SIEMENS

SIMATIC NET

Industrial Ethernet Security SINEC Security Inspector

Operating Instructions

03/2025
C79000-G8976-C701-02

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.

Siemens Aktiengesellschaft
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

C79000-G8976-C701-02
Ⓟ 03/2025 Subject to change

Table of contents

Preface

1

Validity

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

- V1.19

The following expansions and licenses are available for the specified version:

Product name	Product ID
SINEC Security Inspector - Basic	SINECSI
SINEC Security Inspector - Nessus Add on	SINECINS

Required experience

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

- SINEC Security Inspector
  Read this manual for more information
- Network Security
  Understanding the impact of security software on network operations

Purpose of this documentation

This manual supports you when installing, configuring and operating SINEC Security Inspector. It contains information on security scanning with SINEC Security Inspector.

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/29525/man)

On this page, you will also find additional information such as product notices, FAQs, software updates, etc.

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

- Device

  This term refers to all devices supported by SINEC Security Inspector in the network. If the devices differ in the particular context, the product name or type will be used.

- Firewall
  Security module with firewall

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-Inspector_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 (https://www.siemens.com/industrialsecurity).

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

To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under
https://new.siemens.com/cert (https://www.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 can also 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.

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)

Overview

2

Overview

SINEC Security Inspector is a security framework which can be used to automate security testing and to get reproducable security test results. SINEC Security Inspector can also be used to support penetration testing and manual testing for security-critical products and environments.

Currently, the SINEC Security Inspector framework comes with two different kinds of built-in network interfaces:

- Management Interface (MGMT-IF, eth0)
  There is only one management interface installed on a SINEC Security Inspector. This interface allows remote management and operation of SINEC Security Inspector. For further information about network setup, please see section Network setup (Page 14).
- Test Interfaces (TEST-IF, at least one is specified)
  These interfaces are meant to be connected either to the devices under test (targets) or to the networks these devices are connected to. For further information about test interfaces, see section Network (Page 53).

Functions

- Automated Security Testing: Automatically scans and tests your network components and systems for vulnerabilities.
  Test execution is based on built-in test cases or on user-defined test cases with user-defined configurations. These cases interfere with network behavior to varying degrees and can affect the target network in undesirable ways.
- Quick Vulnerability Detection: Identifies security vulnerabilities within minutes, enabling prompt risk assessment and threat mitigation.
- Extensive Testing Capabilities: Utilizes a variety of technologies and methods to conduct a wide range of security tests, offering thorough vulnerability detection.
- Comprehensive Coverage: Regularly checks the security status of your entire OT/IT network, ensuring continuous protection.
- Structured Reporting: Generates clear, detailed reports that summarize test results and display the security status of all devices, helping you understand and address vulnerabilities effectively.
- Compliance and Acceptance Testing: Facilitates Factory Acceptance Tests (FAT), Site Acceptance Tests (SAT), and compliance checks to ensure your systems meet security standards
- Inventory Management: Manages the inventory of your production systems and visualizes lifecycle information for better asset management.

REST Interface

SINEC Security Inspector provides a REST interface for automation and remote control.

Its documentation is available in the "Help" section of SINEC Security Inspector user interface, including a short description and links to the AppConfigs.

Additional information

You can find the latest information and more on the Internet at the following address:

Link: (https://www.siemens.com/global/en/products/automation/industrial-communication/sinec-network-software.html)

Setup

3

To monitor devices, SINEC Security Inspector uses part of the data transfer rate available in the network. This must be taken into account when planning networks in which SINEC Security Inspector will be used.

NOTICE
Device failure and network interruption possible Network interruptions and device failures can occur when executing test cases. Avoid performing tests in productive operation; instead, perform the test cases during maintenance periods.

3.1 System requirements

Minimum hardware requirements

Note

Ensure all free disk space is on a single hard disk.

CPU	Intel i5 or equivalent (i7 or Xeon recommended)
Network Interface Cards	2 (one for management and at least one for testing)
RAM	12 GB (16GB recommended if Nessus is used)
Disc space	500GB HDD, (2TB recommended)
USB bootable device	>2GB

SINEC Security Inspector works with all typical Debian Linux-compatible network cards.

Recommended 4-port Network Interface Card:

- Intel Ethernet Server Adapter I350-T4 (ID for Shopping Card in OneSRM: Article No. 0003629117-00000001).

Note

SINEC Security Inspector requires at least 2 network interfaces: one for remote management and one for scanning/testing.

Recommended hardware

Device	Article No.
SIMATIC IPC 647E	6AG4112-3KX07-6XX1
SIMATIC IPC 627E	6AG4131-3HD30-8AA2
Shuttle DH270XA Barebone	-

Supported virtual environments for SINEC Security Inspector

VM	Version
VMware Workstation	Version 12 or higher
VMware ESXi Server	Version 5.5 or higher

The virtual system must fulfill the following requirements in a virtual environment:

CPU	2 cores in the virtual machine
Network Interface Cards	2 (one for management and at least one for testing)
RAM	12 GiB for the VM (that means 16 GB for the Host)
Disc space	300 GiB free disk space on the host system

Note

Other virtualization technologies

SINEC Security Inspector may also run on other virtualization technologies, like KVM, VirtualBox or Microsoft Hyper-V. Note that only minor support can be given regarding those technologies and that they were not included in the testing process.

3.2 Network setup and configuration

3.2.1 Network setup

Network setup

In order to keep SINEC Security Inspector up-to-date, keep your network connected to the internet to receive updates from the SINEC Security Inspector update server.

For more information about the setup, refer to section How to setup a hardware device (Page 21) or How to setup a virtual machine (Page 26).

For more information on keeping your SINEC Security Inspector up-to-date, refer to section Remote Support (Page 63).

It is recommended to use SINEC Security Inspector behind a firewall in a dedicated network. For more information, refer to section Remote Support (Page 63).

See also

Keeping SINEC Security Inspector up-to-date (Page 40)

3.2.2 Network configuration and management

The section describes how to use the network interfaces and enable ports to connect the SINEC Security Inspector appliance to the update server.

Recommended security components:

- External firewalls with Intrusion Detection System to protect the company network from external attacks.
- DMZ firewalls in the backbone level protect the plant network.
- Security modules protect each individual automation cell.

For more information, refer to section Security recommendations (Page 93).

Network interfaces of SINEC Security Inspector

- Management Interface (MGMT-IF)
  There is only one management interface installed on a SINEC Security Inspector. With the management interface SINEC Security Inspector can be administered remotely.
- Test Interfaces (TEST-IF)
- You can configure up to to five test-interfaces with which SINEC Security Inspector can scan targets or target networks.

Connecting SINEC Security Inspector to your network

For information about the current update server address, IP address, and ports, refer to the chapter Keeping SINEC Security Inspector up-to-date (Page 40).

Preparing your firewall and your installation

SINEC Security Inspector needs a management connection for the remote maintenance and software updates. The following figure shows the typical network setup of SINEC Security Inspector.

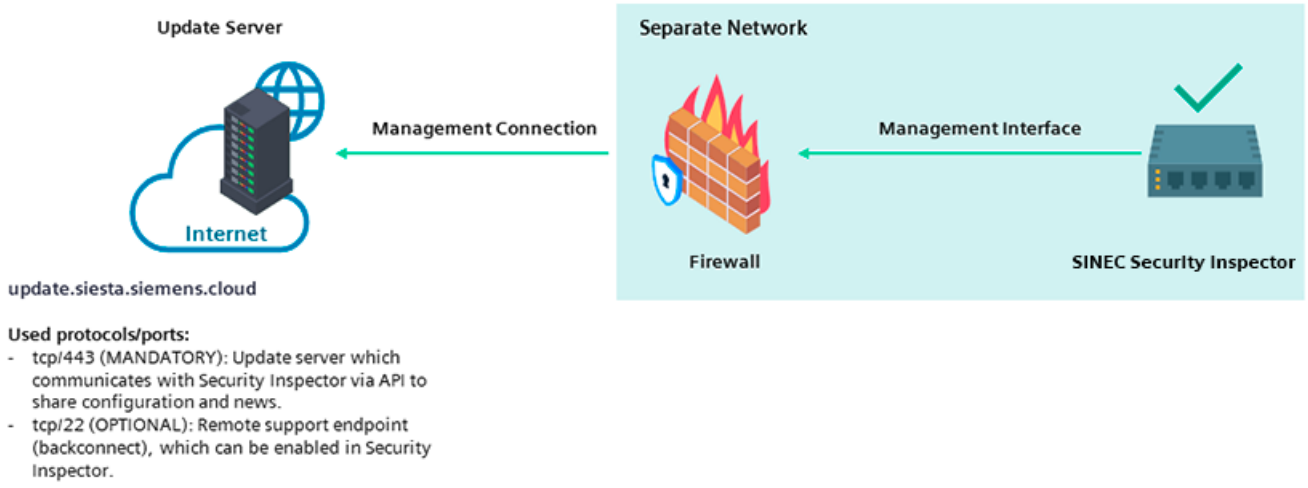


Figure 3-1 Typical network setup

Ensure the following ports are enabled in your firewall:

- TCP/22: Optional SSH command-line access
- TCP/443: SINEC Security Inspector web interface
- TCP/8443: Manual mode for security tools (e.g., Nessus)

If SINEC Security Inspector cannot connect to the update server, it may be due to firewall restrictions.

The SINEC Security Inspector update server is reachable via the Internet, refer to section Provisioning SINEC Security Inspector (Page 58).

Note: SINEC Security Inspector should only be operated within a special separate network, which is managed by the user.

Preferred network topologies for deployment

There are several ways to connect the network interfaces (managemen interface and the test interfaces) of SINEC Security Inspector with your network.

The following options are recommended possibilities to establish a secure connection using SINEC Security Inspector.

- Option A: Both interfaces (Mgmt-IF and Test-IF) of SINEC Security Inspector are within the separate network.

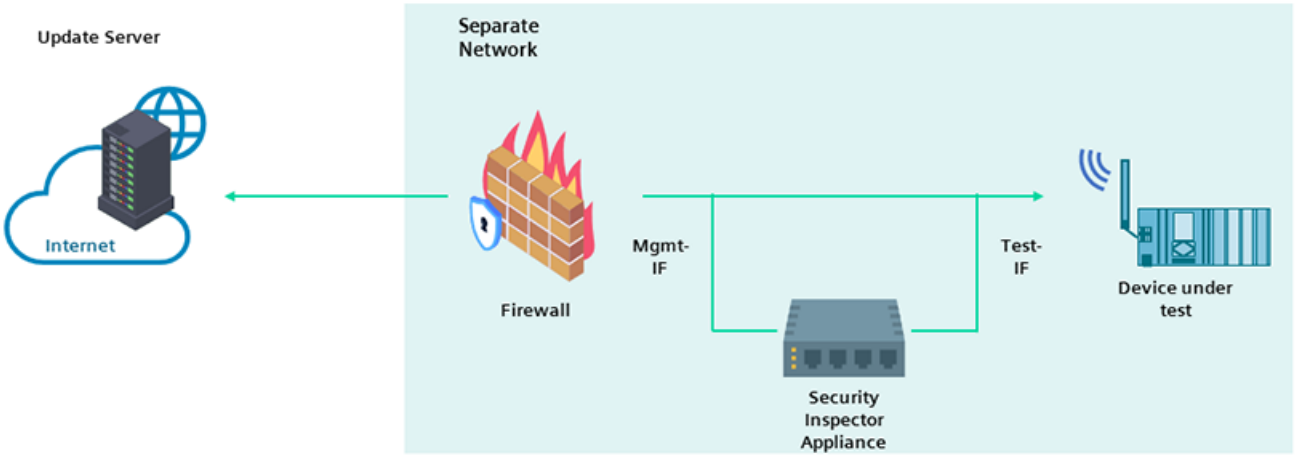


Figure 3-2 Option A

- Option B: Mgmt- interface is in separate network, and Test-nterface is in another network, with a very small test network only containing devices under test.

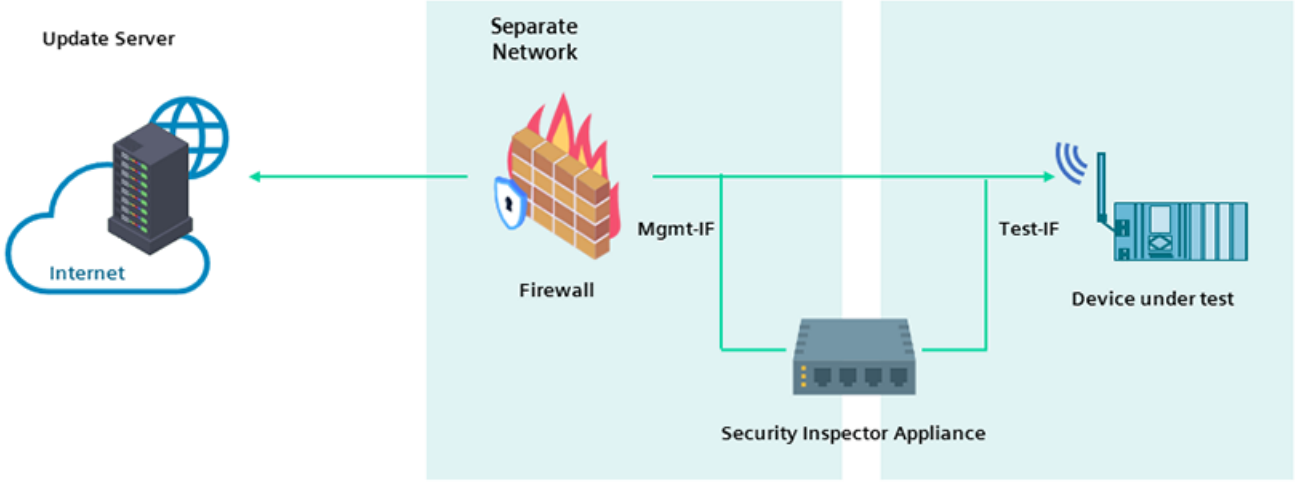


Figure 3-3 Option B

- Option C: Mgmt interface is directly connected to the Internet and Test interface is in a separate network only containing device under tests.

