE-T Broadcom BCM57416
1	SITOP PSU 8200 24 V DC/5 A
1	Security: TPM 2.0

- HPE ProLiant DL360 Gen10+

5.1 Hardware requirements and recommendations

Table 5-4 Alternative Sensor components

Quantity	Component
1	Intel INT Xeon-S 4309Y CPU for HP The processor is the main determinant of the operating speed of the programs. A high-performance processor is more suitable for high traffic volume.
2	16 GB memory The main memory capacity also contributes to the speed of the system. A higher memory capacity is recommended for high traffic volume.
2	800 GB SSD The sensor does not permanently store collected data.
2	Gigabit Ethernet 4 port Base-T i350-T4 adapter Purpose: • Management • Data collection from SINEC Security Monitor Agent • Mirror port connection
2	HPE 500 W flex slot platinum hot pluggable power supply
1	Security: TPM 2.0

5.1.3 Hardware requirements for SSM Server on Virtualization Platforms

The hardware requirements should ensure that the SINEC Security Monitor Server runs properly on the virtualization platform.

You can find more information on VMware in Link: (<https://docs.vmware.com/en/VMware-vSphere/index.html>)

The table below lists the recommended VM's (Virtual Machine) hardware requirements for the SINEC Security Monitor Server virtualization installation:

Table 5-5 VM hardware requirements

Components	Minimum requirement	Recommendation	Comments
Maximum number of protected assets	< 500	500 to 1000	-
Expected traffic	< 10 Mbit/s	10 to 50 Mbit/s	-
Processor	16 Cores	48 Cores	The processor primarily determines the operating speed of the programs. Particularly for larger installations, the high-performance processor is recommended.
RAM	96 GB	160 GB	The capacity of the main memory contributes primarily to the speed of the system. For larger installations, a higher memory capacity is recommended.
Hard drive	2 TB SSD	8 TB SSD	The storage capacity largely decides about the volume of original data that SINEC Security Monitor System can store permanently. The storage time is 180 days by default.

Components	Minimum requirement	Recommendation	Comments
TPM	vTPM is a software-based representation of a physical TPM (Trusted Platform Module) 2.0 chip, it acts as any other virtual device.		
Note: The virtual SSM Sensor within the SSM Server requires additional VM network configurations.			

5.2 Hardware preparation

Before the installation of SSM Server software on the Dell / HPE server and SSM Sensor software on the SIMATIC IPC or HPE server, certain configuration steps are necessary as a first and vital step of hardening as well as for secure decommissioning. These procedures are part of the SINEC Security Monitor's security concept.

Hardware initialization for the HPE ProLiant DL360 and DL380

Configuring secure built-in iLO

iLO (HPE integrated Lights-Out) is a remote administration and monitoring software for HPE servers.

1. Press <F9> during startup to enter the "System Utilities".
2. On the "System Utilities" page, click "System Configuration".
3. On the "System Configuration" page, click "BIOS/Platform Configuration (RBSU)".
4. On the "BIOS/Platform Configuration (RBSU)" page, click "Network Options".
5. On the "Network Options" page, click "Pre-Boot Network Settings".
6. On the "Pre-Boot Network Settings" page, select "Disabled" from the "DHCPv4" drop-down menu.
7. Press <F10> to save the changes.
8. Reboot the system.

Enabling TPM

1. Press <F9> during startup to enter the "System Utilities".
2. On the "System Utilities" page, click "System Configuration".
3. On the "System Configuration" page, click "BIOS/Platform Configuration (RBSU)".
4. On the "BIOS/Platform Configuration (RBSU)" page, click "Server Security".
5. On the "Server Security" page, click "Trusted Platform Module Options".
6. On the "Trusted Platform Module Options" page, select "SHA1 and SHA256" from the "Current TPM 2.0 Active PCRs" drop-down menu.
7. Press <F10> to save the changes.
8. Reboot the system.

Clearing TPM before reinstallation or decommission

Before reinstalling SSM on the device or before decommissioning, you must clear the TPM.

1. Press <F9> during startup to enter the "System Utilities".
2. On the "System Utilities" page, click "System Configuration".
3. On the "System Configuration" page, click "BIOS/Platform Configuration (RBSU)".
4. On the "BIOS/Platform Configuration (RBSU)" page, click "Server Security".
5. On the "Server Security" page, click "Trusted Platform Module Options".
6. On the "Trusted Platform Module Options" page, select "Clear" from the "TPM 2.0 Operation" drop-down menu.
7. Press <F12> to save the changes and exit.
8. Reboot the system.

Configuring RAID

These instructions are just for reference. For more information, refer to the HPE ProLiant DL380 Gen10 Server User Guide.

1. Press <F10> during startup to boot "Intelligent Provisioning".
2. Click "Smart Storage Administrator".
3. Select "Smart Array Controllers" and click "Configure".
4. Click "Create Array".
5. Select all hard disks and click "Create Array".
6. Click "Yes".
7. Select "RAID Level" "RAID 5" and click "Create Logical Drive".

Hardware initialization for the Dell R450

Disable the remote management interfaces

1. Press <F2> during startup to access "System Setup".
2. On the "System Setup Main Menu" page, click "iDRAC Settings".
3. On the "iDRAC Settings" page, click "Network".
4. In the "NETWORK SETTINGS" section, set "Enable NIC" to "Disabled".
5. To save the changes, click "Back", "Finish" and then "Yes".
6. Reboot the system.

Enable TPM

1. Press <F2> during startup to access "System Setup".
2. On the "System Setup Main Menu" page, click "System BIOS".
3. On the "System BIOS Settings" page, click "System Security".
4. On the "System BIOS Settings - System Security" page, set "TPM Security" to "On".
5. Click "TPM Advanced Settings".
6. On the "System BIOS Settings - System Security - TPM Advanced Settings" page, set "TPM2 Algorithm Selection" to "SHA256".

7. To save the changes, click "Back", "Finish" and then "Yes".
8. Reboot the system.

Clearing TPM before reinstallation or decommission

1. Press <F2> during startup to access "System Setup".
2. On the "System Setup Main Menu" page, click "System BIOS".
3. On the "System BIOS Settings" page, click "System Security".
4. On the "System BIOS Settings - System Security" page, set "TPM Hierarchie" to "Clear".
5. To save the changes, click "Back", "Finish" and then "Yes".

Hardware initialization for the SIMATIC IPC 427E

Enabling Trusted Platform Module (TPM) and USB Boot

1. Switch on the SSM Sensor and press <ESC> during the bootup to enter the startup menu.
2. Select "SCU". The "Setup Utility" window opens.
3. Switch to the "Security" tab to view options for TPM.
4. Assign the value "Available" for the "TPM Availability" parameter. If necessary, use <Enter> to set the value.
5. Switch to the "Boot" tab to view options for "USB Boot".
6. Assign the value "Enabled" to the "USB Boot" parameter.
7. To save the changes, press <F10>.
8. Press <Enter>.

Configuring enforce secure boot

1. Switch on the SSM Sensor and press <ESC> during the bootup to enter the startup menu.
2. Select "Secure Boot" Option. The "Administer Secure Boot" window opens.
3. Set the option "Enforce Secure Boot" to "Disabled".
4. To save the changes, press <F10>.
5. Press <Enter>.

Clearing TPM before reinstallation or decommission

Before reinstalling SSM on the device or before decommissioning, you must clear the TPM.

1. Switch on the SSM Sensor and press <ESC> during the bootup to enter the startup menu.
2. Select "SCU". The "Setup Utility" window opens.
3. Switch to the "Security" tab to view options for TPM.
4. Select the "Clear TPM" parameter and change the parameter to "[X]". Press <Enter> to set the value.
5. To save the changes, press <F10>.
6. Press <Enter>.

Storage setup

It is recommended to use RAID 1 for system disks, RAID 5 for data disks and RAID 10 for data disks of large installations. Prepare the server accordingly.

Table 5-6 Data storage options

Type	Hard disk	Available capacity	Advantage	Disadvantage
RAID 1	At least two	Does not exceed the total capacity of the smaller hard drives.	- Read performance doubles. - Provides data redundancy. If data is lost, it can be restored from the duplicate.	- Low disk utilization - High cost
RAID 5	At least three	75% of all hard drives	- High read and write performance - Check mechanism - High space utilization	- Adding more disks to a RAID 5 array leads to decreased security performance and data loss. - When more than one hard drive fail, data is lost.
RAID 10	At least four	50% of all hard drives	Both safety and speed	The disk usage is halved

RAID 1, RAID 5 and RAID 10 compared

5.3 Installation of software

5.3.1 Open firewall ports

Prepare the network prior to the SINEC Security Monitor Server installation to prevent problems during and after the installation.

Table 5-7 SINEC Security Monitor firewall policy requirements

Service/application	Protocol/port	Connection from (<>) to	Service/application	Protocol/port
OT NETWORK (physical SSM Sensor)		-	DMZ ROOM (SSM Server main NIC)	
UDP	UDP/Any	>>>>>>	UDP	UDP/9000
Description: VPN connection from the physical SSM Sensor to the SSM Server				
TCP	TCP/Any	>>>>>>	TCP	TCP/9000
Description: Certificate distribution for physical SSM Sensors				
Monitored clients (SSM Agent)		-	OT NETWORK (physical SSM Sensor)	
TCP	TCP/Any	>>>>>>	TCP	TCP/9000/5046
Description: Data transmission from the SSM Agent to the SSM Server through the physical SSM Sensor				
Monitored clients (SSM Agent)		-	DMZ ROOM (SSM Server main NIC)	

Service/application	Protocol/port	Connection from (<>) to	Service/application	Protocol/port
TCP	TCP/Any	>>>>>>	TCP	TCP/9000/5046
Description: Direct data transmission from the SSM Agent to the SSM Server				
Monitored clients (Agentless)		-	OT NETWORK (physical SSM Sensor)	
TCP	TCP/135	<<<<<<	TCP	TCP/Any
Description: Direct log collection from client PCs through the physical SSM Sensor in Agentless mode (Option 1)				
TCP	TCP/5986	<<<<<<	TCP	TCP/Any
Description: Direct log collection from client PCs through the physical SSM Sensor in Agentless mode (Option 2)				
Monitored clients (Agentless)		-	DMZ ROOM (SSM Server)	
TCP	TCP/135	<<<<<<	TCP	TCP/Any
Description: Direct log collection from client PCs through the SSM Server in Agentless mode (Option 1)				
TCP	TCP/5986	<<<<<<	TCP	TCP/Any
Description: Direct log collection from client PCs through the SSM Server in Agentless mode (Option 2)				
Network devices (SYSLOG)		-	OT NETWORK (physical SSM Sensor)	
SYSLOG	TCP/UDP/Any	>>>>>>	SYSLOG	TCP/UDP/514/6514
Description: Direct collection of network device syslog through the physical SSM Sensor If you customized the log reception ports on the Log Settings page, the corresponding firewall policies should be enabled between the physical SSM Sensor and the SSM Server.				
Network devices (SYSLOG)		-	DMZ ROOM (SSM Server)	
SYSLOG	TCP/UDP/Any	>>>>>>	SYSLOG	TCP/UDP/514/6514
Description: Direct collection of network device syslog through the SSM Server If you customized the log reception ports on the Log Settings page, the corresponding firewall policies should be enabled between the syslog client and the SSM Server.				
Users/client PCs		-	DMZ ROOM (SSM Server)	
HTTPS	TCP/Any	>>>>>>	HTTPS	TCP/8443
Description: User access to the SSM Server WBM				
OPC-UA	TCP/Any	>>>>>>	OPC-UA	TCP/4840
Description: Accessing diagnostic data on the SSM Server or SSM Sensor				

For an overview of all ports in use, refer to Communication ports (Page 21).

5.3.2 Standard accounts

The Linux operating systems are delivered as .img or .iso files. These operating systems have preconfigured standard user accounts for simplified installation and administration purposes.

During the installation process of the SINEC Security Monitor Server and SINEC Security Monitor Sensor, customized user accounts are created. Use these accounts for non-administrative activities that do not require root privileges.

Note

It is strongly recommended to change the passwords which will remain on the system during the system hardening process.

5.3 Installation of software

Table 5-8 Preconfigured standard user accounts

Login name	Initial password	Purpose	Change this password after installation
user	live	Administration account for the Debian live image	Not necessary
admin	admin	Administration account for the SINEC Security Monitor WBM	Yes
Customized user name	Customized password	Account for the SINEC Security Monitor Server	No
Customized user name	Customized password	Account for the SINEC Security Monitor Sensor	No

5.3.3 Software packages

Following table provides a detailed list of software installation and diagnostic packages, along with their corresponding SHA256 checksums and links to the relevant sections of the manual where each package is required.

No.	Package Name	Description	SHA256 Checksum	Relevant Manual Sections
1	ssm-4.9.0-serv-ertpm-prod.wic.tar.xz	Installation package for Server Software on physical hardware with TPM	32b3a7f561dbade2efbe0dd11e8585ea328136655d3239c0cdc1429cafe666f3	VMware with TPM (Page 95)
2	ssm-4.9.0-sensor-tpm-prod.wic.tar.xz	Installation package for Sensor Software on physical hardware with TPM	6ea8669102f25e699bf79e061892be22b24d8014074566284d8012de2b343b92	VMware with TPM (Page 95)
3	ssm-4.9.0-server-nesksim-prod.ova.tar.xz	OVA Image with Server Software for virtual environment (ESXi v7) without TPM via vCenter	0ba0d04394c76ab175767d128a362074d0a241d65f5a34bc92544a774df96c	VMware without vTPM (Page 104)
4	ssm-4.9.0-server-tpm-prod.ova.tar.xz	OVA Image with Server Software for virtual environment (ESXi v7) with TPM via vCenter	453d583ac17bb3b140d461fb5a9190c1b065b47653b5ba9f7743c24c9474d1bb	VMware with TPM (Page 95)
5	ssm-4.9.0-server-tpm-prod.swu.tar.xz	Upgrade package (.swu) for Security Monitor Server software from 4.9 to 4.9.1, both on physical hardware with TPM	453d583ac17bb3b140d461fb5a9190c1b065b47653b5ba9f7743c24c9474d1bb	Updating system components (Page 230)
6	ssm-4.9.0-sensor-tpm-prod.swu.tar.xz	Upgrade package (.swu) for Security Monitor Sensor software from 4.9 to 4.9.1, both on physical hardware with TPM	6c42c1fc578d0c703e6ec0faaad9bb1f6d5f9b6eed08279390d9e15137c8f49a	Updating system components (Page 230)
7	SINEC-Security-Monitor-Agent-4.9.0.exe	Installation file for Agent software	049acd1ff89ef12a70cf6c81b4679e6f3fe8cd146eace94e9350e1145ff164fc	Installing the SINEC Security Monitor Agent on a Microsoft Windows-based asset (Page 156)

5.3 Installation of software

8	SINEC-Security-Monitor-Agent-4.9.0-Update-x64.exe	Upgrade package for SSM Agent Software (x64) from V4.9 to V4.9.1	a08fa46018bde5be9a4bc10974592a21dc7e43b19c36e16be763201dff71ba09	SSM Agent update (Page 240)
9	SINEC-Security-Monitor-Agent-4.9.0-Update-x86.exe	Upgrade package for SSM Agent Software (x86) from V4.9 to V4.9.1	d6dd5872f16f8387735ce0d8e3c4d7efcd5e6f671874c9b18d6d409fe1ae9d0b	
10	SINEC-Security-Monitor-Agent-less-4.9.0.exe	Scripts for configuration of agentless data source(s)	76cbe927b770603b61c54b40e263e8778748430946b6e3a1b08c7f9e4e2f6b86	Preparing and adding a Microsoft Windows computer for agentless security log collection (Page 160)
11	coreshieldbasicmodel.xml	S2L2 diagnostic model for OPC-UA	a6c2d0f7e65da1b5390422af55aa7b7cb562173366116ae1b9721d4931b77b9	OPC UA interface (Page 210)
12	data_acquisition_for_diagnostics_and_analytics-v1.2.xml	S2L2 diagnostic model for OPC-UA	817d2d08433d9665542ce54ab9341d8b7b32c69c735b020393c49f3c3785449	
13	coreshieldrsumodel.xml	S2L2 diagnostic model for OPC-UA	2c40763c55d325550459fb02469825285f49d8fa306459ac9a6e8f303311e56d	
14	usermanagement.xml	S2L2 diagnostic model for OPC-UA	0802a91dc8ef0b6865f009ec4bf32963bf2e0ab4e58b266bf4ab4766728f03a2	
15	dada-v1.3.xml	DADA diagnostic model for OPC-UA	093b44f6dde9f4b4ba9c8cb1a6b43a8963a7b0b99b33482ea6a6140e5e5c7e42	
16	sinec-security-monitor-type-v1.2.xml	SSM shared diagnostic model for OPC-UA	b8422bb1a35596b5200e2e9932e978ace5557dd516ba0b593e914218e3584ac	
17	sinec-security-monitor-server-v1.4.xml	SSM server diagnostic model for OPC-UA	c9f24b501e09257c8cecb85768fa7c4b99c5c6ba80effe662bc3c8a9d88a16b5	
18	sinec-security-monitor-sensor-v1.4.xml	SSM sensor diagnostic model for OPC-UA	3aa13606fc3ae60a8ffbba8b334ed5a07f187b2bf00bbdd27298c562e60ad9a8	
19	sinec-security-monitor-sensor-operationsystem-v1.1.xml	SSM server enhanced system diagnostic model for OPC-UA	340e2002b1ef29fa6efb386ba2d0dd0568b2c24025689304839b31a5cabdb2a8	
20	sinec-security-monitor-server-operation-system-v1.1.xml	SSM sensor enhanced system diagnostic model for OPC-UA	1d06fce5d6c0ef034fb06f4f90918d2bda5eaf0cfaf2faaca012f97306270b5	

5.3.4 SHA256 checksums

Introduction

SINEC Security Monitor installation packages (.tgz, .zip, .img) are provided with a SHA256 checksum to ensure data integrity. These checksums are listed in the SINEC Security Monitor release notes of the respective SINEC Security Monitor version. It is strongly recommended to verify the checksums before proceeding with unpacking the archives.

Verifying a MD5 checksum on Microsoft Windows

1. Press [Windows] +[R].
The "Run" command window opens.
2. Run "cmd" with administrator privileges.
3. Use the `cd` command to navigate to the folder where the installation package is stored.
Example: Execute the command:
`cd downloads`
4. Generate the checksum. Execute the command:
`certUtil -hashfile {file name} SHA256`
5. Compare the generated checksum with the checksum in the release notes.

Verifying a SHA256 checksum on Linux

1. To generate a checksum for a specific installation package, execute the command:
`sha256sum {file name}.tgz`
Example:
`sha256sum /opt/ssm/{SINEC-Security-Monitor-Server-installation-package}.tgz`
2. Compare the generated checksum with the checksum in the release notes.

5.3.5 Verifying signatures of signed installation files

You can follow this procedure to verify the digital signature and certificate of an installation file.

1. Copy the `{installation file}.exe` file to the Microsoft Windows workstation.
2. Right-click the ".exe" file and select "Properties".
3. Select the "Digital Signatures" tab.
4. Select the signature signed as "Siemens AG" and click "Details".
5. Check for the message "This digital signature is OK". This message means the digital signature is valid.
6. Click "View Certificate" and select the "Certification Path" tab.
7. Check for the message "This certificate is OK". This message means the certificate is valid.

5.3.6 Preparing the USB flash drives

Scope

This section describes how to prepare two USB flash drives. The procedure is available for Microsoft Windows and for Linux.

- USB flash drive A (32 GB) for the Debian Live Image
- USB flash drive B (64 GB), exFAT formatted, to hold the compressed SINEC Security Monitor Server and the SINEC Security Monitor Sensor image files.

Note

- There are two different installation image packages, one for the SINEC Security Monitor Server and one for the SINEC Security Monitor Sensor. They should both fit together on one USB flash drive. These image files include the operating system S2L2 Linux.
- Make sure to label the USB flash drives appropriately to avoid confusion.

5.3.6.1 Software packages and applications needed

Table 5-9 Required software packages

Name	Description	Source
rufus.exe	Microsoft Windows helper tool for formatting and creating USB boot disks	Link: (https://rufus.ie/en/)
{debian-live}.iso	Image containing a Debian system that can be booted without modifying any files on your hard drive	Link: (https://cdimage.debian.org/debian-cd/current-live/amd64/iso-hybrid/)
{server image}.tar.xz	Compressed SINEC Security Monitor Server installation package	Official release
{sensor image}.tar.xz	Compressed SINEC Security Monitor Sensor installation package	Official release

NOTICE

Dangerous operating conditions due to intrusion of malicious software

When unauthorized end user devices are connected, malicious software can infiltrate the network and jeopardizes operational safety or system availability.

Only use USB storage media that have been checked and approved by your IT security department. Unsafe USB flash drives can spread malicious software in the network and destroy or damage the entire enterprise network environment or allow intruders in.

5.3.6.2 Preparing USB flash drive A

Prerequisites for USB flash drive A (Microsoft Windows)

- USB flash drive with minimum 32 GB space
- A Microsoft Windows PC
- Rufus (<https://rufus.ie>)
(Rufus is a free software that can convert an ISO image to a USB flash drive.)
- Debian Live Image (current version: `debian-live-12.5.0-amd64-standard.iso`) called '{debian-live}.iso' on the following pages.

Note

Keep the USB flash drive A in storage for decommissioning

The Debian live version on the USB flash drive can be used to overwrite the harddrives for decommissioning the servers/IPC's.

Prepare USB flash drive A (Microsoft Windows)

1. Copy `rufus.exe` and `{debian-live}.iso` to the computer.
2. Verify the SHA256 checksum of the ISO file. Refer to chapter SHA256 checksums (Page 82).
3. Plug the "USB flash drive A" into the computer.
4. Double-click `rufus.exe`.
5. Confirm the "User Account Control" window by clicking "YES".
6. Make the following selections:
 - For "Device", select the USB flash drive.
 - For "Boot selection", select the '{Debian-live}.iso' file in your local system.
 - Set "Persistent partition size" to the maximum size.
 - For "Partition scheme", select "MBR" (default).
 - For "Target system", select "BIOS or UEFI" (default).
 - For "Volume label", enter an appropriate name.
 - For "File system", select "FAT32 (Default)".
 - For "Cluster size", select "16 kilobytes (default)".
 - Click "Start".

The message "ISOHybrid image detected" appears.

7. Select "Write in ISO Image mode" and click "OK".
The message Warning: ALL DATA ON DEVICE WILL BE DESTROYED appears.
8. Click "OK" to prepare the flash drive.

9. Wait until the USB flash drive is "READY".
10. Unplug the USB flash drive.

Prerequisites for flash drive A (Linux)

- USB flash drive with minimum 32 GB space
- A Linux system
- From the SINEC Security Monitor software package: {debian-live}.iso file

Prepare flash drive A (Linux)

1. Log in to the Linux computer with `root` privileges.
2. Copy to the computer:
`cp {debian-live}.iso`
3. Verify the SHA256 checksum of the ISO file. Refer to chapter SHA256 checksums (Page 82).
4. Plug the "USB flash drive A" into the computer.
5. To identify the USB flash drive, execute the command:
`lsblk`
6. If necessary, unmount the USB flash drive with the command:
`umount /dev/sda`
7. To copy the {debian-live}.iso on to the "USB flash drive A", execute the command:
`dd if={debian-live}.iso of=/dev/sda bs=8M status=progress`

5.3.6.3 Preparing USB flash drive B

Prerequisites for USB flash drive B and the installation of the operating system

- USB flash drive with minimum 64 GB space, exFAT formatted
- Image files for SINEC Security Monitor Sensor and SINEC Security Monitor Server:
{Sensor image}.tar.xz, {Server image}.tar.xz

Note

Make sure the USB flash drive is large enough to hold both image files.

Format the USB flash drive B (Microsoft Windows)

1. Plug in the "USB flash drive B".
2. Right-click the "USB flash drive B" in the Windows Explorer and select "FORMAT" from the context menu.
3. In the "Format window", select "File System EXFAT", enter a "Volume label" (optional) and click "START".

4. Confirm the Warning message with "OK".
5. Wait until the message "Format Complete" appears.

Copy the image file to USB flash drive B (Microsoft Windows)

1. Copy the '{Sensor image}.tar.xz' and '{Server image}.tar.xz' files to the "USB flash drive B".
2. Verify the SHA256 checksums of the '{Sensor image}.tar.xz' and '{Server image}.tar.xz' files. Refer to chapter SHA256 checksums (Page 82).

Format the USB flash drive B (Linux) and copy the image files

Prerequisite: exFAT is included and supported by the Linux operating system.

1. Plug in the "USB flash drive B".
2. To find out the name of your USB flash drive, execute the command:
`lsblk`
The easiest way to identify the device is by its size. The device name will look like `/dev/sdx`, and the corresponding disk partition is `'/dev/sdx1'`.
(x = a, b, c, d, etc.)
3. If necessary, unmount the device. Execute the command:
`sudo umount /dev/sdx1`
4. Format the USB device with the exFAT file system. Execute the command:
`sudo mkfs.exfat -n "USB flash drive B" -s 2048 /dev/sdx`
5. Create a mount point for the USB flash drive. Execute the command:
`mkdir /mnt/usb1`
6. To copy the '{Sensor image}.tar.xz' and '{Server image}.tar.xz' files to the USB flash drive B, execute the commands:
`cp {Sensor image}.tar.xz /mnt/usb1`
`cp {Server image}.tar.xz /mnt/usb1`
7. Verify the SHA256 checksums of the '{Sensor image}.tar.xz' and '{Server image}.tar.xz' files.
`sha256sum /mnt/usb1/{Sensor image}.tar.xz`
`sha256sum /mnt/usb1/{Server image}.tar.xz`

5.3.7 Installing the SSM Server software on a physical hardware

Scope

SINEC Security Monitor software runs on S2L2 Linux. This chapter describes the installation of the SINEC Security Monitor Server software and SINEC Security Monitor Sensor software including S2L2 Linux. Debian Linux is used during the installation process to run the installation.

Name	Description
Debian	Enterprise Linux distribution based on freely available Linux source code
CoreShield S2L2 Linux	Industrial grade Linux distribution from Siemens including the CoreShield Security Stack

On-site installation

The installation of the operating system via USB flash drive requires on-site installation. This option is described in this documentation.

SINEC Security Monitor Server hardware interfaces



Interface	Description
H1	Interface of the SINEC Security Monitor Server for communication with the SINEC Security Monitor Sensor or the SINEC Security Monitor Agent; access to the SINEC Security Monitor web page and diagnostics communication
H2	Optional access to the SINEC Security Monitor web page and diagnostics communication
M1	Network traffic mirror port
M2	Optional network traffic mirror port

Figure 5-2 Interfaces of the SINEC Security Monitor Server hardware

5.3.7.1 Software packages and applications needed

Table 5-10 Required software packages

Name	Description	Source
USB flash drive A	Contains bootable Debian Live Image	Refer to chapter Preparing USB flash drive A (Page 84).

USB flash drive B	Contains installation packages for the SINEC Security Monitor Server and the SINEC Security Monitor Sensor	Refer to chapter Preparing USB flash drive B (Page 85).
{server image}.tar.xz	Compressed SINEC Security Monitor Server installation package	Official release
Server-{Instance ID}.zip	Compressed activation file for the SINEC Security Monitor Server	During the installation process for the SINEC Security Monitor Server, this file needs to be requested from your Siemens sales partner.

5.3.7.2 Installing the operating system

Prerequisites for the installation of the SINEC Security Monitor Server

- USB flash drive A and B
- Basic knowledge of Linux administration is required

Installation of the SINEC Security Monitor Server

1. Insert the "USB flash drive A" and "USB flash drive B".
2. Boot the server and press [F11].
3. Select to boot from the "USB flash drive A".
4. After booting up, switch the user to the root account. Execute the command:
`sudo su`
5. Identify the names of the USB flash drives. Execute the command:
`lsblk`
6. Create a mount point for the USB flash drive. Execute the command:
`mkdir /mnt/usb1`
7. To mount the USB flash drive, execute the command:
`mount /dev/sdb1 /mnt/usb1/`
'/dev/sdb1 (USB flash drive B)' is an example for USB flash drive names.

Note

Always mount the partition (e.g., /dev/sdb1), not the raw device (e.g., /dev/sdb), to avoid errors.

8. Go to the USB flash drive B directory /mnt/usb1/. Execute the command:
`cd /mnt/usb1`
To unzip '{server image}.tar.xz', execute the command:
`tar --no-same-owner -xvf {server image}.tar.xz`
9. Copy the '{server image}' to the server disk partition. Execute the commands:
`cd /mnt/usb1/`
`dd if={server image} of=/dev/sda bs=4M status=progress`
10. Remove "USB flash drive B" and reboot the server.

After the reboot, the configuration program starts with an optional disk check.

5.3.7.3 Installation precheck of the disk (optional)

This procedure provides valuable information before starting the installation:

- Disk space utilization by other applications
- Detection of bad sectors on the disk that might need repair

This step is optional. Consider that this step might take a long time, for example 1.5 hours on a 300 GB drive.

1. After the reboot, the "Check disk (optional)" window appears.
2. To start the disk check, click "Yes".

5.3.7.4 Configuring the SINEC Security Monitor Server

Configure the SINEC Security Monitor Server

The configuration program leads you through the network setup of the SINEC Security Monitor Server. The last step before the initialization offers an opportunity to review and modify settings.

For assistance with selecting the correct IP address, refer to chapter Access to the WBM (Page 67).

NOTICE

Mal working of the SINEC Security Monitor System

Bad synchronization of network time, network time zone and hardware clock on the assets and devices of the SINEC Security Monitor System can lead to communication failure during configuration and operation.

It is recommended to use a NTP server for time synchronization. If you do not use a NTP server, ensure that the RTC (hardware clock) on all devices is set to the correct time and time zone, so that the SINEC Security Monitor Sensors can be detected by the SINEC Security Monitor Server.

Note

Connect all network cables before starting this configuration

The configuration of the network interfaces does not work without connected network cables. Connect all required ports to a switch.

1. After the "Check disk (optional)" window, the configuration program continues.
2. Review the list of network interfaces on the device. Select the network interface for the H1 port of the SINEC Security Monitor Server and click "Ok".

3. Enter the IP address for the H1 network interface and click "Ok".
4. Enter the network mask for the H1 network interface and click "Ok".
5. Enter the gateway address for the H1 network interface and click "Ok". If no gateway is available, click "Ok" to continue.
6. To configure the IP address of other network interfaces (NICs), click "Yes". If it is not necessary to configure other network interfaces, click "No".
7. Select the network interface that is used as a monitor port M for the integrated sensor. You can select no network interface or multiple network interfaces and click "Ok".
8. Configure the NTP server address to synchronize the system time with a remote NTP server. At the "Configure NTP server" prompt, you can decide:
 - To use the SSM Server (WBM) as the NTP server and set the IP address automatically to 127.127.1.0 , click "Yes".
 - To use a third-party NTP server, click "No".
Enter the IP address of the NTP server and click "Ok".

Note

If you don't use a NTP server, ensure that the RTC (hardware clock) of all devices is set to the correct time and time zone, so that the SSM Sensors can be detected by the SSM Server.

9. Select your time zone and click "Ok".
For a greater choice of time zones, select "More".
10. Enter a hostname for this system and click "Ok".
The hostname must be a single word without spaces. Example: ssm-server
11. Create a user account for administrative activities, without root privileges
Enter a full name for the user and click "Ok".
12. Enter a password for the new user and click "Ok".
Minimum password requirements:
 - Uppercase and lowercase letters
 - Numbers
 - Special characters
 - 20 characters
13. Re-enter the password for the new user and click "Ok".
14. Check the "Current Configuration" and click "Ok" to continue.
15. To confirm the configuration, select "Save" and click "Ok".
To modify the configuration, select "Modify" and click "Ok".
16. Check the "Current Configuration" and click "Ok" to continue.
17. Wait until the end of the SINEC Security Monitor Server initialization.
18. Click "Ok" and the system reboots.

See also

Configuring the SINEC Security Monitor Sensor (Page 110)

Link: (<https://wiki.debian.org/NetworkConfiguration>)

Cancelling the configuration program

If you click "Cancel" during the configuration program the "Exit Operation" window appears:

- Click "No" to return to the configuration program.
- Click "Yes" to exit the configuration program and continue the boot process.
To re-enter the configuration program after cancelling, simply reboot the device.

5.3.7.5 Logging in to the SINEC Security Monitor System

Note**Use Google Chrome browser**

It is recommended to use Google Chrome browser (version 85 or higher).

Log in to SINEC Security Monitor System on the SINEC Security Monitor Server

1. Open the SINEC Security Monitor Server URL in Google Chrome.
`https://<IP address>:8443/login`
2. Enter the user name. The initial user name is: admin
3. Enter the password. The initial password is: admin
4. If prompted, change your password.
5. Click "Login".

5.3.7.6 Requesting a SINEC Security Monitor license for the SINEC Security Monitor Server

Note: It is recommended to use Google Chrome browser (version 85 or higher).

An overview of the available licenses can be found in section Components and licenses (Page 44).

Requesting a SINEC Security Monitor Server license:

1. Log in to the WBM.
2. Select the "System" > "License" page.
3. Click "Export request file".

4. To request a license, send the `Server-smcRequestBundle-{Instance ID}.zip` file to the following email address:
`activation-ssm.industry@siemens.com`
 Make sure to include the following information from your order notification in your email:
 - Sold-To/Install: <>
 - License Quote: <>
 - P.O.-Number: <>
5. In case you ordered more than one license in your purchase order please state which of them you want to activate with this request.
 You will receive an activation file for the server via email.

Activating the SINEC Security Monitor Server license

The file format of the activation file is `Server-{Instance ID}.zip`

Example: `Server-44163cf7dc711c87750.zip`

The instance ID is unique for each SINEC Security Monitor Server.

1. Log in to the WBM.
2. When this is the first login on this WBM/SSM Server, the "License" page is displayed automatically. If not, select the "System" > "License" page.
3. Click "Browse" and select the `Server-{Instance ID}.zip` file containing the license.
4. Click "Upload".
5. The system reboots. This takes 3-5 minutes.
6. Check the "System" > "License" page again for the result.
 Verify that "Start date" and "End date" are filled in and are displayed with your time zone added in brackets. For example: 2024-06-25 (UTC+02:00)

5.3.7.7 Verifying the installation status of SINEC Security Monitor Server

1. Log in to the WBM.
2. Select the "System" > "Diagnostics" menu to open the "Diagnostics" page.
3. Check the status of all SINEC Security Monitor Server containers.
 A green "●" icon indicates the status is "healthy".

Table 5-11 SINEC Security Monitor Server containers

Container name	Function	Status
server.gateway	Web portal service	Healthy
server.logstash	Rawlog filter	Healthy
server.os	Rawlog storage (OpenSearch)	Healthy
server.pg	User configuration and security event storage	Healthy
server.redis	Data cache	Healthy
server.ca	Asset analysis	Healthy
server.si	Security event processing	Healthy

Container name	Function	Status
server.collector	Data source and SINEC Security Monitor Sensor management	Healthy
server.logforward	Security events and rawlog forwarding	Healthy
server.cm	Certificate Management	Healthy
sensor.logagent	Rawlog collection	Healthy
sensor.prober	Analysis of asset network traffic	Healthy
sensor.zeek	Network traffic analysis	Healthy
sensor.suricata	Network traffic analysis and generation of security events	Healthy

5.3.7.8 Adding the internal SSM Sensor

The internal SSM Sensor is installed as a part of the SSM Server. However, to be able to use it as a SSM Sensor, you must add the internal SSM Sensor manually on the "Configuration" > "Sensor" page.

Refer to chapter Adding Sensors (Page 113) for instructions.

5.3.7.9 Configuring the system time

Ensure that the system time of the SSM Server is correct

Note

This step is mandatory, as time differences in the SINCE Security Monitor System lead to malfunctioning.