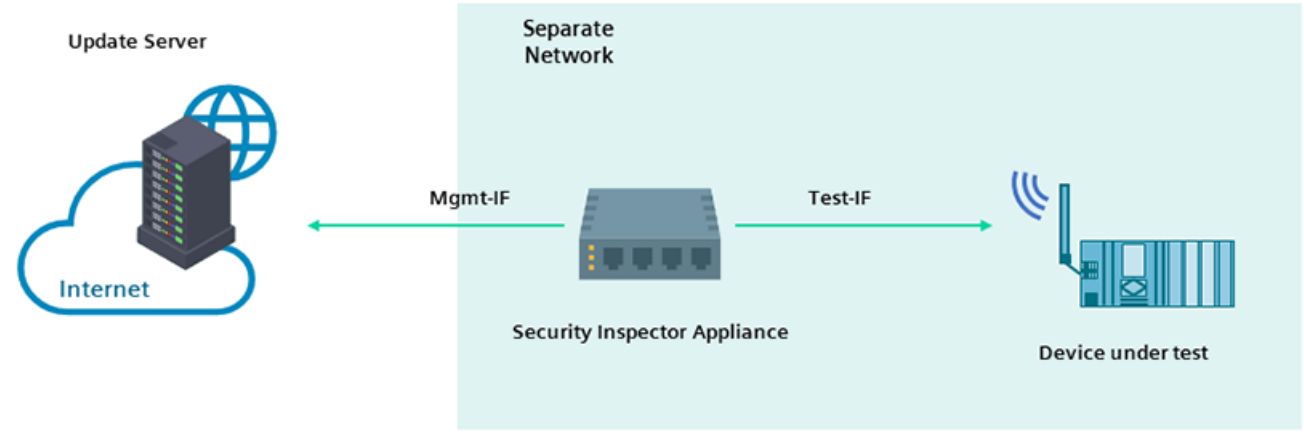


Figure 3-4 Option C

Insecure deployment

Note

Insecure deployment

The user should not use this (or a similar) setup for your network, as SINEC Security Inspector would provide a redundant connection to the Internet that circumvents the already installed firewall.

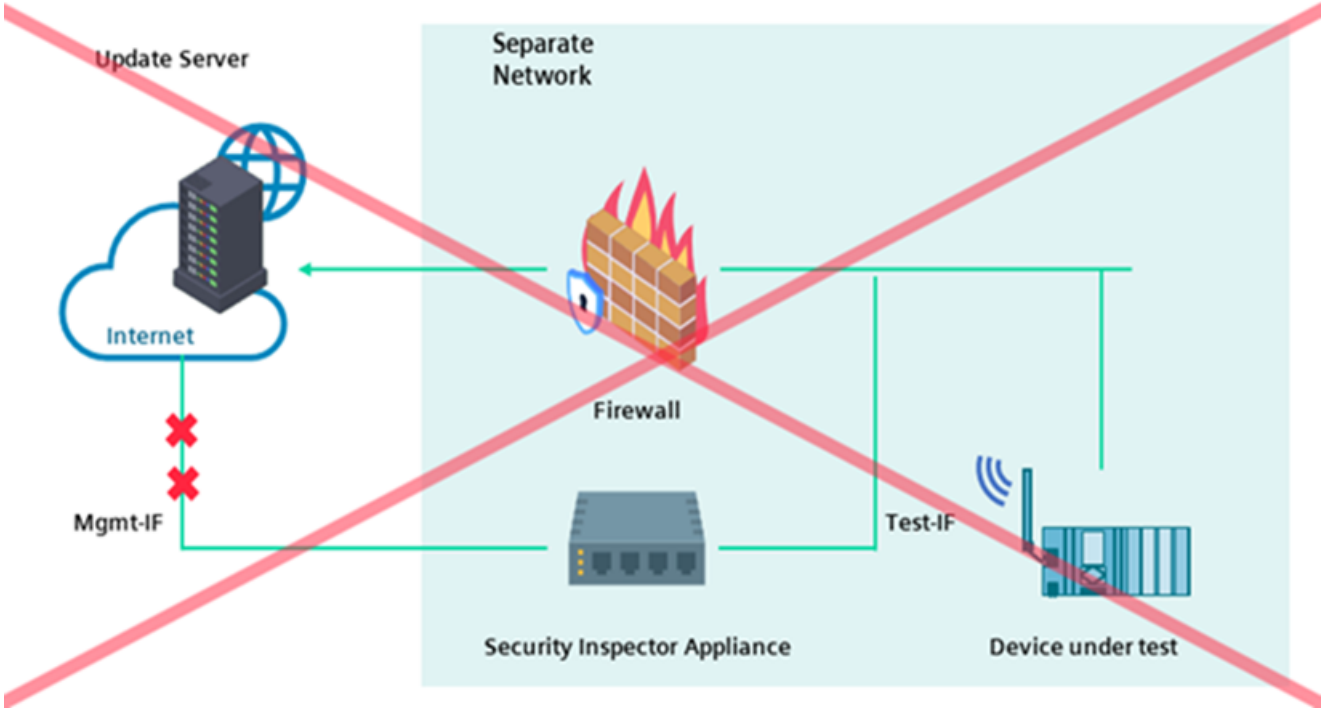


Figure 3-5 Insecure deployment

Target network management

In certain use cases, for example for scanning solution projects or infrastructures, multiple networks have to be scanned. Those networks are often separated through a firewall which restricts access for SINEC Security Inspector and causes problems for certain types of tests.

For use cases where the networks are separated through firewall:

- SINEC Security Inspector supports accessing multiple target networks.

It is recommended to use a hardware-based version of SINEC Security Inspector for this task. However, similar setups can be accomplished by configuring SINEC Security Inspector as a Virtual Machine in VMware Workstation.

For the configuration of multiple target networks:

- SINEC Security Inspector supports the concept of network profiles.

The following figure shows an overview of profiles.

For most use cases, the test interfaces T1 to T5 of SINEC Security Inspector hardware are sufficient. If additional network need to be tested by one SINEC Security Inspector box, either networks must be reconnected, or the following VLAN needs to be set up.

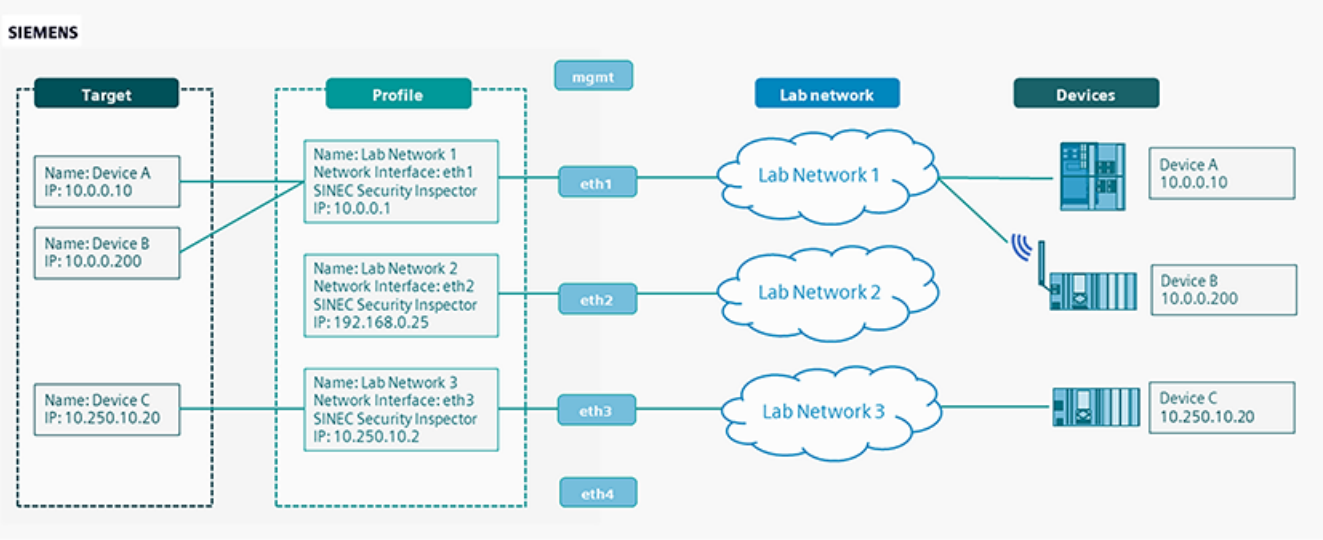


Figure 3-6 Mapping of targets to network profiles

In this setup, a managed switch is connected to SINEC Security Inspector hardware via a single Ethernet link. The switch is connected to all target networks, with each port assigned a unique VLAN ID.

Using IEEE 802.1Q, SINEC Security Inspector and the switch coordinates, it is easy to identify which packet is assigned to each switch port and the corresponding target network. Inside SINEC Security Inspector, it is necessary to assign the corresponding VLAN IDs in the network profiles.

See also

Link (https://en.wikipedia.org/wiki/Network_bridge)

Link: (https://en.wikipedia.org/wiki/Network_address_translation)

Link: (https://kb.vmware.com/s/article/1018697)

Link (https://docs.vmware.com/en/VMware-Workstation-Pro/12.0/com.vmware.ws.using.doc/GUID-0EE752F8-C159-487A-9159-FE1F646EE4CA.html)

3.2.3 Configuring the Management-Interface

Management network configuration

To configure the management interface of the SINEC Security Inspector to the correct subnet, follow these steps:

1. Connect a monitor and keyboard to the SINEC Security Inspector.
2. Press <CTRL>+<ALT>+<F2> simultaneously to access the configuration dialog via the command line.
   In the "Current status" section, you can check the connection status to the update server.
   In the "Current network config" section, you can check the current network settings.
3. Press <E> to start the wizard and follow the prompts to configure the management interface to the correct subnet.

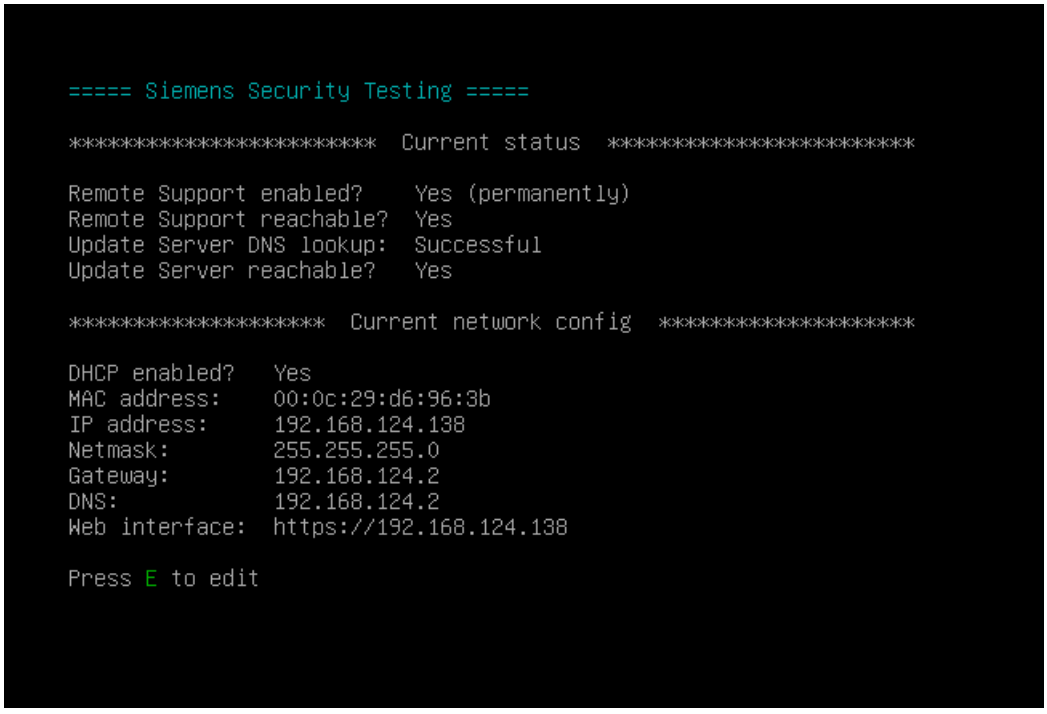


Figure 3-7 Example settings for SINEC Security Inspector

3.3 How to setup a hardware device

To install SINEC Security Inspector on a hardware device, you need to create a bootable USB drive or DVD.

Creating a bootable USB drive

Requirements

- DiskPart (Windows utility) or an external automated tool (e.g., balenaEtcher)
- USB drive (2 GB minimum)
- SINEC Security Inspector Installer ISO file.You can download the installer ISO file from the following location:
  Link: (https://support.sw.siemens.com/en-US/product/206158208)

Creating a bootable USB device

1. Use DiskPart or an automated tool of your choice to burn the ISO to the USB drive.

Creating a bootable DVD

1. Use DVD burning software to burn the ISO to a DVD.

Installation

Use the bootable USB drive or DVD to install SINEC Security Inspector on your hardware device.

3.3.1 How to setup network components for hardware

This section describes how to setup a network component on a hardware environment where SINEC Security Inspector is installed.

Required network interfaces

To install SINEC Security Inspector on a hardware environment, at least 2 physical network interfaces are required:

- **Mgmt-IF**
  The management interface with which SINEC Security Inspector can be administered remotely.
  The Mgmt-IF cannot be used for scanning.
- **Test-IF**
  Up to five test interfaces (T1 to T5) for targets and networks.

Setting up a test interface for scanning

To scan a target or a target network/subnet, a test interface must be configured on the SINEC Security Inspector appliance. Follow the steps in the below sub section to set up a test interface for scanning single target devices or entire target networks.

The following graphic is a schematic representation of how the installed network interface looks with a network profile and how an example target would look.

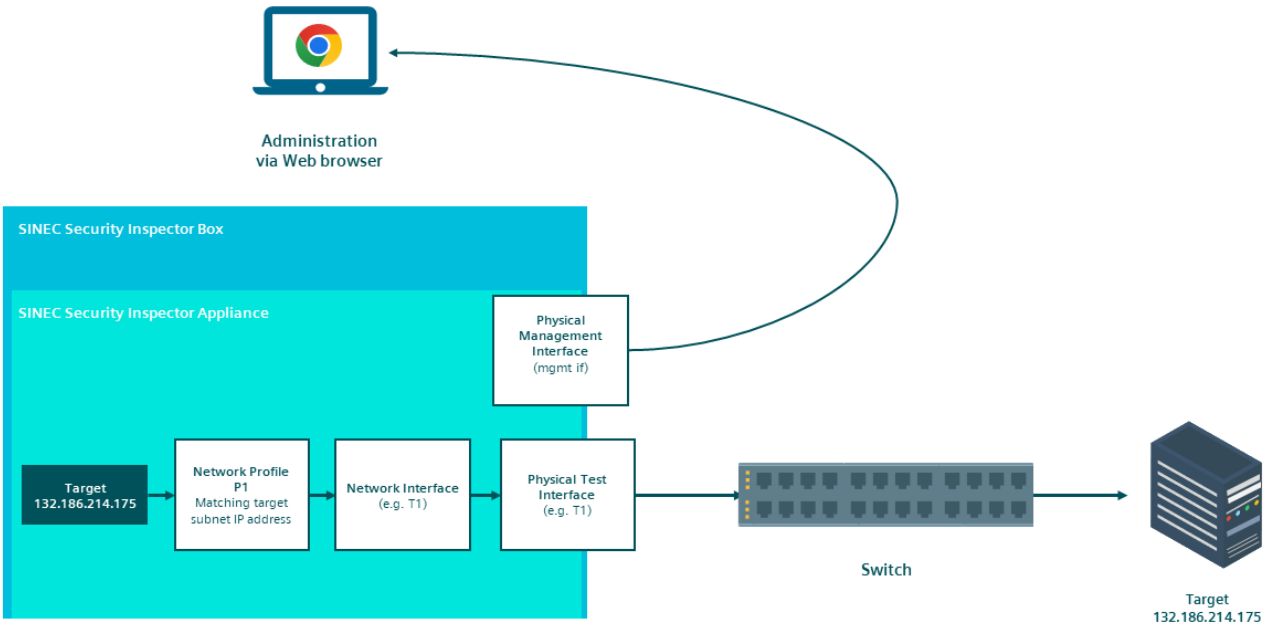


Figure 3-8 Example: Scanning a single target with one Test-IF

Note: The address in the Network Profile may be not in same subnet of target in case when gateway is used and its routing is correctly configured.

Step 1: Install a new network interface

1. Log in to the web interface of SINEC Security Inspector.
2. On the top-right of the screen, click the "Configuration" icon.
3. Navigate to "Configuration" > "Network" option.
4. Select "New Network Interface".
5. On the "New Network Interface" screen, enter the following details:
   - Name
     Assign a memorable name (for example "T1").
   - Device
     Select the available network interface from the drop-down menu.
   - VLAN identifier (optional)
6. Click "Save and Exit".

Under "Network Interfaces", the newly created network interface is visible.

Step 2: Create a new network profile for new network interface

Once you have successfully registered a physical network interface from your hardware as a network interface in SINEC Security Inspector, you need to create a network profile for it.

A network profile helps to reach a target to scan because the network interface doesn't have an IP address yet. Hence, the next step is to create a network profile for your newly created network interface.

To create a new network profile:

1. Log in to the web interface of SINEC Security Inspector.
2. On the top-right of the screen, click the "Configuration" icon.
3. Navigate to "Configuration" > "Network".
4. On the screen, select "New Network Profile".
5. On the "New Network Profile" screen, enter the following details.
   - Name
     Assign a short, memorable name (in our example "P1").
   - Network interface
     Use the drop-down menu to select the Network Interface that you have just set up (in our example: the newly created Network Interface "T1").
   - IPv4 address
     Assign an IP address that matches the target or target network to be scanned.
   - IPv4 netmask
     Enter a netmask here that matches the target network (e.g. 255.255.255.0 or 24).
   - IPv4 default gateway
     If necessary, enter the gateway IP address for accessing the target network.
   - DNS server (optional)
     If available, enter the IP address of your DNS server.
6. After all the details have been entered, click "Save and Exit".

Now you can see the newly created network profile which you have assigned to the newly created network interface.

Note

SINEC Security Inspector does not support the use of colons (":") in network profile host entries.

Now it is possible to reach a target suiting to the IP addresses you have entered while creating the new network profile.

It is also possible to specify IPv6 settings, proxy settings, and IP blacklists. To enter, click "Advanced settings" to unfold an additional menu while creating a new network profile or editing an already existing one. If you have any questions about the IP addresses of your network, ask your network administrator.

Setting up a single test interface with multiple network profiles

To scan targets in diffenrent subnets, SINEC Security Inspector needs a unique IP address for each target located in a different subnet.

You can either:

1) Use multiple network interfaces: Scan each target with a different network inferace and an individual network profile

2) Use a single network interface: Assign multiple network profiles (one for each target) to the same network interface.

This section explains how to create several network profiles and assign them to a single network interface The following picture is a schematic representation of how this will look.

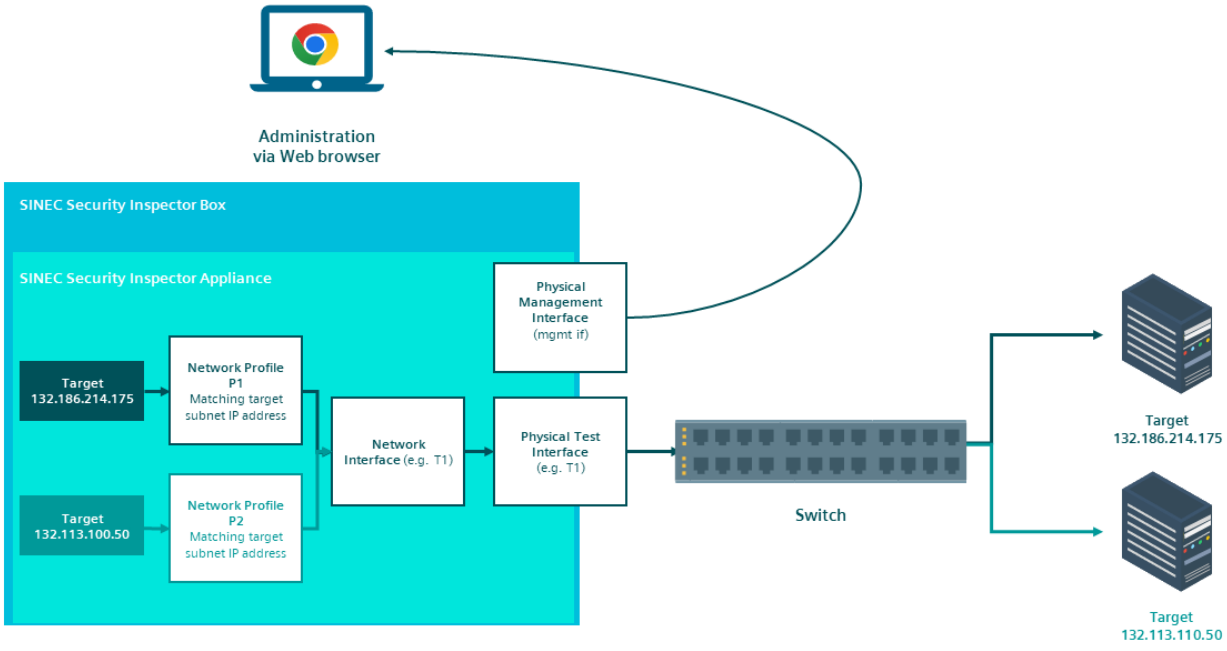


Figure 3-9 Example: Scanning multiple targets with one Test-IF

Note: The address in the Network Profile may be not in same subnet of target in case when gateway is used and its routing is correctly configured.

Assign multiple network profiles to one network interface

If you don't have any network interface installed in your SINEC Security Inspector appliance, install a new one as described in the section "Step 1: Install a new network interface".

The picture above is an example for Test interface. The IP address of the upper target is 132.186.214.175. It may be in the subnet 132.186.0.0/16. The IP address of the lower target is 132.113.100.50 and it may be in the subnet 132.113.100.0/24.

If SINEC Security Inspector has access to both subnets,you are able to scan both targets by creating two network profiles. Each network profile needs:

- a suiting IP address
- a netmask

- a gateway (optional)
- a DNS server (optional)

You can assign both network profiles to the same network interface, if you choose the same network interface from the dropdown menu network interface while creating a new network profile.

Setting up multiple test interfaces

The following picture is a schematic representation of multiple test interfaces set up in parallel.

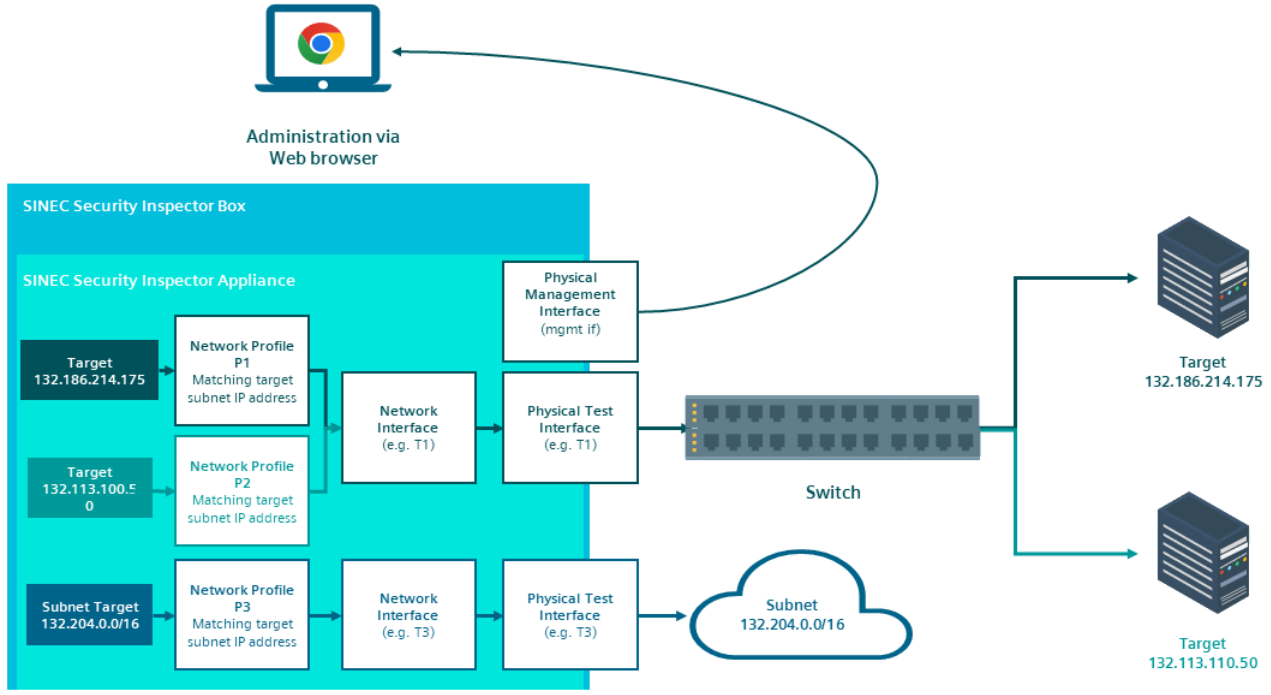


Figure 3-10 Example: Scanning multiple targets with multiple Test-IF

Note: The address in the Network Profile may be not in same subnet of target in case when gateway is used and its routing is correctly configured.

To install a network interface in SINEC Security Inspector for each physical network interface of your hardware, follow the instructions in the section "Step 1: Install a new network interface".

To eate network profiles for each network interface follow the instructions in the section "Step 2: Create a new network profile for new network interface".

Scanning wireless target devices

SINEC Security Inspector does not directly support wireless devices installed in the hardware, so it is not possible to connect directly to Wi-Fi networks with SINEC Security Inspector hardware. There are multiple workarounds for this problem, depending on whether you use the hardware-based version.

Hardware based SINEC Security Inspector

As no directly attached wireless interface is supported by SINEC Security Inspector, it is recommended to connect a device by cable to one of the test network interfaces, which serves as a bridge to the wireless network, a so-called Wi-Fi client. Following Wi-Fi clients are supported with SINEC Security Inspector:

- SCALANCE W720
- SCALANCE W730
- SCALANCE W740

Usually those Wi-Fi clients support multiple modes to connect the Wi-Fi network to SINEC Security Inspector network interface. It is recommended to use the bridging mode, so that direct access from SINEC Security Inspector is possible without any routing or NAT device. This enables availability checks and test cases working on network layers below 3 (IP).

After you have setup the network components and test interface on a hardware device, you can start to setup wizards in SINEC Security Inspector. For more information, refer to Wizard-guided setup (Page 32).

3.4 How to setup a virtual machine

3.4.1 Create a new virtual machine in VMware Workstation Pro

Creating a new Virtual Machine in VMware Workstation Pro

1. Download and install VMware Workstation Pro.
2. Go to VMware Workstation Pro screen and click "Create a New Virtual Machine".
3. Choose "Custom configuration".
4. Choose the Virtual Machine "Hardware Compatibility".
   - Hardware compatibility: Workstation 16.x
   - Compatible with: ESXI Server V5.5 or higher
5. Choose the "Guest Operating System Installation".
   - Install from: Installer Disc image file (iso)
   - Browse and select the installer ISO file that you have downloaded from the following location:
     Link: (https://support.sw.siemens.com/en-US/product/206158208)

6. Choose the Guest Operating System:
   - Guest operating system: Linux
   - Version: Debian 10.x 64-bit
7. Enter the Name of the Virtual Machine and select its location.

   Note

   Name your SINEC Security Inspector like this: "SINEC Security Inspector-XXX", where XXX is the ID of SINEC Security Inspector box.