1. After the SSM Server's installation, execute the command to verify the system time. Use the "operator" user account which was created during the SSM Server's configuration.

```
ssmctl-client system get_system_time --host_ip localhost --service_module server
```
2. If the result of the `get_system_time` command doesn't match the local clock of the computer, execute the command to adjust the SSM Server's system time accordingly:

```
ssmctl-client system set_system_time --date_time "2024-06-24 15:04:05" --host_ip localhost --service_module server
```

Examples of supported time formats (date: yyyy-mm-dd; time: hh:mm:ss; 00:00:00-23:59:59)

- "2024-06-24"
- "2024-06-24 15"
- "2024-06-24 15:04"
- "2024-06-24 15:04:05"

Purpose

Note

- The time zone is set during the SINEC Security Monitor configuration. Change the time zone on the top of the page if required.
 - If no NTP server is available, the default value is 127.127.1.0.
-

During the SINEC Security Monitor Server/Sensor installation process, you can set the time zone and configure a NTP server.

Consequences if the SINEC Security Monitor Server system time is changed in the WBM:

- For "Local clock":
The system time of the SINEC Security Monitor Sensor will be automatically synchronized with the system time of the SINEC Security Monitor Server.
- For "External NTP server":
The system times of SINEC Security Monitor Server and SINEC Security Monitor Sensor will be automatically synchronized with the third-party NTP server.

Configuring the system time and add NTP server addresses

1. Log in to the WBM.
2. Select the "Configuration" > "System" menu.
3. Click the "System Time" tab.
4. Select "Local clock" or "External NTP server".
5. Click the "System Time" field.
6. You can set the system time to "Local clock" or "External NTP server".
7. If necessary, change the NTP server IP address.
You can also add more NTP server IP addresses.
8. Click "Save".
Wait for several minutes for the execution of the changes.

5.3.7.10 Finding the SINEC Security Monitor version number

If it is necessary to get the version number of a SINEC Security Monitor instance for any reason, follow these steps.

1. Log in to the WBM.
2. The SINEC Security Monitor version number is located at the bottom of the menu bar on the left side of the page.
3. To see the full version number, move your mouse over the version number.

5.3.8 Installing the SSM Server software in a virtual environment (ESXi)

5.3.8.1 Software requirements for SSM Server on Virtualization Platforms

The software requirements should ensure that the SINEC Security Monitor Server runs properly on the virtualization platform.

The table below lists the recommended VM's software requirements for the SSM Server virtualization installation:

Table 5-12 VM software requirements

Type	Version	Description
ESXi	V7.0.3 or later	ESXi is installed on physical hardware. ESXi is used to manage VMs with the deployed SSM Server.
vCenter	V7.0.3 or later	vCenter is installed on the physical hardware. vCenter is used to manage multiple ESXi hosts. The release image comes with nESK-SIM, a SSM software trust anchor, eliminating the need for additional reliance on the vTPM functionality.
SSM Server	V4.9.0	SSM Server's virtualized image file as an OVA (Open Virtualization Appliance)

5.3.8.2 VMware with TPM

Notes on reusability and portability

You can import the compiled VM images in OVA format into ESXi as templates and activate them using licenses.

To protect SINEC Security Monitor's product integrity, a virtual machine that has been activated with licenses, cannot be copied (exported/imported) to any other ESXi.

VMware deployment pre-requisites

To ensure a seamless operation of the SSM Server on the VM it is essential to configure specific and crucial settings on the VMware platform.

Specific settings on the VMware platform that need to be configured:

- vTPM configuration
- vSwitch configuration
- SSM Server's image deployment

vTPM configuration overview

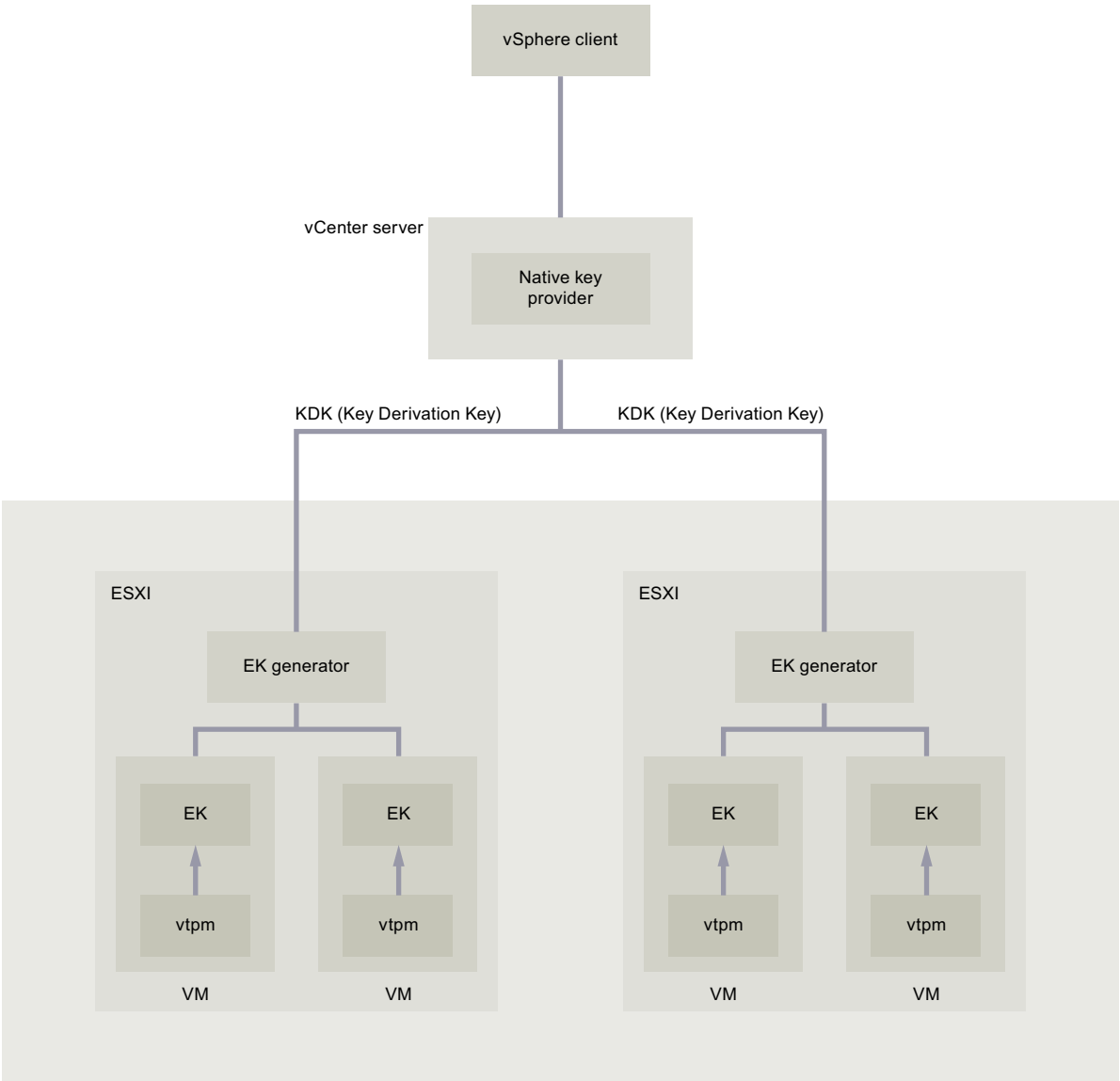
The virtualized SINEC Security Monitor uses VMware's vTPM to replace the physical TPM 2.0 chip of the SSM Server hardware.

When added to a virtual machine, a vTPM enables the guest operating system to create and store private keys.

5.3 Installation of software

vTPM relies on an endorsement key (EK) for secure encryption and decryption. The EK is sourced from a key provider, which is provided and distributed uniformly by the vSphere platform.

The diagram below illustrates the distribution process.



Main Components	Description
Native Key Provider	The Native Key Provider included in the vSphere editions and does not require an external key server. The Native Key Provider is a component that offers a root key and enables encryption technologies, including vTPMs. It plays a vital role in securing the virtual machine data.

5.3 Installation of software

KDK (Key Derivation Key)	The KDK serves as the root key within the Native Key Provider. It is responsible for encrypting and securing the data of virtual machines. Additionally, it facilitates key derivation, ensuring the generation of unique and secure keys for various cryptographic operations.
EK (Endorsement Key)	The EK serves two primary purposes: • The EK helps to uniquely identify a vTPM. • The EK serves as a root of trust for other keys that the vTPM generates for usage in encryption and digital signing. The EK consists of a pair of public and private keys, with the root key provided by Native Key Provider. The EK for all virtual machines under the same vCenter Server is derived from this root key. When a virtual machine is instantiated, the EK is generated and stored in the vTPM. Within the same vCenter, each virtual machine's EK is guaranteed to be unique. Since vTPM is an essentially software component, without additional protective measures, cloning or moving a virtual machine will result in the vTPM, including the EK, remaining unchanged and functioning properly.

Figure 5-3 vTPM component relationship diagram

vTPM configuration steps

Note

You must do this configuration only once for each vCenter

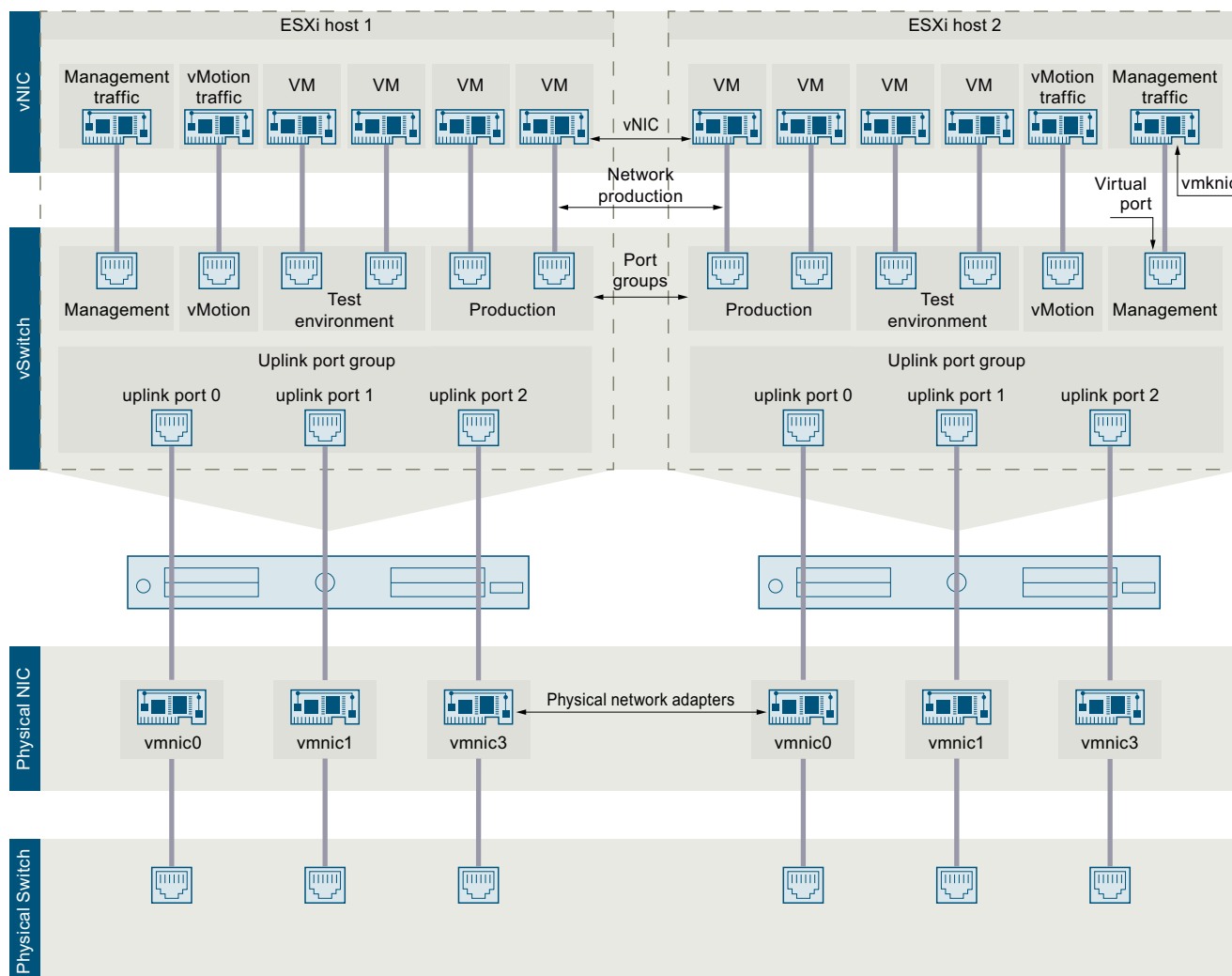
1. Log in to vCenter using valid credentials.
The homepage of the vCenter Server is displayed.
In this example, the vCenter's homepage address is: vcenter01.subdomain.company.com
2. On the Configure tab, open the "Security" > "Key Providers" menu.
Open the "ADD" dropdown list and select "Add Native Key Provider".
3. Enter a valid name and click "ADD KEY PROVIDER".
In this example, the Native Key Provider name is "SSM_KMS".
4. Click "BACK UP".
5. Set a checkmark at "Protect Native Key Provider data with password (Recommended)" and click "BACK UP KEY PROVIDER".
6. Enter a strong password and verify the password.
Set a checkmark at I have saved the password in a secure place and click "BACKUP KEY PROVIDER".
7. Verify the new key provider "SSM_KMS". Ensure that the type is "Native" and status is "Active".

vSwitch configuration overview

The vSwitch configuration is only necessary, if you want to use the SSM Server for network traffic monitoring.

For a network traffic mirror port, a physical NIC on physical hardware is required. You can configure this port in a separate step.

The vSphere Standard Switch is an abstracted network device that is very similar to a physical Ethernet switch. It can bridge traffic internally between virtual machines in the same VLAN and link to external networks.



Main components Description

vNIC These are network adapters present within the virtual machines.

Port Groups These are groups of standard ports that belong to a vSwitch. Each port group on a standard switch is identified by a unique network label specific to the current host.

Physical NIC These are physical network adapters present in the physical machine.

Figure 5-4 vSphere standard switch architecture

vNICs in virtual machines connect to port groups on the vSwitch. Every port group uses one or more physical NICs to handle their network traffic.

vSwitches are an excellent choice for environments that require flexible virtual networking, efficient management, and cost-effective networking solutions. They are particularly well-suited for data centers, cloud computing, VDI, and testing and development environments.

vSwitch configuration steps

Follow these steps to create a network traffic mirror port.

Step 1: Log in and locate ESXi Host

1. Log in to the vCenter.
2. On the left, all devices are listed. Locate the ESXi host for example by its IP address.
In this example, the IP address is 192.168.100.109.

Step 2: Configure Physical Adapter

1. Select the "Configure" tab.
2. Open the "Networking" > "Physical adapters" menu.
3. Note an available physical adapter (e.g. "vmnic2"). This adapter is used for network traffic monitoring and as a mirror port.

Step 3: Create and configure Virtual Switch

1. Open the "Networking" > "Virtual switches" menu.
2. Click "ADD NETWORKING".
The "Add Networking" page opens.
3. For the "Select Connection type" step, select the "Virtual Machine Port Group for a Standard Switch" option and click "NEXT".
4. For the "Select Target Device" step, select "New standard switch".
5. In the "MTU (Bytes)" field, enter "1500" and click "NEXT".
6. For the "Create a Standard Switch" step, assign a free physical network adapter to the new switch.
In the "Assigned adapters" section, click the "+" icon.
Click "NEXT".
7. On the "Add Physical Adapters" to the "Switch" page, all properties of the network adapters are displayed.
Select a network adapter. In this example "vmnic2" is selected.
Click "OK".
8. Back on the "Create a Standard Switch" step, review and validate the selected network adapter and all its properties.
The network adapter is added to the "Active adapters" list.
In this example the network adapter is: "New (vmnic2)".
Click "NEXT".
9. On the "Physical Network Adapters Warning" page, click "OK".
10. For the "Connection settings" step, enter a valid "Network label".
In this example, the label is: "SSM_Monitor"
The "SSM_Monitor" network adapter is only used to monitor traffic.
Click "NEXT".
11. For the "Ready to complete" step, review all settings of the new standard switch and click "FINISH".

Step 4: Verify and edit vSwitch Settings

1. Select the "Configure" tab.
 - Open the "Networking" > "Virtual switches" menu.
 - Verify that the newly added standard switch is listed.
 - In this example, the new standard switch is "vSwitch2".
 - Expand the standard switch and click "EDIT".
2. On the "vSwitch - Edit Settings" page, review the "Properties" step.
 - The value for "MTU (Bytes)" must be "1500".
 - Click "OK".
3. For the "Security" step, set the "Promiscuous mode" to "Accept". Click "OK".
4. For the "Traffic shaping" step, make the following changes:
 - Set the "Status" to "Disabled".
 - Set the "Average bandwidth (kbit/s)" to "100000".
 - Set the "Peak bandwidth (kbit/s)" to "100000".
 - Set the "Burst size (kb)" to "102400".
 - Click "OK".
5. For the "Teaming and failover" step, set "Load balancing" to "Route based on originating virtual port" and click "OK".

You edited all necessary settings.

VMware deployment**OVA template**

The OVA template file is a standardized format used in the VMware platform to create and deploy virtual machines. It also supports dynamic configuration injection, where the final OVA file is generated by dynamically incorporating client parameters.

Build an OVA template

1. Login to vCenter using valid credentials.
2. On the homepage, select the ESXi host on the left side of the window.
In this example, the ESXi host is: 192.168.100.109
3. On top of the page, open the "ACTIONS" > "Deploy OVF Template" menu.
The "Deploy OVF Template" page opens.
4. For the "Select an OVA template" step, select the "Local file" option.
Click "UPLOAD FILES" and click "NEXT".

5.3 Installation of software

5. Browse the local file system and select a valid SSM v4.9.0 server development OVA file.
In this example, the file is: `ssm-4.9.0-Server-tpm-RC6-development.ova`
Click "NEXT".
6. For the "Select a name and folder" step, select a target location for the virtual machine.
In this example, the folder in `vcenter01.subdomain.company.com` is: `DEV`
Click "NEXT".
7. For the "Select a computer resource" step, select the destination computer resource for this operation.
In this example, the computer resource is: `192.168.100.109` in the `DEV TPM` folder.
When the "Compatibility checks succeeded" message is displayed in the "Compatibility" field, click "NEXT".
8. For the "Review details" step, review the extra details.
When everything is ok, click "NEXT".
9. For the "Select storage" step, select the storage for the configuration and disk files.
Set "Select virtual disk format" to "Thick Provision Lazy Zeroed".
Review all storage details, for example: Capacity, Provisioned, Free, Type
Click "NEXT".
10. For the "Select networks" step, select a destination network for each source network, where network traffic should be monitored.
For example, set the target destination network to: `SSM_Monitor` (the network label of the newly added vSwitch).
Click "NEXT".
11. For the "Ready to complete" step, review all selections.
Click "FINISH".
12. After configuration, select the "Monitor" tab.
Open the "Tasks and Events" > "Tasks" menu.
Check the progress and status for relevant tasks, respectively "Deploy OVF template" and "Import OVF package".
Ensure that both tasks are 100% executed successfully without error.
Note that the whole process will take approximately 2 hours to complete.

Adjust virtual machine settings

In the next steps, you configure the virtual machine settings.

Start by accessing the "Edit Settings" page:

1. On the left plain, open `vcenter01.subdomain.company.com > DEV > 192.168.100.109`.
2. In the right window, click the "VMs" tab.
Select "Virtual Machines".
3. Select the "SSM-4.9.0-VM".
4. Right-click "SSM-4.9.0-VM" and select "Edit Settings" from the context menu.

Adjust virtual hardware settings

For the recommended hardware settings, refer to chapter Hardware requirements for SSM Server on Virtualization Platforms (Page 74).

Note

Adjust the virtual hardware settings based on the actual memory and storage capacity.

"CPU: 16, Memory: 96 GB, Hard Disk: 2048 GB" are the recommended minimum hardware requirements.

1. On the "Edit Settings" page, select the "Virtual Hardware" tab.
Adjust virtual hardware settings, for example CPU, Memory, Hard Disk space.
Click "OK" to save.

Configure vTPM

1. On the "Edit Settings" page, click "ADD NEW DEVICE".
Open the "Other Devices" > "Trusted Platform Module" menu.
2. Expand "Security Devices - TPM".
Verify that the value "Present" is displayed.
Click "OK" to save.

Add Network Adapters

Add a new network adapter to collect data and access the WBM.

Note

- You must provide relevant network info and specify which network will be used to collect data and access the WBM.
 - The amount of new network adapters depends on your actual setup and environment.
 - Follow the steps below to add multiple new network adapters if required.
-

1. On the "Edit Settings" page, click "ADD NEW DEVICE".
Open the "Network" > "Network Adapter" menu.
2. Expand "New Network" and select the target network.
3. In this example, the VLAN is: PROD
Click "OK" to save.

Launch the SSM Server installation process

1. Click the "Execute >" icon. The VM is switched on.
The installation process of the virtual SSM Server has launched.
2. The "Check disk (optional)" window appears.
From here, follow the SSM Server configuration routine.
Refer to chapter Configuring the SINEC Security Monitor Server (Page 89).

5.3.8.3 VMware without vTPM

Notes on reusability and portability

You can import the compiled VM images in OVA format into ESXi as templates and activate them using licenses.

To protect SINEC Security Monitor's product integrity, a virtual machine that has been activated with licenses cannot, be copied (exported/imported) to any other ESXi.

VMware deployment pre-requisites

To ensure a seamless operation of the SSM Server on the VM it is essential, to configure specific and crucial settings on the VMware platform.

Specific settings on the VMware platform that need to be configured:

- vSwitch configuration
- SSM Server's image deployment

The basic virtual hardware configurations that need to be considered as well, are among others for example CPU, memory and hard disk size.

vSwitch configuration overview

The vSwitch configuration is only necessary, if you want to use the SSM Server for network traffic monitoring.

For a network traffic mirror port, a physical NIC on physical hardware is required. You can configure this port in a separate step.

- vSwitch configuration is carried out using the ESXi Client. The configuration commands are ultimately sent to the ESXi host for execution, indicating that the vSwitch configuration is performed by the ESXi host.
- vNICs in virtual machines connect to port groups on the vSwitch. Every port group uses one or more physical NICs to handler their network traffic.
- vSwitches are an excellent choice for environments that require flexible virtual networking, efficient management, and cost-effective networking solutions. They are particularly well-suited for data centers, cloud computing, VDI, and testing and development environments.

Main components

- **vNIC**
vNICs are network adapters present within virtual machines.
- **Port groups**
Port groups are groups of standard ports that belong to a vSwitch. Each port group on a standard switch is identified by a unique network label which is specific to the current host.
- **Physical NIC**
Physical NICs are physical network adapters present in the physical machine.

vSwitch configuration steps

Add a new vSwitch

1. Log in to the "ESXi Host Client" using valid credentials.
2. On the Navigator tree on the left side, select the "Networking" menu.
3. On the "Networking" menu, select the "Virtual switches" tab.
4. Click the "Add standard virtual switch" button.
5. In the "Add standard virtual switch" window, enter a valid "vSwitch Name", for example: vSwitch2
6. In the "Security" section, select:
 - For "Promiscuous mode", select "Reject"
 - For "MAC address changes", select "Accept"
 - For "Forged transmits", select "Accept"Click on "ADD" button.
7. The system replies a message that the virtual switch was successfully created.

Add New Port Groups

1. On the "Networking" menu, select the "Port groups" tab.
2. On the "Port groups" tab, click the "Add port group" button.
3. In the "Add port group" window, enter a valid name, for example: SSM_TEST
4. In the "Security" section, select:
 - For "Promiscuous mode", select "Inherit from vSwitch"
 - For "MAC address changes", select "Inherit from vSwitch"
 - For "Forged transmits", select "Inherit from vSwitch"

Note: If the added "Port group" is used to monitor network traffic, "Promiscuous mode" should be set to "Accept".
5. Check and validate the relationship between the added vSwitch and the port group in the "vSwitch topology" section.

VMware deployment

nESK-SIM introduction

nESK-SIM can be regarded as a software trust anchor, comparable to vTPM. It is a software based TPM emulator and integrated into the OVF image. The SSM System uses the UTA API, in the same way as with a TPM, to retrieve encrypted information from nESK-SIM.

nESK-SIM offers a more flexible usage environment because it does not rely on the vCenter server-managed ESXi clusters. It only requires the ESXi host environment.

Build a virtual machine from a OVA Template

The OVA template file is a standardized format used in the VMware platform to create and deploy virtual machines. It also supports dynamic configuration injection, where the final OVA file is generated by dynamically incorporating client parameters.

Instruction steps

1. Obtain the OVA images from Siemens.
2. Log in to the ESXi Client with valid credentials and click "Create/Register VM". The "New virtual machine" window opens.
3. In the "1 Select creation type" section, select "Deploy a virtual machine form an OVF or OVA file" and click "NEXT".
4. In the "2 Select OVF and VMDK files" section, enter a name for the virtual machine, for example: SSM_490_SERVER.
5. Select a valid SSM v4.9.0 Server development OVA file, for example: ssm-4.9.0-Server-tpm-RC7-development.ova
Click "NEXT"
6. In the "3 Select storage" section in the "Standard" area, select the storage for the configuration and disk files.
Check all storage details, for example:
 - Capacity
 - Thin Provisioned
 - Free
 - Type
7. In the "4 Deployment options" section, select an applicable network segment or a zone from the "Network mappings" drop-down list.
8. For "Disk provisioning", select "Thin" and uncheck "Power on automatically". Click "NEXT".
9. In the "5 Ready to complete" section, review all selections and settings. If no changes are necessary, click "FINISH".
10. Navigate to the "Recent tasks" section, and check the progress and status for the relevant tasks.
Pay special attention to "Upload {OVA file}" and "Create VM". Ensure both are 100% executed successfully without error.
The entire process will take about 20 minutes to complete. The duration depends on the actual network environment.

Adjust virtual machine settings

In the next steps, you configure the virtual machine settings as specified in the table "VM hardware requirements".

Start by accessing the "Edit Settings" page:

1. On the left plain, open your machine.
2. In the right window, click the "VMs" tab.
Select "Virtual Machines".

3. Select the "SSM_490_SERVER".
4. Right-click "SSM_490_SERVER" and select "Edit Settings" from the context menu.

Adjust virtual hardware settings

For the recommended hardware settings, refer to chapter Hardware requirements for SSM Server on Virtualization Platforms (Page 74).

Note

"CPU: 16, Memory: 96 GB, Hard Disk: 2048 GB" are the recommended minimum hardware requirements.

Adjust the virtual hardware settings based on the actual memory and storage capacity.

1. On the "Edit Settings" page, select the "Virtual Hardware" tab.
Adjust virtual hardware settings, for example CPU, Memory, Hard Disk space.
Click "OK" to save.

Add Network Adapters

Add a new network adapter to collect data and access the WBM.

Note

- You must provide relevant network info and specify which network will be used to collect data and access the WBM.
 - The amount of new network adapters depends on your actual setup and environment.
 - Follow the steps below to add multiple new network adapters if required.
-

1. On the "Edit Settings" page, click "ADD NEW ADAPTER".
In the "Network Adapter 1" menu, select the added port group name. In the chapter VMware deployment pre-requisites (Page 104), the suggested name was: SSM_TEST
2. Check the "Connect" option and click "SAVE".

Launch the SSM Server installation process

1. Click "> Power on". The installation process of the virtual SSM Server is launched.
2. The "Check disk (optional)" window appears.
From here, follow the SSM Server configuration routine.
Refer to chapter Configuring the SINEC Security Monitor Server (Page 89).

5.3.9 Installing the SINEC Security Monitor Sensor

SINEC Security Monitor Sensor interfaces



Interface	Description
H1	Host interface for communication with SINEC Security Monitor Server (H1 port)
H2	Optional
M	Network traffic mirror port

Figure 5-5 Interfaces of the SIMATIC ICP 427E

5.3.9.1 Software packages and applications needed

Table 5-13 Required software packages

Name	Description	Source
USB flash drive A	Contains bootable Debian Live Image	Refer to chapter Preparing USB flash drive A (Page 84)
USB flash drive B	Contains installation packages for the Linux images for the SINEC Security Monitor Server and the SINEC Security Monitor Sensor	Refer to chapter Preparing USB flash drive B (Page 85)
{sensor image}.tar.xz	Compressed SINEC Security Monitor Sensor installation package	Official release
Sensor-{Instance ID}.zip	Compressed activation file for the SINEC Security Monitor Sensor	During the installation process of the SINEC Security Monitor Sensor, this file needs to be requested from your Siemens sales partner.

Required installation packages and applications

Note

The compressed SINEC Security Monitor Sensor installation package is suitable for all hardware recommendations for the SINEC Security Monitor Sensor.

5.3.9.2 Installing the operating system on the SINEC Security Monitor Sensor

Prerequisites

- USB flash drive A and USB flash drive B
For the preparation of the USB flash drives, refer to chapter Preparing the USB flash drives (Page 83)
- Basic knowledge of Linux administration is required

Installation of the SINEC Security Monitor Sensor

Note

This installation instruction is specific to the SIMATIC IPC 427E.

1. Insert the USB flash drive A and USB flash drive B.
 2. Boot up the sensor and press <ESC>. The Remote View screen opens.
 3. On the Remote View screen, click "BOOT MANAGER".
 4. In the Boot Manager, use the arrow keys to select USB flash drive A and press <Enter>.
 5. To switch the user to the `root` account, after booting up, execute the command:
`sudo su`
 6. To identify the names of the USB flash drives A and B, execute the command:
`lsblk`
 7. To create a mount point for the USB flash drive B, execute the command:
`mkdir /mnt/usb1`
 8. To mount the USB flash drive B, execute the command:
`mount /dev/sdb1 /mnt/usb1/`
`/dev/sdb1` (USB flash drive B) is an example of an USB flash drive name.
 9. To go to the USB flash drive B directory `/mnt/usb1/`, execute the command:
`cd /mnt/usb1`
 10. To unzip {sensor image}.tar.xz, execute the command:
`tar --no-same-owner -xvf {sensor image}.tar.xz`
 11. To go to the root directory, execute the command:
`cd /mnt/usb1`
 12. To copy the S2L2 Linux image to the server disk partition, execute the command:
`dd if={sensor image} of=/dev/sda bs=4M; sync`
 13. Remove the USB flash drive A and B and reboot the computer.
- After the reboot the configuration program starts with an optional disk check.

5.3.9.3 Installation precheck of the disk (optional)

This procedure provides valuable information before starting the installation:

- Disk space utilization by other applications
- Detection of bad sectors on the disk that might need repair

This step is optional. Consider that this step might take a long time, for example 1.5 hours on a 300 GB drive.

1. After the reboot, the "Check disk (optional)" window appears.
2. To start the disk check, click "Yes".

5.3.9.4 Configuring the SINEC Security Monitor Sensor

Configure the SINEC Security Monitor Sensor

The configuration supports you in the network setup of the SINEC Security Monitor System on the SSM Sensor. The last step before the initialization offers an opportunity to review and modify settings.

For assistance with the allocation of network addresses, refer to chapter SSM Sensor interfaces (Page 53) and chapter Communication between SSM Server and SSM Sensor (Page 56).

Note

Connect all network cables before starting this configuration

The configuration of the network interfaces does not work without connected network cables. Connect all required ports to a switch.

1. Review the list of network interfaces of the device.
Select the network interface for the H1 port of the SINEC Security Monitor Sensor and click "Ok".
2. Enter the IP address for the H1 network interface and click "Ok".
3. Enter the network mask for the H1 network interface and click "Ok".
4. Enter the gateway address for the H1 network interface and click "Ok".
If no gateway is available, click "Ok" to continue.
5. To configure the IP address of other network interfaces (NICs), click "Yes".
If it is not necessary to configure other network interfaces, click "No".
6. Select the network interface for monitor port M of the Sensor.
You can select no network interface or multiple network interfaces and click "Ok".
7. Enter the IP address for the WBM (SINEC Security Monitor Server) and click "Ok".

8. Configure the NTP server address. The system synchronizes the system time with a remote NTP server.
Enter the IP address of the NTP server and click "Ok".
If no NTP server is available, click "Ok" to continue. If you enter no IP address, the NTP server address is set to 127.127.1.0.

Note

If no NTP server is used, ensure that the RTC/Hardware-Clock is set to the correct time and timezone to ensure that SSM Sensors can be detected by the SSM Server.

Note**Time settings on SSM Server and SSM Sensor must match**

Otherwise, synchronization between both devices will not work.

9. Select your time zone and click "Ok".
For a greater choice of time zones, select "More".
10. Enter a hostname for this system and click "Ok".
The hostname must be a single word without spaces. Example: ssm-sensor
11. Create a user account for administrative activities, without root privileges.
Enter a full name for the user and click "Ok".
12. Enter a password for the new user and click "Ok".
Minimum password requirements:
 - Uppercase and lowercase letters
 - Numbers
 - Special characters
 - 20 characters
13. Re-enter the password for the new user and click "Ok".
14. Check the "Current Configuration" and click "Ok" to continue.
15. To confirm the configuration, select "Save" and click "Ok".
To modify the configuration, select "Modify" and click "Ok".
16. Check the "Current Configuration" and click "Ok" to continue.
17. Wait for the completion of the "System initialization".
18. The "Sensor public key information" is displayed during the initialization. Click "Ok" to continue.
19. At the end of the "System initialization", click "Ok" and the system reboots.

See also

Configuring the SINEC Security Monitor Sensor (Page 110)

Cancelling the configuration program

If you click "Cancel" during the configuration program the "Exit Operation" window appears:

- Click "No" to return to the configuration program.
- Click "Yes" to exit the configuration program and continue the boot process.
To re-enter the configuration program after cancelling, simply reboot the device.

5.3.9.5 Setting the system time of the SSM Sensor

Ensure that the system time of the SSM Sensor is correct

Note

This step is mandatory, as time differences in the SINEC Security Monitor System lead to malfunctioning.

It is recommended to manage/update the NTP configuration for the SSM Server and SSM Sensor on the WBM.

1. After the SSM Sensor's installation, execute the command to verify the system time. Use the "operator" user account which was created during the SSM Sensor's configuration.

```
ssmctl-client system get_system_time --host_ip localhost --  
service_module sensor
```

2. If the result of the `get_system_time` command doesn't match the local clock of the computer, execute the command to adjust the SSM Sensor's system time accordingly:

```
ssmctl-client system set_system_time --date_time "2024-06-24  
15:04:05" --host_ip localhost --service_module sensor
```

Examples of supported time formats:

- "2024-06-24"
- "2024-06-24 15"
- "2024-06-24 15:04"
- "2024-06-24 15:04:05"

For more information on time settings of the entire SSM System, refer to chapter Configuring the system time (Page 93).

5.3.9.6 Requesting a SINEC Security Monitor license for the SINEC Security Monitor Sensor

Note: It is recommended to use Google Chrome browser (version 85 or higher).

An overview of the available licenses can be found in section Components and licenses (Page 44).

Requesting SINEC Security Monitor Sensor license

1. Log in to the WBM.
2. Select the "System" > "License" page.

3. Open the "Sensor" tab.
4. Click "Export request file" in the row of the new Sensor.
5. Send the `Sensor-smcRequestBundle-{Instance ID}.zip` file to the following email address to request a license:
`activation-ssm.industry@siemens.com`
Make sure to include the following information from your order notification in your email:
 - Sold-To/Install: <>
 - License Quote: <>
 - P.O.-Number: <>
6. In case you ordered more than one license in your purchase order please state which of them you want to activate with this request.
You will receive an activation file for the server via email.

Activating the SINEC Security Monitor Sensor license

The file format of the activation file is `Sensor-{Instance ID}.zip`

Example: `Sensor-44163cf7dc711c87750.zip`

The instance ID is unique for each SINEC Security Monitor Sensor.

1. Log in to the WBM.
2. Select the "System" > "License" page.
3. Open the "Sensor" tab.
4. Verify the Instance ID of the new SINEC Security Monitor Sensor.
5. Open the "System" > "License" page and click the "Sensor" tab.
Compare the instance ID shown with the instance ID of the received license file, then proceed.
If the instance IDs are different, reply to the email with the activation file.
6. Click "Upload activation file".
7. Click "Browse" and select the `Sensor-{Instance ID}.zip` file.
8. Click "Upload".
9. The system reboots.
10. Check the "System" > "License" page again for the successful upload. The SINEC Security Monitor Sensor's status is "Activating".
11. Wait while the SINEC Security Monitor Sensor reboots. Keep refreshing the page until the Sensor's status is "Activated".

5.3.9.7 Adding Sensors

Settings for "Active Probing", "SNMP V1", "SNMP V3" and "Remote Agentless Nodes" are located at the bottom of the "Edit" window of a SINEC Security Monitor Sensor. These settings are not mandatory and can be configured when required.

Add a Sensor

1. Log in to the WBM.
2. Select the "Configuration" > "Sensor" menu.
3. Click on "Add".
4. Enter the required information. Fields marked with "*" are mandatory.
 - ***Name**
Sensor name
 - ***Sensor**
Select a SINEC Security Monitor Sensor from the drop-down list which is not marked with "(Binded)".
For an explanation of "Binded", unbinded and "Inactive", see table "SSM Sensor installation status".
 - **Manage**
Click "Manage" to manage the newly installed SINEC Security Monitor Sensors that are already pushed to SINEC Security Monitor Server but not yet assigned on the page.
 - **Destination**
Destination address (IP address of the SINEC Security Monitor Server)
 - **Monitoring area**
Add the actual network area.
 - **Owner**
Add the name of the owner or manager of the device.
 - ***Internal Networks**
192.168.0.0/24, 10.10.0.0/16 (examples)
5. *To save changes, click "OK".

Note: When a SINEC Security Monitor Sensor does not show up in the "Sensor" drop-down list, ensure a stable network connection between the SINEC Security Monitor Sensor and the SINEC Security Monitor Server.

For an explanation of the SINEC Security Monitor Sensor status icons, refer to table in section Managing Sensors (Page 150).

Table 5-14 SSM Sensor installation status

Status	Description
Unbinded (to be binded)	For example: [192.168.xxx.xxx] sensor.logagent This SSM Sensor is free. You can add it.
Binded	For example: [192.168.xxx.xxx] sensor.logagent (Binded) This SSM Sensor has been installed and is up and running.
Inactive	For example: [192.168.xxx.xxx] sensor.logagent (Inactive) This SSM Sensor has already been installed, but not yet been activated with a license.

5.3.9.8 Verifying the status of SINEC Security Monitor Sensor services

Check the status of the SINEC Security Monitor Sensor containers (prober, zeek, logAgent, suricata).

1. Log in to the WBM.
2. Select the "System" > "Diagnostics" menu to open the "Diagnostics" page.
3. Check the status of all SINEC Security Monitor Sensor containers.
A green "●" icon indicates the status is "healthy".

Table 5-15 SINEC Security Monitor Sensor containers

Container name	Function	Status
sensor.prober	Data analysis of asset network traffic	Healthy
sensor.logagent	Rawlog data collection	Healthy
sensor.zeek	Network traffic analysis	Healthy
sensor.suricata	Network traffic analysis and generation of security events	Healthy

Commissioning

6.1 Initial system configuration

The first login in to the WBM including changing the password for the administrator account happens during the SINEC Security Monitor Server installation process.

Refer to chapter Logging in to the SINEC Security Monitor System (Page 91).

6.1.1 Creating user account

Create user accounts and specify their roles

1. Log in to the WBM.
2. Select the "User Management" > "Roles" menu.
Note: There are three typical roles in SINEC Security Monitor by default:
 - Administrator
 - Auditor
 - OperatorClick "Edit" to edit roles.
Click "Add" to add roles as needed.
3. Navigate to the "User Management" > "Users" menu.
4. Click "Add".
5. Enter the required information (fields marked with "*" are mandatory):
 - *Full Name
 - *User Name
 - *Password and *Repeat password
 - Email address
 - Department
 - Description
 - Roles
 - Read-only (Enabled, Disabled): Read-only mode will disable user's authorization for changing data.
6. Click "OK" to save changes.

User account pages

Table 6-1 Roles page

Function		Description
Add		Add a new role
Edit		Edit the selected role
Delete		Delete a role
Refresh		Refresh the list
		Search for a role name
		Clear the search field
	More	Open the details window for the selected role
	Edit	Edit the details of the selected role
	Delete	Delete the selected role from the SINEC Security Monitor System

Table 6-2 User page

Function		Description
Add		Add a new user
Edit		Edit the selected user
Delete		Delete the selected user
Refresh		Export the list of users as an Excel file
		Search for a user name
		Clear the search field
	More	Open the details window for the selected user
	Edit	Edit the details of the selected user
	Delete	Delete the selected user from the SINEC Security Monitor System

Cybersecurity measures for user accounts

- Each user must have their own user account. Sharing of user accounts between users is not recommended.
- The user must change the initial password when they log in for the first time.
- A secure password must:
 - Have a length of 8–32 characters.
 - Have at least one of the following characters: uppercase letter, lowercase letter, digit, special character.
- Each user account must have a role assigned in accordance with their responsibilities on the SINEC Security Monitor System. Applying the principle of least privilege is recommended.
- To restrict access to only certain pages combined with read-only permission, define a new role with respective access rights to the required pages and create a user account in read-only mode with the restricted role assigned.

6.1.2 Updating the SINEC Security Monitor Intelligence Databases

Updates for the SINEC Security Monitor Intelligence Databases are distributed via Siemens Digital Industries Software Support Center to customers with active subscription (during the purchased term).

- Log in to the "DI SW Support Center (<https://support.sw.siemens.com/en-US>)" on a regular basis and check out what is new.

Upload the SINEC Security Monitor Correlation Rules Library

Correlation rules describe typical security event log sequences of attack behavior.

The SINEC Security Monitor System collects and processes security event log information from the devices in the environment. The security event log information is analyzed by the SINEC Security Monitor System. The result of the analysis is then compared with correlation rules to detect any security event sequences that can indicate anomalies. These anomalies can be a sign of security weaknesses or cyber-attacks.

Correlation rules must be regularly updated.

For more information on the correlation rules page, refer to chapter Managing correlation rules (Page 134).

1. Check the checksum of the SINEC Security Monitor Correlation Rules Library update.
2. Log in to the WBM.
3. Select the "Configuration" > "Correlation Rules" menu.
4. Click "Update Rules". In the "Correlation Rule Library" section, browse for the update file in ".tgz" format.
5. Verify the result of the update in the "Configuration" > "Correlation Rules" > "Update Rules" window.

Update the SINEC Security Monitor Threat Intelligence Library

1. Check the checksum of the SINEC Security Monitor Threat Intelligence Library update.
2. Log in to the WBM.
3. Select the "Configuration" > "Correlation Rules" menu.
4. Click "Update Rules". In the "3rd party Threat Intelligence Library" section, browse for the update file in ".tgz" format.
5. Verify the result of the update in the "Configuration" > "Correlation Rules" > "Update Rules" window.

Maintain the SINEC Security Monitor Vulnerabilities Library

When the product family, model, and firmware version attributes of an asset match with the corresponding attributes of the vulnerability, the vulnerability will be automatically associated with the asset.

1. Log in to the WBM.
2. Select the "Configuration" > "Vulnerability Library" menu to display the Vulnerability Library.
 - **Download vulnerability library**
Download the library as a .zip file to the "Downloads" folder of your computer.
 - **Browse**
Open the browse window to select a vulnerability file for the upload.
 - **Upload vulnerability library**
Start the upload.
 - **Version Information**
Verify the version of the library.
 - Use the search function to filter the information. A search can be organized by CVE ID, severity, summary or description.
 - Clear the search field.
 - **Details**
Display more information about the vulnerabilities.

CVSS scoring mechanism

Table 6-3 Ranking of the Common Vulnerability Scoring System (CVSS)

CVSS 2.0		CVSS 3.0/3.1	
Severity	Base Score Range	Severity	Base Score Range
–	–	Critical	9.0–10.0
High	7.0–10.0	High	7.0–8.9
Medium	4.0–6.9	Medium	4.0–6.9
Low	0.0–3.9	Low	0.1–3.9
–	–	None	0.0

Upload files to the vulnerability library

Note

Only .xlsx or .zip files are supported.

1. Check the checksum of the SINEC Security Monitor Vulnerabilities Library update.
2. Log in to the WBM.
3. Select the "Configuration" > "Vulnerability Library" menu.
4. Click on "Browse" to browse for a ".zip" file.
5. Click on "Upload vulnerability library".
6. Verify the result of the update on the "Configuration" > "Vulnerability Library" page. Move your mouse over the "Version Information" button to see the version information.

6.2 System parameters configuration

6.2.1 Configuring network settings

Purpose

Go to the "Network" page to review and change settings of the network interfaces of the SINEC Security Monitor Server if necessary. As well, mark one network interface as "Main NIC" and specify one or more "Monitor interfaces".

NOTICE
Risk of destroying the whole system setup
Many installed and configured functions of the SINEC Security Monitor system depend on stable connections. Changing the network addresses here can turn the whole system out of order.
It is not recommended to re-configure network settings when the system is up and running.

Only configure the network settings, if changes in the network make it necessary.

1. Log in to the WBM.
2. Select the "Configuration" > "System" menu.
3. Click the "Network" tab.
4. Modify or add "IP address", "Subnet mask" and "Gateway address" for each network interface as required.
5. Select a "Main NIC".

6. Enable "Monitor Interfaces" which monitor network traffic in the network they are connected to.
7. To save changes, click "Save".
8. A popup window appears: "Please confirm the current service status and choose whether to continue or not".
Only select "Confirm" when all status icons in the popup window are green.
Otherwise, it is not recommended to proceed. You have to double-check all abnormal services.
9. Wait several minutes for a network service reboot.

6.2.2 Restricting access control

Purpose

To enhance network security, administrators can restrict access to the IP address of the SINEC Security Monitor System. Only computers within the selected network segment can access the SINEC Security Monitor System.

Configure access control

1. Log in to the WBM.
2. Select the "Configuration" > "System" menu.
3. Click the "Access Control" tab.
4. In the "Allow access from IP address/netmask:" field, enter IP and netmask bits.
Example: 192.168.100.100/24
5. Click "Save" to save the changes.

6.2.3 Configuring system backups

Purpose

To prevent data loss due to misconfiguration or mistakes during operation, perform regular backups. System backups are stored locally or remotely.

Table 6-4 Backup packages of the SSM System

Package	Description
Raw Logs	This package contains monitored traffic data, collected Microsoft Windows logs and endpoint logs.
Security Events	This package contains all generated security events in the SSM Server.
Security Event	This package contains all configuration data of the SSM Server.

For local system backups, refer to chapter Backup configuration settings (Page 222).

Configure regular backups for logs and SINEC Security Monitor System configuration

1. Log in to the WBM.
2. Select the "Configuration" > "System" menu.
3. Click the "Backup" tab.
4. Under "Backup retention days", set how long the backups should be retained before being automatically deleted.
 - 0: No local backups. Backups files are automatically deleted after the backup operation completes.
 - 1...3650: The backup files are retained for as many days as set here. The system will automatically delete any backup files older than the set amount of days.
5. Check "Data set for backup": Select the data sets that you want to backup regularly: Raw log, Security events, System configuration.
6. Select a "Backup plan" from the drop-down list:
 - **Never**
No data backup
 - **Once a Day**
Perform a data backup every day at the set time.
 - **Once a Week**
Perform a data backup every week at the set time.
 - **Once a Month**
Perform a data backup every month at the set time.
7. Set a time for the backup:
Note: The availability of the fields depends on the Backup plan selection.
 - **Day of month**
Select a day of the month for a monthly data backup.
 - **Day of week**
Select a day of the week for a weekly data backup.
 - **Time of Day**
Set a specific backup time in [hours]:[minutes]:[seconds]

8. Check "Backup to remote server":
Check to backup to a remote server. Otherwise, the backup is stored on the local database server.
If the "Backup to remote server" option is checked, the next set of parameters become mandatory.
A remote Linux server needs to be prepared for backup and the details from that process need to be entered in the next set of parameters.
Refer to the section Preparing a remote Linux server for backups (Page 124).
 - **Remote Account**
Enter an account name which gains access to the remote server.
 - **IP address of remote server**
Add the IP address of the remote server for a backup to a remote server.
 - **RSA Public Key (PEM)**
Click "Upload", select a certificate file and click "Open".
9. To save changes, click "Save".

6.2.4 Preparing a remote Linux server for backups

Note**Backup files can not be restored in cross-version mode**

- You can not restore backup files (Raw Logs/Security Event/System Configuration) from a SSM V4.8.0 device on a SSM V4.9.0 device.
Backup files can only be restored on the same version.
 - Do not change file names of backup files.
-

Backup procedure overview

1. A remote Linux server is prepared for receiving backup files via ssh from the SINEC Security Monitor System.
2. A Linux system is used to create the private and public keys that are required for the process.
3. The SINEC Security Monitor System is configured to upload backup files of configuration, raw logs and security events to a remote Linux server in regular intervals.
4. Restoring backup files on the SSM Server is more complicated due to hardening. You have to use an USB flash drive for the data transfer from the remote Linux server to the SSM Server.

Tested environment

Table 6-5 Tested environment for backup file restoration

Component Name	System	Function
Remote Linux server	Debian 12 or CentOS 7	Receive and store backup files.
Linux system	Debian 12 or CentOS 7	Generate public and private keys. Ensure the OpenSSL tool is installed for this purpose.
USB flash drive	Format: exFAT Size: Minimum 32 GB	File transfer from the Linux system and from the remote Syslog server to the SSM Server.
Microsoft Windows workstation	Windows 10/11	Format the USB flash drive using Rufus [7] or the Microsoft Windows formatting function. Link: (https://rufus.ie/en/)

Prepare the USB flash drive

Prerequisites:

- USB flash drive with a size of 32 GB
- A windows computer

This instruction uses Rufus for formatting. When you want to use the Microsoft Windows formatting tool, refer to Preparing USB flash drive B (Page 85).

Formate the flash drive

1. Plug the USB flash drive into a computer.
2. Double click "rufus-{version}.exe".
3. At the popup window "Do you want to allow this app to make changes to your device", select "Yes".
4. In the "Drive Properties" window, fill in the necessary details:
 - Volume label: Enter an appropriate name.
 - Files system: Enter "exFAT".
5. Click "START".
6. When the status bar switches to "READY", unplug the USB flash drive.

Prepare the remote Linux server for receiving backups

Two backups are prepared: os (OpenSearch database) and pg (postgres database).

1. Log in to the remote Linux server.
2. Create a remote account.
In this example, we use {user account} as an account name.

3. To create a directory for the database os using the remote account, execute the command:
`mkdir -p /home/{user account}/osBackup`
4. To create a directory for the database pg using the remote account. Execute the command:
`mkdir -p /home/{user account}/pgBackup`
5. Modify group properties and permissions for the `"/home/{user account}/osBackup"` and `"/home/{user account}/pgBackup"` folders, execute the command:
`chmod -R 750 /home/{user account}/osBackup`
`chmod -R 750 /home/{user account}/pgBackup`
6. To ensure the functionality of SSH (Secure Shell), execute the command:
`ssh {user account}@{remote_ip}`
`remote_ip`: IP address of the remote Linux server, for example: 192.0.2.0

Configure password-free login to the remote Linux server

On the SSM Server, execute the command to configure password-free login to remote Linux server:

1. Log in to the Linux backend of the SSM Server.
2. Execute the command:
`ssmctl-client system sshkey --host_ip localhost --service_module server --remote_ip {1.1.1.1} --remote_account {user account}`
`remote_ip`: IP address of the remote Linux server, for example: 1.1.1.1
`remote_account`: Remote account "{user account}" of the remote Linux server
3. Check and validate that the command is executed successfully.

Generate a public key and a private key on the Linux system

Note: Ensure that the public key and the private key are stored safely. You will need the public key and the private key in the next sections.

1. Install the OpenSSL tool on the Linux system. Check and record the OpenSSL version.
2. Generate the private key. Execute one of the commands:
For OpenSSL version greater or equal than 3.00:
`openssl genrsa -aes256 -passout stdin -out privatekey.pem -traditional 4096`
For OpenSSL version lower than 3.00:
`openssl genrsa -aes256 -passout stdin -out privatekey.pem 4096`
3. Enter a password for the privatekey.pem and press [Enter].
4. To generate the public key, execute the command:
`openssl rsa -in privatekey.pem -passin pass:PwdForPrivatekey -pubout -out publickey.pem`
5. After the initialization, enter the password for the privatekey.pem, and press [Enter].

Configure the remote backup in the WBM

1. Log in to the WBM.
2. Select the "Configuration" > "System" menu.

3. Click the "Backup" tab.
4. Check "Data set for backup": Select the data sets that you want to backup regularly: Raw log, Security events, System configuration.
5. Select a "Backup plan" from the drop-down list:
 - **Never**
No data backup
 - **Once a Day**
Perform a data backup every day at the set time.
 - **Once a Week**
Perform a data backup every week at the set time.
 - **Once a Month**
Perform a data backup every month at the set time.
6. Set a time for the backup:
Note: The availability of the fields depends on the Backup plan selection.
 - **Day of month**
Select a day of the month for a monthly data backup.
 - **Day of week**
Select a day of the week for a weekly data backup.
 - **Time of Day**
Set a specific backup time in [hours]:[minutes]:[seconds]
7. Select "Backup to remote server".
8. Enter the parameters of the remote Linux server:
 - **Remote Account**
Enter an account name.
 - **IP address of remote server**
Add the IP address of the remote server.
 - **RSA Public Key (PEM)**
Click "Upload", select a certificate file and click "Open".
9. To save changes, click "Save".

Copy backup files to the USB flash drive

As preparation to the restore of the SSM Server, access the remote Linux server to collect backup files.

1. Log in to the remote Linux server.
2. Plug in the USB flash drive that was formatted to the "exFAT" file system format.
3. To identify the USB flash drive, execute the command:
`lsblk`

4. To mount the USB flash drive to remote Linux server, execute the command:

```
mount /dev/sdb1 /mnt/usb1
```

/dev/sdb1: The disk symbol of the USB flash drive
/mnt/usb1: The mounted root directory of the USB flash drive
5. To copy the encrypted backup file, for example "system_configuration_20231229.tar.enc", to the root directory of the formatted USB flash drive, execute the command:

```
cp /home/{user account}/pgBackup/  
system_configuration_20231229.tar.enc /mnt/usb1
```

Copy the private key file to the USB Flash Drive

Access the Linux system and add the private key file to the USB flash drive.

1. Log in to the remote Syslog server.
2. Plug in the USB flash drive that was formatted with the exFAT file system format.
3. To identify the USB flash drive, execute the command:

```
lsblk
```
4. To mount the USB flash drive to the Linux system. Execute the command:

```
mount /dev/sdc1 /mnt/usb2
```

/dev/sdc1: The disk symbol of the USB flash drive
/mnt/usb2: The mounted root directory of the USB flash drive
5. Copy the private key file (privatekey.pem) to the root directory of the formatted USB flash drive. Execute the command:

```
cp /home/{user account}/pgBackup/privatekey.pem /mnt/usb2
```

Restore the remote backup to the SSM Server

Note

Do not change the file names of backup files.

1. Insert the USB flash drive into the SSM Server.
2. To identify the USB flash drive, execute the command:

```
lsblk
```

3. To mount the USB flash drive and copy the files from the USB flash drive to a specific backup directory on the SSM Server. Execute the command:

- Raw Logs (os):

```
ssmctl-client system upload_backup --host_ip localhost
--service_module server --usb_disk "/dev/sdb2"
--backup_file "raw_logs_20231130.tgz.enc"
```
- System Configuration (pg):

```
ssmctl-client system upload_backup --host_ip localhost
--service_module server --usb_disk "/dev/sdb2"
--backup_file "system_configuration_20231229.tar.enc"
```
- Security Events (pg):

```
ssmctl-client system upload_backup --host_ip localhost
--service_module server --usb_disk "/dev/sdb2"
--backup_file "security_events_20231213.tar.enc"
```

/dev/sdb2: Disk symbol of the USB flash drive.

4. Commands to restore the backup data:

- Raw Logs (os):

```
ssmctl-client os restore_data
--restore_file "raw_logs_20231130.tgz.enc"
--host_ip localhost --service_module server --usb_disk "/dev/
sdb2"
--private_key privatekey.pem --private_key_pass {1234}
```
- System Configuration (pg):

```
ssmctl-client pg restore_data
--restore_file "system_configuration_20231229.tar.enc"
--host_ip localhost --service_module server --usb_disk "/dev/
sdb2"
--private_key privatekey.pem --private_key_pass {1234}
```
- Security Events (pg):

```
ssmctl-client pg restore_data
--restore_file "security_events_20231213.tar.enc"
--host_ip localhost --service_module server --usb_disk "/dev/
sdb2"
--private_key privatekey.pem --private_key_pass {1234}
```

{1234}: Password of the private key.

5. Check and validate that the command is executed successfully.
6. To remove the privatekey.pem file from the USB flash drive, execute the commands:

```
cd /mnt/usb2
rm -rf privatekey.pem
```

"/mnt/usb2": The mounted root directory of the USB flash drive.

See also

Configuring system backups (Page 122)

6.2.5 Setting up email notifications

Purpose

To add settings for the report and notification emails, access the "Email notification" page.

Prerequisite

Create an email account on the email server for the SINEC Security Monitor System.

Configure email notification

Note

The SINEC Security Monitor System sends emails via SMTP protocol. POP3 and IMAP were tested for receiving protocols on the email server.

1. Log in to the WBM.
2. Select the "Configuration" > "System" menu.
3. Click the "Email Notifications" tab.
4. Enter the required information. Fields marked with "*" are mandatory.
Add settings for the email server:
 - ***SMTP server**
Address of the email server
 - ***SMTP server port**
Port used for outgoing emails
 - ***SMTP user name**
User name for the email account
 - ***SMTP password**
Password for the email account
5. For a more secure email communication with authentication, check "Enable SSL communication".
6. To download a client certificate, click "Download".
7. For a more secure email communication, check "Enable server authentication".
8. At "Import a server certificate" browse for a X.509 certificate in .pem format and click "Upload"

9. The report notification template is used to configure report emails. For this purpose, also enable "Send email notification" in the "Configuration" > "Report" menu.
Add settings for the Template for report notifications:
 - ***Email address** (of report receiver)
Add at least one email address; separate multiple addresses by commas.
 - ***Email subject**
Example: Report from SINEC Security Monitor.
 - **Email text**
Example: Please find attached the monthly Cybersecurity Report.
10. The event notification template is used to configure notification emails. For this purpose, also configure "Email notifications" in the "Configuration" > "Notification" menu,
Note: The same settings are used for system event notifications and security event notifications.
Add settings for the template for security event notifications:
 - ***Email address** (of notification receiver)
Add at least one email address; separate multiple addresses by commas.
 - ***Email subject**
Example: Security event notification. Priority: High!
 - **Email text**
Example: Cybersecurity notification. Act immediately!
11. To save changes, click "Save".

6.2.6 Configuring general log settings

Purpose

The "Log Settings" page has three tabs. The "Log Storage" tab handles storage period and storage thresholds. To forward logs to other systems, configure the "Log Forwarding" tab. To receive logs, configure the "Log Reception" tab.

Configure log storage

Note

- When reaching the "Storage warning threshold", a message appears: "Log Storage Space Exceeds Threshold".
 - When reaching the "Storage maximum threshold", the system deletes the oldest entries in the log storage.
-

1. Log in to the WBM.
2. Select the "Configuration" > "Log Settings" menu.
3. Click the "Log Storage" tab.

4. Enter the required information. Fields marked with "*" are mandatory.
 - *Storage period (days)
Enter a number of days. Default value: 180
 - *Storage maximum threshold (%)
Enter a percentage. Default value: 80
 - *Storage warning threshold (%):
Enter a percentage. Default value: 60
 - *Self-monitor storage period (days): Enter a number of days, default value: 180.
Self-monitoring relates to logs collected from the SSM Server and the SSM Sensors.
Note: The percentages relate to the total available storage space for logs.
5. Click "Save".

Configure log forwarding

Refer to chapter Configuring security log forwarding to third-party systems (Page 148).

Configure ports to receive logs

1. Log in to the WBM.
2. Select the "Configuration" > "Log Settings" menu.
3. Click the "Log Reception" tab.
4. Available ports:
Default values: 514, 6514
Enter additional ports if required. Separate multiple ports with commas.
Note: This field is mandatory. You can not leave this field empty.
5. Click "Save".

Refer to Communication ports (Page 21).

6.2.7 Configuring asset types and zones

Purpose

The SINEC Security Monitor System detects all assets in the network and uses algorithms and models to identify device attributes, for example asset type or asset zone. However, the user might want to customize these settings and adjust them to the needs of the target environment.

Operational baselines (asset types and zones), security baselines, monitoring rules and reports should be configured after setting up the SINEC Security Monitor System in the environment.

6.2.7.1 Setting asset types

Change the asset type

The SINEC Security Monitor System assigns asset types using a derivation algorithm. Users can customize asset types and assign different asset types to each asset when the asset types selected by the SINEC Security Monitor System do not fit the realities of the OT environment.

Customize asset types

1. Log in to the WBM.
2. Select the "Configuration" > "Asset Setting" menu and click the "Asset Type" tab.
3. Click "Add".
4. Enter an asset type and select an asset zone from the drop-down list.
The following asset zones are available by default:
 - Operations & Control
 - Supervisory Control
 - Control
 - Process
 - Enterprise Servers
 - Enterprise Network
 - UndefinedClick "OK" to save changes.

Assign new asset types to assets

1. Log in to the WBM.
2. Select the "Assets" > "Assets" menu.
3. Choose an asset where the asset type does not match.
4. Click the "Edit" button in the "Actions" column.
5. Select a new asset type from the drop-down list.
6. Click "OK" to save changes.

6.2.7.2 Setting asset zones

Change the asset zone

Asset zones (areas of information) are assigned by the SINEC Security Monitor Server based on the Purdue model, in correspondence with the asset type. When the assigned asset zones do not meet the site requirements of the target environment, users can customize asset zones and assign a different asset zone to each asset type.

Customize asset zones

1. Log in to the WBM.
2. Select the "Configuration" > "Asset setting" menu and click the "Asset Zone" tab.
3. Click "Add".
4. Enter an asset zone name.
5. Click "OK" to save changes.

Assign new asset zones

1. Log in to the WBM.
2. Select the "Assets" > "Assets" menu.
3. Choose an asset where the asset zone does not match.
4. Click the "Edit" button in the "Actions" column.
5. Select a new "Asset zone" from the dropdown list.
The following Asset zones are available by default:
 - Operations & Control
 - Supervisory Control
 - Control
 - Process
 - Enterprise Servers
 - Enterprise Network
 - Undefined
6. Click "OK" to save changes.

6.2.8 Managing correlation rules

Correlation rules

The SINEC Security Monitor System defines some common security threat events in industrial control environments, which are mainly divided into the following categories:

- Assets
- Applications
- Vulnerabilities
- User accounts
- Networks

- Operation
- Etc.

By setting monitoring rules, administrators can choose to control the threat events according to actual work scenarios.

Adjust correlation rules

Correlation rules are pre-configured. You can adjust the configuration as needed.

1. Log in to the WBM.
2. Select the "Configuration" > "Correlation Rules" menu.
3. Choose a rule and click "Edit" at the end of the row.
4. Enter the required information (fields marked with "*" are mandatory):
 - ***Name**
Add a significant name.
 - ***Event type** (Alert, Warning, Event)
Select an event type representing the severity of the rule.
 - ***Remark**
Add a brief statement.
 - ***Threshold**
To generate a security event, the threshold indicates how many assets must meet the criteria within the time window.
 - ***Time window (ms)**
Indicates the rule monitoring period
 - **Script** (can not be configured)
DSL query script for an OpenSearch query (programming code of the rule).
5. Click "OK" to save changes.

Functions of the Correlation Rules page

Table 6-6 Correlation Rules page

Function	Description
Enable Selected	Change the status of the event rule to "Enabled"
Disable Selected	Change the status of the event rule to "Disabled"
Delete Selected	Delete all selected event rules
Download correlation rules	Download selected rules to the workstation

Update Rules	Import in batch: - Correlation Rule Library 3rd party Threat Intelligence Library - Siemens Threat Intelligence Library Note: Siemens Threat Intelligence Library files are no longer provided. Refer to Updating the SINEC Security Monitor Intelligence Databases (Page 119).
Search	Search by rule ID or rule name
Clear	Clear the search field

6.2.8.1 Configuring anomaly baselines

Purpose

Anomaly baselines help identify abnormal behaviors by managing allow lists (permitted items) and deny lists (restricted items). These baselines apply to applications, communication links, USB devices, IP addresses, and user accounts. By effectively managing these lists, you can detect unauthorized actions such as installing unapproved applications, using unregistered USBs, adding unknown IP addresses, establishing new communication links, or using unauthorized accounts.

Types of Anomaly baselines

- **Applications**
Put applications detected in the environment on the allow list or deny list.
- **Communication links**
Put communication links between two devices detected in the environment on the allow list or deny list.
- **USB devices**
Put USB devices detected in the environment on the allow list or deny list.
- **IP addresses**
Put IP addresses detected in the environment on the allow list or deny list.
- **Accounts**
Put user accounts detected in the environment on the allow list or deny list.

Working with allow lists and deny lists

When a new item appears in the monitored network and is not on the allow or deny list, a security event is triggered as a "Warning". A system administrator or qualified expert should review and decide on the appropriate list placement for these entries.

Once an item is added to the Allow List, no security event will be generated in the future.

Here are some practical examples:

- When a newly detected Application is not found on the Allow List or on the Deny List, a security event with event type Warning will be generated and listed.
In the SSM Server WBM, navigate to the "Security Events" > "Security Events" page and filter the security event ID and name "[954] Unexpected Application" to find the security event.
On the "Configuration" > "Anomaly Baseline" page, you can create a new application baseline and add the new application either to the Allow List or to the Deny List.
- For a newly detected Communication Link that is not found on Allow List or on the Deny List, a security event with event type Warning will be generated and listed.
In the SSM Server WBM, navigate to the "Security Events" > "Security Events" page and filter the security event ID and name "[204] New APP flow" to find the security event.
On the "Configuration" > "Anomaly Baseline" page, you can create a new Communication Link baseline and add the new Communication Link either to the Allow List or to the Deny List.
- For a newly detected USB Device, that is not found on Allow List or on the Deny List, a security event with event type Warning will be generated and listed.
In the SSM Server WBM, navigate to the "Security Events" > "Security Events" page and filter the security event ID and name "[955] Unauthorized USB Plugin" to find the security event.
On the "Configuration" > "Anomaly Baseline" page, you can create a new USB Device baseline and add the new USB Device either to the Allow List or to the Deny List.
- For a newly detected IP Address, that is not found on Allow List or on the Deny List, a security event with event type Warning will be generated and listed.
In the SSM Server WBM, navigate to the "Security Events" > "Security Events" page and filter the security event ID and name "[842] Unexpected IP" to find the security event.
On the "Configuration" > "Anomaly Baseline" page, you can create a new IP Address baseline and add the new IP Address either to the Allow List or to the Deny List.
- For a newly detected User Account, that is not found on Allow List or on the Deny List, a security event with event type Warning will be generated and listed.
In the SSM Server WBM, navigate to the "Security Events" > "Security Events" page and filter the security event ID and name "[960] Unauthorized accounts used on Windows" to find the security event.
On the "Configuration" > "Anomaly Baseline" page, you can create a new User Account baseline and add the new User Account either to the Allow List or to the Deny List.

Handling Security Events

1. To handle the Security Event go to the Security "Security Events" > "Security Events" page.
2. Locate the security event, and click "Edit" in the "Actions" column.
3. Mark the "Action" as "Abnormal", "Normal", or "Irrelevant",
4. Mark the "Status" as "Processing", "Processed" or "Closed"
5. In the "Add to anomaly baseline" dropdown list, select "None", "Allow List" or "Deny List".
6. By selecting "Upgrade" or "Downgrade", you can change the classification of the event, refer to section Upgrading or downgrading security events (Page 140).
7. Click "Related Log" or open the "Log Details" window, and check out all related security log details.

Anomaly baseline page

The first tab of the "Configuration" > "Anomaly baseline" page allows baselines to be set for responses to certain actions or triggers.

Any security event in the environment that is not on the allow list, or that is on the deny list, causes an event alert and causes a security event notification.

Table 6-7 Anomaly baseline page

Function	Description
Add	Add a new policy or new policies
Edit	Edit the selected policy
Delete	Delete the selected policy
Refresh	Refresh the table
Add all to Allow List	Add all policies to the allow list.
Add all to Deny List	Add all policies to the deny list.
Delete All	Delete all policies.
All types	Select a type (All Types, Allow List, Deny List) for filtering the search results.
Search	Search for name, vendor, version, description
Clear	Clear all search fields

Access the anomaly baseline page

1. Log in to the WBM.
2. Select the "Configuration" > "Anomaly Baseline" menu.

Note

When configuring baselines, it is possible to add more than one policy in a single step. Just check more than one entity.

Configure the applications baseline

1. Log in to the WBM.
2. Select the "Configuration" > "Anomaly Baseline" menu.
3. Select the baseline type "Applications" from the drop-down menu.
4. Click "Add".
5. Enter the required information (fields marked with "*" are mandatory):
 - Select applications from the list by checking the checkboxes.
 - *Type: Select "Allow List" or "Deny List".
 - Description: Add a description.
6. Click "OK" to save changes.

Configure the communication links baseline

1. Log in to the WBM.
2. Select the "Configuration" > "Anomaly Baseline" menu.
3. Select the baseline type "Communication links" from the drop-down menu.
4. Click "Add".
5. Enter the required information (fields marked with "*" are mandatory):
 - *Source: 192.168.1.0/24
 - *Destination: 192.168.0.0/24
 - Protocol: TCP, UDP, ICMP
 - Port: Enter a port in the field and press [Enter] to confirm adding a new port.
 - *Type: Select "Allow List" or "Deny List".
 - Description: Add a description.

Note: IP addresses shown here are examples only.
6. Click "OK" to save changes.

Configure the USB devices baseline

1. Log in to the WBM.
2. Select the "Configuration" > "Anomaly Baseline" menu.
3. Select the baseline type "USB devices" from the drop-down menu.
4. Click "Add".
5. Enter the required information (fields marked with "*" are mandatory):
 - Select USB devices from the list by checking the checkbox.
 - *Type: Select "Allow List" or "Deny List".
 - Description: Add a description.
6. Click "OK" to save changes.

Configure the IP addresses baseline

1. Log in to the WBM.
2. Select the "Configuration" > "Anomaly Baseline" menu.
3. Select the baseline type "IP addresses" from the drop-down menu.
4. Click "Add".

5. Enter the required information (fields marked with "*" are mandatory):
 - *IP adresse: 192.168.1.0
 - *Type: Select "Allow List" or "Deny List".
 - Description: Add a description.
 - Select a period from the calendar.
6. Click "OK" to save changes.

Configure the accounts baseline

1. Log in to the WBM.
2. Select the "Configuration" > "Anomaly Baseline" menu.
3. Select the baseline type "Accounts" from the drop-down menu.
4. Click "Add".
5. Enter the required information (fields marked with "*" are mandatory):
 - Select user accounts from the list by checking the checkbox.
 - *Type: Select "Allow List" or "Deny List".
 - Description: Add a description.
6. Click "OK" to save changes.

6.2.8.2 Upgrading or downgrading security events

Purpose

Security events are automatically classified as Event, Warning, or Alert according to their severity.

The "Configuration" > "Anomaly baseline" page also allows security events to be upgraded or downgraded in severity for specific assets. Use the "Event Upgrade/Downgrade" tab to do this.

For example, if the SINEC Security Monitor system rates a security event as an "Alert", you can downgrade the security event to "Warning", if the administrators classifies it as not severe.

Table 6-8 Upgrade/Downgrade functions

Function	Description
Add	Add a new upgrade or downgrade
Edit	Edit an upgrade or downgrade
Delete	Delete the selected upgrade or downgrade
Refresh	Refresh the table
All Types	Select type (All Types, Upgrade, Downgrade) for filtering the search results.

Search	Search for event ID, description
Clear	Clear all search fields

Access the event upgrade/downgrade tab

1. Log in to the WBM.
2. Select the "Configuration" > "Anomaly Baseline" menu.
3. Select the "Event Upgrade/Downgrade" tab.

Upgrade/Downgrade an event

1. Log in to the WBM.
2. Select the "Configuration" > "Anomaly baseline" menu.
3. Select the "Event Upgrade/Downgrade" tab.
4. Click "Add".
5. Enter the required information (fields marked with "*" are mandatory):
 - *Upgrade/Downgrade: Upgrade or downgrade.
 - *Event Type: Select an event type from the drop-down list.
 - Event Action: Add an asset IP address.
Note: To match any value, leave it empty.
The content of this field varies depending on the event type.
 - Description: Add a description.
6. Click "OK" to save changes.