8. Enter the number of processors and cores per processor in the "Processor Configuration screen. (Minimum: 2 CPU cores. Recommended: 4 CPU cores)
9. Enter the amount of memory in "Memory for the Virtual Machine" screen. (Minimum: 8 GB memory. Recommended: 16 GB memory)
10. Choose your preferred "Network Type".
11. Select "I/O Controller Types".
12. Select a "Disk Type".
13. Select a "Disk".
14. "Specify Disk Capacity": Specify where the disk file should be stored.

    Note

    Ensure your physical hard drive has sufficient space.

    Older VMs need 200 GB, newer ones need 300 GB. Insufficient space will cause the VM to crash. Ensure this space is available on a single hard drive.

15. Click "Finish" to complete the VM creation.
    Your new VM is added to the VMware Workstation Pro.

3.4.2 Configure virtual machine

Overview

After you have created a new virtual machine of VMware workstation, you should configure and verify the machine from its settings area.

Configuring a new virtual machine in VMware Workstation Pro

1. Right-click on the newly created virtual machine (for example, SINEC Security Inspector-XXX) and select "Settings".
2. Under "Hardware" tab, check the CPU and memory size according to your hardware resources.
   The following are minimal and recommended resources that CPU and memory size should possess.
   Minimum required resources:
   Memory: 8 GB RAM
   Processors: 2 CPU cores
   Recommended resources:
   Memory: 16 GB RAM
   Processors: 4 CPU cores
3. Click "Add" to add a new network adapter for testing target networks and devices.
4. Configure the network connection based on available networks and settings.

For more information regarding how to configure the test interface using NAT or in bridged mode, refer to section How to setup network components for virtual Security Inspector (Page 29).

Note

Configuring Virtual Environment for Successful Scan Results

If you are not getting any scan results despite your target being marked as "Reachable" in the Targets Tab, it may be due to a misconfiguration of the Virtual Environment where SINEC Security Inspector is run. Please follow the steps below to configure the virtual environment correctly:

- For Microsoft Hyper-V:
  Enable MAC address spoofing to ensure successful scan results.
- For VMware ESXi Server:
  Enable promiscuous mode, MAC address changes, and forged transmits to allow SiESTA to obtain scan results.

3.4.3 Configure virtualization support

Overview

To configure virtualization support:

1. On the "Virtual Machine Settings" screen, under "Hardware", click "Processors".
2. On the left under "Virtualization engine" section, select option "Virtualize Intel VT-x/EPT or AMD-V/RVI". And click "OK".
3. You can alternatively set the "Preferred mode" from "Automatic" to "Intel VT -x or AMD-V". Click "OK".

Result

Your virtual machine is now configured.

Note

If you are moving an already existing SINEC Security Inspector virtual machine, it is necessary to choose "I moved it", otherwise the configuration is wrong.

After the user has configured its virtual machine, use the Debian installer to install SINEC Security Inspector. For more information about how to begin the installation process on virtual machine, refer to chapter Installation (Page 37).

3.4.4 How to setup network components for virtual Security Inspector

This chapter describes the setup process of network components on Virtual Machine (VM) where SINEC Security Inspector is installed, including restoring default network settings, configuring bridge mode, and setting up test interfaces.

Restoring default network settings

If network configuration issues arise, it may be necessary to restore the default settings. This will erase all custom configurations.

Restoring default network settings

1. Open VMware Workstation.
2. Turn off all virtual machines that are currently installed
3. Click "Edit" > "Virtual Network Editor" to open the virtual network editor.
4. Click "Change settings" at the bottom of the screen.
5. Confirm that you allow changes to devices by clicking "Yes".
6. Click "Restore Defaults".
7. Confirm that you want to restore the default settings for the network by clicking "Yes". The default settings for the virtual network will be restored.

Setting up bridge mode for VMware workstation

To connect a virtual network interface in bridge mode to a physical network interface on your computer:

1. Right-click on the network icon in the taskbar of the host system and select "Open Network & Internet settings" option.
2. On the "Network Status" window, under "Advanced network settings", choose "Network and Sharing Center" option.
3. Select the network interface to which bridge mode should be activated (for example, Ethernet).

4. In the following window click "Properties".
5. On the dialog box, confirm to allow this app to make changes to the device.
6. You can view a list of properties of the network interface, which can be switched on or off by checking its box.
7. Ensure that the "VMware Bridge Protocol" option is checked.
8. Click "OK" to save all settings by confirming each dialog.

Adding a test interface over NAT

Each network interface must be added manually to your SINEC Security Inspector.

1. Open VMware Workstation.
2. Switch to SINEC Security Inspector (click on the tab named SINEC Security Inspector _XXX).
3. Ensure that SINEC Security Inspector is turned of.
4. Click "Edit virtual machine".
5. On the Virtual Machine Settings screen, click "Add".
6. Within the hardware types options, select "Network Adapter" and click "Finish.
7. Select the newly added network interface "Network Adapter 2".
8. On the right of the window, select the following:
   - "Device status" > "Connect at power on"
   - "Network connection" > "NAT: used to share the host's IP address" or "Bridged: Connected directly to the physical network" depending on how the network is configured in the host system.
9. Click "Advanced".
10. At "MAC Address", click "Generate" to assign a MAC address to the new network interface.

    Note

    Please ensure to never use identical MAC addresses for different network interfaces. The MAC address is a unique identifier for each network interface with which it can be clearly identified and therefore should not be assigned twice.

11. Click "Ok" to confirm the configuration.

Creating a new virtual network interface

If you need a new virtual network interface (VMnetX) follow these steps:

1. Open VMware Workstation.
2. Turn off all virtual machines that are currently installed.
3. Click "Edit" and click "Virtual Network Editor".
4. Click "Change Settings" at the bottom of the screen.
5. On the dialog box, click "Yes" to confirm that you want to allow changes to the device.

6. Click "Add Network".
7. Select a VMnet from the dropdown menu (for example, VMnet2), and click "OK".
   The newly created VMnet (for example, VMnet2) is added the list of all available VMnet entries.
8. Select the newly added VMnet and under "VMnet Information" and select the option "Bridged".

You can assign your newly created virtual network interdace to your SINEC Security Inspector as a network adapter, to use it for target testing.

Assigning the virtual network interface in bridged mode as test interface (test-IF)

1. Open VMware Workstation
2. Select SINEC Security Inspector VM.
3. Ensure that SINEC Security Inspector VM is turned off (shut down).
4. Click "Edit virtual machine settings.
5. On the left window, under "Hardware", select the network interface (Network Adapter) to which you want to assign the virtual network interface in bridged Mode.
6. On the right window, under "Network connection, select "Bridged: Connected directly to the physical network" option.
7. Optionally check "Replicate physical network connection state", to renew the IP address of your virtual test interface each time you move the physical machine from one wired or wireless network to another. This option is recommended for mobile machines, for example notebooks.
8. Click "OK" to setup a Test-IF network interface in Bridged Mode.

Using USB Network Interface

Instead of using installed physical network interfaces you can also use USB network interfaces or USB Ethernet adapter as network interface.

To be able to use USB devices in a VM, a USB controller must be installed and added to SINEC Security Inspector.

Adding a USB controller

To add a USB controller to SINEC Security Inspector VM:

1. Open VMware Workstation.
2. Switch to SINEC Security Inspector VM.
3. Make sure that SINEC Security Inspector is turned off (shut down).
4. Click "Edit virtual machine" settings.
5. Click "Add".
6. Under "Hardware, select the USB Controller and click "Finish".

he USB controller is now available, so you can connect the USB Ethernet adapter to your host machine.

The USB Ethernet adapter is now registered in their host system and can only be used by the host system To be able to use the USB Ethernet adapter in SINEC Security Inspector VM, the user has to detach it from the host system and assign it to SINEC Security Inspector VM.

Connecting the USB Network Interface Detach a USB device to use it with SINEC Security Inspector

1. Plug the USB Ethernet adapter into a USB port on your host machine.
2. Start the SINEC Security Inspector VM.
3. At the bottom of the VMware Workstation window, locate the USB device icons.
4. Hover over the USB symbol to identify the connected USB Ethernet adapter.
5. Right-click on the USB Ethernet adapter icon and select Connect (Disconnect from Host).

Now you can use the connected USB Ethernet adapter as a network interface in the SINEC Security Inspector VM.

Scanning wireless target devices

Since SINEC Security Inspector does not directly support wireless devices, you can configure the Wi-Fi adapter on your host system and use NAT mode for the VM:

1. Connect to the wireless network using your host operating system.
2. Ensure that the second network adapter in VMware Workstation's VM settings is set to "NAT"

Now you are able to test the Wi-Fi network from SINEC Security Inspector VM.

Note

Availability checks in web user interface will not work, and some tests, which work on network layers below 3 (IP), will not work either in this setup.

Final steps

After the network components and test interface on VM are set up, start to setup wizards. For more information about how to begin with process to setup wizards, refer to Wizard-guided setup (Page 32).

3.5 Wizard-guided setup

To get started with SINEC Security Inspector run the following two wizards:

- "First Time Setup Wizard"
- "Network Setup Wizard"

3.5.1 First Time Setup Wizard

The First Time Setup Wizard guides you through the first configurations of SINEC Security Inspector:

- Adding users
- Setting the time
- Configuring updates
- Downloading required resources.

Steps

1. Log into SINEC Security Inspector using the admin credentials.
2. Click "Wizards". and select "Start" for the "First Time Setup wizard".
3. On the step "User account", it is recommended to configure additional user accounts for different users. Skip this step if there is no need for additional users.
4. On the step "Time", configure the time of SINEC Security Inspector. It is recommended to configure NTP servers. Specify a NTP server that is reachable from your network – do not forget to specify the correct time zone.
   - To find a NTP server, open the command prompt by pressing <Win> + <R> and typing "cmd".
   - Enter the command "`w32tm /query /status`" and the property named "Source" will show the hostname of the NTP server configured on your Windows machine.
   - Use the command "`nslookup [hostname of NTP server]`" to find the IP address of the NTP server. Enter this IP address in the time settings and click "Update Time Configuration".
5. The step "Provision", only appears if the provisioning is not done yet.
6. On the step "Update settings" configure the update settings.
   - Select "auto" option for automatic updates or "manual" for manual updates.
   - Choose the time and days when maintenance should be performed.
   - You can also configure a proxy server, if needed.
   - For virtual SINEC Security Inspector:
     To enable immediate updates set the value for "Perform Maintenance at" to empty.
   - Make sure that the update server is accessible via HTTPS (443) and optionally SSH (22) and that no firewall is blocking the traffic.

   After all details are entered, click "Save Update Configuration".
7. On the step "Check for updates" , the system will check for and install updates automatically.
8. On the step "Security Tool Release subscription", configure the Security Tool Release subscriptions by selectig the option 'Use default configuration" or manually configure the tool subscriptions. Click "Save subscription settings".

9. On the step "Select Default Resources", select the default resources depending on the use case (optional), and click "Install Selected Resources".
10. On the step "Finish", click "Finish Wizard" to complete the First Time Setup Wizard.

Starting the Network Setup Wizard

After you have configured SINEC Security Inspector for the first use and the Security Inspector is operational, it is necessary to configure the "Network Setup Wizard". The setup process starts immediately after finishing the "First Time Setup Wizard".

3.5.2 Network Setup Wizard

Overview

SINEC Security Inspector comes without a preconfigured test network interface. You can set up the test interface using the Network Setup Wizard, which starts automatically after the First Time Setup Wizard, or can be manually triggered from the wizards page.

Using the Network Setup Wizard

This wizard guides you through the configuration of the network settings and verifies the functionality of the provided configuration.

1. Click "Start" to begin the process.
2. Step "Setup Network Interface": Set up the network interface by using an existing interface or by creating a new one.
   This interface is a virtual instance of a physical interface of SINEC Security Inspector.
   Click "Continue".
3. Step "Setup Network Profile": Set up the network profile associated with the previously created network interface. Definite the IP configuration of the network profile. Enter following information:
   - Name
   - Network interface
   - IPv4 address
   - IPv4 netmask
   - DNS server (if available, this will allow SINEC Security Inspector to list the system names in the reports which will make analysis much easier)
4. After the time is set, click "Update Time Configuration".
5. Step "Verify Connectivity": Enter the IP and an open port of a reachable target. Click "Start Scan" to test network connectivity and the verification scan starts.
6. Step "Scan Evaluation": View the scan results. "Success" indicates that the network is properly configured. Otherwise a message will show, that the setup is not correct.
7. The step "Result" displays the result whether the network is set up correctly or not.

Result

After First Time and Network wizard is complete, the user can begin to use to scan targets.

Installation and login

4

4.1 Installation

Ensure that the minimum system requirements are met and the virtual or hardware environment is set up.

To install a SINEC Security Inspector version 1.19 or higher, you need to install a standard Debian system and then execute the SINEC Security Inspector installation script.

Note

Installation procedures may vary slightly depending on your user environment.

Summary

The following is the list to brief the steps to go through the installation process:

1. Debian Installation with Netinst Image:
   - Create a single partition
   - Create a user named admin-user
   - Install only the SSH server and standard system utilities.
2. Execute the `install.sh` Script with Bash:
   - Run as the root user
   - Do not execute via an SSH session
3. Provisioning

Detailed installation instructions

Note

You need Internet connectivity during the installation process to fetch the latest packages from debian.org.

1. Download the netinst CD image “amd64” from Debian's official website: Link: (https://www.debian.org/releases/bookworm/debian-installer/).
   and write the image to a USB stick,
   For a guide from Debian, please refer to Debian Bookworm Installation Guide:
   Link: (https://www.debian.org/releases/bookworm/i386/apa)
2. Boot the machine from the USB stick and start the installation.