6.2.9 Configuring security reports

Purpose

The SINEC Security Monitor System issues regular reports to inform about the overall security situation of the monitored OT environment. Follow the instructions below to configure these reports.

Configure report parameters

1. Log in to the WBM.
2. Select the "Configuration" > "Report" menu.

3. Enter the required information (fields marked with "*" are mandatory):

- *Company Name
Enter the company name.
- *Report Cycle
Monthly: The report is automatically generated on the first day of each month.
Weekly: The report is automatically generated at 1:00 a.m. every Monday.
- *Send email notification
Enabled: The report is automatically sent as an email attachment.
Disabled: The report is not sent as an email attachment.
- Language
Select from English, Chinese, or German.
- *Retention period (days)
Enter an integer number greater than zero to determine how long the reports are to be stored.

You can enter the optional settings that are added to the front page of the report.

4. Click "Save" to save changes.

Go to the "Report" menu to download reports from the past or to export customized reports. Refer to chapter Generating a security monitoring report (Page 202).

For email settings for reports, refer to chapter Setting up email notifications (Page 130).

6.2.10 Configuring system notifications

Purpose

The notification page enables notifications to be set up so they can be sent in the event of particular system or security event notifications.

The lists on these tabs list all possible system and security events. Add an appropriate notification type (Popup window, Sound alarm, Email notification) for each event. Use the buttons on the page to assist the selection of notification types for the events.

- **Enable all notifications**
Set checkmarks for all system/security events in the list for all notification categories (popup window, sound alarm, email notification).
- **Enable pop-up notifications only**
Set checkmarks for all system/security events in the list for notification by popup window. The notification popup window will appear in the WBM.
- **Enable notification sound only**
Set checkmarks for all system/security events in the list for notification by sound alarm. The notification will be announced by a sound.
- **Enable email notifications only**
Set checkmarks for all system/security events in the list for notification by email. The configured email recipient will get an email notification.

- **Disable all notifications**
Remove all checkmarks
- **Message content**
Add appropriate message content for each event.

Accessing event notifications

1. Log in to the WBM.
2. Select the "Configuration" > "Notifications" menu.
3. Select the "System Event Notifications" on the first tab of the page.
4. Click "Save" to save changes.
5. Select "Security Event Notifications" on the second tab of the page.
6. Click "Save" to save changes.

Note: There are only 14 system events, but a few hundred security events.

For instructions to set up email notifications please refer to chapter Setting up email notifications (Page 130).

Example: Configuring notifications for license and certificate expiry

Add an appropriate notification type (Popup window, Sound alarm, Email notification) for each event.

Table 6-9 System events about license and certificate expiry

Event ID	Event Name
9011	The license will expire in one month.
9012	The license has expired but not exceeded the time limit of three months.
9013	The certificate is about to expire.
9014	The certificate has expired.

1. Log in to the WBM.
2. Select the "Configuration" > "Notifications" menu.
3. Select the "System Event Notifications" on the first tab of the page.
4. Select a "Notification type" for all events concerning license expiry.
5. Click "Save" to save changes.

6.3 Setting the SINEC Security Monitor working mode

For more information on working modes, refer to chapter Working modes (Page 49).

Set the SINEC Security Monitor System to learning mode

Note

Set Learning Mode for about two weeks

Let the SINEC Security Monitor System run in Learning Mode for about two weeks to collect sufficient data from the environment

1. Log in to the WBM.
2. Select the "Configuration" > "System" menu.
3. Select the "Working Mode" tab.
4. Click "Learning Mode".

Review and adjust collected data

1. Log in to the WBM.
2. Select the "Configuration" > "Anomaly Baseline" menu.
The baselines listed in this menu are sorted into the following categories:
 - Applications baseline
 - Communication links baseline
 - USB devices baseline
 - IP addresses baseline
 - Accounts baseline
3. Review baselines and policies and, if necessary, edit or add policies.
Refer to chapter Configuring anomaly baselines (Page 136).

Set the SINEC Security Monitor System to operational mode

It is recommended to enable Learning Mode for at least two weeks. The SINEC Security Monitor System can be switched to Operational Mode when all baselines are complete and is ready for use. In Operational Mode everything new in environment will trigger a notification.

1. Log in to the WBM.
2. Select the "Configuration" > "System" menu.
3. Select the "Working Mode" tab.
4. Click "Operational Mode".

6.4 Certificate management

6.4.1 Overview

The "Configuration" > "Certificate Management" page bundles certificate management for general CA certificates, SINEC Security Monitor Server (WBM) certificates and SINEC Security Monitor Sensor certificates.

Table 6-10 Overview of CA and TLS certificates

Tab	Name	Purpose	Max. number	Import/export	File format or type
CA Certificate	osaca	Certificate signing	1	Import, export	X.509 certificate in PEM format
SSM Server	gateway.osa.siemens.com	Digital Signature, Key Encipherment TLS Web Server Authentication	1	Import	PKCS#12, JKS
	logstash.osa.siemens.com	Digital Signature, Key Encipherment TLS Web Server Authentication, TLS Web Client Authentication	1	Import	PKCS#12, JKS
	ssmctl.grpc.osa.siemens.com	Digital Signature, Key Encipherment TLS Web Client Authentication	1	Import	PKCS#12, JKS
	collector.osa.siemens.com	Digital Signature, Key Encipherment TLS Web Server Authentication	1	Import	PKCS#12, JKS
	gateway.email.osa.siemens.com	Digital Signature, Key Encipherment TLS Web Client Authentication	1	Import	PKCS#12, JKS
	syslog-ng.osa.siemens.com	Digital Signature, Key Encipherment TLS Web Server Authentication, TLS Web Client Authentication	1	Import	PKCS#12, JKS
	logforward.osa.siemens.com	Digital Signature, Key Encipherment TLS Web Client Authentication	1	Import	PKCS#12, JKS
Sensor	agent.osa.siemens.com	Digital Signature, Key Encipherment TLS Web Client Authentication	1 per sensor	Import	PKCS#12, JKS
	beats.osa.siemens.com	Digital Signature, Key Encipherment TLS Web Client Authentication	1 per sensor	Import	PKCS#12, JKS
	grpc.server.osa.siemens.com	Digital Signature, Key Encipherment TLS Web Server Authentication	1 per sensor	Import	PKCS#12, JKS
	syslog-ng.osa.siemens.com	Digital Signature, Key Encipherment TLS Web Server Authentication, TLS Web Client Authentication	1 per sensor	Import	PKCS#12, JKS
Agent	agent.osa.siemens.com	Digital Signature, Key Encipherment TLS Web Client Authentication	1 per agent	Import	PKCS#12, JKS
	beats.osa.siemens.com	Digital Signature, Key Encipherment TLS Web Client Authentication	1 per agent	Import	PKCS#12, JKS

Passwords

Key store certificates are password-protected. For the certificate import, enter a key store password and a key pair password.

6.4.2 Managing certificates

Import a Customer CA certificate

The system stores only one Customer CA certificate. Repeated importing overwrites the already imported Customer CA certificate.

1. Log in to the WBM.
2. Select the "Configuration" > "Certificate management" menu.
3. Select the "CA Certificate" tab.
4. Click "Import".
The "Import" window opens.
5. Browse for a X.509 Root CA certificate in ".pem" format.
6. Click "Upload".

new certificate record with CA Type as "Customer CA" is displayed in the list.

Import a Customer Communication Certificate to the Sensor

1. Click on the "Sensor" tab.
2. Select the target Sensor from the list.
3. Find the certificate record with Subject as "CN=beats.osa.siemens.com".
4. Click on the "Import" button.
5. A new window will pop up.
6. Click on the "Browse" button.
7. Select the Customer Communication Certificate file in PKCS#12 format.
8. Enter the Key Store Password.
9. Enter the Key Pair Password.
10. Click on the "OK" button
11. Ensure that the Communication Certificate is imported successfully.

View CA certificate information

1. Log in to the WBM.
2. Select the "Configuration" > "Certificate management" menu.

3. Select the "CA Certificate" tab.
4. Click "More" in the "Action" column.
The "Certificate Information" window opens.

Export the CA certificate

1. Log in to the WBM.
2. Select the "Configuration" > "Certificate management" menu.
3. Select the "CA Certificate" tab.
4. Click "Export."
The `OSACA.pem` file is downloaded to your computer.

View a TLS certificate

1. Log in to the WBM.
2. Select the "Configuration" > "Certificate management" menu.
3. Select a tab, choose between "Server", "Sensor" and "Agent".
4. For Sensor or Agent, select a device from the drop-down menu.
5. Click "More" in "Actions" column.
6. The "Certificate Information" window opens.

Import a TLS certificate

1. Log in to the WBM.
2. Select the "Configuration" > "Certificate management" menu.
3. Select a tab, choose between "Server", "Sensor" and "Agent".
4. For Sensor or Agent, select a device from the drop-down menu.
5. Click "Import" in the "Actions" column.
The "Import" window opens.
6. Enter the required information. Fields marked with "*" are mandatory.
 - ***Key Store Type**
Select the certificate type from the drop-down menu.
Select from: PKCS#12 (default), JKS.
 - ***Key Store File**
Click "Browse" and select the certificate file.
Note: The certificate container must have only one entry (with corresponding private key).
 - **Key Store Password**
Enter the password of the certificate container, when available.
 - **Key Pair Password**
Enter the password for access to the key in the key store, when available.
7. Click "OK".

6.5 Third-party system integration

Table 6-11 Supported third-party systems

Systems	Description
The SINEC Security Monitor System supports receiving or forwarding data in standard syslog data format (RFC3164 or RFC5424).	The security administrator can configure the third-party systems to forward their data to the SINEC Security Monitor System for in-depth analysis. At the same time, SINEC Security Monitor can not only configure the original logs and security events of the SINEC Security Monitor System but also forward the configured original logs and security events of the SINEC Security Monitor System to third-party systems in syslog mode.

6.5.1 Configuring security log forwarding to third-party systems

1. Log in to the WBM.
2. Select the "Configuration" > "Log Settings" menu.
3. Select the "Log Forwarding" tab.
4. Enter the required information. Fields marked with "*" are mandatory.
 - ***IP address**
Enter the IP address of the third-party server to receive the forwarded logs.
 - ***Port**
Enter the port used for receiving forwarded logs.
 - ***Protocol**
Select a communication protocol: Select TLS (default), TCP or UDP.
 - ***RFC**
Select a RFC standard for the log format. Select RFC3164 or RFC5424 (default). Refer to Security Forwarding Data Format (Page 247).
 - ***Data source**
Select what kind of data you want to forward: Check "Raw logs" and "Security events".
5. For the TLS protocol:
 - Download a client certificate (osaca.pem).
 - Check "Enable server authentication".
 - Upload a server certificate.
The server certificate must be a X.509 certificate in ".pem" format.
6. To save changes, click "Save".
The service restarts, this takes several minutes.
7. Log in to the third-party system to verify the reception of raw logs or security events.

Preparing, adding, and managing data sources

7.1 SINEC Security Monitor Sensor

7.1.1 Adding Sensors

Settings for "Active Probing", "SNMP V1", "SNMP V3" and "Remote Agentless Nodes" are located at the bottom of the "Edit" window of a SINEC Security Monitor Sensor. These settings are not mandatory and can be configured when required.

Add a Sensor

1. Log in to the WBM.
2. Select the "Configuration" > "Sensor" menu.
3. Click on "Add".
4. Enter the required information. Fields marked with "*" are mandatory.
 - ***Name**
Sensor name
 - ***Sensor**
Select a SINEC Security Monitor Sensor from the drop-down list which is not marked with "(Binded)".
For an explanation of "Binded", unbinded and "Inactive", see table "SSM Sensor installation status".
 - **Manage**
Click "Manage" to manage the newly installed SINEC Security Monitor Sensors that are already pushed to SINEC Security Monitor Server but not yet assigned on the page.
 - **Destination**
Destination address (IP address of the SINEC Security Monitor Server)
 - **Monitoring area**
Add the actual network area.
 - **Owner**
Add the name of the owner or manager of the device.
 - ***Internal Networks**
192.168.0.0/24, 10.10.0.0/16 (examples)
5. *To save changes, click "OK".

Note: When a SINEC Security Monitor Sensor does not show up in the "Sensor" drop-down list, ensure a stable network connection between the SINEC Security Monitor Sensor and the SINEC Security Monitor Server.

For an explanation of the SINEC Security Monitor Sensor status icons, refer to table in section Managing Sensors (Page 150).

Table 7-1 SSM Sensor installation status

Status	Description
Unbinded (to be binded)	For example: [192.168.xxx.xxx] sensor.logagent This SSM Sensor is free. You can add it.
Binded	For example: [192.168.xxx.xxx] sensor.logagent (Binded) This SSM Sensor has been installed and is up and running.
Inactive	For example: [192.168.xxx.xxx] sensor.logagent (Inactive) This SSM Sensor has already been installed, but not yet been activated with a license.

7.1.2 Managing Sensors

1. Log in to the WBM.
2. Select the "Configuration" > "Sensor" menu.

Refresh the Sensor list

1. Log in to the WBM
2. Select the "Configuration" > "Sensor" menu.
3. Click the "Refresh" button to refresh the list of Sensors.

Check the performance

1. Log in to the WBM.
2. Select the "Configuration" > "Sensor" menu.
3. Note the color of the status icon.
4. Select the "System" > "Diagnostics" menu for more information.

Status icon

The color of the status icon indicates the status of the SINEC Security Monitor Sensor.

Table 7-2 Status icons

Status icon	Explanation
Blue	Normal status. The "Stop" or "Start" buttons are shown in the "Collect Logs" column.
Red	Failure status. The "Stop" or "Start" buttons are not shown in the "Collect Logs" column.
Blinking	The SINEC Security Monitor System is trying to connect to the SINEC Security Monitor Sensor.

Start data collection

1. Log in to the WBM.
2. Select the "Configuration" > "Sensor" menu.
3. Click the "Start" button in the "Collect Logs" column of the list.

Stop data collection

1. Log in to the WBM.
2. Select the "Configuration" > "Sensor" menu.
3. Click the "Stop" button in the "Collect Logs" column of the list.

Delete a SINEC Security Monitor Sensor

1. Log in to the WBM.
2. Select the "Configuration" > "Sensor" menu.
3. Select a SINEC Security Monitor Sensor.
4. Click the "Delete" button to delete the SINEC Security Monitor Sensor.
5. Confirm with the "OK" button.

Manage registered SSM Sensor data

SSM Sensors periodically send registration data to the SSM Server.

The "Manage" window lists registration data of SSM Sensors which are registered to the SSM Server but not binded in the WBM.

You can use the "Manage" window to clean up useless registration data.

When a SSM Sensor is no longer needed, you can remove it from the WBM.

As a second step, you can delete the registration data of this device in the "Manage" window.

Note: The "Manage" button of the "Configuration" > "Sensor" menu is only available in the "Edit" window, when at least SSM Sensor is configured in the WBM.

You can also access the "Manage" button in the "Add" window.

Remove registration data

1. Log in to the WBM.
2. Select the "Configuration" > "Sensor" menu.
3. To access the "Manage" window, click "Edit" for a random SSM Sensor.
4. Click "Manage".
5. Identify the SSM Sensor's registration data that you want to remove.
6. Click "Delete" in the "Actions" column.

7.1.3 Editing a Sensor

The "Offline time" setting is only available here in the "Edit" window.

1. Log in to the WBM.
2. Select the "Configuration" > "Sensor" menu.
3. Select a sensor and click "Edit".
4. Enter the required information in the "Basic Info" fields (fields marked with "*" are mandatory):
 - ***Name**
Name of the Sensor.
 - ***Sensor**
The drop-down list shows all available SINEC Security Monitor Sensors.
 - **Manage**
Option to manage the newly installed SINEC Security Monitor Sensors already pushed to SINEC Security Monitor Server but not yet assigned on the page.
 - **Destination**
Destination address (IP address of the SINEC Security Monitor Server).
 - **Monitoring area**
IP range of assets monitored by this SINEC Security Monitor Sensor
 - **Owner**
Optional
 - ***Offline time (seconds)**
7,200 (default). If an asset is not found in this time, it is considered offline.
 - ***Internal networks**
Add internal networks separated by comma ",".
Format: 192.186.100.0/24
Internal networks are network segments whose network flow should be monitored by the SINEC Security Monitor Sensor.
5. Click "OK" to save changes.

Advantages and disadvantages of Active Probing

When using passive monitoring, you might not be able to get all required details of the detected assets. For these cases, you can enable the Active Probing feature, so that more accurate asset details can be retrieved. The system can automatically associate security events with those assets, based on the correlation rules, the vulnerability library and the threat library.

Active Probing is an intrusive technique and can therefore have impact for example on running or calibrated devices. Active Probing should only be applied if the risks are known, understood and acceptable.

Active Probing can be configured in order to reduce the potential impact. Configure Active Probing with caution.

Note

Active Probing is disabled by default.

Using Active Probing is not mandatory. You can configure Active Probing later if required.

Add the active probing configuration

1. Log in to the WBM.
2. Select the "Configuration" > "Sensor" menu.
3. Select a sensor and click "Edit".
4. Scroll down.
5. In the "Active Probing Configuration", configure the active detection parameters of the SINEC Security Monitor Sensor (fields marked with "*" are mandatory):
 - ***Active probing**
Enabled or Disabled (default).
 - ***Time range**
00:00 to 23:59 (default).
 - **Asset interval (seconds)**
60 (default). The interval is the time between the detection of one device and the detection of a second device.
 - **Packet interval (seconds)**
10 (default). The interval is the time between two packets being sent when the same device is probed.
 - **Supported protocol**
Select the protocol to which the asset responds: SNMP, PN-DCP, S7, ModBus, EtherNet/IP
 - ***NMAP parameters** for OS (operating system) detection
 - "Limit" (-osscan-limit): Limit OS detection to only designated hosts.
At least ensure that the host has one open port and one closed port respectively.
 - "Guess Parameters" (-osscan-guess)(default): Aggressively guess the system type of the hosts.
This scan may result in a significant decrease in accuracy, but it will provide you with as many potential operating systems as possible.
6. Click "OK" to save changes.

Add SNMP settings

Prerequisite: "Active probing" must be enabled and "SNMP" must be selected as a "Supported Protocol".

1. Log in to the WBM.
2. Select the "Configuration" > "Sensor" menu.

7.1 SINEC Security Monitor Sensor

3. Select a sensor and click "Edit".
4. Scroll down for "SNMP V1" and "SNMP V3" settings.
5. Add SNMP V1 parameters as needed:
 - **Device IP**
IP address of the assets that should be detected, for example 10.11.8.52
 - **Community**
"public" (default); other devices may use different values, for example: "private".
 - **Arguments**, for example
"-t 1": set timeout time to 1 second
"-v 1": set version to 1
All parameters should be entered in order and separated by spaces.
6. Add SNMP V3 parameters as needed:
 - **Device IP**
IP address of the assets that should be detected, for example 10.11.8.52.
 - **Vlan ID**
Virtual local area network ID where the assets are located, for example 2060.
 - **Community**
"public" (default); other devices may use different values, for example: "private".
 - **Arguments**, for example:
"-t 1": set timeout time to 1 second
"-v 1": set version to 1
All parameters should be entered in order and separated by spaces.
 - **Auth Type** (Authentication type) values:
"authPriv": Authentication and encryption (tested and validated)
"noAuth": No authentication (tested and validated)
"auth": Authentication only
 - **Username**
Username of an asset, for example: remoteuser1
 - **Password**
Authentication password for authentication types "authPriv" and "auth".
 - **Crypted Password**
Encryption password, for authentication type "authPriv".
7. Click "OK" to save changes.

Add remote Agentless Nodes

Note

Refer to chapter Preparing and adding a Microsoft Windows computer for agentless security log collection (Page 160).

1. Log in to the WBM.
2. Select the "Configuration" > "Sensor" menu.

3. Select a sensor and click "Edit".
4. Scroll down and click the "Remote Agentless Nodes" tab.
5. Activate the "System Log" options:
 - System
 - Security
 - Application
6. Click "Add remote Agentless Node" and add:
 - IP address
 - Domain name
 - User name
 - Password
7. For authentication, download a "Client CA Certificate".
8. Upload an "Agentless node CA Certificate". It must be a X.509 certificate in ".pem" format.
9. Select a "Security Grade".
Refer to table "Security Grades" in chapter Preparing and adding a Microsoft Windows computer for agentless security log collection (Page 160) for information on security grades.
10. Click "OK" to save changes.

Modify a Sensor's network configuration

1. Log in to the WBM.
2. Select the "Configuration" > "Sensor" menu.
3. Select a sensor and click "Edit".
4. Scroll down and click the "Network" tab.
5. For each Network interface, there are following options
 - **Name and State**
of the interface are displayed.
 - **Monitor interface**
You can check this option to enable it as a monitor interface.
 - ***IP address**
IP address of the network interface
 - ***Subnet mask**
Subnet mask of the network interface
 - **Gateway**
Gateway of the network interface
 - **Main NIC**
You can check this option to enable it as a main network interface.
6. Click "Save" to save changes.

7.2 SINEC Security Monitor Agent

7.2.1 Installing the SINEC Security Monitor Agent on a Microsoft Windows-based asset

Prerequisites

- This procedure requires administrator privileges.
- The SINEC-Security-Monitor-Agent-4.9.0.exe file from the SINEC Security Monitor software package is required.

Table 7-3 Supported operating systems

Operating system	Version	Operating system build
Microsoft Windows 2012 RC Server	R2	9600
Microsoft Windows 2016 Server	10.0.14393	14393.447
Microsoft Windows 2019 Server	10.0.17763.107	17763.1
Microsoft Windows 10 Pro	2004	19041.264
Microsoft Windows 10 Pro	20H2	19042
Microsoft Windows 10	21H2	19044

Installation of the SINEC Security Monitor Agent

During the SINEC Security Monitor Agent software installation, a destination IP address needs to be entered. The data flow goes from the SINEC Security Monitor Agent to the SINEC Security Monitor Server via the Sensor. In this scenario, the destination IP address is an IP address of the SINEC Security Monitor Sensor.

Refer to chapter Communication between SSM Agent and SSM Server or SSM Sensor (Page 59) to determine the correct IP address.

1. Copy the {SINEC Security Monitor Agent}.exe file to the Microsoft Windows workstation.
2. Verify the signature of the SINEC Security Monitor Agent installation package for authenticity and integrity:
Refer to chapter Verifying signatures of signed installation files (Page 82).
3. Uncompress the {SINEC Security Monitor Agent}.exe file.
4. For a 64-bit operating system, go to the 'windows_x64' folder.
For a 32-bit operating system, go to the 'windows_x86' folder.
5. Run `installer.exe` with administrator privileges.
6. When prompted, enter the IP address of the workstation.
7. When prompted, enter the destination IP address, to which the SINEC Security Monitor Agent transfers the logs. This address could be either the SINEC Security Monitor Sensor's or the SINEC Security Monitor Server's IP address. Refer to the scenarios above to select the correct destination IP address.

8. Generate an agent public key:
To exit, select "N".
To keep the public key displayed for consistency check, select "Y" when you add the data source after the Agent installation on the SINEC Security Monitor WBM.
9. Press [Windows] + [R].
The "Run" command window opens.
10. Run 'services.msc' and check the status of the SINEC Security Monitor LogAgent and the UpdateAgent service on the "Extended" tab.
The "Status" should be displayed as "Running" and "Startup Type" should be displayed as "Automatic".

7.2.2 Enabling and Configuring USB Event Logging on Windows Devices

Enabling USB Event Logging on Windows Devices

By default, USB event logging is disabled on Microsoft Windows devices. To track USB plug-in and plug-out events, you must enable this feature on the SSM Agent host computer or any other computer that needs to log these events.

- When a USB flash drive is plugged into a Windows computer, the following Event IDs will appear in the "Operational Log" of the Windows Event Viewer: 2003, 2004, 2006, 2010, 2100, 2101, 2105, and 2106.
- When a USB flash drive is removed from a Windows computer, Event IDs 2100 and 2102 will be recorded in the "Operational Log" of the Windows Event Viewer.

Since USB event logging is disabled by default, you need to enable it to monitor this information.

Follow these steps to enable USB event logging on the OSA Agent host computer:

1. Open Event Viewer: On the SSM Agent host computer, open the Event Viewer application.
2. Open Operational Log Properties: On the left side of the Event Viewer window, navigate to "Applications and Services Logs," then "Microsoft," and then "Windows." Under "Windows," select "DriverFrameworks-UserMode," and right-click on "Operational."
3. Enable Logging: In the "Log Properties - Operational (Type: Operational)" window, check the option labeled "Enable logging."
4. Save Changes: Click "OK" to save the changes.

USB event logging should now be enabled, allowing you to monitor USB plug-in and plug-out events on your Windows computer.

Modify the winlogbeat.yml File

After installing the SSM Agent, follow these steps to modify the winlogbeat.yml file:

1. On your Microsoft Windows computer, navigate to the following path:
`C:\Program Files\Siemens\LogAgent\winlogbeat.yml`
2. Open the winlogbeat.yml file with a suitable text editor (for example, Notepad++).

7.2 SINEC Security Monitor Agent

3. In the winlogbeat.yml file, find the section labeled:
winlogbeat:
 event_logs:
4. Under the event_logs section, add the following lines:
 -ignore_older:1h
 -name:Microsoft-Windows-DriverFrameworks-UserMode/Operational
5. Save your changes and close the text editor.
6. Press [Windows] + [R] to open the Run command window.
7. Type `services.msc` and press [Enter] to open the Services management console.
8. In the Services console, find and select the "logagent" service.
9. Restart the "logagent" service by right-clicking on it and selecting "Restart".
Following these steps will ensure that USB event logging is enabled and properly configured on your Windows computer, allowing you to monitor USB plug-in and plug-out events effectively.

7.2.3 Adding a data source in agent mode

Instructions for adding a supervisor PC in agent mode as a data source after the SINEC Security Monitor Agent software has been installed on the computer.

1. Log in to the WBM.
2. Select the "Configuration" > "Data Sources" menu and click "Add".

3. Add data source in Agent Mode.
Enter the required information. Fields marked with "*" are mandatory.
 - ***Collection mode**
Select "Agent".
 - ***Name**
Enter a name for the Agent data source.
 - ***Agent**
Select the data source from the drop-down menu.
For an explanation of "Binded" and unbinded, see table "SSM Agent installation status".
 - **Manage:**
Click "Manage". The "Manage" window shows data sources already pushed to the SSM Server but not yet registered to the page.
 - **Destination**
Destination IP address of the SINEC Security Monitor Sensor
 - ***Operating system**
Select the operating system of the client for log collection.
Available operating systems: Windows, Linux, Others
 - ***Asset**
The asset type of the client for log collection.
Available asset types: General, Linux Host, Windows Host, WinCC, Firewall, Switch
 - **System log**
Type of log collected. Only for Microsoft Windows-based data sources.
Activate the options: System, Security, Application

Note

You cannot add a data source if the certificate file is already in use by another SINEC Security Monitor Agent. If this is the case, an error message appears: "The current agent uses the same certificate as agent [IP address][user name]. Please reinstall the agent or replace the current certificate with an unused certificate."

4. Click "Add application log".
5. Enter a log name.
For example: test
6. Add a log path (.txt, .log for example).
For example: C:\Users\admin\Desktop\test.txt
7. To save changes, click "OK".

Table 7-4 SSM Agent installation status

Status	Description
Unbinded (to be binded)	For example: [192.168.xxx.xxx] Computer_Production_A This SSM Agent is free. You can add it.
Binded	For example: [192.168.xxx.xxx] Computer_Production_B (Binded) This SSM Agent has been installed and is up and running.

7.2.4 Verifying a SINEC Security Monitor Agent after installation

Verify the result of the configuration on the logs page

1. Log in to the WBM.
2. Select the "Security Events" > "Logs" menu.
3. Select the corresponding data source from the "All data sources" drop-down menu.
4. If events are displayed on the list, data collection is successful.

7.3 Agentless security log collection

7.3.1 Preparing and adding a Microsoft Windows computer for agentless security log collection

Introduction

For security log collection from Microsoft Windows devices without installing the SINEC Security Monitor Agent software, two methods of remote data acquisition are introduced.

- **WinRM configuration**
WinRM uses Windows Remote Management (WinRM) over TLS for remote data acquisition from Microsoft Windows endpoints.
- **Remote WMI configuration**
Remote WMI uses the Windows Management Instrumentation (WMI) protocol for remote data acquisition.

Note

- WinRM offers better security and compatibility. It is preferable to use WinRM for remote data collection.
 - The Microsoft Windows operating systems in the table below were tested without additional security patches installed. If the target computer has newer security patches installed, it is preferable to use WinRM.
-

Supported deployment scenarios for agentless security log collection

Refer to chapter Agentless communication with the SSM Server (Page 62).

Table 7-5 Supported Microsoft Windows operating systems for agentless security log collection

Operating system	Version	OS build	Remote WMI	WinRM
Microsoft Windows 7	Ultimate	6.1.7600	Supported	Supported (Security grade ≥ 2)

Microsoft Windows 10 Enterprise	1607	10.0.14393	Supported	Supported (Security grade = 5)
Microsoft Windows 10 Pro	1709	10.0.16299	Not supported	Supported (Security grade = 5)
Microsoft Windows 10 LTSC	1809	10.0.17763	Supported	Supported (Security grade = 5)
Windows 10 Pro	1903	10.0.18362	Supported	Supported (Security Grade =5)
Microsoft Windows 10 Pro	1909	10.0.18363	Supported	Supported (Security grade = 5)
Windows 10 Pro	2004	10.0.19041	Non-supported	Supported (Security Grade =5)
Microsoft Windows 11	22H2	10.0.22621	Not supported	Supported (Security grade ≥ 2)
Microsoft Windows Server 2016 Standard	R2	10.0.14393	Not supported	Supported (Security grade = 5)
Microsoft Windows Server 2019	R2	10.0.17763	Not supported	Supported (Security grade = 5)

Definition of security grades

The following security grades are defined according to the "Siemens Level" to rate cryptographic algorithms.

Table 7-6 Security grades to rate cryptographic algorithms

Security grade	Criteria for algorithms
5	No known problems with the algorithm suite or its application. The cipher suite provides Perfect Forward Secrecy (PFS).
4	No known problems with the algorithm suite or its application. The cipher suite does not provide Perfect Forward Secrecy (PFS).
3	At least one problematic aspect is known for the cipher suite. Without mitigation, the application is not recommended.
2	Two problematic aspects are known for the cipher suite. The application is not recommended.
1	The cipher suite application requires specific consideration and may be used with certain boundary conditions.
0	The cipher suite is regarded as broken and should not be used anymore.

Prerequisites

These procedures require administrator privileges and Microsoft Windows administrator training.

Enabling USB Event Logging on Windows Devices

For information on how to enable USB event logging, refer to chapter Enabling and Configuring USB Event Logging on Windows Devices (Page 157).

7.3.1.1 Configuring WinRM

Installing agentless log collection over WinRM is the recommended procedure.

Note

When the CPU or memory usage of a remote Microsoft Windows endpoint exceeds 80% for more than 25 seconds, the remote WinRM acquisition for this endpoint will be suspended automatically until its system resources become sufficient again.

Prerequisite

As the log collection is routed via the SSM Sensor, first, an SSM Sensor must be installed. Then the WinRM configuration can be added to the SSM Sensor installation.

Environment information

Table 7-7 Environment information

Component name	IP address (examples)	Version (examples)	Description
Server	10.11.60.248	4.9.0	SINEC Security Monitor Server
Sensor	172.30.1.131	4.9.0	SINEC Security Monitor Sensor
Agentless Package	n/a	SINEC-Security-Monitor-Agent-Less-4.9.0-{version}.zip	This package is used for WinRM environment setup, including creating a self-signing certificate on a CA workstation and setup of the WinRM service on a Microsoft Windows client. This package is released as a .zip file. Before using it, extract it to an appropriate location.
CA Workstation A*	10.11.0.207	Microsoft Windows 10 21H2	This Workstation serves as the Certification Authority (CA) when the organization does not have a Public Key Infrastructure (PKI). It issues certificates for all the Microsoft Windows clients.
Windows Client B*	172.30.1.110	Microsoft Windows 10 1909	This Microsoft Windows client is a machine located in the production line, which is the data source of WinRM.
User Workstation C*	10.11.60.188	Microsoft Windows 10 21H2	This Microsoft Windows workstation is used by the installer. It is used for connecting to SSM's web portal and perform configuration operations.

* You can use the same Microsoft Windows computer for all these functions if the computer can access the WBM.

Note

The installation instructions in this chapter refer to the component names in the table "Environment information".

Identify the components carefully to avoid confusion.

Manage the execution policy

During the installation procedure on "CA workstation A" and "Windows Endpoint C", you set the execution policy to `RemoteSigned -Force` in the Windows PowerShell. This is necessary to run the installation. After the installation, set the execution policy back to the original state.

1. Command to query the current execution policy before the installation:
`Get-ExecutionPolicy`
2. Note the reply of the Windows PowerShell.
For example: `Restricted`
3. After the installation, set the execution policy back to the previous state, for example: `Restricted`.
Command:
`Set-ExecutionPolicy Restricted`

Note: If setting the execution policy fails, you also need to change the Windows Group Policy. Refer to link (https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_execution_policies?view=powershell-7.4)

Configuration workflow

Note

Customize the Client CA certificate `osaca.pem`

You can upload a custom client CA certificate to the SSM Server. For more information see Managing certificates (Page 146).

You find the main workflow for the WinRM configuration below:

1. Copy and unzip the "SINEC-Security-Monitor-AgentLess-4.9.0-{version}.zip" to the CA Workstation A.
Refer to section "Generate certificates on the CA Workstation A".
2. On the CA Workstation A, generate certificates.
Refer to section "Generate certificates on the CA Workstation A".
3. Copy the entire "SINEC-Security-Monitor-AgentLess-4.9.0-{version}\agentless\WinRM" directory to the User Workstation C.
Content of the WinRM directory at this point:
 - generated Endpoint certificates
 - configuration scriptsRefer to section "Generate certificates on the CA Workstation A".

7.3 Agentless security log collection

4. On User Workstation C, access the WBM.
 - Download the Client CA certificate `osaca.pem` or the customized Client CA certificate `customerca.pem`, if available.
 - Place the Client CA certificate into the "SINEC-Security-Monitor-AgentLess-4.9.0-{version}\agentless\WinRM\cert" directory.
 - Upload the Agentless node CA certificate `endpointca.pem` from the "SINEC-Security-Monitor-AgentLess-4.9.0-{version}\WinRM\cert" directory on the SSM Server. Refer to section "Download and upload the certificate on User Workstation C".
5. Copy the entire "SINEC-Security-Monitor-AgentLess-4.9.0-{version}\agentless\WinRM" directory from User Workstation C to Windows Client B.
Content of the WinRM directory at this point:
 - downloaded Server certificate
 - generated Endpoint certificates
 - configuration scriptsRefer to section "Run the configuration script on the Windows Client B".
6. On the Windows Client B, run the configuration scripts and set the account name and password for WinRM remote data acquisition.
Refer to section "Run the configuration script on the Windows Client B".
7. On the User Workstation C, access the WBM.
Add remote agentless nodes using the configured account name and password on Windows Client B.
Refer to section "Add Remote Agentless Nodes on User Workstation C".
8. Verify the configuration results.
Refer to sections "Verify the result of the configuration in the audit log" and "Verify the result of the configuration on the logs page".

Generate certificates on the CA workstation A

Certificates are created on CA Workstation A and distributed to the Windows Client B and the User Workstation C.

1. Copy the "SINEC-Security-Monitor-AgentLess-4.9.0-{version}.zip" to the CA Workstation A and unzip.
2. Run the Windows PowerShell as an Administrator.
3. Test the current execution policy.
For instructions, refer to section "Manage the execution policy"
4. Run the command to set the execution policy of the system:
`Set-ExecutionPolicy RemoteSigned -Force`
5. Go to the CertToolkit directory.
`cd C:\{path}\SINEC-Security-Monitor-AgentLess-4.9.0-{version}\agentless\CertToolkit`
6. Run the script.
`.\CertGenerator.ps1`

7. At the prompt, enter the IP address of the Windows Client B and press "Enter".
Example: 172.30.1.110
The cert package is generated.
8. Copy the entire "SINEC-Security-Monitor-AgentLess-4.9.0-{version}\agentless\WinRM" directory to the Windows Client B and the User Workstation C. This directory contains all needed certificates and configuration scripts.
9. Set the execution policy back to the previous state.

Download and upload the certificates on User Workstation C

In this step, the certificates for authentication are downloaded, uploaded and distributed.

1. Log in to the WBM.
2. Select the "Configuration" > "Sensor" menu, select the SSM Sensor and click "Edit".
3. Scroll down and select the "Remote agentless node" tab.
4. Click "Download" to download the client CA certificate "osaca.pem" or "customerca.pem".
5. Place the client CA certificate "osaca.pem" or "customerca.pem" into the "SSM agentless setup package 4.9.0-{version}\agentless\WinRM\cert" directory.
6. Click "Upload" and navigate to "SSM agentless setup package 4.9.0-{version}\agentless\WinRM\cert".
7. Select the file "endpointca.pem" and click "Open".
8. Click "OK".
9. Copy the entire "SSM agentless setup package 4.9.0-{version}\agentless\WinRM" directory from the User Workstation C to the Windows Client B.

Run the configuration script on the Windows Client B

During the following process, a user account for WinRM remote acquisition is created on the device and the device is configured for WinRM.

1. Run the Windows PowerShell as an administrator.
2. Go to the directory where the script package is located.
`cd C:\{path}\WinRM`
3. Test the current execution policy.
For instructions, refer to section "Manage the execution policy"
4. Run the command to set the execution policy of the system:
`Set-ExecutionPolicy RemoteSigned -Force`
5. Run the script:
`.\SetupWinRM.ps1`
This process takes a few minutes.
6. At the prompt, enter an account name.
Example: agentlessReader

7.3 Agentless security log collection

7. Enter a password for the account "agentlessReader" and confirm the password.
Example: `passw0rd`
8. Enter the IP address of the SSM Sensor.
Example: `172.30.1.131`
9. Set the execution policy back to the previous state.

Add Remote Agentless Nodes on the User Workstation C

1. Log in to the WBM.
2. Select the "Configuration" > "Sensor" menu, select the SSM Sensor and click "Edit".
3. Scroll down and select the "Remote agentless node" tab.
4. To add more than one agentless data source, click "Add Remote agentless node" as often as needed.
5. Enter the information for each Microsoft Windows client as required:
 - System logs: Activate the options: System, Security, and Application
 - Enter the IP address of the Microsoft Windows Client B.
Example: `172.30.1.110`
 - Enter the domain name of the network.
Example: `Production_A`
 - Enter the account name of the account that was created on the Windows Client B.
Example: `agentlessReader`
 - Enter the password.
Example: `passw0rd`
6. Select a security grade:
For more information on security grades, refer to the table "Definition of security grades" in chapter Preparing and adding a Microsoft Windows computer for agentless security log collection (Page 160).
 - If you add one agentless node: Select the appropriate security grade from the drop-down menu for your agentless node.
 - If you add multiple agentless nodes: If you added more than one agentless node, you must select the security grade that includes the security grades of all added endpoints.
7. Click "OK".

Firewall policy requirements

Note: WinRM uses port TCP 5986 to provide services. Corresponding firewall policies are required.

Table 7-8 Required settings

Service	Protocol/port	Source IP	To	Service	Protocol/port	Destination IP
WinRM	TCP/ANY	{SENSOR-IP}	>>>	WinRM	TCP/5986	{Client-IP}

Verify the result of the configuration in the audit log

1. Log in to the WBM.
2. Select the "System" > "Audit Log" menu.
3. Enter "winrm" into the "Search" field and click "Search".
4. If a message "sensor_XXX.XXX.XXX.XXX: windows_host_YYY.YYY.YYY.YYY is collected by winrmbeat" turns up in the Audit Log, WinRM has successfully started collecting logs.

Verify the result of the configuration on the logs page

1. Log in to the WBM.
2. Select the "Security Events" > "Logs" menu.
3. Select the Microsoft Windows client from the "All data sources" drop-down menu.
4. When many events are listed, the installation was successfully.

Removing the Winrmbeat (WinRM) configuration from Microsoft Windows Clients

If collection of event logs from a Microsoft Windows client is no longer required, follow these steps:

1. Run the Windows PowerShell as an administrator.
2. Go to the directory where the script package is located.
`cd C:\{path}\WinRM`
3. Run the command to set the execution policy of the system:
`Set-ExecutionPolicy RemoteSigned -Force`
4. Run the script:
`.\ClearWinRM.ps1`
The script removes firewall rules, cert mapping and account privileges.
5. Enter "Y" to delete the account.
If you enter "N", the account will still be displayed in the system.

7.3.1.2 Configuring Remote WMI

This solution is less preferable. Use WinRM if possible.

The installation of agentless security log collection requires creation of an user account on the Microsoft Windows computer. The account name "agentlessReader" is an example used in this instruction.

Note

As Microsoft changed the remote management authentication mechanism from Microsoft Windows 10 2004 (OS Build 19041.264), the SINEC Security Monitor remote WMI acquisition feature is not applicable to this version or higher versions.

Environment information

Table 7-9 Environment Information

Component name	IP address (examples)	Version	Description
Server	10.11.60.248	4.9.0	SINEC Security Monitor Server
Sensor	172.30.1.131	4.9.0	SINEC Security Monitor Sensor
Windows Client	172.30.1.110	Windows 10 1909	Microsoft Windows endpoint - located in the production line; - data source of Remote WMI

Create a standard user account on the Microsoft Windows client

1. Press [Windows] + [R].
2. The "Run" command window opens.
3. Enter `lusrmgr.msc` to open the "Local Users and Groups (Local)\Users" snap-in.
4. Right-click "USERS" to open the "New User" dialog.
5. Create a new local user. Examples for user credentials:
 - User name: agentlessReader
 - Full name: agentlessReader
 - Description: agentlessReader
 - Password: Passw0rd
6. Make sure "User must change password at next logon" is not checked.
7. Click "Create".
8. On the "Local Users and Groups" page, click "Groups" and select the group "Event Log Readers".
9. Right-click "Event Log Readers" and click "Properties" from the context menu.
10. Click "Add" and enter the object name "agentlessReader" (the user name of the user created in step 5). Click "OK".
11. An entry for "agentlessReader" is shown in the section "Members". Click "OK".
12. On the "Local Users and Groups" page, click "Groups" and select the group "Distributed COM Users".
13. Right-click "Distributed COM Users" and click "Properties" from the context menu.
14. Click "Add" and enter the object name "agentlessReader" and click "OK".
15. An entry for "agentlessReader" shows in the section "Members". Click "OK".
16. On the "Local Users and Groups" page, click on "Users", right-click the new user "agentlessReader" and select "Properties" from the context menu.

17. On the "agentlessReader" "Properties" page, click the "Member of" tab.
18. Remove the "agentlessReader" from the "Users" group. Select "Users" and click "Remove".

Assign remote query permissions to the standard user

1. Press [Windows] + [R].
The "Run" command window opens.
2. Enter `wmicmgmt.msc` and click "OK".
The "wmimgmt" snap-in opens.
3. Right-click "WMI Control (Local)" and select "Properties" from the context menu.
4. Select the "Security" tab.
5. Select the "Root" > "CIMV2" namespace.
6. Click on the "Security" button in the lower right corner of the window.
7. If the "agentlessReader" is not available, click "Add". Enter "agentlessReader" and click "OK".
8. Click "Apply" and "OK" to leave the "Security for ROOT\CIMV2" window.
9. Click "OK" to leave the "WMI Control (Local) Properties" window.
10. Close the console window.

Configuring UAC remote restrictions (optional)

This configuration of the registry is optional. If log forwarding from the client does not work, follow these steps to disable UAC remote restrictions.

Note

Serious problems might occur if the registry is edited wrongly.

The damages could require a complete re-installation of the operating system and result in data loss.

Exercise extreme caution when using the registry editor. Back up the registry before making any changes.

1. Press [Windows] + [R].
The "Run" command window opens.
2. Enter `regedit` and press [Enter].
The registry opens.
3. Navigate to the following registry subkey and click on it:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

4. Locate the "LocalAccountTokenFilterPolicy" registry entry.
If this registry entry does not exist, add it to the registry following these steps and then continue:
 - Right-click the empty part of the pane on the right side of the window, select "New" and select "DWORD (32-bit) Value".
 - Type "LocalAccountTokenFilterPolicy" and press [Enter].
5. Right-click "LocalAccountTokenFilterPolicy" and select "Modify" from the context menu.
6. In the Value data field, type "1", and click "OK".
7. Exit the registry editor.

Configuring hotfix privileges for non-administrator users

Purpose

In order to allow the SSM agentless mode to collect system hotfix information via the WMI service, you need to configure specific user permissions for non-administrator domain users. Follow the steps below to set up these permissions:

Step 1: Modify Registry Permissions

1. Press [Windows] + [R] on your keyboard to open the "Run" command window.
2. Type `regedit` and press [Enter] to open the Registry Editor.
3. Navigate to the following registry subkey:
4. `Computer\HKEY_CLASSES_ROOT\AppID\{752073A2-23F2-4396-85F0-8FDB879ED0ED}`
5. Right-click on the subkey and select "Permissions..."
6. Select the Administrators account and check the "Full Control" option.
7. Click on "Advanced", then change the owner to Administrators.
8. Click "Apply", then "OK" to close windows.

Step 2: Configure DCOM Permissions

1. Press [Windows] + [R] on your keyboard to open the "Run" command window.
2. Type `dcomcnfg` and click "OK" to open the "Component Services" window.
3. Navigate to:
`Console Root\Component Services\Computer\DCOM Config\Trusted Installer Service`
4. Right-click on "Trusted Installer Service" and select "Properties".
5. Go to the "Security" tab and click "Edit..." under "Launch and Activation Permissions".
6. Click "Add", then select "agentlessReader" in the "Select Users or Groups" window.
7. Check the "Local Launch" and "Local Activation" options for the "agentlessReader" account.
8. Click "OK" to close all pop-up windows.
9. Under the "Security" tab, click "Edit..." under "Access Permissions".

10. Click "Add", then select "agentlessReader" in the "Select Users or Groups window".
11. Check the "Local Access" option for the "agentlessReader" account.
12. Click "OK", then "Apply" to save the changes and close all pop-up windows.

Step 3: Restart Services

1. Press [Windows] + [R] on your keyboard to open the "Run" command window.
2. Type `services.msc` and click "OK" to open the "Services" window.
3. Locate and restart the Windows Management Instrumentation service.
4. Locate and restart the Windows Remote Management (WS-Management) service.

By following these steps, you will configure the necessary permissions to allow non-administrator domain users to access system hotfix information through the WMI service

Customizing firewall rules on Microsoft Windows

Purpose

To allow a remote device to connect to a local WMI, firewall rules for Remote Procedure Call (RPC) and Window Management Instrumentation (WMI) need customization.

Prerequisites

- This procedure requires administrator privileges on the Microsoft Windows computer.
- The SINEC Security Monitor Sensor's IP address is needed.

Customizing the remote procedure call (RPC) rule

1. Press [Windows] + [R].
The "Run" command window opens.
2. Enter `wf.msc` and press [Enter].
The "Windows Defender Firewall with Advanced Security" snap-in opens.
3. In the left column, select "Inbound Rules".
4. In the Actions column on the right, click "New Rule..."
The "New Inbound Rule Wizard" opens.
5. At step "Rule Type", select "Custom" and click "Next".
6. At step "Program", select "This program path" and click "Browse..."
7. Select `svchost.exe` from the Microsoft Windows' "System" folder and click "Customize..."
The "Customize Service Settings" dialog opens.
8. Select "Apply to this service".
9. Select "Remote Procedure Call (RPC)" from the list and click "OK" to return to the "Program" window.
10. Click "Next >"
11. A dialog appears. To continue, click "Yes".

12. At step "Protocol and Ports", select and enter:
 - Protocol type: TCP
 - Protocol number: 6
 - Local port: Specific Ports
 - Enter: 135
 - Remote port: All Ports
13. Click "Next >".
14. At step "Scope", in the remote IP addresses section, select "These IP addresses" and add the SINEC Security Monitor Sensor's IP address.
15. Click "Next >" twice.
16. At step "Name", enter "_Allow_SSM_RPC" and click "Finish".

Customize rules for Windows Management Instrumentation (WMI)

1. Press [Windows] + [R].
The "Run" command window opens.
2. Enter `wf.msc` and press [Enter].
3. The "Windows Defender Firewall with Advanced Security" snap-in opens.
4. In the left column, select "Inbound Rules".
5. In the "Actions" column on the right, click "New Rule..."
6. The "New Inbound Rule Wizard" opens.
7. At step "Rule Type", select "Custom" and click "Next".
8. At step Program, select "This program path" and click "Browse..."
9. Select `svchost.exe` from the Microsoft Windows' System folder and click "Customize...."
The "Customize Service Settings" dialog opens.
10. Select "Apply to this service".
11. Select "Windows Management Instrumentation" from the list and click "OK" to return to the "Program" window.
12. Click "Next >".
13. A dialog appears. To continue, click "Yes".
14. At step "Protocol and Ports", select and enter:
 - Protocol type: TCP
 - Protocol number: 6
 - Local port: All Ports
 - Remote port: All Ports
15. Click "Next >".
16. At step "Scope" in the remote IP addresses section, select "These IP addresses" and add the SINEC Security Monitor Sensor's IP address.

17. Click "Next >" twice.

18. At step "Name", enter "_Allow_SSM_WMI" and click "Finish".

Firewall policy requirements

Note

WMI uses port TCP 135 for services. Corresponding firewall policies are required.

Table 7-10 Required settings

Service	Protocol/ port	Source IP	To	Service	Protocol/ port	Destination IP
WMI	TCP/Any	{Sensor IP address}	>>>	RPC	TCP/135	{Client IP address}
WMI	TCP/Any	{Sensor IP address}	>>>	WMI-DCOM	TCP/Dynamic	{Client IP address}

Adding agentless data sources

In the WBM, the agentless data sources are added to a SINEC Security Monitor Sensor. If not yet present, install a SINEC Security Monitor Sensor first. Then add Remote Agentless Nodes to the SINEC Security Monitor Sensor.

1. Log in to the WBM.
2. Select the "Configuration" > "Sensor" menu and click "Edit" in the "Actions" column.
3. Scroll down and select the "Remote Agentless Nodes" tab.
4. To add more than one agentless data source, click "Add remote AgentLess node" as often as needed.
5. Enter the information for each client as required:
 - System logs: Activate the options System, Security, Application
 - Enter the IP address (example: 172.30.1.94)
 - Enter the domain name (example: cdc)
 - Enter the account name (example: agentlessReader)
 - Enter the password (example: Passw0rd)

Note: Authentication with certificate and security grade is not used for Remote WMI.
6. Click "OK".

Verify the result of the configuration in the audit log

1. Log in to the WBM.
2. Select the "System" > "Audit Log" menu.

7.4 No agent data sources

3. Enter "hmibeat" into the "Search" field and click "Search".
4. If a message "sensor_xxx.xxx.xxx.xxx: windows_host_yyy.yyy.yyy.yyy is collected by hmibeat" turns up in the "Audit Log", WMI has successfully started collecting logs.

Verify the result of the configuration on the Logs page

1. Log in to the WBM.
2. Select the "Security Events" > "Logs" menu.
3. Select the Microsoft Windows client from the "All data sources" drop-down menu.
4. When many events appear on the list, data collection is successful.

See also

Preparing and adding a Microsoft Windows computer for agentless security log collection (Page 160)

7.4 No agent data sources

The SINEC Security Monitor System can collect device logs from various systems like supervisor PCs, industrial control network devices, PLCs, and Linux workstations. Every system can be added as a data source.

Add industrial control network devices, PLCs, and Linux workstations as data sources in "**no agent**" mode.

7.4.1 Adding a data source in no agent mode

The WBM supports the adding of network devices as data sources, such as firewalls and switch devices.

Note

Prepare the firewall and switch by configuring the log data forwarding on their respective configuration web pages. Refer to the manufacturer's documentation for instructions.

1. Log in to the WBM.
2. Select the "Configuration" > "Data Sources" menu and click "Add".

3. Add data source in no agent mode.
Enter the required information. Fields marked with "*" are mandatory.
 - ***Collection mode**
Select "No agent".
 - ***Name**
Name of the device.
 - ***IP address**
IP address of the device.
 - **Operating System**
Select the operating system of the client for log collection.
Available operating systems: Windows (default), Linux, Others
 - ***Protocol**
Select the protocol used to collect logs.
Available protocols: TLS (default), TCP, UDP
 - TLS protocol**
For bidirectional authentication and encrypted communication:
Download the server certificate and distribute the server certificate to your syslog clients.
Import the client certificate of your syslog client.
You must configure your network device's syslog client accordingly.
 - TCP protocol**
You must configure your network device clients to forward syslog over the TCP protocol.
 - UDP protocol**
You must configure your network device clients to forward syslog over the UDP protocol.
 - ***Security Grade**
This option is available when you select the TLS protocol.
Refer to table "Security Grades" in chapter Preparing and adding a Microsoft Windows computer for agentless security log collection (Page 160) for information on security grades.
 - ***Port**
Port number used by the device.
Available ports: 514 (default), 6514
 - ***Asset**
Select the type of the device.
Available device types: General (default), Linux Host, Windows Host, WinCC, Firewall, Switch
Note: Windows Host and WINCC are not applicable for No Agent mode.
 - **Destination**
Select the IP address of the SINEC Security Monitor Sensor to which the data source shall send its data.
Select the integrated sensor running on the SINEC Security Monitor Server, if the data should go directly to the SINEC Security Monitor Server.
For more information on selecting the correct IP address, refer to chapter No Agent communication with the SSM Server (Page 64).
4. To save changes, click "OK".
The SINEC Security Monitor Server updates its Wireguard configuration file.

7.4 No agent data sources

Note:

- You need to distribute the Server Certificate to all devices, which want to communicate with the SSM Server.
- To upload a client certificate, get a CA certificate for the endpoint. For more information, refer to Configuring WinRM (Page 162), section "Generate certificates on the CA workstation A".

Manage No Agent data sources

1. Log in to the WBM.
2. Select the "Configuration" > "Data Sources" menu.
3. Click "Refresh".
4. Verify that the newly added data source is displayed and listed.

Verify the syslog collection status

1. Log in to the WBM.
2. Select the "Security Events" > "Logs" menu.
3. At "All data sources", select your data source.
4. Check the collected syslogs.

7.4.2 Configuring an endpoint for syslog data collection

This chapter describes the integration of a Siemens SCALANCE router as an example.

Table 7-11 Tested endpoints

Operating system	Version	Note
SCALANCE M800/S615 Firmware	V05.00.00	–

Table 7-12 Firewall requirements

Service	Protocol/ port	Source/ IP address	To	Service	Protocol/ port	Destination IP address
syslog	TCP/UDP/Any	{syslog device IP address}	>>>	syslog	TCP/UDP/ 514/6415	{Sensor IP ad- dress} or {Server IP address}

Activate the syslog client and configure the syslog server

1. Log in to the router's administration website.
2. In the "System" menu, select "Syslog Client".

3. Check "Syslog Client".
4. Enter the "Syslog Server Address". In our scenario, the correct IP address is the IP address of the SINEC Security Monitor Sensor (see scenarios above).
5. Click "Create".
The "Syslog Server Address" appears in the table.

Add agentless data source

1. Log in to the WBM.
2. Select the "Configuration" > "Data Sources" menu and click "Add".
3. For "Collection Mode", check "No Agent".
4. Enter the required information. Fields marked with "*" are mandatory.
 - ***Name**
Name of the device.
 - ***IP address**
IP address of the device.
 - **Operating System**
Operating System of the device, for example "Linux".
 - ***Protocol**
Protocol used, for example "TLS".
Note: For the TLS protocol, authentication with server certificate download and client certificate upload is enabled to ensure bi-directional authentication and encrypted communication.
 - ***Security Grade**
This option is available when you select the TLS protocol.
For information on security grades, refer to table "Security Grades" in chapter Preparing and adding a Microsoft Windows computer for agentless security log collection (Page 160).
 - ***Port**
Port number used by the device.
Protocol used, for example "6514".
 - ***Asset**
Asset type, for example "Linux Host"
Note: Windows Host and WINCC are not applicable for No Agent mode.
 - **Destination**
Select the SINEC Security Monitor Sensor as the traffic goes over the SINEC Security Monitor Sensor to the SINEC Security Monitor Server.
For more information on selecting the correct IP address, refer to chapter No Agent communication with the SSM Server (Page 64).
5. To save changes, click "OK".

Note:

- You need to distribute the Server Certificate to all devices, which want to communicate with the SSM Server.
- To upload a client certificate, get a CA certificate for the endpoint. For more information, refer to Configuring the WinRM tool (Page 162), section "Generate certificates on the CA workstation A".

Verify syslog collection status

1. Log in to the WBM.
2. Select the "Security Events" > "Logs" menu.
3. Select the data source from the "All data sources" drop-down menu.
4. If many events appear on the list, data collection is successful.

7.4.3 Preparing Linux systems for log data forwarding

Step	Action
1	On the Linux system: To add the SINEC Security Monitor Sensor's IP address to <code>/etc/rsyslog.conf</code> , open the rsyslog configuration file.
2	Add to <code>rsyslog.conf</code> : <code>*.*@{SINEC Security Monitor Sensor's IP address}</code>

For information on adding the data source in agentless mode to the SINEC Security Monitor Server, refer to chapter Adding a data source in no agent mode (Page 174).

7.5 Managing log data sources

Select the "Data Sources" page to manage "Agent" and "No Agent" data sources.

Refresh the data source list

Log in to the WBM.

Select the "Configuration" > "Data Sources" menu.

Click the "Refresh" button to refresh the list of log data sources.

Status icon

The color of the status icon indicates the status of the data source.

Table 7-13 Status icons

Status icon	Explanation
Blue	Normal status, in service. The Stop or Start buttons are shown in the Collect Logs column.
Red	Abnormal status, out of service. The Stop or Start buttons are not shown in the Collect Logs column.
Blinking	The SINEC Security Monitor System is trying to connect to the data source.

Start data collection

1. Log in to the WBM.
2. Select the "Configuration" > "Data Sources" menu.
3. Click the "Start" button in the "Collect Logs" column of the list.

Stop data collection

1. Log in to the WBM.
2. Select the "Configuration" > "Data Sources" menu.
3. Click the "Stop" button in the "Collect Logs" column of the list.

Delete a data source

1. Log in to the WBM.
2. Select the "Configuration" > "Data Sources" menu.
3. Select a data source by checking the check box.
4. To delete the data source, click the "Delete" button.
5. Confirm with the "OK" button.

Data Source Diagnostics

The Data Source Diagnostics lists diagnostic information on data sources, for example operating system, created time and modified time.

1. Log in to the WBM.
2. Select the "Configuration" > "Data Sources" menu.
3. Click the "Data Source Diagnostics" button.

Upgrade history

The "Upgrade history" lists the software updates of a SINEC Security Monitor Agent.

1. Log in to the WBM.
2. Select the "Configuration" > "Data Sources" menu.
3. Click the "Upgrade history" button in the "Actions" column.

Manage registered SSM Agent data

SSM Agents periodically send registration data to the SSM Server.

The "Manage" window lists registration data of SSM Agents which are registered to the SSM Server but not binded in the WBM.

You can use the "Manage" window to clean up useless registration data.

When a SSM Agent is no longer needed, you can remove it from the WBM.

As a second step, you can delete the registration data of this device in the "Manage" window.

Note: The "Manage" buttons of the "Configuration" > "Data Sources" menu is only available, when at least one SSM Agent is configured in the WBM.

Remove a SSM Agent

1. Log in to the WBM.
2. Select the "Configuration" > "Data Sources" menu.
3. Click the "Stop" button in the "Collect Logs" column for the SSM Agent, when available.
4. To remove the SSM Agent, click "Delete".
5. To access the "Manage" window, click "Edit" for a random SSM Agent.
6. Click "Manage".
7. Identify the SSM Agent's registration data that you want to remove.
8. Click "Delete" in the "Actions" column.

Operator control

8.1 Monitoring the security situation

OT environments are generally stable. Security threats can cause immense damage yet may remain unnoticed for long periods. It is therefore critical to closely monitor the network and the assets. The information in this chapter gives some hints as to what kind of security events to look out for that could indicate threats.

Managing assets

Assets in industrial production environments are generally relatively stable. The addition of new assets to a stable environment requires extra validation.

- New Asset: An asset appears for the first time.
- Offline Asset: An asset was offline.
- Change Asset: Asset properties have changed.

Monitoring security events in the network

Industrial production environments require stable network services. A network overload can indicate Denial of Service (DoS) attacks or other abnormal transmissions, which require close attention to prevent adverse impacts to the supported processes or business functions.

Typical network security events with an adverse impact:

- Denial of Service (DoS Attack)
- Malware infection or activity
- OT Network Equipment Overload/Failure
- Abnormal network communication

Managing secure user accounts

User accounts in production networks require strict protection. Any security events indicating risks to user account security require a close follow-up.

Typical security risks related to user accounts:

- Weak/default password
- Plaintext password authentication
- Privileged user account creation
- Shared user accounts

Observing changes to applications

Changes to applications, including patches, upgrades, and additions, in industrial production environments can introduce risks that may cause severe impact to operations. Changes and their release into industrial production environments shall follow defined processes and procedures to minimize such risks.

Typical risks related to applications:

- Unauthorized application installation
- Untrusted application publisher
- Vulnerable application
- Unauthorized resource access within application

Keeping an eye on operational activities

Irregular or suspicious activities from operations or maintenance may cause unpredictable behavior in industrial production systems that affect the safety of operations. It is necessary to monitor and act upon detected conspicuous risk behaviors in operations and maintenance processes.

- Maintenance activity: Includes on-site maintenance or remote maintenance on the production system, e.g., PLC restart, program modification
- USB activity: USB storage usage activities within the specified monitoring period, e.g., USB plugin/pluginout
- Backup activity: Backup software running activities within the specified monitoring period, e.g., backup start, backup failure

Enabling USB Event Logging on Windows Devices

For information on how to enable USB Event Logging, refer to chapter Enabling and Configuring USB Event Logging on Windows Devices (Page 157).

8.2 Accessing the SINEC Security Monitor Server

Prerequisites

- User name and password
- Google Chrome browser (version 85 or higher)
- URL or IP address of the SINEC Security Monitor Server

Login

1. Enter the URL into the search field of the browser to open the SINEC Security Monitor Server: `https://{ip address}:8443/login`
2. Enter the user name.
3. Enter the password.
4. Click "Login".

Logout

1. In the upper right corner of the browser window, open the drop-down list by clicking the arrow at the user name.
2. Click "Logout".

Change password

1. In the upper right corner of the browser window, open the drop-down list by clicking the arrow at the user name.
2. Click "Change Password".
Password requirements:
 - Length of 8–32 characters
 - The password must contain at least one of each character:
 - Uppercase letter
 - Lowercase letter
 - Digit
 - Special character

8.3 Typical usage scenarios

8.3.1 Analyzing security events

The security administrator can analyze security events, find the source of the problem, and register the status of handling the security event.

Find a detailed description of all features on the "Security events" page in chapter Handling security events (Page 203).

Access the security events page

If a security event, anomaly, or unusual behavior has been discovered in the "Dashboard" or "Assets" menu, the associated security event can be consulted in the security event list for in-depth information.

1. Log in to the WBM.
2. Select the "Security Events" > "Security Events" menu.

Example

In the event of an asset-related incident, the security administrator can search for the associated security event with the asset, query when the asset went online, the IP address of the online asset and other related information.

Table 8-1 Security events menu

Function	Description
Zoom in	Clicking on a bar in the diagram zooms in to check out specific days and events.
Zoom out	Clicking on the "Back" button in the upper right corner of the diagram zooms out.
Arrows	Clicking on the arrow signs on both sides of the diagram scrolls up and down the timeline.
"Edit" button	Edit a security event entry in the list.
"Related Log" button	View security event log data and details.
Tree Map Chart	Open the "Tree Map Chart" to see how many security events of each kind were handled or not handled.
Change History	The list lists handled security events.
Batch Processing	Handle several security events at once.
Basic Search	Select calendar, category, status, data source, events, and columns.
Calendar	Select a period.
Advanced Search	Clicking "Basic Search" accesses "Advanced Search". Use operators to select specific security events.

The security administrators are responsible for confirming and handling the new online asset according to the enterprise security response process.

8.3.2 Monitoring operations in all six dimensions

Purpose

Siemens has developed monitoring indicators categorized into six key dimensions. These six dimensions include:

- Asset
- Network
- Vulnerability
- Application
- User account
- Operation and Maintenance (O&M)

The SINEC Security Monitor System provides different monitoring indicators for each of these dimensions to help security administrators ensure security.

8.3.2.1 Getting an overview on security statistics

Purpose

The "Security Situation" page gives a quick overview of security statistics in all six dimensions.

Open the security situation page

1. Log in to the WBM.
2. Select the "Dashboard" > "Security Situation" menu.
3. Select a specific period in the calendar to compare with past weeks or months.

Operational risk chart

The "Operational Risk" chart shows how the risk is distributed over the six dimensions.

Assets chart

The "Assets" chart provides statistics about asset types and quantities.

Network diagram

The "Network" diagram shows the daily network traffic per sensor for the selected period.

Vulnerabilities

The "Vulnerabilities" diagram shows the number of assets with high vulnerabilities on different device types, e.g., clients, IT devices, switches and endpoints.

Applications

The "Applications" list shows newly added applications and the IP addresses of the computers where the applications are installed.

The diagram ranks communication traffic per protocol.

User accounts

The "User Accounts" chart shows a list of new presented user accounts and a diagram of user account activities.

Operation

The "Operation" chart shows the number (in brackets "()") of detected backups, USB storage plugins, on-site maintenance and remote maintenance.

Table 8-2 Operations

Activity	Description
Backup	Backup software running activities within the specified monitoring period, e.g., backup start, backup failure
USB storage	USB storage usage activities within the specified monitoring period, e.g., USB plugin/plugout
Onsite maintenance	On-site maintenance on a production system, e.g., program modification
Remote maintenance	Remote maintenance on a production system, e.g., PLC restart

8.3.2.2 Asset dimension

Purpose

As OT systems are quite stable compared to IT networks, any asset changes (new asset, asset offline or asset attributes change) to an industrial control network in a production environment should draw the attention of the security administrator.

Any asset changes will be monitored and recorded by SINEC Security Monitor.

Open the Network Topology tab

1. Log in to the WBM.
2. Select the "Dashboard" > "Network" menu.
3. Click the "Network Topology" tab.

If an asset on the screen is flashing, it means an asset change has been detected. For example, a flashing asset icon indicates that the asset has been integrated online.

More information on the "Network Topology" tab

Flashing box on an assets

- Yellow box on an asset: There are Warning security events available that are associated with this asset.
- Red box on an asset: There are Alert security events available that are associated with this asset.

Modifying the network topology and other features

- You can move the assets with the mouse (drag and drop).
- You can increase and decrease the view by clicking the magnifying glass icon.

- You can enter "Edit" mode by clicking the pencil icon.
 - In "Edit" mode, the "Click asset to select / Right-click link to remove" message text is displayed. Select an asset, the message text changes to "Select another asset to add link / Click again to discard selection". When you select another asset, you can save, undo, or discard the change.
 - Locate an existing communication link between two devices, right-click the link. Click "Delete". You can save, undo, or discard the change.
- You can filter the view by clicking the filter icon and selecting categories.
- You can filter by date.
- You can jump to the asset inventory information, when you double-click an asset icon.
- You can inspect the network load of routers.

8.3.2.3 Network dimension

Purpose

As an OT system can be considered a stable network, any data traffic in the OT system is smooth and regular in this environment. Any "Unknown Traffic" activity should come to the attention of the security administrator. Such activity can be monitored with the SINEC Security Monitor System.

Open the security event page

1. Log in to the WBM.
2. Select the "Dashboard" > "Security Events" menu. The first tab is the "Statistics" tab.

When correlated security events such as "New APP Flow" are displayed, it indicates that communication links (app flows) have been detected in the OT system.

1. Log in to the WBM.
2. Select the "Security Events" > "Security Events" menu.
3. Select an "Unknown Traffic" security event in the "All events" pulldown menu.
4. Find out on which asset and when the "Unknown Traffic" was detected. Manage the threat.
5. Click the "Edit" button to record and track the security event processing information.
6. Click "OK" to save any changes.

Find a detailed description of all features of the "Events" page in chapter Handling security events (Page 203).

Correlated security events

Correlated security events, for example an unexpected application displaying on the "Security Events" > "Security Events" page or the "Dashboard" > "Network" > "Communication Links" tab, are an indication that attack threats have been detected in the OT system. The security administrator can search through these security events, querying the time when the threat was detected, on which asset it was detected and other related information.

Select a connection line to reveal details about that application connection on the "Communication Links" tab.

The "Communication Links" tab can also be used to sort assets into different zones via drag and drop.

The security administrators are responsible for managing assets with unauthorized application threats according to the enterprise security response process.

1. Log in to the WBM.
2. Select the "Security Events" > "Security Events" menu.
3. Select an "Unexpected Application" security event in the "All events" pulldown menu.
4. Find out on which asset and when the "Unexpected Application" was detected. Manage the threat.
5. Click the "Edit" button to record and track the security event processing information.
6. Click "OK" to save any changes.

Find a detailed description of all features of the "Events" page in chapter Handling security events (Page 203).

More information on the "Communication Links" tab

Open the "Communication Links" tab:

1. Log in to the WBM.
2. Select the "Dashboard" > "Network" > "Communication Links" tab.

The "Communication Links" tab shows assets in your asset zones and communication traffic between assets represented by lines.

Colors of the lines

- Red indicates that the total communication data volume between these two devices is the largest volume in the entire monitoring area, based on current communication statistics within the last hour.
- Blue indicates that the traffic is lower.

The "Link details" window

When you click a line between two assets, the "Link details" window opens. The window shows the network addresses of both assets and a graphic representing the communication data volume for each communication protocol. The colors in this window have no specific meaning.

The "Others" zone

When a detected asset is not found on the "Assets" > "Assets" table, the system will associate this asset with the "Others" zone. When you click the "Others" zone, you can see which assets are located there.

No shows

Occasionally, there is no link shown between two assets. That means, no connection information was detected in the monitored traffic. There is no communication link available between those two devices.

The display of the communication links is refreshed about every 10 seconds.

8.3.2.4 Vulnerability dimension

Purpose

As an OT system does not usually follow a regular patching schedule (commonly used in IT to manage system vulnerabilities), the SINEC Security Monitor helps the security administrator to identify and manage high-risk vulnerabilities in the current system and track changes in vulnerabilities by providing industrial device vulnerability monitoring functions.

Open the asset list

1. Log in to the WBM.
2. Select the "Assets" > "Assets" menu.

When a critical vulnerability icon appears in the "Vulnerability" column, the monitored asset is exposed to critical threats.

Click the icon indicating the high-risk vulnerability to go to the vulnerability page and search for more information about the vulnerability and its remedy.

The security administrator is responsible for dealing with industrial control devices being exposed to vulnerability threats in accordance with the enterprise security response process.

After the vulnerability risk is eliminated, the security administrator can access the "Assets" > "Assets" page to check whether the number of vulnerabilities has decreased.

Refer to chapter Managing asset monitoring (Page 195).

8.3.2.5 Application dimension

Purpose

As the applications installed on an OT asset are generally stable, any applications deployed in the OT environment and the amount of network traffic (communication links) caused by these applications are generally also stable.

The installation of additional applications to the OT asset, unexpected application behavior or unusual data traffic should draw the attention of the security administrator. Such security events can be monitored with the SINEC Security Monitor System.

Access the application dashboard

1. Log in to the WBM.
2. Select the "Dashboard" > "Applications" menu.

The page shows information on the most installed applications, the most recently installed applications and how the applications are sorted according to the operating system.

8.3.2.6 User account dimension

Purpose

As the user accounts defined on OT assets are usually stable, any change to user accounts or privileges (including user account additions, privilege escalations, and other abnormal conditions etc.) occurring on any industrial device should draw the attention of the security administrator.