3. Select the language, your country, the locale, and your keyboard setting. Recommendation:
   - Language: English
   - Locale: United States (en_US.UTF-8)
   - Keyboard Setting: American English or German
4. Enter a hostname for the system. Choose a meaningful name, such as the SINEC Security Inspector ID (e.g., Inspector123).
5. Optional: Configure the domain name.
6. Configure a password for the root user.
7. Create a new user for the system with the exact username "admin-user" (this username is required for the process to function correctly).
   The "full name" field can be left blank.
8. Configure your timezone if required.
9. Set up the partitions of the system. Use the option “Guided - use entire disk” to set up the disk as one partition:
   - Select the disk (be careful not to select the USB stick if shown)
   - Select for partitioning: “All files in one partition (recommended for new users)”.
   - Select “Finish partitioning and write changes to disk”.
   - Write changes to disks?" Choose “Yes”.
10. Wait for the base system to be installed.
11. Choose “No” to skip the scanning for additional installation media.
12. Configure the package manager. For example:
    a) Debian archive mirror country: Germany
    b) Debian archive mirror: deb.debian.org
13. Configure a proxy if needed.
14. Do not participate in the popularity contest.
15. Select and install system utilities and SSH server:
    - Uncheck “GNOME”.
    - Uncheck “Debian Desktop environment”.
    - Check “SSH server”.
    - Check “standard system utilities”.
16. Wait for the installation to finish.
17. Install the bootloader:
    - Choose “Yes”.
    - Device for bootloader installation: Make sure to select your hard disk and not the USB drive, e.g., “`/dev/vda`”.
18. Reboot the system.
19. At this time the operating system is installed. Then the system needs to be rebooted to continue with setting up SINEC Security Inspector on the system.

20. On the VMware workstation, restart the virtual machine to reboot the system. Click "Restart".
21. After reboot, the system asks optionally to decrypt the hard disk. Enter the configured password for the hard disk that you provided during the installation at step 8.
22. After the system is decrypted the administrator needs to log in with username "admin-user" and the configured user password that you provided during the installation at step 6.
23. To setup SINEC Security Inspector the user needs to become root by entering the command `sudo su` followed by entering the "admin-user" password. The command prompt changes from '$' to '#' at the end.
24. Download the Inspector installation script from the Siemens Digital Industries Software Website:
    Link: (https://support.sw.siemens.com/en-US/product/206158208)
    and copy it to the OS, via the command:
    `scp c:\temp\install.sh admin-user@Inspector-123:~\`
    Note: The script can only be executed from the base directory "~".
25. Type and run the following command `install.sh` to start the setup.
    For virtual environment, an option comes to choose a management network interface (in this case '0'); this is the interface which is used to access SINEC Security Inspector webinterface and for SINEC Security Inspector to connect to the update server.
    For hardware boxes connect a cable to the port before you run the command `install-sh` command and search for the interface with the state "up".
26. After selecting the installation starts and prints out installation messages. This might take a while. Please don't interrupt this process!
27. After a successful setup of SINEC Security Inspector the web user credentials, fingerprints and a path to the file with the password should be displayed.

    Note

    Keep the note of credentials getting displayed on the following screen capture, or use SSH after the installation to get the credentials. For more information about how to fetch credentials, refer to the section "How to fetch login credentials for web interface".

28. Now the network configuring console is started on the second console.
    Press <Ctrl>+<Alt>+<F2> to make it accessible. Configuring the network settings is possible by pressing <E>.
29. Reboot the device as it is necessary to apply the changes.
30. Now SINEC Security Inspector is installed and you can login on the web interface by visiting: `https//<Application-ip>` in a browser.
    After you log into SINEC Security Inspector you are prompted to change the password for the user. It is recommended to change the email and username to keep your credentials unique and safe.

How to fetch login credentials for web interface

If you have missed noting your credentials from step 26, you can still fetch them with the help of following steps.

1. Log into SINEC Security Inspector via SSH (for example, Putty) using "admin-user" and the password from the setup on step 6.
2. Execute the following command:
   `sudo cat /opt/siesta/webcc_data/credentials.txt`
3. After the command is successfully executed, you can view your login credentials for the web interface.
   These credentials are valid only for first login, and you must change the password to be able to enter any configuration screens.

Note

After the user has installed SINEC Security Inspector (on virtual or hardware environment), they should provision their system once to enable the system to fetch for any future updates. For information about how to provision SINEC Security Inspector refer to section Provisioning SINEC Security Inspector (Page 58).

4.2 Keeping SINEC Security Inspector up-to-date

4.2.1 Why is it so important to update

Updates in the SINEC Security Inspector are grouped into 3 categories:

1. SINEC Security Inspector
   (updates for the SINEC Security Inspector core system)
2. SINEC Security Inspector toolset
   (updates for security tools, test cases and result checkers)
3. Security updates (security updates and operating system updates)

Updates for SINEC Security Inspector

SINEC Security Inspector is subject to continuous development and improvement. To benefit from that keep your SINEC Security Inspector always updated.

Updates include new features and bugfixes.

Updates for the SINEC Security Inspector toolset

- **Security Tools**
  SINEC Security Inspector tools are regularly updated, so we regulary release new Security Tool Releases (STRs) to include the latest software versions. Using outdated STRs means that you are not checking for the latest vulnerabilities.
- **Test Cases**
  Are updated continuously to extend features and fix bugs.
- **Result Checkers**
  Are periodically updated to support evaluation of new and improved testing methods.

4.2.2 How to update

SINEC Security Inspector

A banner on the upper left corner on the SINEC Security Inspector web interface shows, whenever an update is available.

Configuring automatic updates of the SINEC Security Inspector Toolset

To configure automatic updates the SSI toolset, including Security Tools, Test Cases and Result Checkers follow these steps:

1. Go to "Configuration".
2. Select "Update".
3. Click "Edit" at the bottom of the page.
4. Next to "SINEC Security Inspector", choose "Auto".

Configure automatic installation of new Security Tool Releases (STRs)

1. Go to the "Security Tools" page.
2. Click on "Manage Subscription".
3. Check the box for "Automatically install new SINEC Security Inspector Releases".
4. Ensure the "Keep currently used" box is checked.
5. Set "Number of latest releases to keep" based on your needs (Recommendation: 1 for lightweight VMs; more than 1 for system test environments with regression testing).

Repeat steps 1-5 for each tool you want to automatically update with the new SINEC Security Inspector Releases.

SINEC Security Inspector toolset

Automatic update of SINEC Security Inspector toolset & automatic installation of new Security Tool Releases

Please follow the instructions given on Security Tool Releases (STRs) updates configuration to automatically update the SINEC Security Inspector toolset, to configure STRs updates and to manage their subscriptions.

EOL (End of Life) test cases

Test cases that are not developed and supported any further will be set to EOL. Nevertheless, they will still be available for customers who want to use it. For almost every EOL test case there is a new test case which substitutes it. Therefore we recommend to use the new test cases.
It's noted in the description of the EOL test case, shown on the related EOL resources article, and we also notify you in the news stream on the dashboard.

Fixed versions of test cases

For the latest test cases there are also historical test cases with older versions. The fixed (frozen) versions are neither updated nor changed.

The fixed versions can be found under the test cases when clicking on "Install Test Case".

Cloned test cases

Once a default SINEC Security Inspector test case is cloned, we are no longer able to update the cloned test cases.
Our recommendation is to use cloned test cases only when you want to modify the test case configuration and adapt it to your needs. For regression testing we recommend to use fixed versions of test cases (see above).

Security updates

We recommend the security updates to be set to "auto". That can be done in the following way:

1. Go to "Configuration".
2. Select "Update".
3. Click "Edit" at the bottom of the page.
4. Next to "Security Updates" choose "Auto".

Breaking changes

Breaking changes always have to be resolved manually.

Go to the "Configuration" > "Update" page and check the breaking changes at the bottom. The changelogs have also to be read before the update can take place.

For more information on breaking changes have a look at AUTOHOTSPOT.

4.3 User login and logout

For best performance use SINEC Security Inspector with Firefox or Chrome. Avoid using Internet Explorer due to known issues.

Login

1. Connect and accept the certificate warning.
2. The login screen will appear.
3. Enter the initial credentials "SINEC Security Inspector" and click "Sign in".
4. On your first login, you have to update the SINEC Security Inspector credentials. This won't change the SSH credentials for the "admin-user" account.
5. To manage or change credentials later, refer to section Users (Page 61).

Logout

Log out after each session by clicking "Logout" in the top right corner.

See also

SSL/TLS Certificate (Page 59)

4.4 Reset user password

Follow these steps to reset the credentials for a web interface user:

1. Access the command line of your SINEC Security Inspector via SSH.
2. Navigate to the `/opt/siesta/code/support` directory by entering the command `cd /opt/siesta/code/support`.
3. To see all available options, run the command `./web-user-passwd-reset.sh -h`.
   This command will display usage information, such as listing all users, changing a user password, or printing help.
4. To change the password for a specific user, run the command `./web-user-passwd-reset.sh -r USERNAME`.
   This action will generate a one-time password for the user to access the web interface.
5. Use the one-time password to log in to the web interface. SINEC Security Inspector will prompt the user to reset their password upon initial login.

By following these steps, you can successfully reset a user password and ensure secure access to the SINEC Security Inspector web interface.

Web interface

5

The SINEC Security Inspector provides an integrated web interface that can only be accessed via the management interface.

The REST interface is part of the web interface. The documentation of the REST interface is available in the "help" section of SINEC Security Inspector user interface.

5.1 Dashboard

The "Dashboard" tab in the SINEC Security Inspector web interface provides an overview about the latest updates, current status of the framework, and provides access to relevant links for detailed information and support.

Widgets in the dashboard

With the "Configuring the dashboard" button on the top right, you can set the number of displayed widgets.

The following widgets are configurable:

- **News**
  Provides updated news, such as changes and new features of SINEC Security Inspector, new releases, important actions/reminders, upcoming training sessions, webinars, etc.
- **SINEC Security Inspector status**
  Displays the current SINEC Security Inspector status such as current version of SINEC Security Inspector framework, whether there are any updates to be performed, license validity, availability of remote support, hard disk size/usage, RAM size/usage, number of tasks in queue, current system load, etc.
- **SINEC Security Inspector toolset updates**
  Provides the current update status of SINEC Security Inspector framework. If the installed version is up to date, then the system will display "Your toolset is up to date"; otherwise, the system will prompt the user to update it to the most recent version.

- **SINEC Security Inspector optimization**
  Provides key notifications/tasks to be performed by the end user to optimize the performance of SINEC Security Inspector framework. To perform the highlighted task, the end user needs to click on the "Show" button (under the "Action" column) located in the same row of the table next to each of the respective tasks.
- **Support & feedback**
  Provides useful links for further information and support.
  - **Help**
    The given links will navigate the you to the "Help" section of SINEC Security Inspector.
  - **Report a bug on our support platform**
    This link can be used to report any bug which you encounters while working on SINEC Security Inspector.

Note

Besides the current system time and system date, the bottom right corner also displays important system health parameters. It is recommended to monitor the disk usage and check for a low system load in an idle state of SINEC Security Inspector.
A high system load with no task execution (idle state) is an indicator that there is a problem in SINEC Security Inspector. Consider a reboot (administrator only), see chapter Shut down (Page 63), or submit a ticket at the SINEC Security Inspector support page for support.

5.2 Wizards

The wizards make it easier for new users to get started with SINEC Security Inspector. The wizards show the most important SINEC Security Inspector workflows in just a few steps. Following wizards are available:

- **First Time Setup Wizard**
  Guides the user through the initial setup of SINEC Security Inspector.
- **Network Setup Wizard**
  Guides the user through the configuration of the network settings and verifies the functionality of the provided configuration.
- **Automated Target Detection Wizard**
  Scans a given subnet and creates a SINEC Security Inspector target for each online IP address.
- **Bulk Add Targets Wizard**
  Quickly creates multiple SINEC Security Inspector targets using a CSV-formatted input.
- **Factory Scan Wizard**
  Scans one or more subnet targets using tests suitable to be run in factories.

5.3 Security Tools

Overview

SINEC Security Inspector uses various security tools housed in virtual machines to keep the software in a stable state. These virtual machines, known as Security Tool Releases (STRs), ensure that both the tool engines and all plugins stay consistent.

Installing STRs

After installing the SINEC Security Inspector framework, you can easily add the Security Tools you need.

1. Open the SINEC Security Inspector web interface and navigate to the "Security Tools" section. You will see a list of security tools that are available for installation based on your specific licenses and order.
2. Find the security tool you want and click the "Install" button next to it.
   To install several tools at once, click anywhere on each tool's row (the row will turn light green). Then, click the "Install Selected Security Tool Releases" button at the bottom of the table.

After successfully installing a security tool release, you can view further details such as version history and related changelogs. Click on the +/- (expand/collapse) toggle button in the table to access this information.

Automatic Installation

1. Click the "Manage subscription" button to:
   - Trigger automatic installation of new STRs within the selected group.
   - Specify the number of older STRs to retain during new installations. If you leave the "Number of latest releases to keep" field blank, no STRs will be removed when new ones are installed.
2. Save settings:
   - Click "Save and Exit" too save your settings. The action will take place during the next maintenance window.
   - Click "Save and Start" to immediately install the latest STR.

Keeping Specific STRs

To prevent certain STRs from being removed, check the "Keep currently used" checkbox for the desired STRs. If older STRs are manually installed, this checkbox will be automatically marked for those STRs.

5.4 Test Cases

The "Test Cases" tab contains the list of available test cases (configuration for security tools) along with their Name, Version, Tags and Last Edit and editing functionality which allows them to be edited. There are certain predefined test cases which are not editable and can only be executed and cloned. The "Actions" column provides two sets of additional features:

- **Edit**
  Allows editing of the selected test cases.
- **More actions**
  Contains features like Clone, Export and Uninstall, helping users to clone, export or uninstall the test case.

On the top of the Test Cases table, SINEC Security Inspector framework provides features to install a specific test case, to create a new test case and to import selected test case(s) by clicking the "Install Test Case", "New Test Case", and "Import Test Cases(s)" buttons respectively.

Once the user clicks the "Install Test Case" button, the system navigates the user to the "Test Cases available for installation" page, wherein the user can view the entire list of test cases which are available for installation.

To install a single test case, the user can select the specific test case from the row and click on the "Install" button.
To install all the test cases at once, the user can click on the "Select All" check box button at the bottom left corner of the table and click on the "Install Selected Test Case" button next to it.

The workflow for the "New Test Case" feature is like the one described below. Refer to the "New Test Case" feature explained below.
The "Import New Test Case" feature allows the user to upload the test case from the own system.

On the bottom left corner of the test cases table there are features such as:

- **New Test Case**
  This feature allows to create a new test case and assigning name, description, changelog, tags, read-only to prevent non-admin users from editing these test cases, and selection of a security tool release which will become the basis for the new test case. For more information on “New Test Case”, visit section "Install a Test Case" in chapter Security tools (Page 65).
- **Select All**
  This feature allows selection of the entire list of test cases which are present within the “Test Cases” table.
- **Deselect All**
  This feature allows deselection of all the test cases that were selected.
- **Remove/Uninstall Selected Test Cases**
  This feature removes and uninstalls all the selected test cases.

5.5 Targets

The "Targets" tab contains the list of available targets along with their Availability status, ID, Name, Tags, Host, Network Profile and Last Edit.

The "Actions" column provides two sets of additional features:

- **Edit**
  Allows editing of the selected target.
- **More actions**
  Which contains features like Remove, Clone, and Export, helping users to remove, clone or export the selected target respectively. For more information on these features and on targets, visit section Targets (Page 69).

To create a SINEC Security Inspector test target, the following options are available:

- Create a new target from scratch
- Clone an existing target
- Import a target from a file

Create a new target from scratch

To create a new target from scratch, the user needs to click the "New Target" button located at the top of the targets list table. Once the user clicks the "New Target" button, the system navigates the user to the "New Target" page

A new target can be specified by supplying values for at least the "Name", "Target", and "Network profile" fields. The "Name" field is a free-text field. The "Target" field requires a valid IP address, IP subnet value or hostname. It is also possible to describe the target in the "Description" field.

Specification of an IP address

It is recommended to specify a single IPv4 or IPv6 address as a SINEC Security Inspector target, because many security tools support only a single IP address.

Specification of an IP subnet (target)

The syntax after the name is supported. Ranges specified by the "-" sign are not supported.

The specification of an IP subnet for a SINEC Security Inspector target is not fully supported by all Security Tool Releases by design:

- Nmap: fully supported
- Nessus: fully supported

Selection of network profile

By default, the network profile marked as "Default" is selected, see section Network (Page 53).

Clone from an existing target

To clone from an existing target, the user must click on the "More actions" radio button situated under the "Actions" column and select the "Clone" option from the drop-down list.

Once the user clicks on the "Clone" option, the system creates the clone of the selected target and navigates the user to the "Editing page of the cloned target to make any necessary edits. On the same page, the system generates the notification for successful cloning of the target within the light green box at the top of the page. By navigating to the respective fields, the user can make the necessary edits and save the cloned target by clicking on the "Save" or

"Save & Exit" button at the bottom of the "Editing" page. The user can cancel the operation at any time by clicking on the "Cancel" button.

Import new target from file

To import a new target from an existing file, the user needs to click on the "Import New Target" button. Once the user exercises this option, the system allows the user to upload the target from the system.
On the bottom left corner of the "Targets" table there are features such as:

- **New Target**
  This feature allows the user to create a new target, assign the new target a name, define the target IP, network profile, tags, description, attributes, and specifications as described in the "Create a new target from scratch" section above. For more information visit section Targets (Page 69).
- **Select All**
  This feature allows the user to select the entire list of targets which are present within the "Targets" table.
- **Deselect All**
  This feature allows the user to deselect all the targets that were selected.
- **Export Selected Targets**
  This feature allows the user to export the selected targets from the list.
- **Delete Selected Targets**
  This given feature allows the user to delete the selected targets from the list.

5.6 Result Checkers

The "Result Checkers" tab contains a list of the installed result checkers along with their description within the columns, e.g., "Name" of RC, "Version" of RC, "Tags", "Last Edit" date and time of RC and Actions. The Result Checker script allows the automatic evaluation of the test result against user-defined specifications. SINEC Security Inspector provides predefined Result Checker scripts which can be modified or extended.

Editing the result checkers is not recommended. However, if you want to edit a particular result checker you can do so by clicking on the "More actions" button in the "Actions" column and selecting the "Edit" option from the drop-down list. For more information on importing, installing, and editing Result Checkers, refer to section Result Checkers (Page 70).

5.7 Test Scenarios

A test scenario is a combination of test case(s), target(s), security tool releases(s), and optional result checker. It represents a reproduceable test that may be started by the user.

The Test Scenarios tab contains column such as:

- **ID**
  This column contains unique numerical values to identify the test scenarios.
- **Name**
  This column contains specific names of test scenarios.

- **Versions**
  This column contains version numbers of test scenarios.
- **Tags**
  This column contains specific labels or categories that can be used to sort, filter and search user entries.
- **Targets**
  This column contains the names of the targets.
- **Test Case: Used Tool**
  This column contains the names of test cases used along with their latest compatible release information.
- **Last Edit**
  This column contains the date & time of the last edit done on test scenarios.
- **Actions**
  This column can "Start", "Edit", "Delete", "Clone" and "Export" a test scenario.

There are more features in the Test Scenarios tab, such as "New Test Scenario", "Import Test Scenario", "Start", "Edit", "Clone" and "Export". For more information on these features, visit section Test scenarios (Page 71).

5.8 Task Queue

The task queue shows all the tasks that are currently being executed or will be executed in the future. A task is either a test scenario, any other task involving starting security tools, such as manual mode, or a system task, such as a tool installation.

The "Task Queue" tab contains columns such as: "ID", "Name", "Owner", "Tags", "Not before". To know more about the columns State, Overall progress and Actions, visit section Task queue (Page 82). There is an "Abort all" button on the bottom left of the "Task Queue" page. Selecting this feature allows the user to cancel all task execution after confirmation.

5.9 Task History

All tasks that were executed in the past, e.g., if a test scenario was executed, all test results will be accessible in the "Task History" tab. Task History has the columns: ID, Name, Targets, Tags, Owner, "Started" date, Duration and State of the tasks. For more information on the "Result" column, visit section Test result evaluation (Page 83), and to know more about the "Actions" column, visit section Task queue (Page 82).

5.10 Configuration

General features of SINEC Security Inspector can be found by selecting the "Configuration" menu item, which is present at the top right corner of the SINEC Security Inspector "Application" tab. Selecting "Configuration" opens a drop-down menu which contains the features Audit Log, Backups, General, Network, Email etc.

5.10.1 Audit Log

It is possible to obtain an overview of the executed tasks on SINEC Security Inspector ("Configuration" > "Audit Log").

5.10.2 Backup & Restore

SINEC Security Inspector allows the creation of backups of the application ("Configuration" > "Backup & Restore"). The backup contains all test and configuration data, for example test cases or tools stored on SINEC Security Inspector. An existing backup from an old SINEC Security Inspector can be restored to another/new SINEC Security Inspector.

Create a backup

1. Navigate to "Configuration" > "Backup & Restore"
2. Click on "Create a backup", then on "Start backup creation" to begin the backup process.
3. You can create a new backup, download and save it.
4. After a backup is created, a Backup file and Token are generated.
5. Store the Backup file and the associated Token securely for future use. Ensure there is enough storage space available for the backup.

Restore a backup

Note

Restoring a backup overwrites all current user data, settings and installed tools and test cases with the data from the selected backup.

1. In order to restore a backup, select and upload an existing backup file.
2. Enter the associated token so that the backup can be decrypted. The token is received during the creation process.
3. As soon as SINEC Security Inspector has restored the backup, the provisioning must be configured.
4. In the last step, select the resources to re-install in SINEC Security Inspector.

5.10.3 General

SINEC Security Inspector provides some global debugging features ("Configuration" > "General"). They allow general monitoring of the test runs and SINEC Security Inspector itself, as well as several possibilities to configure password policies.

The following settings are available for general configuration:

- **Save tool debug logs to scan results**
  Retrieves all available log files from the used Security Tool Release and adds them to the test result (default: false).
- **Automatically check reachability of targets with arping**
  It enables the automatic availability check of all targets when visiting a target-related web interface page. This option could lead to a high network load with a large number of targets (default: true).
- **Syslog server**
  To consolidate logs at a central server, SINEC Security Inspector can be configured to send its internal logs to a syslog server via UDP (default: none).
- **Minimum memory in MB**
  Setting for minimum working memory (RAM). SINEC Security Inspector uses tools which need large amounts of memory to perform well. Nessus, for example, requires a minimum of 4 GB. Additionally, some resources must be added for SINEC Security Inspector itself. In general, it is not recommended to use SINEC Security Inspector with less than 6 GB of memory. There will be a warning message if there is an attempt to execute test scenarios with less memory.
- **Use Siemens CA for Nessus tests**
  It enables the Siemens Certificate Authorities for Nessus tests.

The following settings are available to configure password policies:

- Minimum length of password
- Minimum number of different character classes (lowercase, uppercase, digits, symbols)
- Expire password after number of days
- Password has to differ from this many prior passwords

Note

In case of a problem with SINEC Security Inspector, it is possible to generate a package with debugging information by selecting "Schedule retrieval of debugging information". This action schedules a task which collects different log files and other information into a zip file.

5.10.4 Network

The test interface must be configured ("Configuration" > "Network") properly to access (e.g., scan) the target(s) with SINEC Security Inspector. It is possible to specify IPv4 and IPv6 settings – whereby at least one IP version must be configured to run tests.

Network profiles link to network interfaces, allow selection of a physical network device (eth1, eth2, etc.) and optional VLAN interfaces configured with VLAN IDs. These profiles can be assigned to targets and can be used by test scenarios and manual mode testing.

Each of SINEC Security Inspector available physical network interfaces (except the management interface) can be used for testing a different network subnet or a server.

The following figure shows an example of internal mapping of targets to network profiles and network profiles to network interfaces.

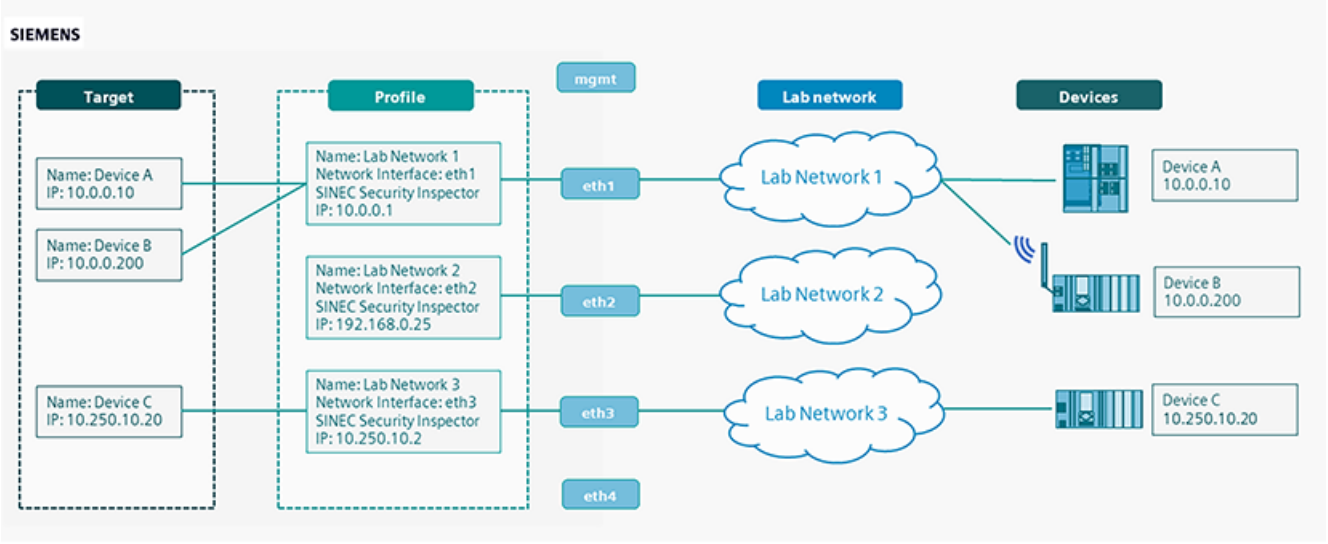


Figure 5-1 Mapping of targets to network profiles

This feature enables testing of multiple network subnets with only one SINEC Security Inspector.

To connect more networks than physical interfaces, it is possible to make use of VLAN tagging.

The figure below shows a setup where just one SINEC Security Inspector test interface network link is used together with optional VLAN tagging (IEEE 802.1Q) using an additional external managed switch. This setup helps to further increase the number of subnets which can be tested at once by SINEC Security Inspector.