Access the accounts dashboard

1. Log in to the WBM.
2. Select the "Dashboard" > "Accounts" menu.

When correlated security events such as "Create User on Microsoft Windows" are displayed, it indicates a user account change has been detected in the monitored asset.

1. Log in to the WBM.
2. Select the "Security Events" > "Security Events" menu.
3. Select a "Create User on Microsoft Windows" security event in the "All events" pulldown menu.
Find out on which asset and when the user account change was detected. Manage the threat.
4. Click the "Edit" button to record and track the security event processing information.
5. Click "OK to save any changes.

Find a detailed description of all features on the "Event" page in chapter Handling security events (Page 203).

8.3.2.7 Operation and maintenance dimension

Purpose

Enterprises often lack effective and unified user account management, unified allocation of resources and permissions and operational process audits or an effective means of monitoring these for system maintenance, even if related O&M management processes are available.

During maintenance, planned or unplanned, abnormal activities will be detected and reported. By monitoring O&M behaviors, the SINEC Security Monitor System strengthens the security management for remote maintenance of the OT system and devices, standardizes the O&M processes, and reduces the security risks to ensure enterprise productivity.

Any unexpected O&M behavior should draw the attention of the security administrator.

Access the security event dashboard

1. Log in to the WBM.
2. Select the "Dashboard" > "Security Events" menu.
3. Have a look at the statistics charts on the "Statistics" tab.
4. Have a look at the risk lists on the "Risk Assessment" tab.

Note

It is highly recommended to use the "Security Events" page as the starting point to get an overview of the security situation in the network.

Monitoring O&M alerts

Examples of O&M alerts:

- RDP on Microsoft Windows
- S7-1500 syslog: CPU warm restart
- PN-DCP: Reset factory setting

Once the threats above are detected, the security administrators must verify the compliance of the O&M behavior according to the enterprise O&M process.

1. Log in to the WBM.
2. Select the "Security Events" > "Security Events" menu.
3. Search for the O&M security event.
Find out where and when the maintenance was performed and manage the security threat.
4. Click the "Edit" button to record and track the security event processing information.
5. Click "OK" to save any changes.

Monitor remote maintenance behaviors

Enterprises may often need remote support from external engineers and technical experts from third party vendors in their regular O&M work. In these cases, temporary remote access via Internet is also necessary, but this leads to risks to OT security if there is a lack of effective means to monitor and record such maintenance behaviors.

The SINEC Security Monitor System supports users to monitor all remote access security events and ensures the standard and safety of remote maintenance behaviors.

Examples of remote maintenance security events:

- TeamViewer: TeamViewer is used for support activities.
- Unexpected IP: A new IP address appears in the network.

Once threats are detected, the security administrators need to verify the compliance of the remote maintenance behavior according to the enterprise maintenance processes.

1. Log in to the WBM.
2. Select the "Security Events" > "Security Events" menu.
Search for the remote maintenance security event.
3. Find out when and from which remote user account the maintenance was performed and manage the security threat.
4. Click the "Edit" button to record and track the security event processing information.
5. Click "OK" to save any changes.

Find a detailed description of all features of the "Security Events" page in chapter Handling security events (Page 203).

8.3.3 Managing the use of USB storage devices in an OT environment

Purpose

Security events caused by improper use of peripherals can occur due to on-site maintenance engineers in the OT environments generally lacking effective measures to manage the use of USB storage.

The SINEC Security Monitor supports USB storage monitoring functionalities to manage USB disk management issues in the OT system.

These measures include authorizing USB devices, and sending alerts when unauthorized USB storage devices are used.

Authorize the compliant USB storage device

1. Log in to the WBM.
2. Select the "Configuration" > "Anomaly Baseline" menu and select the anomaly baseline USB Devices.
3. Click the "Add" button. The "Add" window displays information on the USB devices detected in the environment.
These records are created by the detection of a USB plug-in security event on an asset device in the environment.
4. Select a USB device in the list.
 - Allow List: Approve the usage of the selected USB device.
 - Deny List: Block the selected USB device. Attempting to use this USB device in the environment generates a security event.
5. Add a description (optional).
6. Click "OK" to save changes.

Monitoring USB alerts

Example of USB alerts:

- Unauthorized USB Plugin: An unauthorized USB device was plugged into an asset.

The security administrators are responsible for handling the asset machine where the USB device was improperly used, according to the enterprise security response process.

1. Log in to the WBM.
2. Select the "Security Events" > "Security Events" menu.
3. Search for the USB security event.
Find out where and when the USB device was used and manage the security threat.
4. Click the "Edit" button to record and track the security event processing information.
5. Click "OK" to save any changes.

Find a detailed description of all features of the Event page in chapter Handling security events (Page 203).

8.3.4 Detecting intrusion threats

Purpose

ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) is a model and knowledge base reflecting the attack behavior of each attack life cycle.

It is developed from a project that enumerates and categorizes tactics, techniques, and procedures (TTP) after a Microsoft Windows system shuts down to improve detection of malicious activities.

The ATT&CK model is currently divided into two areas, PRE-ATT&CK (covering the first two stages of the attack chain model), and ATT&CK for Enterprise (covering the last five stages of the attack chain model). For mobile devices, there is also ATT&CK for Mobile.

The SINEC Security Monitor System monitors the relevant attack threats in the OT system based on the attack life cycle proposed by the ATT&CK framework (Recon, Weaponize, Deliver, Exploit, Control, Execute and Maintain).

The SINEC Security Monitor System enables the security administrator to conduct real-time monitoring and management of typical monitoring objectives, such as DNS Beacon and high-risk vulnerabilities Recon.

Access the security events dashboard

1. Log in to the WBM.
2. Select the "Dashboard" > "Security Events" menu.
3. Have a look at the statistics charts on the "Statistics" tab.
4. Have a look at the risk lists on the "Risk Assessment" tab.

It is highly recommended to use the security events page as the starting point to get an overview of the security situation in the network.

Monitor intrusion threats

Examples of intrusion threats:

- DNS: DNS Beacon
 - SMBv1: DoublePulsar Recon: High-risk vulnerabilities Recon
1. Log in to the WBM.
 2. Select the "Security Events" > "Security Events" menu.
 3. Search for the intrusion security event.
 4. Find out when and where the threat was detected and manage the security threat.
 5. Click "Edit" to record and track the security event processing information.
 6. Click "OK" to save any changes.

The security administrators are responsible for handling the threat according to the enterprise security response processes.

Find a detailed description of all features of the "Event" page in chapter Security monitoring operation (Page 195).

8.3.5 Monitoring malware threats

Purpose

The SINEC Security Monitor System provides related functions for monitoring and responding to possible malware threats in an OT system. The security administrator can monitor and respond to the malware threats in the OT system through related functions.

Access the security event dashboard

1. Log in to the WBM.
2. Select the "Dashboard" > "Security Events" menu.
3. Have a look at the statistics charts on the "Statistics" tab.
4. Have a look at the risk lists on the "Risk Assessment" tab.

It is highly recommended to use the security events page as the starting point to get an overview of the security situation in the network.

Monitor malware threats

Example of malware threats:

- WannaCry

When a security event related to WannaCry, for example, is displayed, this indicates that a suspicious threat of WannaCry infection has been detected in the monitored network.

1. Log in to the WBM.
2. Select the "Security Events" > "Security Events" menu.
3. Select a WannaCry security event in the "All events" pulldown menu.
Find out on which asset and when the WannaCry infection threat was detected and find a description on infection symptoms in the "Remarks" column.
4. Manage the threat.
5. Click the "Edit" button to record and track the security event processing information.
6. Click "OK" to save any changes.

The security administrators are responsible for handling the threat asset according to the enterprise security response process.

Find a detailed description of all features of the Security Events page in chapter Handling security events (Page 203).

8.4 Security monitoring operation

8.4.1 Managing asset monitoring

Purpose

SINEC Security Monitor System monitors assets of the OT system in real time and displays information such as asset changes, applications installed on the assets and correlated vulnerabilities on the interface.

Administrators can quickly locate problems by referring to the corresponding information page. Asset information can also be maintained as needed.

8.4.1.1 Assets dashboard

Purpose

The "Assets" dashboard displays an overview of assets in the SINEC Security Monitor System.

Access the assets dashboard

Asset statistics are shown in diagrams on the "Statistics" tab.

1. Log in to the WBM.
2. Select the "Dashboard" > "Assets" menu.

Note: The statistics in the first row indicate the distribution of assets in zones.

The asset inventory tab

The "Asset Inventory" tab contains a table with all assets detected in the environment.

Table 8-3 Assets menu

Function	Description
Show online Assets only	Check to toggle all offline assets in the list between displayed and hidden
Search	Criteria for a search include IP address, MAC address, vendor, name, asset type, description
Clear	Clear the search field
More	Select to open a window showing more detailed information on this asset

8.4.1.2 Monitoring assets

Network topology

1. Log in to the WBM.
2. Select the "Dashboard" > "Network" menu to access the network topology tab.

Asset changes in the OT network are shown on the network topology tab:

- When an asset attribute changes, the mouseover information box of the corresponding asset icon displays the latest five changes.
- When an asset goes online, the asset icon appears with a green frame.
- When an asset goes offline, the asset icon becomes darker than the online assets.

Network statistics

Use the network statistics tab to get an overview of network traffic.

1. Log in to the WBM.
2. Select the "Dashboard" > "Network" menu.
3. Select the "Statistics" tab.

The "Statistics" tab contains charts on "Top data volume by protocol", "Top DNS request by assets", "Top active hosts" and "Top network events by sensor".

The information can be filtered by protocol or asset. A mouseover reveals total numbers.

Security events

1. Log in to the WBM.
2. Select the "Security Events" > "Security Events" menu to access the Security Events chart and list.

The "Security Events" page allows administrators to detect asset event information in real time.

8.4.1.3 Maintaining assets

Manage asset information

The SINEC Security Monitor provides an asset maintenance function. Users can manage device information as required for a complete dataset of the asset.

1. Log in to the WBM.
2. Select the "Assets" > "Assets" menu to access the Assets list.

Table 8-4 Assets menu

Function	Description
Add	Adds new assets that are not yet on the list Enter the required information (fields marked with "*" are mandatory): Hardware: • Product family: Add the product category • Product model: Add the product model • Product firmware: Add the firmware version • *IP address: Add the IP address of the product • *MAC address: Add the MAC address of the product • *VLANs: Add the VLAN where the product is located • Device name: Add the name of the device • Alias: Add an alias name. When a device has a name and an alias, the alias is displayed first. • Vendor: Add the manufacturer of the asset • Areas: Select a SINEC Security Monitor Sensor • Asset type: Select a type from the drop-down list • Asset zone: Select a zone from the drop-down list • Owner: Enter a name for the asset owner • Details: Add details if required • Significance: Select a level of significance from the drop-down menu: CRITICAL, HIGH, MEDIUM, LOW • Location: Add a location • Allow List: Select "Yes" to add an asset to the allow list. Otherwise, select "No". • Provider: Add provider's name Clicking the "Add new field" button adds a new field (up to 20 device attributes can be added).
Display	Display an asset on the network topology chart on the "Dashboard" > "Network" page. Select the asset first and then click "Display".
Hide	Hide an asset on the network topology chart on the "Dashboard" > "Network" page. Select the asset and click "Hide".

8.4 Security monitoring operation

Merge	Select the assets to be merged and click "Merge" to combine them into one asset. • If the IP address and VLANs of the merged assets are different, the IP information is merged and displayed in the IP Address field of the asset. • If the MAC addresses of the merged assets are different, the MAC information is merged and displayed in the MAC Address field.
Download	Download the asset information in .xlsx format.
Basic Search	Use the search function to filter the information for IP address, MAC address, vendor, name, asset type, and description.
Advanced Search	SINEC Security Monitor also provides an advanced search function, where multiple search conditions can be specified. The logical operator is AND.
Clear	Clear the search field.
Columns	Specify the columns to be shown in the list. Pre-defined columns are shown by default.
More	Show all asset details.
Edit	Edit asset information. Information identified by the SINEC Security Monitor System cannot be edited.
Delete	Delete an asset.

8.4.1.4 Monitoring asset vulnerabilities

The SINEC Security Monitor System can automatically associate vulnerability information with discovered assets based on the included security vulnerability library.

Scores are marked to facilitate quick reactions to prevent hackers from exploiting vulnerabilities.

Table 8-5 Vulnerability labels

Color	Severity level	Action
Black	Critical	Unacceptable risk: urgent action is required
Red	High	Unacceptable risk: action is required
Orange	Medium	Acceptable risk: mitigation subject to management decision
Yellow	Low	Acceptable risk: no action required

Discover vulnerabilities on assets

Note

Vulnerabilities are displayed and classified based on the information in the respective vulnerability libraries, for example the NIST CVE database.

In some cases resolutions for these vulnerabilities that are published as security advisories are available but not reflected in the database entry yet. This can lead to vulnerabilities that are actually fixed.

1. Log in to the WBM.
2. Select the "Assets" > "Assets" menu to display the asset list.
3. Review the "Vulnerability" column for vulnerability icons. Moving the mouse over this icon displays vulnerability IDs.
4. Click the vulnerability icon to navigate to the "Assets" > "Vulnerabilities" page and view the vulnerabilities associated with the specific asset. By hovering over the affected asset count you will see the MAC Addresses and IP Addresses of all affected hosts. For further device information you can also click on this number.
5. To return to the "Assets" > "Assets" menu, click the number in the "Affected assets" column. The page only lists the affected assets.

Note:

You can use the CVE-ID to look up further information and available resolutions or security advisories, for example on the NIST webpage.

For more information on CVE IDs, see:

Link: (<https://www.cvedetails.com>)

Access vulnerability information

1. Log in to the WBM.
2. Select the "Assets" > "Vulnerabilities" menu to display the Vulnerabilities list.
3. Select the "More" button in the "Details" column.
Find detailed information on the vulnerability as well as a list of affected assets.
4. Click "More" in an affected asset's row to view detailed information on the asset.
The "Details" window lists asset information on the following tabs:
 - Asset details: Network settings and discovery times
 - Vulnerabilities: Vulnerabilities concerning this asset
 - Installed applications: Applications installed on this asset
 - User accounts: User accounts found on this asset
 - Patch: Patches installed on this asset

8.4.2 Monitoring asset user accounts

Purpose

The administrator needs to have certain user account information to improve the security of the OT network environment. The user accounts details, user account permissions and user account usage information on the asset devices in real time must be known for the administrator to manage the use of the OT user accounts in a timely manner. If abnormal behavior in a user account is detected, an alert is issued.

Access the user accounts list

1. Log in to the WBM.
2. Select the "Assets" > "Accounts" menu.

The "Accounts" page shows the assets along with their "IP address", "VLANs", "MAC address" and "Device name".

The "Number of accounts" column shows the number of user accounts installed on the asset device. Click on the number to display user account details.

The "Details" window lists the following details that were retrieved from the monitored assets:

- **User name**
User name of the account
- **Full name**
Full name of the account
- **Account type**
Account type, for example: "Local account"
- **Privileges**
Privileged user accounts are accounts with a group SID (Security Identifier) ending with 5xx.
Examples for privileged user accounts:
 - Administrators, SID S-1-5-32-544
 - Distributed COM Users, SID S-1-5-32-562
 - Hyper-V Administrators, SID S-1-5-32-578
 - Network Configuration Operators, SID S-1-5-32-556
 - Power Users, SID S-1-5-32-547
 - Remote Management Users, SID S-1-5-32-580
 - System Managed Accounts Group, SID S-1-5-32-581

For more information on SIDs, refer to Microsoft Learn: Security identifiers (<https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-identifiers>).
- **Enabled**
"Enabled" refers to the account property "Account is disabled" in the Microsoft Windows "Local Users and Groups" snap-in.
- **Description**
Description of the account

8.4.3 Monitoring applications

Purpose

To improve the security of the OT network environment, the administrator needs to know the details of the software installed on the asset devices (supervisor PCs) in real time. When an abnormal application is installed on a computer, an alert is given.

Get a quick overview of applications

1. Log in to the WBM.
2. Select the "Dashboard" > "Applications" menu.

This page displays a chart for the "Top installed applications" as well as a list of the "Most recent installed applications". There is also a chart showing the organization of the application according to the operating system (click to zoom in for more details).

Access application details

1. Log in to the WBM.
2. Select the "Assets" > "Applications" menu to open the list of applications in the environment.

The list shows Name, Vendor, Version, Vulnerabilities and the number of Hosts where the application is installed. Current vulnerabilities are shown in the "Vulnerabilities" column. Mouseover the vulnerability field to show more details.

The "Applications" list can be searched for name, version, and vendor. Click the "Clear" button to clear the search field.

Click the number in the "Hosts" column to show a list of assets where the application is installed.

Click the "Details" button to show more information on the asset, including vulnerabilities, installed applications, user accounts, and patches.

8.4.4 Central security log management

Purpose

This page is used to centrally manage all collected logs.

Access the logs page

1. Log in to the WBM.
2. Select the "Security Events" > "Logs" menu to open the logs list.

Table 8-6 Logs menu

Function	Description
Calendar	Select a specific period
Monitored security logs, Self-monitoring logs	Filter security logs based on security log types: Monitored security logs: Logs collected from all data sources Self-monitoring logs: Logs collected from the SSM Server and the SSM Sensors
All data sources	Select a specific data source
Basic search	All fields: Select a field (fields are derived from log file code) Search keywords: Perform a keyword search (full text search)

Advanced search	The advanced search enables multiple search criteria to be entered simultaneously
Clear	Clear all search fields
Columns	Select or deselect columns in the list
More	Display the log code of the selected log

Note: The more information in this list, the longer a search can take.

8.4.5 Generating a security monitoring report

Purpose

SINEC Security Monitor provides functions to create security monitoring reports and export system audit reports. The security administrator can download security monitoring reports according to actual needs.

8.4.5.1 Downloading the security report

Report page

The "Report" page provides scheduled reports for download and an export function for customized reports.

Export a report

SINEC Security Monitor System provides a function to manually download a .zip file, containing a report in .pdf format and seven tables in .csv file format. The report period can be adjusted according to needs.

1. Log in to the WBM.
2. Select the "Report" menu.
3. Click the "Create new report" button.
4. Select the report period and click on "Create new report".
5. Confirm the pop-up message with "OK".
6. Click "Close" to close the window.
7. Find the report packed in a .zip file in your system's Downloads folder.
8. Click "OK".

Exported reports are exported as .zip files. The .zip file contains:

Table 8-7 Files included in the .zip file

File	Description
{Name-of-Report}.pdf	Contains a report summarizing data from the report period and in-depth information about cybersecurity in the industrial production environment.
Account.csv	Contains accounts detected in the industrial production environment.
Application.csv	Contains applications detected in the industrial production environment.
Asset.csv	Contains assets detected in the industrial production environment.
Malwares.csv	Contains malware detected in the industrial production environment.
Networks.csv	Contains network threats detected in the industrial production environment.
USB Activities.csv	Contains USB security events detected in the industrial production environment.
Vulnerabilities.csv	Contains vulnerabilities detected in the industrial production environment.

Download a report

Scheduled reports are ready for download or can be configured to be received by email.

To obtain a report from the Report page, use the Download button in the Actions column to download a .zip file containing the selected report.

For the configuration of scheduled reports, refer to sections:

Configuring security reports (Page 141)

Setting up email notifications (Page 130)

8.5 Handling security events

8.5.1 Monitoring risks

Purpose

The "Risk Assessment" page displays a "Risk Ranking" diagram showing the areas of the system returning the greatest number of risks detected for the selected period.

Table 8-8 Risk assessment functions

Function	Description
Period	Filter the diagram by period (day, week, or month)
Rank No.	Filter the diagram by rank (5, 10, or 20) Risks are ranked by the total number of detected security events within the selected period in a descending order.
Calendar	Select a period

Access the risk assessment page

1. Log in to the WBM.
2. Select the "Security Events" > "Risk Assessment" menu to open the "Risk Assessment" page.
3. Click a risk square to open a specific diagram and security events list for this risk type only.

The Security Events diagram shows the number of occurrences of the security event detected over a period.

Note

Click on the information bars in the "Security Event" diagram to zoom in. Use the "Back" button to go back (zoom out).

8.5.2 Monitoring and responding to security events

Monitor and track security events

Use this function to analyze and handle security events generated during the monitoring process, and to follow any security event trends.

Access the security events page

1. Log in to the WBM.
2. Select the "Security Events" > "Security Events" menu to open the security events page.

Table 8-9 Security Events functions

Function	Description
Zoom in	Clicking on a bar in the diagram zooms in and allows you to check out specific days and events
Zoom out	Clicking on the "Back" button in the upper right corner of the diagram zooms out
Arrows	To scroll up and down the timeline click on the arrow signs on the left and right of the diagram
"Edit" button	Edit a security event entry in the list
"Related Log"	See relevant logs. A "More" button shows more details about that log
"Tree Map Chart"	Open the Tree Map Chart to see how many security events of each kind were handled or not handled
"Change History"	See security events that have been actioned. A "Revoke" button in the Action column cancels the previous operations

"Batch Processing"	Handle security events in batches Select and enter: • Deadline: Deadline for security event handling • Supervisor: Supervisor of security event handling • Approver: Approver of security event handling • Action: Analysis result of the security events (Abnormal, Normal, Irrelevant) • Status: Process status of security event handling (Processing, Processed, Closed) • Add to anomaly baseline: Add security event to Allow List or Deny List • Upgrade/Downgrade: Upgrade or downgrade the security event by severity (alert, warning, event). Only the selected security event will be upgraded or downgraded. Older or future security events of this specific type are not processed. • Save to Upgrade/Downgrade: Check to upgrade or downgrade this security event and future security events of this specific type. Older security events of this specific type are not processed. Batch Process Filter: • Data Source: Select a data source • Status: Select a status (Not handled, Processing, Processed, Closed) • Select an event • Fill in Source Address and Destination Address as requested depending on the selected security event Click the "Search" button When the search results fit, click the "OK" button to start the batch process
Calendar	Select a specific period
Basic search	Select category, status, data source, and events
Advanced search	Specify multiple search conditions (the logical operator is AND)
Columns	Select or deselect columns in the list

The chart shows the number of security events (y-axis) per day (x-axis).

Note: Display and hide specific event types by checking and unchecking them in the top right corner of the screen.

Table 8-10 Security Event types

Color	Event type	Criteria
Red	Alert	High risk security event requiring mitigation action
Orange	Warning	Medium risk security event with the need for action
Blue	Event	Low risk security event, logging only

Usage scenario

Select a corresponding time range using the calendar to filter data. Click the histogram's bars to zoom into the data. Click the "Back" button to return. Use the left arrow to select the previous period or the right arrow to select the next period.

Perform a query across multiple dimensions:

- Select Period
- Category
- Status
- Data Source
- Event ID or Event name
- Event Type

Tree map chart

Click the "Tree Map Chart" button to see the security event distribution. The distribution chart is divided into three major blocks: Alert, Warning and Event.

The current security events of the system can be viewed by scrolling with the mouse using the scroll wheel and clicking on each box.

Security events response and handling

Security events generated by the SINEC Security Monitor System can be handled by the administrator.

Security events can be traced in the original log and a change history shows the results of the security event handling. The administrator can subsequently analyze and manage alert events.

Follow these steps to log the processing of events:

1. Log in to the WBM.
2. Select the "Security Events" > "Security Events" menu to open the security events page.
3. Open the list of security events to check for any indicators of abnormality.

4. Click "Edit" if a security event is identified as abnormal and requires action.
Enter the information depending on the situation:
 - **Action**
Analysis result of security events (Abnormal, Normal, Irrelevant).
 - **Status**
Process status of security event handling (Processing, Processed, Closed).
 - **Approver**
Approver for security event handling.
 - **Supervisor**
Supervisor of security event handling.
 - **Deadline**
Deadline for security event handling.
 - **Add to anomaly baseline**
Add to Allow or Deny List.
 - **Upgrade/Downgrade**
Upgrade or downgrade the security event by severity (alert, warning, event).
5. Click "OK" to save changes.

8.5.3 Analyzing security event trends

Purpose

This function can be used by users to view the security event status and correlated vulnerability information in the network environment.

Access the statistics tab of the security events dashboard

The statistics tab contains four charts. Use the calendar function to select a specific period for these charts.

1. Log in to the WBM.
2. Select the "Dashboard" > "Security Events" menu to open the security event page. First tab is the "Statistics" tab.

Security Trend

Security event distribution (y-axis) over time (x-axis) for each security event type:

- Alert (red)
- Warning (orange)
- Event (blue)

All security events in the network environment are included.

Top Events by Source

View the "Top Events by Source" in the network environment with IP address and security event count.

Top Events by Type

View the top security events in the network environment by the number of security events.

Top Events by Destination

View the top security event destinations in the network environment with IP address and security event count.

Access the risk assessment tab of the security event dashboard

The risk assessment tab contains five charts. Use the calendar function to select a specific period for these charts.

1. Log in to the WBM.
2. Select the "Dashboard" > "Security Events" menu.
3. Select the "Risk Assessment" tab.

Accounts with risks

The chart shows the security event distribution (y-axis) over time (x-axis) for each security event type (alert, warning, event) for a specific user account.

Top 5 risks

This chart shows a list of the current top 5 security events, ranked by number of occurred security events in one day.

Assets with malware detected

The list lists all assets where malware has been detected.

For example: A registry item created by WannaCry is detected on host xxx.xxx.xxx.xxx.

Anomaly List

The list lists all assets where anomaly events have been detected.

Malware Traffic

The list lists all assets where malware traffic has been detected.

For example: WannaCry Kill Switch DNS is detected from host xxx.xxx.xxx.xxx.

Maintenance

9.1 Diagnostics

9.1.1 Diagnostics tools

9.1.1.1 Diagnostics page

Purpose

The "Diagnostics" page provides a full overview of the current condition of the SINEC Security Monitor System. Use this page to identify and diagnose system issues, being aware that this page is for information purposes only. Tools to maintain the SINEC Security Monitor System, e.g., rebooting the SINEC Security Monitor System, starting SINEC Security Monitor Agents and SINEC Security Monitor Sensors, etc. can be found on their respective pages.

Accessing the diagnostics page

1. Log in to the WBM.
2. Select the "System" > "Diagnostics" menu to open the "Diagnostics" page.

Introduction

This page shows nodes (SINEC Security Monitor Servers, SINEC Security Monitor Sensors) and services and the associated health status icons in the navigation panel on the left. Select a node to display detailed diagnostic information in the main section of the page.

Table 9-1 Health status

Health status color	Meaning
Green	Normal state
Orange	Service required
Red	Failure

Diagnostic information for services

The information displayed for each service depends on its function and is different for each service.

Download latest log

1. Log in to the WBM.
2. Select the "System" > "Diagnostics" menu to open the "Diagnostics" page.
3. Click "Download latest log" in the upper right corner of the page.
4. The log is downloaded in .tgz file format to the "Downloads" folder of the local computer.
5. Unpack the archive file to access the syslog files.

9.1.1.2 Security self-monitoring**System alarm page**

The "System" > "System Alarm" page lists System Event Notifications and Security Event Notifications.

A shortcut to the "System Alarm" page is the Notifications button in the upper right corner of the WBM.

These notifications are delivered by email notification, sound alarm, or pop-up window, when configured. If you miss a notification, you find them all listed here.

To configure notifications, refer to chapter Configuring system notifications (Page 142).

Audit log page

The "System" > "Audit Log" provides data about the usage of the SINEC Security Monitor Server. For example, successful user logins, failed user logins, and user password changes.

9.1.1.3 OPC UA interface

SINEC Security Monitor provides data for OPC UA applications. For the documentation of the diagnostic data model, a machine-readable XML definition of the diagnostic data model for SINEC Security Monitor is supplied with this documentation.

Table 9-2 SINEC Security Monitor Server

Component	Provided file
SINEC Security Monitor Server	sinec-security-monitor-server-operationsystem-v1.0.xml sinec-security-monitor-server-v1.3.xml sinec-security-monitor-type-v1.1.xml dada-v1.3.xml
SINEC Security Monitor Sensor	sinec-security-monitor-sensor-operationsystem-v1.0.xml sinec-security-monitor-sensor-v1.3.xml sinec-security-monitor-type-v1.1.xml dada-v1.3.xml

Requirements for SINEC Security Monitor for integration into an installation structure:

Table 9-3 Integration requirements

Requirement	Result	Comment
Bandwidth	2 Mbit/s	The SINEC Security Monitor System writes diagnostic data to OPC UA by timer. The timer's interval is 10 s, and the size of the diagnostic data is about 250 kB each second. The resulting minimum bandwidth is 2 Mbit/s.
Protocols	TCP	Written data to OPC UA use TCP protocols for diagnostic communication.
Security level	Basic security mode	–

Diagnostics interfaces

For assistance with selecting the correct IP addresses for the SSM Server and the SSM Sensor, refer to the following chapters:

SSM Server: SSM Server diagnostics communication (Page 68)

SSM Sensor: SSM Sensor diagnostics communication (Page 69)

Access the OPC UA diagnostic server

Table 9-4 OPC UA login credentials

Name	Data
URL	OPC.TCP://{SSM Server/Sensor IP address}:4840/
Username	admin
Password	Instance ID of the SSM System

Obtain the instance IDs of the SSM System

1. Log in to the WBM.
2. For the SSM Server, go to "System" > "Licence" and select the "Server" tab.
3. For the SSM Sensor, go to "System" > "Licence" and select the "Sensor" tab.
4. Copy the instance IDs and use the instance IDs as passwords to access the OPC UA server of the SSM Server and the SSM Sensor.

Firewall policy requirements

The OPC-UA diagnostics service uses port TCP 4840 to provide services. Corresponding firewall policies are required.

Find the required settings in the table below:

Table 9-5 OPC UA firewall policy requirements

Service	Protocol/ port	Source IP	to	Service	Protocol/ port	Destination IP
OPC-UA	TCP/ANY	Operator PC	>>>>>>	OPC-UA	TCP/4840	SSM Server/ Sensor IP address

Hardware diagnostics

Hardware diagnostics data is mainly collected by monitoring the SSM Server and SSM Sensor.

1. In your OPC UA client application, navigate to the "Server" or "Sensor" node.
2. Click the Hardware node.
Here you can find hardware diagnostic data about the SSM Server and SSM Sensor.

Examples for hardware diagnostics data:

- CPU
- Container
- License
- Main storage
- Network adapters

Service diagnostics

Service diagnostics data is mainly collected by monitoring the SSM Server and SSM Sensor.

1. In your OPC UA client application, navigate to "Server" or "Sensor" node.
2. Click the "Service" node.
Here you can find service diagnostic data about the SSM Server and SSM Sensor.

Examples for Service diagnostics data of the SSM Server:

- CA
- Certificate
- Collector
- Gateway
- PG
- OS
- Redis
- SI
- Logstash
- Logforward

- CM
- Prober
- Zeek
- Suricata
- Logagent

Examples for Service diagnostics data of the SSM Sensor:

- Prober
- Zeek
- Suricata
- Logagent

Method calls

As of SSM V4.9.0, the SINEC Security Monitor System supports OPC UA method calls. Method calls are a way to interact with the SINEC Security Monitor System via the OPC UA client.

NOTICE
Danger of data loss, take great care when using method calls Some method calls allow to reset or rollback the SSM System. Do not use these functions unless the usage is intended.

The usage of method calls depends on the OPC UA client program you use. Follow the manufacturer's instructions.

Accessing method calls

1. In your OPC UA client application, click on the "Server" > "Operating System" node.

Get the system and application logs

System and application logs include S2L2 Linux system logs and application logs.

For example:

- Gateway application logs
- OpenSearch application logs
- Agent application logs

Getting the system and application logs

1. In your OPC UA client application, navigate to the Server or Sensor node and right-click the "Operating System" > "GetLog" option.
2. Select the "Call" option.

3. To download the logs for the specified services, enter the details (input argument, log file) in the pop-up window.
4. Click "Call".

Input arguments for "Service":

- Enter the name of the service, for example S2L2, gateway, si, collector, ca, logstash. Refer to the column "Key" value in the following Server system and application log list or Sensor system and application log list.
- Only "Key" values are supported. The input is case sensitive.

Output arguments for "Log file":

- Enter the log file format ".tgz".
- When you click Save, a file with suffix ".tgz" will be downloaded and saved locally.

Table 9-6 Server system and application log list

No	Items	Key
1	S2L2 Linux	s2l2
2	Gateway	gateway
3	SI	si
4	Collector	collector
5	CA	ca
6	CM	cm
7	Agent	agent
8	Filebeat	filebeat
9	Hmibeat	hmibeat
10	Winrmbeat	winrmbeat
11	Suricata	suricata
12	Redis	redis
13	Sensor	sensor
14	Opensearch	os
15	Logstash	logstash
16	Logforward	logforward
17	Postgresql	postgresql
18	Zeek	zeek
19	Diagnostic Integrator	di
20	SSMCTL	ssmctl

Table 9-7 Sensor system and application log list

No	Items	Key
1	S2L2 Linux	s2l2
2	Agent	agent
3	Filebeat	filebeat

No	Items	Key
4	Hmibeat	hmibeat
5	Winrmbeat	winrmbeat
6	Suricata	suricata
7	sensor	sensor
8	Zeek	zeek
9	Diagnostic Integrator	di
10	SSMCTL	ssmctl

Get the system and application runtime information

System and application runtime information includes for example:

- System storage
- System memory
- System performance
- System time zone and time
- Docker containers information
- Application (OpenSearch) running information

Getting the system and application runtime information

1. In your OPC UA client application, navigate to the Server or Sensor node and right-click the "Operating System" > "GetRuntimeInformation" option.
2. Select the "Call" option.
3. To download the specified information, enter the details (output argument) in the pop-up window.
4. Click "Call".

Output arguments for the "Runtime file":

- Enter the runtime file format ".tgz".
- The runtime file package in ".tgz" format is downloaded and saved locally.

Get the system and application configuration information

System and application configuration information includes for example:

- IP and network card configuration information
- Root CA certificate and SMC certificate information
- System configuration file
- WireGuard configuration file
- Artifact information

Getting the system and application configuration information

1. In your OPC UA client application, navigate to the Server or Sensor node and right-click the "Operating System" > "GetConfigurationInformation" option.
2. Select the "Call" option.
3. To download the specified files and information, enter the details (output argument) in the pop-up window.
4. Click "Call".

Output arguments for the "Configuration file":

- Enter the configuration file format ".tgz".
- The Configuration file package in ".tgz" format is downloaded and saved locally.

Update via update script

Perform system and application updates with the update script. Update system and application configuration or data with the flexible and customized update scripts.

1. In your OPC UA client application, navigate to the Server or Sensor node and right-click the "Operating System" > "UpdateViaUpdateScript" option.
2. Select the "Call" option.
3. Enter the details (input and output argument) in the pop-up window.
4. Click "Call".

Input argument for the "UpdatePackage":

- Upload the signed and encrypted update package. The name of the update package must be: "update.tgz.enc"

Input argument for the "Signature":

- Upload the signature file for the update package. The name of the signature file must be: "update.xml"

Output Arguments for the "UpdateOutput":

- The output depends on the execution of the updated script. If there is an output, it will be downloaded as a ".tgz" file with the file name "update.output.tgz".

Restart containers

Restart a specific docker container.

1. In your OPC UA client application, navigate to the Server or Sensor node and right-click the "Operating System" > "RestartContainer" option.
2. Select the "Call" option.
3. Enter the details (input argument) in the pop-up window.
4. Click "Call".

Input argument for a "Container Name":

- Enter the name of the container, for example: collector, gateway, logstash
- This parameter is case sensitive.
- Any specific container can be restarting using this call.

Clean logs

Currently only the rolled back logs are cleaned up.

1. In your OPC UA client application, navigate to the Server or Sensor node and right-click the "Operating System" > "CleanLogs" option.
2. Select the "Call" option.
3. To clean up the archived/rolled back old log files, click "Call".

Time configuration

Update the system time that was entered by the user with the standard format time.

1. In your OPC UA client application, navigate to the Server or Sensor node and right-click the "Operating System" > "TimeConfiguration" option.
2. Select the "Call" option.
3. Enter the details (input argument) in the pop-up window.
4. Click "Call".

Input arguments for the "System Time":

- Enter the time in the following standard format: yyyy-MM-dd HH:mm:ss
For example: 2024-01-01 08:00:00

Note when modifyig the time:

- The time cannot be earlier than the system initialization time and the start time of the license validity period.
- For the SSM Server: The time cannot be later than the expiration time of internal communication certificate and the end time of the license validity period
- For the SSM Sensor: The time cannot be later than the end time of the license validity period.