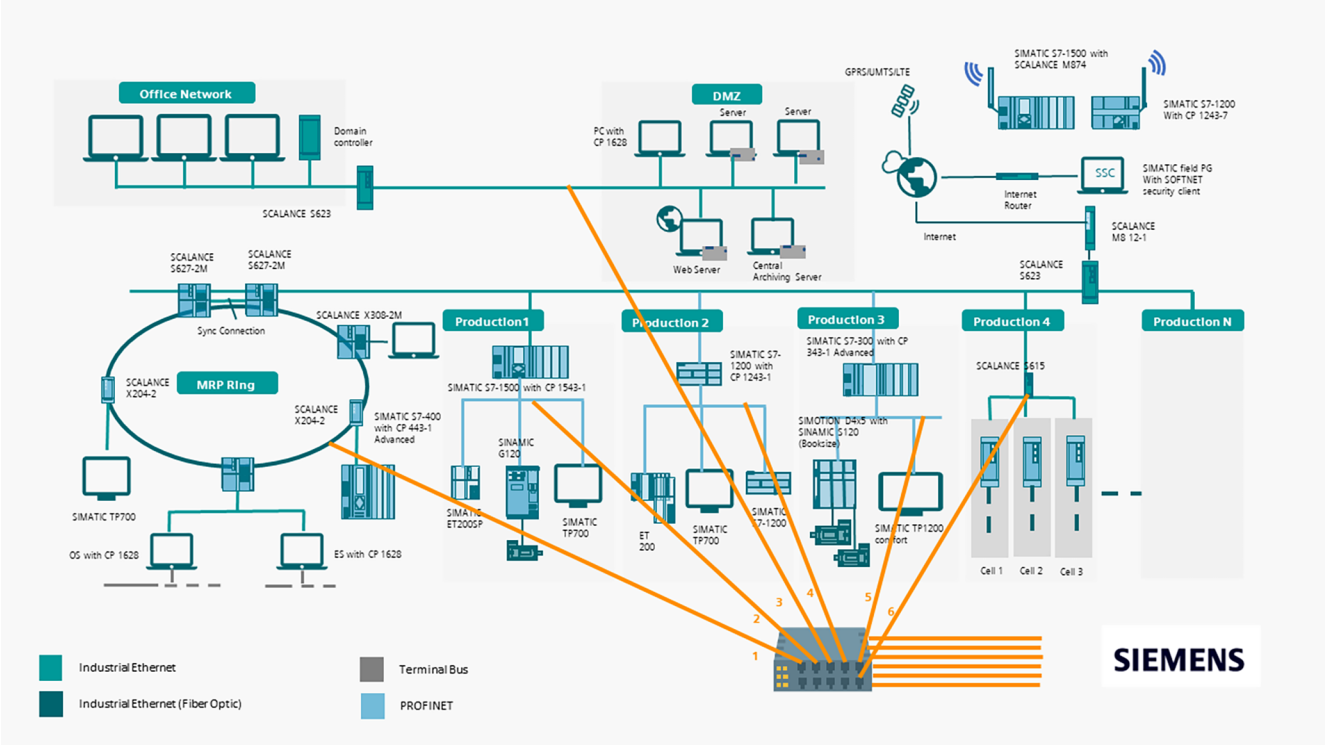


Figure 5-2 Security Inspector and VLAN tagging

5.10.4.1 Network interfaces

As a first step, network interfaces must be configured. Select "New Network Interface".

The name of the interface must be provided, and the physical network interface (device) which has a MAC address must be selected. Additionally, a VLAN ID can be configured.

The MAC address can be used to identify the physical interface. After the new network interface is configured, this task should be allowed some time to finish.

Removal of network interfaces is not allowed if they are mapped to network profiles.

5.10.4.2 Network profiles

After creating one or more network interfaces, these can be assigned to network profiles, where configuration options, such as the IP address, the subnet mask etc. of the network interface are specified.

A new profile can be created by selecting "New Network Profile" in the upper right corner.

The network interface can be assigned using the drop-down box. Selecting the "Default" check box preselects the network profile for creating a new target.

Keep in mind that:

- Multiple network profiles can be assigned to the same network interface.
- All test cases are executed with the source IP address, which is configured for the used network profile.
- All test cases are executed through eth1. This interface is bridged with the physical interface configured in the network profile.

Removal of network profiles is not allowed if they are used by targets. Hovering over the "Remove" button causes a warning to appear.

5.10.5 Email

With the email configuration ("Configuration" > "Email"), SINEC Security Inspector can send email notifications on completed test scenarios to the configured email address.

If the email settings are successfully configured, a green message will be displayed, and a test email will be sent to the configured email address. To edit the email configuration, select the "Edit" button. To modify the data again and test the current configuration, select the "Send Test Email" button. The third option is to reset the email configuration. It is only possible to send one test email for each configuration.

If the configuration is defective, a message appears indicating that there was a problem sending the test email. There is also a dashboard message providing information about this failed send attempt.

There is a more detailed explanation of the error directly below the red message in "Failed Emails". The red "Clear list" button will permanently clear the list of failed emails and remove the notification from the dashboard.

5.10.6 Provisioning

The provisioning ("Configuration" > "Provisioning") is an exchange of key and licensing information between SINEC Security Inspector and the update server.

By default, SINEC Security Inspector does not have permission to install security tool releases, test cases, result checkers, or any updates. If a monitor is connected to SINEC Security Inspector, a not provisioned SINEC Security Inspector console screen will be prompted as shown in the example below.

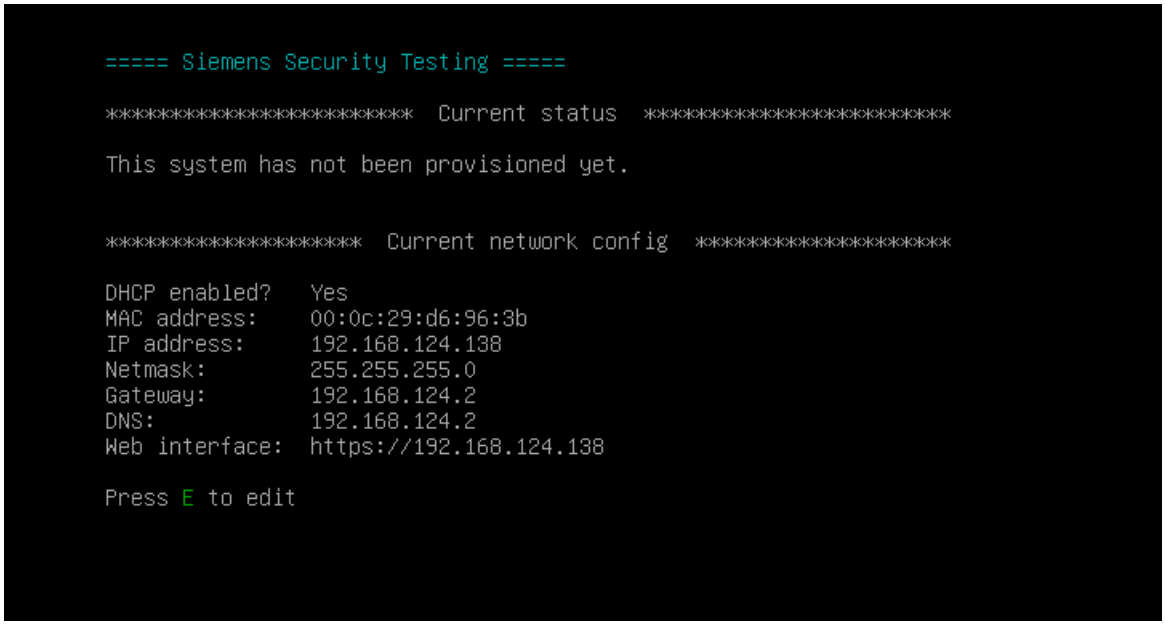


Figure 5-3 Appearance of a not provisioned Security Inspector

If a monitor is connected to the provisioned SINEC Security Inspector system, a console screen appears as you can see in the figure below:

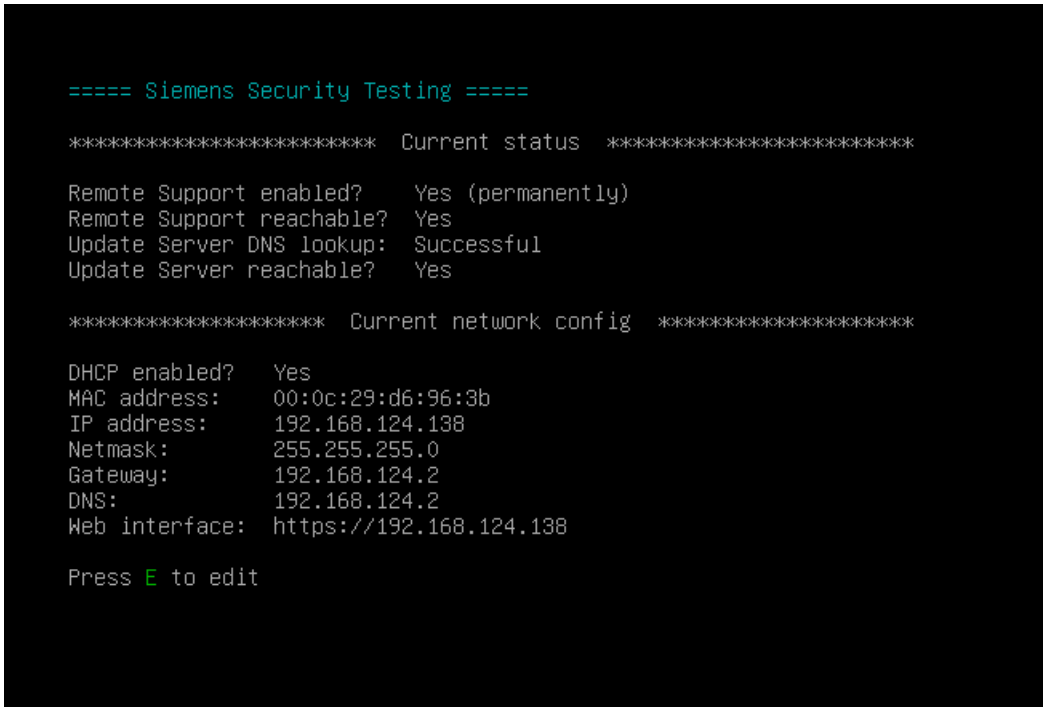


Figure 5-4 Status of Security Inspector after provisioning

5.10.6.1 Provisioning SINEC Security Inspector

Overview

SINEC Security Inspector usually has to be provisioned just once. But sometimes it is necessary to reprovision SINEC Security Inspector.

For an older provisioning format, it might be required to perform a full reprovisioning as described below.

With the newer format, the user can just download a new provisioning response file from the portal and upload it to SINEC Security Inspector. The download button gets disabled, if the old format is used.

Steps

To start the process of provisioning:

1. Log into SINEC Security Inspector using the "admin user" credentials.
2. On the top-right of the screen, click "Configuration" icon.
3. Click on "Configuration" > "Provisioning".
4. On the "Provisioningn" screen, under step 1, click "Provisioning request" button to download the provisioning request.
5. Send the provisioning request to "sts.ct@siemens.com" and specify provisioning belongs to which SINEC Security Inspector ID from the order confirmation mail (otherwise license assignment is not possible) as response.
6. A "provisioning response" file containing the ID number will be sent from "sts.ct@siemens.com".
7. Upload the provisioning response to SINEC Security Inspector.
8. After the file is uploaded, click "Start Provisioning" to provision SINEC Security Inspector.

Configuration of network interfaces and network profiles

After you have provisioned SINEC Security Inspector you should proceed to the configuration of network interfaces and network profiles.
For more information about how to configure the network components, refer to the following mentioned article for virtual or hardware environment, respectively.

5.10.7 Shared Attributes

Shared Attributes ("Configuration" > "Shared Attributes") help to easily use identical target attributes for several different targets.

Shared attributes can be protected from other SINEC Security Inspector users by security groups.

In this menu, (global) attributes for multiple targets can be added or removed. To add a new shared attribute, select the "New Shared Attribute".

New shared attribute:

- **Reference**
  Enter a short and distinctive name for this attribute that is easy to remember.
- **Security group**
  Optionally, choose one of the currently available security groups to define whether this shared attribute is confidential or not. At this time, it is only possible to select one security group for a specific shared attribute.
- **Value**
  The actual value of the target attribute, which replaces the reference.

Note

If a target in a test scenario that uses a shared attribute is in use, the security group of this shared attribute must be the same security group as the one selected in the test scenario. If the selected security groups differ, the test scenario cannot be started.

5.10.8 Security Groups

Security Groups ("Configuration" > "Security Groups") restrict access to confidential information entered in shared attributes and used in targets to a defined user group.

Security groups can be added, removed, or managed in this menu. To add a new security group, select "New Security Group". Enter a name and choose which currently available users should be part of the group. A green key symbol means that the logged in user is a member of this security group. A yellow key symbol means that the logged in user is not a member of this security group. Only security groups with a green key symbol can be modified by the currently logged in user.

Note

- An administrator sees the remove button, but a user does not. The reason is to clean up the SINEC Security Inpector after a user/administrator leaves.
- The user, who creates the new Security Group, is automatically added, and cannot be deselected.

5.10.9 SSL/TLS Certificate

5.10.9.1 SSL/TLS Certificate

SINEC Security Inspector is shipped with a self-signed SSL certificate. To trustfully integrate SINEC Security Inspector within your infrastructure, a custom certificate provided by your certificate authority can be uploaded to SINEC Security Inspector ("Configuration" > "SSL").

For more information please refer to section How to upload and use SSL/TLS certificates (KB) (Page 60).

5.10.9.2 How to upload and use SSL/TLS certificates (KB)

This chapter describes how to upload and use SSL/TLS certificates in SINEC Security Inspector.

In the "Configuration" section of SINEC Security Inspector, the user can upload TLS server certificates, or they can decide to use a self-signed one. If the user wants to use system with proper TLS certificates, they should use the CER format.

Note

If the user's browser won't trust the Root CA and the Intermediate CAs which signed the Certificate, the user has to provide the certificate chain.

If the user don't know how to get a valid certificate, they should ask network administrator to upload and use it.

Upload certificate

To upload a certificate:

1. Log into SINEC Security Inspector.
2. Go to "Configuration" > "SSL/TLS Certificate".
3. On the "SSL/TLS Certificate Configuration" screen, click "Edit".
4. On the screen, select "Upload new certificates" option, and upload the signed certificates in CER Format.

Certificate

The user must upload the signed certificate which they got from their Registration Authority (RA). It is mandatory that the certificate is in CER format (with .cer extension).

The user can also open the certificate file in a plain text editor and check if the structure looks similar like the following:

```
-----BEGIN CERTIFICATE-----
MI...
...
-----END CERTIFICATE-----
```

Certificate key

The user needs to upload the private key for certificate in the CER format.

The key was generated together with the Certificate Signing Request (CSR), which was later signed by the RA.

As it is a private key, the user should have it, or they should get it from the RA.

The user must ensure if the key is in the correct format. To check:

- Open the key file in a plain text editor and check if the structure starts with the following:

```
-----BEGIN RSA PRIVATE KEY-----
...
```

- If the key file starts with BEGIN PRIVATE KEY, it is necessary to convert it using open SSL to RSA private key using the following command:

```
openssl rsa -in <private_key_file>.key -out <rsa_private_key>.key
```

Certificate chain (optional)

If the user's browser won't trust the Root CA and the Intermediate CAs which signed the certificate, the user must provide the certificate chain in the CER format. Usually, the user gets the chain from the RA, inside a managed infrastructure, that's usually not necessary.