Restart WireGuard

Restart the WireGuard tunnel.

1. In your OPC UA client application, navigate to the Server or Sensor node and right-click the "Operating System" > "RestartWireGuard" option.
2. Select the "Call" option.
3. Click "Call" to restart the WireGuard tunnel.

9.1.1.4 Packet capture

Purpose

The SINEC Security Monitor System allows the creation of packet captures. After capturing, the packet captures are shown in the list in the lower part of the "Packet Capture" page.

Using packet capture

1. Log in to the WBM.
2. Select the "System" > "Packet Capture" page.
3. Enter required information (fields marked with "*" are mandatory):
 - *Please select the sensor: Select a SSM sensor from the pulldown list.
 - *Time Frame: Select a duration between 1–7,200 seconds.
 - *Maximum packet count: Enter a maximum packet count, the maximum is 100,000 pkts.
 - Filter: Enter a port number for the capture port between 1–65535, for example: 80.
4. Click "Start Capture" to start the capture.
5. Click "Stop Capture" to stop the capture or wait until the message "Successfully executed the operation." appears on the screen.
6. Click "Refresh" to refresh the page, clear the form and find the result in the list below.
7. Click "Download" in the Action column of the list to download the capture file.

9.1.1.5 Audit Log

Purpose

The "Audit Log" page contains a diagram with the number of system logs on the y-axis and the selected period on the x-axis. Below the diagram is a list listing all system logs. Frequent log types include, for example, "User login", "User logout", "Security event", "System restart".

The term "Audit Log" refers to the functionality of the system to record any occurrences of events in monitored devices as well as in the system itself. The stored logfile contains information about the event, the user that caused this event, a timestamp and additional information.

The Message column shows the result of the action, for example "Login failed", "A USB device was plugged in".

Table 9-8 Audit Log functions

Function	Description
Calendar	Select a period
User name	Select an user from the drop-down list.
Log type	Select a log type from the drop-down list. Log types represent actions users can perform on the SINEC Security Monitor System.

"Delete all records"	Remove all records
"Delete selected"	Check a system log and click "Delete selected" to delete a system log
"Download audit log"	Check a system log and click "Download audit log" to download a system log
"Search"	Search for an audit log message
"Reset"	Clear the search field

Accessing the Audit Log page

1. Log in to the WBM.
2. Select the "System" > "Audit Log" page.

9.1.2 Fault messages

404 – page not found

The SINEC Security Monitor Server cannot be accessed.

1. Press <F5> in the browser.
2. If necessary, repeat pressing <F5> until the login page appears.
3. Contact the system administrator to confirm that the connection is working.

9.1.3 Troubleshooting

9.1.3.1 SINEC Security Monitor Server problems

No access to the SINEC Security Monitor Server

1. Confirm that the client is connected to the network.
2. Contact the system administrator to confirm that the client is authorized to access the system.

User name or password forgotten

The WBM allows five attempts to enter the password within an one-hour period. If the login attempts exceed that limit, the account becomes locked. To reset the password of this user account, contact the system administrator.

Webpage displays messy code or incorrect contents

It is recommended to use Google Chrome browser (version 85 or higher).

9.1.3.2 Security monitoring problems

No traffic in the network topology or the network topology is not generated

1. Log in to the WBM.
2. Open the "Configuration" > "Sensor" page to confirm whether the Sensor status is blue (healthy). If the status is red, restart the Sensor device.

If the problem cannot be solved, contact the system administrator for network troubleshooting.

Assets such as switches or routers do not show in the network topology

Switches and routers should always show in the network topology

1. Log in to the WBM.
2. Go to "Dashboard" > "Assets" > "Asset Inventory" and check the type of the router or switch. If there is a wrong asset type, for example endpoint, it needs to be changed manually.
3. Go to "Assets" > "Assets", select the asset and click "Edit". Select the correct asset type and click "OK".

Refer to chapter Adding a data source in agent mode (Page 158).

Logs list in the Security Events menu is empty

1. Log in to the WBM.
2. Open the "Configuration" > "Data Sources" page.
3. Confirm whether the system is configured with log data sources.
4. View the status of the log data sources in the list.
5. If the status is red, contact the system administrator for system collection troubleshooting.

Refer to section "Status Icon" in chapter Managing log data sources (Page 178).

9.2 Corrective maintenance

9.2.1 Software maintenance

9.2.1.1 Log data diagnosis

Interfaces to download log data

When the hardware or a service of the SINEC Security Monitor System is abnormal, the administrator can analyze the cause of the problem by downloading the log data of the hardware and services.

The log download function includes downloading hardware (SINEC Security MonitorServer and SINEC Security Monitor Sensor) and service log.

Table 9-9 Log data addresses

Hardware or service	URL
SINEC Security Monitor Server	/admin/diagnostic/log/server/node?hostId=XXXX
SINEC Security Monitor Sensor(s)	/admin/diagnostic/log/sensor/node?hostId=XXXX
Gateway service	/admin/diagnostic/log/server/service/gateway
SI service	/admin/diagnostic/log/server/service/si
CA service	/admin/diagnostic/log/server/service/ca
CM service	/admin/diagnostic/log/server/service/cm
Collector service	/admin/diagnostic/log/server/service/collector
OpenSearch service	/admin/diagnostic/log/server/service/opensearch
Redis service	/admin/diagnostic/log/server/service/redis
Logstash service	/admin/diagnostic/log/server/service/logstash
Logforward service	/admin/diagnostic/log/server/service/logforward
Prober service	/admin/diagnostic/log/server/service/prober
Zeek service	/admin/diagnostic/log/server/service/zeek
Suricata service	/admin/diagnostic/log/server/service/suricata
LogAgent service	/admin/diagnostic/log/server/service/logAgent
Virtual SINEC Security Monitor Sensor service	/admin/diagnostic/log/sensor/service?hostId=XXXX

For instructions on downloading the latest logs, refer to Diagnostics page (Page 209).

9.3 Preventive maintenance

9.3.1 Reinstalling the SINEC Security Monitor Server

Note

If you want to reinstall SINEC Security Monitor Server, you must install the entire SINEC Security Monitor System again.

See also

Backup configuration settings (Page 222)

9.3.1.1 Backup configuration settings

The following options for handling backups are available:

On the WBM:

- Create or schedule backups
- Restore backups

Create a backup on the WBM

1. Log in to the WBM with administrator privileges.
2. Select the "System" > "Backup List" menu.
3. Click "Backup Now".
4. Select System configuration as a target and click "OK".
5. The new backup will appear in the "Backup List".

Schedule regular backups

For setting up scheduled backups, refer to chapter Configuring system backups (Page 122).

Restore a backup on the WBM

Note

It is not possible to upload backup files here.

1. Log in to the WBM with administrator privileges.
2. Select the "System" > "Backup List" menu.
3. Select a backup from the Backup List and click "Restore".

9.3.2 Reinstalling the SINEC Security Monitor Sensor

Note

If you want to reinstall SINEC Security Monitor Sensor services, you must install the entire SINEC Security Monitor System again.

9.3.3 Reinstalling the SINEC Security Monitor Agent

9.3.3.1 Uninstalling the SINEC Security Monitor Agent

Note

The SINEC Security Monitor Agent must be uninstalled before it can be reinstalled.

Prerequisites

- Administrator privileges on the Microsoft Windows computer are needed for this procedure.
- `uninstaller.exe` from the SINEC Security Monitor Agent software package

Uninstalling

1. Run `uninstaller.exe` with administrator privileges.
2. When prompted, enter "Y" to delete the logagent directory.
3. Wait for the procedure to finish.
4. Press [Win] +[R].
5. The Run command window opens.
6. Run `services.msc` and check if the `LogAgent` and the `UpdateAgent` services on the Extended tab disappeared.

9.3.4 Checking for system updates

System updates

1. Perform a regular check for hotfixes and system updates.
Keep the software you are using up to date. Check regularly for security updates and apply them.
2. To obtain system updates contact your Siemens sales or project representative.

9.3.5 Rebooting the SINEC Security Monitor System

Purpose

A system can be rebooted to solve a number of system issues. During the reboot the system will not be available.

Rebooting the server will shut down all the sub-systems and modules and restart all the services. This action will take several minutes.

Reboot the SINEC Security Monitor Server

1. Log in to the WBM.
2. Select the "System" > "Reboot" menu.
3. Click "Reboot Server".

Reboot the SINEC Security Monitor Sensor (IPC)

Use the power switch on the device to switch the IPC off and on.

Reboot the SINEC Security Monitor Sensor (HPE)

Before powering down the device for any upgrade or maintenance procedures, perform a backup of critical server data and programs.

When the device is in standby mode, auxiliary power is still being provided to the system.

To power down the device, use one of the following methods:

- **Controlled Shutdown:** Press and release the "Power On/Standby" button. This method initiates a controlled shutdown of applications and the operating system before the device enters standby mode.
- **Forced Shutdown:** Press and hold the "Power On/Standby" button for more than 4 seconds to force the device to enter standby mode. This method forces the device to enter standby mode without properly exiting applications and the operating system. If an application stops responding, the user can use this method to force a shutdown.
- **Remote Management (iLO):** Use Integrated Lights-Out (iLO) on HPE servers for remote power management, such as powering on/off or rebooting the server, and monitoring server health. This method provides remote access and management capabilities without needing physical access to the server.

Before proceeding, verify the device is in standby mode by observing that the system power LED is amber.

To power up the device, press the "Power On/Standby" button.

9.3.6 Updating the vulnerability library and correlation rules

Vulnerability library and correlation rules need to be updated regularly in order to ensure that the latest vulnerabilities are detected.

Refer to chapter Updating the SINEC Security Monitor Intelligence Databases (Page 119)

9.3.7 Managing backups

Purpose

The Backup List page lists available backups and allows backups to be created, downloaded, or restored.

Regular backups can be configured on the "Configuration" > "System" > "Backup page".

Backups created in previous versions, like for example V4.7.1, are not displayed on the "Backup page".

Refer to chapter Configuring system backups (Page 122)

Note

Backup files can not be restored in cross-version mode.

You can not restore backup files (Raw Logs/Security Event/System Configuration) from a SSM V4.8.0 device on a SSM V4.9.0 device.

Backup files can only be restored on the same version.

Access the backup list

1. Log in to the WBM.
2. Select the "System" > "Backup List" menu.

Table 9-10 Backup List functions

Function	Description
Calendar	Select a period
"Backup Now"	Run a backup at this moment
"Restore"	Restore a backup on the Server

9.3.8 Using the test mode

Purpose

The Test Mode allows you to test the SINEC Security Monitor System and to become familiar with the WBM. Upload packet captures from a target environment and check out how SINEC Security Monitor acts.

Test Mode is just a set of useful tools for testing purposes. It cannot be switched on or off.

Note

Do not use the Test Mode on an actual live system!

To run SINEC Security Monitor in Test Mode, upload network packet captures in .pcap or .pcapng file format to the SINEC Security Monitor System. This allows you to observe, how SINEC Security Monitor works in a specific environment or to fuel SINEC Security Monitor with data in a test environment for demonstration purposes.

The "Clear all data" function removes all raw logs and deletes all generated assets and security events but does not remove configuration data.

Uploading packet captures

Note

A maximum packet size of 100 Megabyte is supported.

1. Log in to the WBM.
2. Select the "System" > "Test mode" menu to access the "Upload Packet" tab.
3. Click "Browse" to select a .pcap or .pcapng file.

Clearing all data

NOTICE**Danger of data loss. All information collected by the SINEC Security Monitor System will be lost!**

The "Clear all data" button deletes all collected information (raw logs, generated assets, and security events) from the system.

This button is made for testing purposes or decommissioning. Do not click on this button on a LIVE system.

1. Log in to the WBM.
2. Select the "Configuration" > "Data Sources" menu.
3. Click "Stop" for all data sources.

4. Select the "Configuration" > "Sensor" menu.
5. Click "Stop" for all sensors.
6. Select the "System" > "Test mode" menu.
7. Select the "Clear all data" tab.
8. Click "Clear all data".

9.3.9 Checking system alarms

Purpose

The "System Alarm" page displays information on event notifications, separated into "System Event Notifications" and "Security Event Notifications" tabs.

This page is purely for information purposes, these tables cannot be edited or sorted.

Accessing system alarms

1. Log in to the WBM.
2. Select the "System" > "System Alarm" menu.
3. Check "System Event Notifications" listed on the first tab of the page.
4. Check "Security Event Notifications" listed on the second tab of the page.

Configure system and security event notifications

1. Log in to the WBM.
2. Select the "Configuration" > "Notifications" menu.
3. Check "System Event Notifications" listed on the first tab of the page.
4. Set check marks for the notifications required.
5. Check "Security Event Notifications" listed on the second tab of the page.
6. Set check marks for the notifications required.
7. Click "Save".

9.3.10 SINEC Security Monitor Agent remote update

Configuring SSM Agent remote updates

Configuring SSM Agent remote updates

The "Configuration" > "Agent Update" page allows to upload the latest SINEC Security Monitor Agent software packages and to update the SINEC Security Monitor Agent software on workstations in the network remotely.

Note

The Agent Update feature is not supported for SINEC Security Monitor 4.8.0. For updates, the SINEC Security Monitor Agent software needs to be uninstalled before the installation of a newer version.

This feature was not supported for the last SINEC Security Monitor version 4.8.0. The enhanced encryption techniques require a unique certificate file for each agent installation for the communication with SINEC Security Monitor Server or SINEC Security Monitor Sensor. If there is a need to update the SINEC Security Monitor Agent software from an older version to a version of 4.9.0 or higher, you must uninstall and re-install the SINEC Security Monitor Agent software.

For more information, refer to chapter Reinstalling the SINEC Security Monitor Agent (Page 223).

Exploring the agent update page

Accessing the agent update page

1. Log in to the WBM.
2. Select the "Configuration" > "Agent Update" menu.

Add a software package

1. Log in to the WBM.
2. Select the "Configuration" > "Agent Update" menu.
3. To open the "Add" window, click "Add".
4. Click "Browse" and select the software package.
5. Click "OK" to start an upload.
6. The software package appears in the table.

Delete a software package

1. Log in to the WBM.
2. Select the "Configuration" > "Agent Update" menu.
3. Select one or more records in the table.

4. Click "Delete".
5. Click "OK" in the popup window.

Compare the checksum

1. On a PC, unpack the update package ".zip" file with a suitable application, for example "7-zip".
2. Open the file "manifest.yml" with a suitable application, for example "Notepad++".
3. Compare the checksum in the file "manifest.yml" with the checksum on the "Agent Update" page.

To verify the signature of the {installation-file}.exe for authenticity and integrity, refer to chapter Verifying signatures of signed installation files (Page 82).

Update the SSM Agent software on a workstation

1. Log in to the WBM.
2. Select the "Configuration" > "Agent Update" menu.
3. Click "Update" in the "Actions" column of the software package.
4. Select one or more machines with SSM Agent installed.
5. Click "OK".

Access the upgrade history

1. Log in to the WBM.
2. Select the "Configuration" > "Agent Update" menu.
3. Click "Upgrade history" in the "Actions" column of a software package.
4. Check out the installation history of all machines.

Download a software package to your PC

1. Log in to the WBM.
2. Select the "Configuration" > "Agent Update" menu.
3. Click "Download" in the "Actions" column of the required software package.
4. The SSM Agent software package downloads to your PC.

Note: The "Checksum" verifies the data integrity of a software package. Use SHA256 to verify the checksum of the downloaded file. Refer to chapter SHA256 checksums (Page 82).

9.4 Updating system components

9.4.1 Overview of the upgrade process

Supported SSM Version

This manual and script supports the upgrade from SSM V4.9.0 to V4.9.1.

Migration steps

The SSM migration from V4.9.0 to V4.9.1 consists of 6 major stages:

1. Migration of the SSM Server
2. Migration of the physical SSM Sensor
3. Migration of the SSM Agent
4. Check the Agentless log collection data after the upgrade
5. Check the No Agent log collection data after the upgrade
6. Update the SSM Intelligence Libraries

Note

- The procedure distinguishes between the virtual SSM Sensor which is a part of the SSM Server, and the physical SSM Sensor which is installed on its own device.
 - For the liveCD preparation, a USB flash drive (with a minimum storage size of 64 GB) is used as a medium. The liveCD is a USB flash drive with Debian Live Image installed.
 - Upgrade procedures distinguish between "local" and "remote". This chapter describes a local procedure. Access to the devices is necessary.
-

SSM Server migration steps

The local upgrade procedure of the SSM Server from V4.9.0 to V4.9.1 covers:

1. **Check the SSM System V4.9.0 overall status**
Before the upgrade, check the SSM System V4.9.0 overall status, validate that the SSM System V4.9.0 runs well and that it is ready for the upgrade.
2. **Acceptance Test:**
Execute the command to perform acceptance test, check Server container and services status before upgrade.
3. **Upload the SSM Server update package:**
Download the SSM Server update package, unzip the package and execute the command to upload the package.
4. **Launch the update:**
Execute the command to launch the SSM Server update.

5. **Acceptance test:**
Execute the command to perform an acceptance test, check the SSM Server containers and service status.
6. **Double-check the SSM Server upgrade status:**
Execute the commands to update the recovery partition and double-check and confirm the SSM Server upgrade status.
7. **Check the new version:**
Access the WBM to verify the new version V4.9.1.
8. **Check the SSM Server services and container status:**
On the "System" > "Diagnostics" page, check all SSM Server services and container status.
9. **Rollback:**
If any failure occurred during the SSM Server upgrade process, execute the command to rollback.

Physical SSM Sensor migration steps

The local upgrade procedure of the SSM Sensor from V4.9.0 to V4.9.1 covers:

1. **Acceptance test:**
Execute the command to perform an acceptance test, check the SSM Sensor containers and service status.
2. **Upload the SSM Sensor update package:**
Download the SSM Sensor update package, unzip the package and execute the command to upload the package.
3. **Launch the update:**
Execute the command to launch the SSM Sensor update.
4. **Acceptance test:**
Execute the command to perform an acceptance test, check the SSM Sensor containers and service status.
5. **Double-check the SSM Sensor upgrade status:**
Execute the commands to update the recovery partition and double-check and confirm the SSM Sensor upgrade status.
6. **Check the SSM Sensor services and container status:**
On the "System" > "Diagnostics" page, check all SSM Sensor services and container status.
7. **Rollback:**
If any failure occurred during the SSM Sensor upgrade process, execute the command to rollback.

SSM Agent migration steps

The SSM Agent upgrade is performed on the WBS.

1. **Check the SSM Agent status:**

On the "Configuration" > "Data Sources" page, check the SSM Agent status, and validate that the latest SSM Agent data is received successfully.

2. **Perform Agent Update to V4.9.1 if Required:**

On the "Configuration" > "Data Sources" page, upload the SSM Agent 4.9.0 update package file and perform a SSM Agent upgrade.

Check the Agentless log collection

Verify the functioning of the Agentless log collection on the WBS.

1. **Check Agentless status:**

On the "Security Events" > "Logs" page, check the Agentless log collection and validate that the latest Windows security events are received successfully.

Check the No Agent log collection

Verify the functioning of the No Agent log collection on the WBS.

1. **Check No Agent status:**

On the "Configuration" > "Data Sources" page, check all No Agent data source status. Validate on the "Security Events" > "Logs" page that the latest No Agent data is received successfully.

Upgrade packages

The following packages are used for the upgrade procedures.

No.	Component	Package	Description
1	SSM Sensor	ssm-4.9.1-sensor-tpm-prod.swu.tar.xz	SSM Sensor Local Upgrade Package
2	Artifact Metadata	artifactInfo.xml	Artifact Metadata for SSM Sensor
3	SSM Server	ssm-4.9.1-server-tpm-prod.swu.tar.xz	SSM Sensor Local Upgrade Package
4	Artifact Metadata	artifactInfo.xml	Artifact Metadata for SSM Server
5	Correlation Rule Library	Correlation_Rule-signed.zip	SSM V4.9.1 the latest version of Correlation Rule Library
6	3rd Party Threat Intelligence Library	ET-Pro-Ruleset-signed.tgz	SSM V4.9.1 the latest version of 3rd Party Threat Intelligence Library
7	Vulnerability Library	Vulnerability-osa-491-2024.4-signed.zip	SSM V4.9.1 the latest version of Vulnerabilities Library

9.4.2 SSM Server software update

Preparation

Before the upgrade, access the WBM. Use the diagnostics tools and dashboards to verify the wellbeing of the SSM System.

1. Check the SSM V4.9.0 system status.
For example:
 - SSM Server services
 - SSM Server docker containers
 - SSM Sensor services
 - SSM Sensor docker containers
2. Verify that all features of SSM V4.9.0 are running well.
For example:
 - Network communication
 - Network load
 - Log collection, log aggregation, log forwarding
 - Security logs audit
 - Security events
 - Risk management
 - AS asset discovery
 - Vulnerability management
 - Anomaly detection
 - Network packet capturing
3. Perform an acceptance test, to check Sensor containers and services status before upgrade.
When the SSM V4.9.0 system runs well, it is ready for the upgrade.

Note

The following instruction require Linux administration experience.

Upload the SSM Server update package

Prerequisites:

- USB flash drive (with a minimum storage size of 64 GB, exFAT formatted) as a medium for data transfer.
- The user account that was created during the SSM Server installation process

Installation steps:

1. Download the SSM Server upgrade package file from the software distribution platform.
Link: (<https://support.sw.siemens.com/en-US>)
`ssm-4.9.1-server-tpm-prod.swu.tar.xz`
2. Extract the ".tar.xz" file. Inside you will find a *.swu and *.xml file.
3. Transfer the *.swu and *.xml file to the SSM Server using a removable medium.
4. Execute the command to upload the SSM Server update package.
`ssmctl-client local_update upload --service_module server`
5. When the message "Please select the removable media" appears, select your USB flash drive by pressing the appropriate key.
For example, for "/dev/sdc1 U 40.6G", it is required to press the key "1".
6. Check and verify that the upload of the update package file is executed successfully.
The message given by the system is: "Upload file successfully"

Launch the SSM Server update

Note

The Server update proces takes about 20 minutes followed by a system reboot that takes about 10 minutes to complete.

1. After uploading the update package, execute the command to launch the SSM Server update:
`ssmctl-client local_update launch_update --service_module server --from 4.9.0 --to 4.9.1`
2. Check and verify that the launch of the update process is executed successfully and the system is rebooting automatically.
The message given by the system is: "Launch update successfully."
3. If any failure occurred during the update launch update process, the error message displayed is: "Current system is in failed state. Please rollback the system first"

Acceptance test

1. After the system reboot, execute the command to perform an acceptance test:
`ssmctl-client system acceptance_test --service_module server`
2. Check and verify that the "ustate" field is displayed as "0 (OK)".

States of the "ustate" field	Consequences
0 (OK)	State after a successfull acceptance test.
1 (INSTALLED)	Wait.
2 (TESTING)	Wait.
3 (FAILED)	Installation failed.

3. Validate that all SSM Server services status are displayed as "Active".

Server Service Name	Status
check-startup.service	Active
docker.service	Active
metricbeat	Active
heartbeat-elastic	Active
syslog-ng.service	Active
ssmctl-server.service	Active
lic-status.service	Active
create-docker-network.service	Active
automatics-start.service	Active
custom-startup	Active
wireguard	Active
s2l2 system	Active

4. Validate that all docker container status are displayed as "Up (Healthy)".

Server docker container name	Status
server.logforward	UP (Healthy)
server.ca	UP (Healthy)
server.si	UP (Healthy)
server.gateway	UP (Healthy)
server.cm	UP (Healthy)
server.logstash	UP (Healthy)
server.collector	UP (Healthy)
server.redis	UP (Healthy)
server.os	UP (Healthy)
server.logagent	UP (Healthy)
server.pg	UP (Healthy)
sensor.zeek	UP (Healthy)
sensor.logagent	UP (Healthy)
sensor.suricata	UP (Healthy)
sensor.prober	UP (Healthy)

5. Note the "Current system version". This information is necessary in case a rollback needs be performed.

Confirm the SSM Server upgrade status

1. Execute the command to update the recovery partition:

```
ssmctl-client local_update update_recovery_partition --
service_module server
```
2. Check and verify that the update recovery partition module is executed successfully.
The message given by the system is: "UpdateRecoveryPartition module execute successfully."

3. Execute the command to perform another acceptance test to check the SSM Server upgrade status:

```
ssmctl-client system acceptance_test --service_module server
```

4. Check and verify that the "ustate" field is displayed as "0 (OK) "
5. Validate that all SSM Server services status are displayed as "Active".
6. Validate that all docker container status are displayed as "Up (Healthy)".

Check the version number in the WBM.

1. Log in to the WBM.
2. The SINEC Security Monitor version number is located at the bottom of the menu bar on the left side of the page.
3. To see the full version number, move your mouse over the version number.

Check services and containers in the WBM.

1. Log in to the WBM.
2. Select the "System" > "Diagnostics" menu to open the "Diagnostics" page.
3. Check the status of all SSM Server services:

- metricbeat
- heartbeat-elastic
- syslog-ng
- ssmctl-server

Verify that the status is displayed as "Active".

4. Check the status of all SSM Server docker containers:

- pg
- os
- redis
- si
- ca
- gateway
- collector
- logstash
- logforward
- cm

Verify that the status is displayed as "Up (Healthy)".

5. Check the docker container status of the integrated SSM Sensor:

- zeek
- logagent
- suricata
- prober

6. Verify that the status is displayed as "Up (Healthy)".

If any failure occurred during the migration process of the SSM Server, you must rollback the SSM System to V4.9.0 before starting again with the migration.

Execute below commands to rollback to version 4.9.0:

```
ssmctl-client local_update rollback --service_module server --to 4.9.0
```

Note

The current system version is shown during the acceptance test.

9.4.3 SSM Sensor software upgrade

Upload the SSM Sensor update package

Prerequisites:

- USB flash drive (with a minimum storage size of 64 GB, exFAT formatted) as a medium for data transfer.
- The user account that was created during the SSM Sensor installation process

Installation steps:

1. Download the SSM Sensor upgrade package file from the software distribution platform.
Link:

```
ssm-4.9.1-sensor-tpm-prod.swu.tar.xz
```

2. Copy the package `ssm-4.9.1-sensor-tpm-prod.swu.tar.xz` file to the SSM Sensor using the removable medium.

3. Unzip the ".tar.xz" file.

4. Execute the command to upload the SSM Sensor update package.

```
ssmctl-client local_update upload --service_module sensor
```

When the message "Please select the removable media" appears, select your USB flash drive by pressing the appropriate key.

For example, for `/dev/sdc1 U 40.6G`, it is required to press the key "1".

5. Check and verify that the upload of the update package file is executed successfully.
The message given by the system is: "Upload file successfully"

Launch the SSM Sensor update

Note

The Sensor update process takes about 20 minutes followed by a system reboot that takes about 10 minutes to complete.

1. After uploading the update package, execute the command to launch the SSM Sensor update:

```
ssmctl-client local_update upload --service_module sensor
```
2. Check and verify that the launch of the update process is executed successfully and the system is rebooting automatically.
The message given by the system is: "Launch update successfully."
3. If any failure occurred during the update launch update process, the error message displayed is: "Current system is in failed state. Please rollback the system first"

Acceptance test

1. After the system reboot, execute the command to perform an acceptance test:

```
ssmctl-client system acceptance_test --service_module sensor
```
2. Check and verify that the "ustate" field is displayed as "0 (OK)".
3. Validate that all SSM Sensor services status are displayed as "Active".

Server Service Name	Status
check-startup.service	Active
docker.service	Active
metricbeat	Active
heartbeat-elastic	Active
syslog-ng.service	Active
ssmctl-server.service	Active
lic-status.service	Active
create-docker-network.service	Active
automatics-start.service	Active
custom-startup	Active
wireguard	Active
s2l2 system	Active

4. Validate that all docker container status are displayed as "Up (Healthy)".

Server docker container name	Status
sensor.zeek	UP (Healthy)
sensor.logagent	UP (Healthy)
sensor.suricata	UP (Healthy)
sensor.prober	UP (Healthy)

Confirm the SSM Server upgrade status

1. Execute the command to update the recovery partition:

```
ssmctl-client local_update update_recovery_partition --service_module sensor
```
2. Check and verify that the update recovery partition module is executed successfully.
The message given by the system is: "UpdateRecoveryPartition module execute successfully."
3. Execute the command to perform another acceptance test to check the SSM Sensor upgrade status:

```
ssmctl-client system acceptance_test --service_module sensor
```
4. Check and verify that the "ustate" field is displayed as "0 (OK) "
5. Validate that all SSM Sensor services status are displayed as "Active".
6. Validate that all docker container status are displayed as "Up (Healthy)".

See also

Link: (<https://support.sw.siemens.com/en-US>)

Check services and containers in the WBM.

1. Log in to the WBM.
2. Select the "System" > "Diagnostics" menu to open the "Diagnostics" page.
3. Check the status of all SSM Sensor services:
 - metricbeat
 - heartbeat-elastic
 - syslog-ng
 - ssmctl-serverVerify that the status is displayed as "Active".
4. Check the docker container status of the SSM Sensor:
 - prober
 - zeek
 - logagent
 - suricata
5. Verify that the status is displayed as "Up (Healthy)".

If any failure occurred during the migration process of the SSM Sensor, you must rollback the SSM System to V4.9.0 before starting again with the migration.

Execute below commands to rollback to version 4.9.0:

```
ssmctl-client local_update rollback --service_module sensor --to 4.9.0
```

9.4.4 SSM Agent update

Considerations

- The SSM System provides a remote upgrade feature that simplifies the SSM Agent update steps.
- The Agent Update feature is supported in the current SSM version V4.9.0. The Agent Update feature is not supported on SSM version V4.8.0.
- The SSM Agent V4.8.0 software is compatible with the SSM Agent V4.9.0 software. There is no need to do the SSM Agent upgrade during the migration from 4.8.0 to 4.9.0. But, when you want to migrate to SSM V4.10.0 in the future, you have to upgrade all SSM Agents to V4.9.0 first.
- When required, you can upload the latest Agent update packages to the WBM to upgrade all SSM Agents from V4.8.0 to V4.9.0.
- For more information on the Agent Update feature, refer to SINEC Security Monitor Agent remote update (Page 228).

Verify the SSM Agent status in the WBM

1. Log in to the WBM.
2. Select the "Configuration" > "Data Sources" menu.
3. Check the status of your SSM Agents.
 - A red status icon indicates "out of service".
 - A blue status icon indicates "in operation".
4. Verify that the latest SSM Agent data is received successfully, and the SSM Agent collects the following data:
 - Application logs
 - Security logs
 - System logs
 - User account data
 - Data about installed Windows programs data
 - Patch information

Perform a SSM Agent update to V4.9.0

1. Upload the update package.
 - Log in to the WBM.
 - Select the "Configuration" > "Agent Update" menu.
 - To open the "Add" window, click "Add".
 - Click "Browse" and select the software package `SINEC-Security-Monitor-Agent-4.9.0-Update-x86-{version}.zip` which is extracted from the software package `SINEC-Security-Monitor-Agent-4.9.0-Update-x64.exe`
 - Click "OK" to start an upload.
The software package appears in the table.
Check the agent update information: package name, timestamp, checksum, operating system, architecture, target version, minimum system version, description, and actions.
2. To remotely update the Agent software on the Windows clients/data sources:
 - Click "Update" in the "Actions" column of the software package.
 - Select one or more devices with SSM Agent installed.
 - Click "OK".
 - Click "Upgrade History" to check the detailed upgrade information: timestamp, data source, IP, package name, current version, operating system, architecture, status, update time, checksum, and error message.

For new installations of the SSM Agent software:

1. Click "Download" to download the installation package to your local machine.
2. Run the installation.

For more information, refer to Installing the SINEC Security Monitor Agent on a Microsoft Windows-based asset (Page 156).

9.4.5 Checking data sources

9.4.5.1 Checking Agentless log collection after the migration

Verify that Agentless log collection is working

Note

After a successful upgrade of the SSM Sever and SSM Sensor from V4.9.0 to V4.9.1, all Agentless data will be retained and restored. There is no need for an Agentless data source configuration.

1. Log in to the WBM.
2. Select the "Security Events" > "Logs" menu.

3. Select a Microsoft Windows client from the "All data sources" drop-down menu.
4. Verify that the latest Windows security events are received and listed.

Verify that No Agent log collection is working

Note

After a successful upgrade of the SSM Sever and SSM Sensor from V4.9.0 to V4.9.1, all No Agent data will be retained and restored. There is no need for an No Agent data source configuration.

Verify the No Agent status in the WBM

1. Log in to the WBM.
2. Select the "Configuration" > "Data Sources" menu.
3. Check the status of your No Agents.
A red status icon indicates "out of service".
A blue status icon indicates "in operation".

Verify that the latest No Agent data is received successfully

1. Log in to the WBM.
2. Select the "Security Events" > "Logs" menu.
3. Select the data source from the "All data sources" drop-down menu.
4. If many events appear on the list, data collection is successful.
The No Agent data sources collect syslog data from the following data sources:
 - Endpoints
 - Network devices
 - Other systems

9.4.6 Updating the SSM Intelligence Database

9.4.6.1 Updating the SSM Intelligence Database

Note

- After the migration from V4.9.0 to V4.9.1, the Correlation Rules and the Vulnerability Library are retained and compatible with SSM V4.9.1. An update is not mandatory.
 - It is a good opportunity to update the SSM Intelligence Database at this stage.
-

For update instructions, refer to chapter Updating the SINEC Security Monitor Intelligence Databases (Page 119).

Decommissioning, dismantling, and disposal

Remove all collected data

Remove all data collected on the SINEC Security Monitor System on the page "System" > "Test Mode" > "Clear all data". This procedure does not remove configuration data.

Uninstall software

SINEC Security Monitor Server: If you want to uninstall the SINEC Security Monitor Server, you must reinstall the entire SINEC Security Monitor System.

SINEC Security Monitor Sensor: If you want to uninstall the SINEC Security Monitor Sensor, you must reinstall the entire SINEC Security Monitor System.

SINEC Security Monitor Agent: See chapter Uninstalling the SINEC Security Monitor Agent (Page 223)

Clearing TPM

As a part of the decommissioning routine, you must clear the TPM.

Refer to chapter Hardware preparation (Page 75) for instructions for each device.

Permanently wipe hard drives of sensitive data

SINEC Security Monitor Sensor procedure

When the device was delivered with an operating system (Microsoft Windows), a USB stick containing system restoration tools was part of the package. The procedures "Restore entire hard disk" and "Restore system partition" will only delete all data, user settings and existing authorizations or license keys and restore the original operating system.

Alternatively: Use the Debian live USB flash drive to wipe the hard drives using Linux tools. This procedure will take some time.

1. Insert the "USB flash drive A" (Debian live system).
2. Boot up the sensor and press [ESC]. The "Remote View" screen opens.
3. On the "Remote View" screen, click "Boot Manager".
4. In the "Boot Manager", use the [Arrow up and arrow down] keys to select "USB flash drive A" and press [Enter].
5. After booting up, log in with `root`.
6. To show the file system, execute the command:
`lsblk`

7. If necessary, unmount the hard drive first:

```
sudo umount /dev/{sdX} -l
```

Note: {sdX} is the name of the target drive.

8. To fill the hard drive with random characters, use this command:

```
dd if=/dev/urandom of=/dev/{sdX} bs=1M
```

Note: {sdX} is the name of the target drive.

SINEC Security Monitor Server procedure

HP provides a one-button secure erase feature. Refer to the link below for more information.

Link: (https://support.hpe.com/hpesc/public/docDisplay?docId=a00018320en_us&docLocale=en_US&page=ref-secure-system-erase.html)

Dell provides data security by using the system erase feature. Refer to the link below for more information.

Link: (<https://dl.dell.com/manuals/common/dell-emc-system-erase-poweredge-idrac9.pdf>)

Listing SSMCTL Commands

Using SSMCTL commands

The SSMCTL commands are used at the prompt of the Siemens CoreShield S2L2 Linux backend. You can use the Operator login name and password that was created during the SSM Server and SSM Sensor configuration.

After the installation of the SSM Server and SSM Sensor devices, the systems are hardened. That means, remote access is not possible. You have to equip the devices with monitor, keyboard and mouse to use the Linux backend.

Obtain a list of SSMCTL command

To obtain a list of current commands, you have to access the internal help page of the command.

1. Log in to the Linux backend.
2. Enter the command:
`ssmctl-client --help`
3. Take screenshots of the results for further reference.

Security Forwarding Data Format

A.1 Security Forwarding Data Format

SINEC Security Monitor supports RFC3164 and RFC5424 protocols. Find below the data format and samples for raw logs and security events for the transport protocols TCP, UDP and TLS.

RFC3164 Raw Logs fields (TCP, UDP, TLS)

Table A-1 Raw log forwarding data format RFC3164 (TCP, UDP, TLS)

Field name	Sample data	Comments
Port	46502	Source port number
MSG	{'msg':'xxx','host':'xxx'}	Message content
MSG-Content-PRI	<13>	Digital from 0 to 191: [9] means ALERT [12] means WARNING [13] means EVENT [14] means LOG
MSG-Content- TIMESTAMP	2024-01-15T05:30:01.383+00:00	Generated date and time
MSG-Content-HOSTNAME	"name!":\0.0.0.0\	Sender host name
MSG-Content- APP-NAME	LOGSTASH	Sender process name
MSG-Content- PROCID	-	Sender PID
MSG-Content-MSGID	-	Message ID
MSG-Content- STRUCTURED-DATA	-	Structured data of the message
@timestamp	2024-01-15T05:45:25.455Z	Generated date and time
@version	1	RFC version

RFC3164 Raw Logs sample (TCP)

```
{
  "message": "<13>Jul 25 02:29:32 {\"name\": \"server.logforward\"}
LOGSTASH[-]: 2024-07-25T02:29:32.451996452Z
{name=server.logforward}
{
  \"status\": \"Y\", \"component\": \"SI\", \"device_ip\": \"10.11.0.139\",
  \"extra_fields\": \"{\\\"dataSrcIP\\\": \\\"10.11.0.139\\\"}\"
  , \"event_change\": \"{\\\"user\\\": null, \\\"action\\\": null, \\\"
  \"policy\\\": null, \\\"status\\\": \\\"unprocessed\\\", \\\"
  \"approver\\\": null, \\\"deadline\\\": null, \\\"supervisor\\\":
  null, \\\"updateTime\\\": null, \\\"saveUpdownGrade\\\": null, \\\"
  \"updateEventType\\\": null}\"
  , \"logs\": [
    {
      \"c2gw55ABFnRBwQdXcJVG\", \"asset\": null, \"@timestamp\": \"2024-07-2
      5T00:05:01.005674004Z\", \"siem_time\": \"2024-07-25T00:00:30.000Z\", \\
      \"application\": null, \"notification\": null, \"tags\": [\"input-
      postgres-
      event\"], \"event_type\": \"event\", \"id\": 336642529792512, \"update_ti
      me\": \"2024-07-25T00:00:30.573646Z\", \"remarks\": \"Special
      privileges assigned to new logon on Windows host
      10.11.0.139\", \"traffic\": null, \"name\": \"Admin Login on
      Windows\", \"@version\": \"1\", \"correlation_info\": null, \"sensor_id\"
      : \"3a42ed04522aad3a2a6c1c5b791c4c55\", \"event_id\": \"918\", \"cia_lev
      el\": \"integrity\", \"insert_time\": \"2024-07-25T00:00:30.573644Z\"}
      , \"host\": \"10.11.72.50\", \"@timestamp\": \"2024-08-19T02:56:09.397Z\", \"port\"
      : 43344, \"@version\": \"1\"}
    ]
  }
}
```

RFC3164 Raw Logs sample (UDP)

```
{"@timestamp":"2024-08-19T02:41:55.144Z","@version":"1","message":"<
13>1 2024-08-19T02:41:38.258+00:00 {"name":"server.logforward"}
LOGSTASH - - - 2024-08-19T02:41:38.258638547Z
{name=server.logforward} {"input":
{"type":"log"},"@timestamp":"2024-08-19T02:41:37.936Z","proto":
"tcp","dpt":443,"log":{"file":{"path":"/opt/zeek/
logs/current/
conn.log"}},"src":"10.11.0.106","rt":1724035290991,"spt":64
478,"cn1":0,"ad_local_resp":false,"orig_pkts":3,"tags":
["zeek","beats_input_raw_event"],"cn2":156,"history":"S",
"resp_pkts":0,"app":"tcp_443","FACTORY_ID":"10001","agent\
":
{"version":"8.10.4","name":"sensor.logagent","ephemeral_id\
":"cbc18556-0489-4c7a-
a795-07cdcb228063","id":"60eaf81a-15f9-4777-9d98-
cce884cf67b1","type":"filebeat"},"vlan":1000,"ad_local__orig
":true,"GROUP_ID":"siemens","cn3":0,"smac":"90:8d:6e:8a:3b
:85","dataSrcIP":"10.11.60.191","host":"sensor.logagent","
fields":
{"collector_node_id":"sensor.logagent","sensor_id":191,"gl2_s
ource_collector":"A6060600FFFBEBBFBYS7YY3"},"ecs":
{"version":"8.0.0"},"cat":"conn","LINE_ID":"1001","duse
r":"S0","offset":252879010,"uid":"CgSbCB22fndFbwsRJ3","dma
c":"d4:2c:44:fb:fd:c8","dst":"13.107.42.16"}
\n","host":"172.17.0.1"}
```

RFC3164 Raw Logs sample (TLS)

```
{ "@version": "1", "host": "10.11.60.233", "@timestamp": "2024-08-19T03:21:06.193Z", "port": 55074, "message": "<13>Aug 19 03:20:47\n{ \"name\": \"server.logforward\" } LOGSTASH[-]:\n2024-08-19T03:20:47.655304009Z {name=server.logforward}\n{ \"src\": \"10.11.9.50\", \"fields\":\n{ \"gl2_source_collector\": \"E4060300FFFB8B0FVMware420fd1987c37ab59ef97c2175fa0ff05\", \"sensor_id\": 245, \"collector_node_id\": \"sensor.logagent\" }, \"tags\":\n[ \"suricata\", \"beats_input_raw_event\" ], \"resp_pkts\": 0, \"cat\": \"suricata_event\", \"log\": { \"file\": { \"path\": \"/var/log/suricata/suricata_event.json\" }, \"dst\": \"10.11.60.245\", \"event_type\": \"flow\", \"GROUP_ID\": \"siemens\", \"input\":\n{ \"type\": \"log\", \"app\": \"failed\", \"uid\": 1764347346711452, \"LINE_ID\": \"1001\", \"ecs\":\n{ \"version\": \"8.0.0\", \"spt\": 56713, \"out\": 261, \"in\": 0, \"FACTORY_ID\": \"10001\", \"rt\": 1723766400000, \"proto\": \"UDP\", \"flow_start\": 1723766366000, \"dataSrcIP\": \"10.11.60.245\", \"host\": \"sensor.logagent\", \"dpt\": 514, \"agent\":\n{ \"name\": \"sensor.logagent\", \"type\": \"filebeat\", \"id\": \"ab2b764c-0b8b-4d1f-a511-ca514612452b\", \"version\": \"8.10.4\", \"ephemeral_id\": \"6504e846-bff1-429a-ab59-1b4b9975be92\" }, \"@timestamp\": \"2024-08-16T00:00:00.773Z\", \"interface\": \"ens192\", \"offset\": 168296904, \"orig_pkts\": 1 } } }
```

RFC3164 Security Event fields (TCP, UDP, TLS)

Table A-2 Security event forwarding data format RFC3164 (TCP, UDP, TLS)

Field name	Sample data	Comments
@version	1	Version
port	57338	Source port number
host	10.11.60.246	Source host IP address
@timestamp	2024-01-15T05:21:39.423Z	Generated date and time
MSG	{'msg': 'xxx', 'host': 'xxx'}	Message content
MSG-Content-PRI	<13>	Digital from 0 to 191: [9] means ALERT [12] means WARNING [13] means EVENT [14] means LOG
MSG-Content-TIME-STAMP	1/15/2024 5:19	Generated date and time
MSG-Content-HOST-NAME	\"name\": \"server.logforward\"	Sender host name
MSG-Content-APP-NAME	LOGSTASH	Sender application name
MSG-Content-PID	[-]	Sender PID
TAG SEPERATOR	:	Separator between HEADER and MSG

RFC3164 Security Event sample (TCP)

```
{ "host": "10.11.60.233", "@timestamp": "2024-08-19T02:58:16.187Z", "port": 49060, "@version": "1", "message": "<13>Aug 19 02:57:29 {\\\"name\\\": \\\"server.logforward\\\"} LOGSTASH[-]: 2024-08-19T02:57:29.065706889Z {name=server.logforward} {\\\"status\\\": \\\"Y\\\", \\\"update_time\\\": \\\"2024-08-15T23:58:02.227150Z\\\", \\\"extra_fields\\\": \\\"{\\\"dataSrcIP\\\": \\\"172.30.4.25\\\"}\" \\\", \\\"component\\\": \\\"SI\\\", \\\"tags\\\": [\\\"input-postgres-event\\\", \\\"application\\\": null, \\\"event_type\\\": \\\"event\\\", \\\"sensor_id\\\": \\\"E3060500FFFBEBBFR6952246\\\", \\\"device_ip\\\": \\\"DESKTOP-OEM3AMD\\\", \\\"siem_time\\\": \\\"2024-08-15T23:57:43.000Z\\\", \\\"traffic\\\": null, \\\"asset\\\": null, \\\"id\\\": 340535064351232, \\\"insert_time\\\": \\\"2024-08-15T23:58:02.227147Z\\\", \\\"notification\\\": null, \\\"event_id\\\": \\\"900\\\", \\\"correlation_info\\\": null, \\\"remarks\\\": \\\"An account was successfully logged on Windows host 172.30.4.25\\\", \\\"name\\\": \\\"Windows Login\\\", \\\"@timestamp\\\": \\\"2024-08-16T00:00:00.497161261Z\\\", \\\"cia_level\\\": \\\"integrity\\\", \\\"logs\\\": [\\\"mDV5WJEBV2Z5wKWD8Dku\\\", \\\"event_change\\\": \\\"{\\\"user\\\": null, \\\"action\\\": null, \\\"policy\\\": null, \\\"status\\\": \\\"unprocessed\\\", \\\"approver\\\": null, \\\"deadline\\\": null, \\\"supervisor\\\": null, \\\"updateTime\\\": null, \\\"saveUpdownGrade\\\": null, \\\"updateEventType\\\": null}\" \\\", \\\"@version\\\": \\\"1\\\"}\" }
```

RFC3164 Security Event sample (UDP)

```
{ "@timestamp": "2024-08-19T02:41:55.144Z", "@version": "1", "message": "<13>1 2024-08-19T02:41:38.258+00:00 {\\\"name\\\": \\\"server.logforward\\\"} LOGSTASH - - - 2024-08-19T02:41:38.258638547Z {name=server.logforward} {\\\"input\\\": {\\\"type\\\": \\\"log\\\", \\\"@timestamp\\\": \\\"2024-08-19T02:41:37.936Z\\\", \\\"proto\\\": \\\"tcp\\\", \\\"dpt\\\": 443, \\\"log\\\": {\\\"file\\\": {\\\"path\\\": \\\"/opt/zeek/logs/current/conn.log\\\"}}, \\\"src\\\": \\\"10.11.0.106\\\", \\\"rt\\\": 1724035290991, \\\"spt\\\": 64478, \\\"cn1\\\": 0, \\\"ad_local__resp\\\": false, \\\"orig_pkts\\\": 3, \\\"tags\\\": [\\\"zeek\\\", \\\"beats_input_raw_event\\\", \\\"cn2\\\": 156, \\\"history\\\": \\\"S\\\", \\\"resp_pkts\\\": 0, \\\"app\\\": \\\"tcp_443\\\", \\\"FACTORY_ID\\\": \\\"10001\\\", \\\"agent\\\": {\\\"version\\\": \\\"8.10.4\\\", \\\"name\\\": \\\"sensor.logagent\\\", \\\"ephemeral_id\\\": \\\"cbc18556-0489-4c7a-a795-07cdcb228063\\\", \\\"id\\\": \\\"60eaf81a-15f9-4777-9d98-cce884cf67b1\\\", \\\"type\\\": \\\"filebeat\\\", \\\"vlan\\\": 1000, \\\"ad_local__orig\\\": true, \\\"GROUP_ID\\\": \\\"siemens\\\", \\\"cn3\\\": 0, \\\"smac\\\": \\\"90:8d:6e:8a:3b:85\\\", \\\"dataSrcIP\\\": \\\"10.11.60.191\\\", \\\"host\\\": \\\"sensor.logagent\\\", \\\"fields\\\": {\\\"collector_node_id\\\": \\\"sensor.logagent\\\", \\\"sensor_id\\\": 191, \\\"gl2_source_collector\\\": \\\"A6060600FFFBEBBFBYS7YY3\\\", \\\"ecs\\\": {\\\"version\\\": \\\"8.0.0\\\", \\\"cat\\\": \\\"conn\\\", \\\"LINE_ID\\\": \\\"1001\\\", \\\"duser\\\": \\\"S0\\\", \\\"offset\\\": 252879010, \\\"uid\\\": \\\"CgSbCB22fndFbwsRJ3\\\", \\\"dmac\\\": \\\"d4:2c:44:fb:fd:c8\\\", \\\"dst\\\": \\\"13.107.42.16\\\"} \\\"n\\\", \\\"host\\\": \\\"172.17.0.1\\\" }
```

RFC3164 Security Event sample (TLS)

```
{ "@timestamp": "2024-08-19T03:23:41.852Z", "@version": "1", "message": "<
13>Aug 19 03:23:26 { \"name\": \"server.logforward\" } LOGSTASH[-]:
2024-08-19T03:23:26.646479322Z {name=server.logforward}
{ \"status\": \"Y\", \"update_time\": \"2024-08-15T23:56:04.866349Z\", \"
extra_fields\": \"{\\\"shost\\\": \\\"DESKTOP-2INVVOB\\\", \\
\\\"sensor_ids\\\": \\\"E3060500FFFBEBBFR6952246\\\"}
\\\", \"component\": \"SI\", \"tags\": [\"input-postgres-
event\\\", \"application\": null, \"event_type\": \"warning\\\", \"sensor_id
\\\": \"E3060500FFFBEBBFR6952246\\\", \"device_ip\": \"DESKTOP-2INVVOB\\\", \"
siem_time\": \"2024-08-15T23:56:03.079189Z\\\", \"traffic\": null, \"asset
\\\": null, \"id\\\": 340534823995905, \"insert_time\": \"2024-08-15T23:56:04
.866347Z\\\", \"notification\": null, \"event_id\\\": \"956\\\", \"correlation_
info\\\": null, \"remarks\\\": \"Account login attempt in high frequency on
Windows host DESKTOP-2INVVOB\\\", \"name\\\": \"Frequently
Login\\\", \"@timestamp\\\": \"2024-08-16T00:00:00.477875937Z\\\", \"cia_leve
l\\\": \"integrity\\\", \"logs\":
[\"qTV4WJEBV2Z5wKWDCQki\\\", \"oTV4WJEBV2Z5wKWDCQka\\\", \"_jV3WJEBV2Z5wKW
D3QTh\\\", \"AjV3WJEBV2Z5wKWD3QXk\\\", \"JjR3WJEBV2Z5wKWDhPvm\\\", \"EjR3WJEB
V2Z5wKWDhPvI\\\", \"_TV3WJEBV2Z5wKWD3QTf\\\", \"xTV4WJEBV2Z5wKWDNA3f\\\", \"I
zR3WJEBV2Z5wKWDhPvg\\\", \"oTV3WJEBV2Z5wKWDSABx\\\"], \"event_change\\\": \"{
\\\"user\\\": null, \\\"action\\\": null, \\\"policy\\\": null, \\
\\\"status\\\": \\\"unprocessed\\\", \\\"approver\\\": null, \\
\\\"deadline\\\": null, \\\"supervisor\\\": null, \\\"updateTime\\\":
null, \\\"saveUpdownGrade\\\": null, \\\"updateEventType\\\": null}
\\\", \"@version\\\": \"1\\\"} \", \"host\": \"10.11.60.233\", \"port\": 59730 }
```

RFC5424 Raw Logs fields (TCP, UDP, TLS)

Table A-3 Raw log forwarding data format RFC5424 (TCP, UDP, TLS)

Field name	Sample data	Comments
Host	10.11.60.242	Source host IP address
MSG	{'msg': 'xxxx', 'host': 'xxx'}	Message content
MSG-Content-PRI	<13>	Digital from 0 to 191: [9] means ALERT [12] means WARNING [13] means EVENT [14] means LOG
MSG-Content-VERSION	1	RFC version
MSG-Content- TIMESTAMP	2024-01-12T01:23:01.104+00:00	Generated date and time
MSG-Content-HOSTNAME	\"name\": \"0.0.0.0\"	Sender host name
MSG-Content- APP-NAME	LOGSTASH	Sender process name
MSG-Content- PROCID	-	Sender PID
MSG-Content-MSGID	-	Message ID
MSG-Content- STRUCTURED-DATA	-	Structured data of the message

Field name	Sample data	Comments
Port	57488	Source port number
@timestamp	2024-01-15T05:39:13.447Z	Generated date and time
@version	1	RFC version

RFC5424 Raw Logs sample (TCP)

```
{
  "message": "<13>1 2024-08-19T02:56:29.583+00:00
  {
    \"name\": \"server.logforward\" } LOGSTASH - - -
    2024-08-19T02:56:29.583132915Z {name=server.logforward}
    {
      \"out\": 1875, \"flow_start\": 1720907292000, \"rt\": 1720907469000, \"offset\": 185026399, \"host\": \"sensor.logagent\", \"in\": 2737, \"agent\": {
        \"name\": \"sensor.logagent\", \"id\": \"3fe4290f-ae81-4fa4-ab12-117390c2bfe7\", \"version\": \"8.10.4\", \"ephemeral_id\": \"e07c345b-3067-4067-8ef4-7984e04ea7df\", \"type\": \"filebeat\", \"log\": {
          \"file\": { \"path\": \"/var/log/suricata/suricata_event.json\" }, \"in_iface\": \"eno1\", \"orig_pkts\": 10, \"dpt\": 9000, \"dst\": \"10.11.60.248\", \"app\": \"tls\", \"GROUP_ID\": \"siemens\", \"spt\": 58113, \"src\": \"10.11.58.12\", \"FACTORY_ID\": \"10001\", \"proto\": \"TCP\", \"dataSrcIP\": \"10.11.60.248\", \"input\": {
            \"type\": \"log\", \"tcp\": {
              \"psh\": true, \"rst\": true, \"tcp_flags_ts\": \"1e\", \"ack\": true, \"syn\": true, \"fin\": true, \"tcp_flags\": \"1f\", \"tcp_flags_tc\": \"1b\", \"state\": \"closed\", \"ecs\": {
                \"version\": \"8.0.0\", \"LINE_ID\": \"1001\", \"resp_pkts\": 10, \"cat\": \"suricata_event\", \"event_type\": \"flow\", \"@timestamp\": \"2024-07-13T21:51:09.427Z\", \"uid\": \"454673661957376\", \"tags\": [
                  \"suricata\", \"beats_input_raw_event\" ], \"fields\": {
                    \"collector_node_id\": \"sensor.logagent\", \"gl2_source_collector\": \"57060500FFFBEBBFGBCM8F3\", \"sensor_id\": 248 } }, \"host\": \"10.11.60.248\", \"port\": 52514, \"@timestamp\": \"2024-08-19T02:59:20.614Z\", \"@version\": \"1\" }
            }
          }
        }
      }
    }
  }
}
```

RFC5424 Raw Logs sample (UDP)

```
{ "@version": "1", "@timestamp": "2024-08-19T02:42:57.404Z", "host": "172.17.0.1", "message": "<13>1 2024-08-19T02:42:40.526+00:00\n{\\\"name\\\":\\\"server.logforward\\\"} LOGSTASH - - -\n2024-08-19T02:42:40.526922735Z {name=server.logforward} {\\\"input\\\":\n{\\\"type\\\":\\\"log\\\"},\\\"flow_start\\\":0,\\\"metadata\\\":{\\\"flowbits\\\":\n[\\\"ET.dcerpc.endians\\\"]},\\\"@timestamp\\\":\\\"2024-08-19T02:42:39.646Z\\\"\n,\\\"proto\\\":\\\"TCP\\\",\\\"dpt\\\":135,\\\"log\\\":{\\\"file\\\":\n{\\\"path\\\":\\\"/var/log/suricata/\nsuricata_event.json\\\"}},\\\"pkt_src\\\":\\\"wire/\npcap\\\",\\\"src\\\":\\\"10.11.60.139\\\",\\\"rt\\\":1724035359000,\\\"spt\\\":33082,\\\"tags\\\":\n[\\\"suricata\\\",\\\"beats_input_raw_event\\\"],\\\"event_type\\\":\\\"dcerpc\\\",\\\"FACTORY_ID\\\":\\\"10001\\\",\\\"in_iface\\\":\\\"eno1\\\",\\\"dcerpc\\\":\n{\\\"rpc_version\\\":\\\"5.0\\\",\\\"response\\\":\\\"UNREPLIED\\\",\\\"call_id\\\":1,\\\"request\\\":\\\"ALTER_CONTEXT\\\"},\\\"agent\\\":\n{\\\"version\\\":\\\"8.10.4\\\",\\\"name\\\":\\\"sensor.logagent\\\",\\\"ephemeral_id\\\":\\\"211ec92b-1191-450c-b49a-eb9b72931de6\\\",\\\"id\\\":\\\"2f5b4bca-0650-4b9a-a0b3-718565d641da\\\",\\\"type\\\":\\\"filebeat\\\"},\\\"GROUP_ID\\\":\\\"siemens\\\",\\\"dataSrcIP\\\":\\\"10.11.60.139\\\",\\\"host\\\":\\\"sensor.logagent\\\",\\\"fields\\\":\n{\\\"collector_node_id\\\":\\\"sensor.logagent\\\",\\\"sensor_id\\\":139,\\\"gl2_source_collector\\\":\\\"E3060500FFFBEBBFR6952248\\\"},\\\"ecs\\\":\n{\\\"version\\\":\\\"8.0.0\\\"},\\\"cat\\\":\\\"suricata_event\\\",\\\"LINE_ID\\\":\\\"1001\\\",\\\"offset\\\":101300936,\\\"uid\\\":1704192476598021,\\\"dst\\\":\\\"172.30.4.31\\\"}\\\"}\\n\"}
```

RFC5424 Raw Logs sample (TLS)

```
{ "@timestamp": "2024-08-19T05:03:37.158Z", "@version": "1", "message": "<13>1 2024-08-19T05:03:20.988+00:00 { \"name\": \"server.logforward\" } LOGSTASH - - - 2024-08-19T05:03:20.988174744Z {name=server.logforward} { \"src\": \"172.30.2.138\", \"dcerpc\": { \"response\": \"BINDACK\", \"call_id\": 1, \"rpc_version\": \"5.0\", \"request\": \"BIND\", \"interfaces\": [ { \"uuid\": \"99fcfec4-5260-101b-bbcb-00aa0021347a\", \"version\": \"0.0\", \"ack_result\": 0 } ] }, \"fields\": { \"gl2_source_collector\": \"E3060500FFFBEBBFR6952246\", \"sensor_id\": 138, \"collector_node_id\": \"sensor.logagent\", \"tags\": [ \"suricata\", \"beats_input_raw_event\", \"cat\": \"suricata_event\", \"log\": { \"file\": { \"path\": \"/var/log/suricata/suricata_event.json\" } }, \"dst\": \"172.30.4.25\", \"event_type\": \"dcerpc\", \"GROUP_ID\": \"siemens\", \"input\": { \"type\": \"log\", \"uid\": 1970032584896929, \"LINE_ID\": \"1001\", \"ecs\": { \"version\": \"8.0.0\", \"spt\": 49722, \"rt\": 1723766400000, \"FACTORY_ID\": \"10001\", \"pkt_src\": \"wire/pcap\", \"proto\": \"TCP\", \"flow_start\": 0, \"dataSrcIP\": \"172.30.2.138\", \"host\": \"sensor.logagent\", \"dpt\": 135, \"agent\": { \"name\": \"sensor.logagent\", \"type\": \"filebeat\", \"id\": \"51b469df-7b01-4485-946f-b0166f0a1576\", \"version\": \"8.10.4\", \"ephemeral_id\": \"c2551dff-6a05-4ea7-bf57-56fde672239b\" } }, \"@timestamp\": \"2024-08-16T00:00:00.408Z\", \"interface\": \"eno1\", \"offset\": 69291177 }\", \"host\": \"10.11.60.233\", \"port\": 58650 }
```

RFC5424 Security Event fields (TCP, UDP, TLS)

Table A-4 Security event forwarding data format RFC5424 (TCP, UDP, TLS)

Field name	Sample data	Comments
Host	10.11.60.242	Source host IP address
MSG	{'msg': 'xxx', 'host': 'xxx'}	Message content
MSG-Content-PRI	<13>	Digital from 0 to 191: [9] means ALERT [12] means WARNING [13] means EVENT [14] means LOG
MSG-Content-VERSION	1	RFC version
MSG-Content-TIMESTAMP	2024-01-12T01:23:01.104+00:00	Generated date and time
MSG-Content-HOSTNAME	{\"name\": \"0.0.0.0\"}	Sender host name
MSG-Content-APP-NAME	LOGSTASH	Sender process name
MSG-Content -PROCID	-	Sender PID
MSG-Content-MSGID	-	Message ID

Field name	Sample data	Comments
MSG-Content-STRUCTURED-DATA	-	Structured data of the message
Port	57400	Source Port number
@timestamp	2024-01-15T05:39:13.447Z	Generated date and time
@version	1	RFC Version

RFC5424 Security Event sample (TCP)

```
{
  "@timestamp": "2024-08-19T03:00:53.740Z",
  "host": "10.11.60.248",
  "port": 41300,
  "message": "<13>1 2024-08-19T02:57:59.330+00:00\n{\\\"name\\\":\\\"server.logforward\\\"} LOGSTASH - - -\n2024-08-19T02:57:59.330049540Z {name=server.logforward}\n{\\\"resp_pkts\\\":5,\\\"out\\\":1152,\\\"in_iface\\\":\\\"eno1\\\",\\\"offset\\\":19889\n8116,\\\"host\\\":\\\"sensor.logagent\\\",\\\"in\\\":420,\\\"uid\\\":178751206333482\n0,\\\"dst\\\":\\\"10.11.60.248\\\",\\\"log\\\":{\\\"file\\\":{\\\"path\\\":\\\"/var/log/suricata/suricata_event.json\\\"}},\\\"fields\\\":\n{\\\"collector_node_id\\\":\\\"sensor.logagent\\\",\\\"gl2_source_collector\\\":\n\\\"57060500FFFBEBBFBGBCM8F3\\\",\\\"sensor_id\\\":248},\\\"dpt\\\":9000,\\\"app\\\":\n\\\"http\\\",\\\"input\\\":\n{\\\"type\\\":\\\"log\\\"},\\\"flow_start\\\":1723766161000,\\\"cat\\\":\\\"suricata_e\nvent\\\",\\\"src\\\":\\\"10.11.38.200\\\",\\\"tags\\\":\n[\\\"suricata\\\",\\\"beats_input_raw_event\\\"],\\\"proto\\\":\\\"TCP\\\",\\\"ecs\\\":\n{\\\"version\\\":\\\"8.0.0\\\"},\\\"LINE_ID\\\":\\\"1001\\\",\\\"GROUP_ID\\\":\\\"siemens\\n\n\\\",\\\"rt\\\":1723766400000,\\\"tcp\\\":\n{\\\"tcp_flags_tc\\\":\\\"1b\\\",\\\"fin\\\":true,\\\"syn\\\":true,\\\"psh\\\":true,\\\"tc\np_flags\\\":\\\"1b\\\",\\\"ack\\\":true,\\\"tcp_flags_ts\\\":\\\"1b\\\",\\\"state\\\":\\\"cl\nosed\\\",\\\"agent\\\":{\\\"id\\\":\\\"b4a43fad-\nac6f-44ce-96b2-3f10380b69bb\\\",\\\"ephemeral_id\\\":\\\"0997de53-7b17-4884-\n8b86-59e1e417cdba\\\",\\\"type\\\":\\\"filebeat\\\",\\\"name\\\":\\\"sensor.logagent\n\\\",\\\"version\\\":\\\"8.10.4\\\"},\\\"orig_pkts\\\":5,\\\"@timestamp\\\":\\\"2024-08-\n16T00:00:00.892Z\\\",\\\"dataSrcIP\\\":\\\"10.11.60.248\\\",\\\"event_type\\\":\\\"f\nlow\\\",\\\"spt\\\":62923,\\\"FACTORY_ID\\\":\\\"10001\\\"}}\", \"@version\": \"1\"}
```

RFC5424 Security Event sample (UDP)

```
{ "host": "172.17.0.1", "message": "<13>1 2024-08-19T02:54:16.616+00:00\n{\\\"name\\\":\\\"server.logforward\\\"} LOGSTASH - - -\n2024-08-19T02:54:16.616025842Z {name=server.logforward}\n{\\\"@timestamp\\\":\\\"2024-08-19T02:54:15.887Z\\\",\\\"log\\\":\n{\\\",\\\"rt\\\":1724036055000,\\\"tags\\\":\n[\\\"windows\\\",\\\"subjectHostName\\\":\\\"DESKTOP-7Q7CU2F\\\",\\\"eventId\\\":51\n56,\\\"FACTORY_ID\\\":\\\"10001\\\",\\\"shost\\\":\\\"DESKTOP-7Q7CU2F\\\",\\\"agent\\\":\n{\\\"version\\\":\\\"8.10.4\\\",\\\"name\\\":\\\"DESKTOP-7Q7CU2F\\\",\\\"ephemeral_id\\\":\n\\\"1c705708-04e6-404d-a9b1-3031d4a0a716\\\",\\\"id\\\":\\\"f6320901-2161-440c-a428-7daa3aa31a0f\\\",\\\"type\\\":\\\"winlogbeat\\\",\\\"type\\\":\\\"wineventlog\\\",\\\"actTaskName\\\":\\\"Filtering Platform Connection\\\",\\\"event\\\":\n{\\\"provider\\\":\\\"Microsoft-Windows-Security-Auditing\\\",\\\"original\\\":\\\"Windows 筛选平台已允许连接。\\n\\n\\n 应用程序信息:\\n\\n\\t 进程 ID:\\t\\t\\t3256\\n\\t 应用程序名称:\\t\\t\\t\\device\\t\\t\\t\\harddiskvolume2\\t\\t\\t\\program files\\t\\t\\t\\siemens\\t\\t\\t\\logagent\\t\\t\\t\\updateagent.exe\\n\\n\\n 网络信息:\\n\\n\\t 方向:\\t\\t\\t 出站\\n\\t 源地址:\\t\\t\\t172.30.1.137\\n\\n\\t 源端口:\\t\\t\\t64350\\n\\t 目标地址:\\t\\t172.30.1.139\\n\\n\\t 目标端口:\\t\\t\\t9000\\n\\n\\t 协议:\\t\\t\\t6\\n\\n\\n 筛选器信息:\\n\\n\\t 筛选器运行时 ID:\\t0\\n\\n\\t 层名称:\\t\\t\\t 连接\\n\\n\\t 层运行时 ID:\\t48\\\",\\\"outcome\\\":\\\"success\\\",\\\"code\\\":\\\"5156\\\",\\\"created\\\":\\\"2024-08-19T02:54:16.930Z\\\",\\\"kind\\\":\\\"event\\\",\\\"sourceName\\\":\\\"Microsoft-Windows-Security-Auditing\\\",\\\"computer_name\\\":\\\"DESKTOP-7Q7CU2F\\\",\\\"GROUP_ID\\\":\\\"siemens\\\",\\\"provider_guid\\\":\\\"{54849625-5478-4994-a5ba-3e3b0328c30d}\\\",\\\"dataSrcIP\\\":\\\"172.30.1.137\\\",\\\"category\\\":\\\"winEvent/Security/Microsoft-Windows-Security-Auditing\\\",\\\"version\\\":1,\\\"keywords\\\":[\\\"审核成功\\\"],\\\"logfile\\\":\\\"Security\\\",\\\"level\\\":\\\"信息\\\",\\\"fields\\\":{\\\"collector_node_id\\\":\\\"DESKTOP-7Q7CU2F\\\",\\\"gl2_source_collector\\\":\\\"c9cda44030d63701d301d42d9560d66c\\\",\\\"ecs\\\":{\\\"version\\\":\\\"8.0.0\\\",\\\"cat\\\":\\\"winEvent\\\",\\\"msg\\\":\\\"Windows 筛选平台已允许连接。\\n\\n\\n 应用程序信息:\\n\\n\\t 进程 ID:\\t\\t\\t3256\\n\\n\\t 应用程序名称:\\t\\t\\t\\device\\t\\t\\t\\harddiskvolume2\\t\\t\\t\\program files\\t\\t\\t\\siemens\\t\\t\\t\\logagent\\t\\t\\t\\updateagent.exe\\n\\n\\n 网络信息:\\n\\n\\t 方向:\\t\\t\\t 出站\\n\\n\\t 源地址:\\t\\t\\t172.30.1.137\\n\\n\\t 源端口:\\t\\t\\t64350\\n\\n\\t 目标地址:\\t\\t172.30.1.139\\n\\n\\t 目标端口:\\t\\t\\t9000\\n\\n\\t 协议:\\t\\t\\t6\\n\\n\\n 筛选器信息:\\n\\n\\t 筛选器运行时 ID:\\t0\\n\\n\\t 层名称:\\t\\t\\t 连接\\n\\n\\t 层运行时 ID:\\t48\\\",\\\"LINE_ID\\\":\\\"1001\\\",\\\"opcode\\\":\\\"信息\\\"}\\n\\\",\\\"@timestamp\\\":\\\"2024-08-19T02:54:33.481Z\\\",\\\"@version\\\":\\\"1\\\"}
```

RFC5424 Security Event sample (TLS)

```
{
  "message": "<13>1 2024-08-19T05:05:23.085+00:00",
  "name": "server.logforward",
  "LOGSTASH": "2024-08-19T05:05:23.085379058Z {name=server.logforward}",
  "status": "Y",
  "update_time": "2024-08-15T23:55:04.887079Z",
  "extra_fields": {
    "shost": "windows7_21",
    "sensor_ids": "E3060500FFFBEBBFR6952246",
    "component": "SI",
    "tags": [
      "input-postgres-event",
      "application": null,
      "event_type": "warning",
      "sensor_id": "E3060500FFFBEBBFR6952246",
      "device_ip": "windows7_21",
      "siem_time": "2024-08-15T23:55:03.221783Z",
      "traffic": null,
      "asset": null,
      "id": "340534701130240",
      "insert_time": "2024-08-15T23:55:04.887077Z",
      "notification": null,
      "event_id": "956",
      "correlation_info": null,
      "remarks": "Account login attempt in high frequency on Windows host windows7_21",
      "name": "Frequently Login",
      "@timestamp": "2024-08-16T00:00:00.457894514Z",
      "cia_level": "integrity",
      "logs": [
        "XzR3WJEBV2Z5wKWDNfTH",
        "YDR3WJEBV2Z5wKWDNfTH",
        "ZDR3WJEBV2Z5wKWDNfTH",
        "rzR2WJEBV2Z5wKWDreUO",
        "rTR2WJEBV2Z5wKWDreUM",
        "XDR2WJEBV2Z5wKWDgeEZ",
        "RjR2WJEBV2Z5wKWD2ut2",
        "WzR3WJEBV2Z5wKWDNfTH",
        "YjR3WJEBV2Z5wKWDNfTH",
        "YjR2WJEBV2Z5wKWDgeEi"
      ],
      "event_change": {
        "user": null,
        "action": null,
        "policy": null,
        "status": "unprocessed",
        "approver": null,
        "deadline": null,
        "supervisor": null,
        "updateTime": null,
        "saveUpdownGrade": null,
        "updateEventType": null
      },
      "@version": "1",
      "@timestamp": "2024-08-19T05:05:40.829Z",
      "@version": "1",
      "host": "10.11.60.233",
      "port": 45366
    ]
  }
}
```

Index

G

Glossary, 13

H

Haupteintrag, 98

S

Service & Support, 13

SIMATIC NET glossary, 13

T

Training, 13