5.10.10 Time

Setting up a common time base for your testing environment can be quite beneficial, as the timestamps of SINEC Security Inspector test results and logs, as well as the logs within the tested targets, will align properly. Therefore, it is recommended to configure at least one NTP server for time synchronization ("Configuration" > "Time").

SINEC Security Inspector supports manual time specification and automatic time synchronization with at least one reachable NTP server.

- Use NTP
  If the NTP server(s) are unknown, there is an easy way to find out which NTP server is configured on the Windows machine, refer to First Time Setup Wizard (Page 33).
- Set Date/Time manually
  This option allows you to set the date and time manually.

5.10.11 Users

Administrators can add, remove, or manage users in this menu ("Configuration" > "Users"). The password needs to comply with the password policies specified in the menu "Configuration" > "General". For details, refer to section General (Page 52).

Note

When editing user privileges, note that at least one user must have admin privilege.

To add a user, select "New user" and fill out all required fields. There are four user roles available:

- **Admin**
  An administrator can perform all administrative tasks, such as reconfiguring the network or managing users on the SINEC Security Inspector. Administrators also have more rights in managing test configurations.
- **User**
  A user is intended to just run scans.
- **ReadOnly**
  A user who only has read access to the User Interface (UI).
- **Backup**
  A user who can only schedule Backup tasks.

The table below lists all user privileges in detail:

C: Create

R: Read

U: Update

D: Delete

X: Option is enabled

Component / Role	User	Admin	ReadOnly	Backup
General Configuration		RU		
Network Configuration	CRUD	RU		
Backup		CRUD		CRUD
Activate Debug Logs		RU		
Finished Tasks	R	RD	R	
Own Finished Tasks	RD	RD	R	
Result Checker	CRU	CRUD	R	
Security Tool Release	R	CRUD	R	
Shutdown / Maintenance		X		
STR Manual Mode	X	X		
Target	CRUD	CRUD	R	
Running Task	R	CRUD	R	
Own Running Task	CRU	CRUD	R	
Test Case	CRU	CRUD	R	
Test Scenario	CRUD	CRUD	R	
Modify User Role		CRUD		

Note

When adding a new user, it is recommended to set the "Needs to reset password" option. This option will prompt the new user to change the password on first login and can be found above the "Save and Exit" button when creating a new user.

The user who creates the new security group is automatically added and cannot be deselected.

5.10.12 Wipe User Data

Users can run multiple tests on the network with SINEC Security Inspector. This results in more and more data being stored on SINEC Security Inspector, which fills up the hard disk. The user has now the possibility to reset SINEC Security Inspector to its original state ("Configuration" > "Wipe User Data"). This also means that all the user data is deleted.

The affected data is listed in the "Wipe User Data" info box and comprises:

- Audit log entries
- Custom result checkers

- Custom test cases
- Targets
- Test scenarios (etc..)

When the process is finished, the message "All user-related data has been deleted" will be displayed in a green box at the top of the page.

Note

On SINEC Security Inspector, all customer-specific data is deleted from the hard disk. This includes the data that was created and/or imported by users themselves. It does not include deletion of the Security Tool Releases and test cases that were installed from the SINEC Security Inspector installation menu.

5.10.13 Remote Support

With this feature, it is possible to allow remote support connections ("Configuration" > "Remote Support"). This feature is used when it is necessary to debug a problem and it allows the Customer Support access to the underlying OS.

Remote access can be blocked by selecting the button "Disallow Remote Support Connections".

If remote support connections are blocked, you can choose to allow remote access to SINEC Security Inspector for certain time slots, for example for 1 hour.

5.10.14 Shut down

To shut down or reboot the SINEC Security Inspector, either the power button on the SINEC Security Inspector should be pressed, followed by a cold start, or the "Shut down" option in the "Configuration" menu should be selected.

A window in which it is possible to select "Shut down" or "Reboot" appears after the "Shut down" button is selected in the "Configuration" menu.

5.11 Help

Documentation resources of SINEC Security Inspector can be found by selecting the "Help" menu item.

Most importantly, links to documentation on the SINEC Security Inspector website with general information about SINEC Security Inspector itself, to SINEC Security Inspector documentation and a version changelog can also be found on this tab. In addition, there are links to the REST API documentation, as well as to client code snippets. As additional information, the help page also provides the public key fingerprints of SINEC Security Inspector.

Test configuration

6

SINEC Security Inspector main task is to execute and evaluate security tests. The test execution is based on configurable test scenarios. These test scenarios combine four basic elements of SINEC Security Inspector: Security Tool Release (STR), Test Case (TC), Targets and a Result Checker (RC).

The main purpose of each element is:

- **STR**
  Deliver a clean and reproducible execution environment for the included security tools.
- **TC**
  Define which tests are executed.
- **Targets**
  Define the properties of the system/device/network under test.
- **RC**
  Allow automatic evaluation of test results against a user-defined specification.

6.1 Security tools

SINEC Security Inspector uses several security tools. These tools are encapsulated in virtual machines to maintain a defined software state. This ensures that the tool engines, as well as all plugins, remain in a fixed state. These virtual machines are called "Security Tool Releases" (STR).

After selecting "Install Security Tool Release", a menu is shown where one or more STRs can be selected to be installed on SINEC Security Inspector. By selecting "Install" in the row of a single STR, only the selected STR is installed. By selecting several STRs at once, it is possible to install all of them at the same time by selecting "Install Selected Security Tool Releases" at the bottom of the page.

After the installation of an STR, further details, such as the version history and related changelogs, can be found in its description. The description can be opened by clicking on the "+" (plus).

All installed STRs on SINEC Security Inspector are grouped by name (Nessus etc.). On top of every group, there is a grey row that contains its name and the button "Manage subscription".

By selecting it, it is possible to trigger automatic installation of new STRs that belong to that group and specify the number of older STRs to keep on the SINEC Security Inspector when installing new ones.

Leaving the field "Number of latest releases to keep" blank in this menu means that no STRs are removed from the SINEC Security Inspector when new ones are installed. The settings are saved by selecting the "Save and Exit" button. In this case, the action takes place in the next maintenance window. The latest STR will be installed if the "Save and Start" option is selected. By selecting the field "Keep" of an STR, it is possible to prevent only certain STRs from being removed.

If older STRs are manually installed, the field "Keep" will be automatically marked for these STRs.

For more details, refer to section How to update (Page 41).

Install a test case (TC):

A new SINEC Security Inspector does not contain pre-installed test cases. For further information, refer to section Wizard-guided setup (Page 32). This means that the page is empty at "Menu" > "Test Cases". By selecting "Install Test Case", it is possible to install some.

- **Install a specific TC**
  By selecting "Install" in the row of a test case, an install task is scheduled to install this test case.
- **Install several TCs at once**
  By selecting one or more test cases, the button "Install Selected Test Cases" at the bottom of the page becomes accessible. An install task is scheduled after selection for every selected test case, and all are installed at once.

Note

Test cases that are no longer developed further or supported will be set to End of Life. Nevertheless, they are still available to users who want to use them. The End of Life test cases are hidden by default. Please select the checkbox "Show EOL Test Cases" at "Menu" > "Test Cases" > "Install Test" to list them again.

A basic set of test cases can also be installed directly with the "First Time Wizard". For more information, refer to section First Time Setup Wizard (Page 33).

6.2 Test cases

6.2.1 Test cases

This chapter describes the available test cases which are categorized as per their use case.

Target Setup

Target Interoperability

- **Target Interoperability Test**
  Checks whether a target is correctly configured for credentialed (internal) scans.

Target Maintenance

- **Test Case Utils Target Cleanup**
  Removes scan artifacts from the target. May occur for aborted test cases.

Asset discovery

Generic: For generic asset discovery

- **Asset and Vulnerability Discovery (SiESTA OT Scanner)**
  Searches for assets using Ethernet based ICS protocols and reports vulnerabilities for common Siemens OT devices.

Hosts: Host discovery

- **Asset Discovery (Hosts, Ping Scan)**
  Executes Nmap ping scan to discover reachable hosts.

Environment specific scans

Port Scans

- **Infrastructure Port Scan (Nmap, well-known TCP ports, common UDP ports):**
  Port scan with reduced TCP port range for IT infrastructures.
- **Product Port Scan (Nmap, all UDP ports, version detection)**
  Port scan with full UDP port range for product testing.
- **Solution Port Scan (Nmap, all TCP ports, common UDP ports)**
  Port scan with full TCP and ICS-specific UDP port range for solutions.

Vulnerability Scans

- **Infrastructure Scan (Nessus, w/o UDP, safe checks)**
  Policy for infrastructure scans focusing on speed and a reduction of false-positive results.

Discovery scans

- **Discovery Scan (all TCP/UPD ports, features and NSE Scripts)**
  Executes all available/applicable Nmap NSE scripts on all discovered open ports.
- **Discovery Scan (Nessus, Patch Report)**
  Uses Nessus plugin 66334 "Patch Report" to scan for missing security patches.

Security Auditing

- **Discovery Scan (OS Enumerations)**
  Gathers security relevant information from Windows and Linux operating systems.

Malware

- **Malware Scan (McAfee)**
  Performs an anti-virus scan with McAfee command-line scanner on both Windows and Linux systems.

Vulnerability Scans

- **Vulnerability Scan (Nessus)**
  Performs a Nessus vulnerability scan using the default "Advanced Scan" policy.

Templates

These template test cases are an ideal starting point for creating custom test cases.

Test Cases

- **Hello Word Template Test Case**
  Minimal test case for educational purposes.
- **Test Case Utils Reference Test Case**
  Reference test case that shows the capabilities of the SINEC Security Inspector test case utils.

6.2.2 General structure

A test case is a zip archive containing the following files:

- **meta.yml**
  Metadata of a test case (identical structure for all security tools).
- **config.txt** [optional]
  Textual configuration, like command line parameters. The structure of this file depends on the security tool used.
- **config.bin** [optional]
  Zip archive to store tool and test case specific configuration. The structure of this file depends on the security tool used.

6.2.3 Tool-specific structure

6.2.3.1 Nessus

SINEC Security Inspector uses the Nessus internal database to store test case configurations. Thus, a Nessus test case must contain the following two files inside a single ZIP-archive named "config.bin":

- global.de
- nessusd.db

6.2.3.2 Nmap

SINEC Security Inspector uses the Nmap to ensure that the correct target is defined and that correct output formats are produced. File 'config.txt' contains the parameters which are passed to Nmap.

6.2.3.3 Generic

Generic tool controller is used for different tool classes. It means that the test cases have their own security tools.

6.3 Targets

6.3.1 Targets

To create a SINEC Security Inspector test target, the following options are available:

- Create a new target from scratch
- Clone an existing target
- Import a target from a file

A new target can be created by supplying values for at least the "Name", "Target", and "Network profile" fields. The "Name" field is a free-text field. The "Target" field requires a valid IP address, IP subnet value or hostname. It is also possible to describe the target in the "Description" field.

For more information please refer to section Target attributes, specifications and scenarios (Page 71).

Specification of an IP address

It is recommended to specify a single IPv4 or IPv6 address as a SINEC Security Inspector target, because many security tools only support a single IP address.

Specification of an IP subnet (Target)

By design, the specification of an IP subnet for a SINEC Security Inspector target is not fully supported by all Security Tool Releases:

- Nmap: fully supported
- Nessus: fully supported

Selection of network profile

By default, the network profile marked as "Default" is selected, see section Network (Page 53).

6.3.2 Target attribute validation

6.3.2.1 Concept

The target attribute validation allows the defined target attributes to be checked with respect to their correctness and existence. For example, it defines which attributes are valid and which structure is defined.

Defining the target attribute validation is not mandatory but highly recommended.

6.3.2.2 Definition

Target attribute validation logic is defined at the bottom of SINEC Security Inspector test case page in a YAML-syntax enabled text box called "Validation of Target Attributes". Find help on the syntax used by clicking on the link called "here" below the text box. Certain validation rules are available which allow the range of the timeout parameter to be limited from 1 to 999, for example.

In this section, the target attribute example below is used to show how the target attribute validation mechanism works within SINEC Security Inspector.

6.3.2.3 Validation

The actual validation mechanism is part of SINEC Security Inspector test scenario handling and is triggered when a task is queued for execution. For example, if a test case is used where credentials are required, but no credentials are specified, then the test scenario will not be started. SINEC Security Inspector outputs a validation error message and does not allow the task to be created if a user wants to execute this test scenario.

6.4 Result Checkers

A Result Checker (RC) is a specific program which allows automated evaluation of test results with a given specification. It requires a dedicated runtime environment using special Result Checker Security Tool Releases (STRs).

The description and intended use of each result checker can be displayed by selecting the title.

Additional documentation and Result Checker resources can be accessed by clicking the "Documentation" button, which covers the documentation about the result checker, the changelog and the "Downloads" field.

- Result Checker usage documentation and changelog
  It is possible to check the documentation by selecting the "Documentation" button. The documentation itself and the changelog are visible here.
- Result Checker downloads (e.g., specification files)
  After the "report.xlsx" is downloaded from the "Downloads" tab and opened, the result evaluation is accessible as Excel sheet. This Excel sheet allows the user to receive the test results. It will also show whether the test run failed or passed, together with details of the tests. The user receives the results after the completion of a test scenario.

Result Checkers vary with respect to their attributes/supported actions. SINEC Security Inspector supports three different Result Checker types:

- **Default**
  Default Result Checkers are updated during centrally managed SINEC Security Inspector updates.
- **Fixed**
  For the latest Result Checkers, there are also historical Result Checkers with older versions. The fixed (frozen) versions are neither updated nor changed.
- **Custom**
  Imported Result Checkers or cloned default Result Checkers can be fully modified.

To maintain a specific version of a Result Checker on the SINEC Security Inspector, the following options are available:

- Clone an existing Result Checker (recommended)
- Import a Result Checker as a zip file

Please contact the SINEC Security Inspector team to request support with writing custom Result Checkers by opening a new request in our support platform.

6.5 Test scenarios

6.5.1 Target attributes, specifications and scenarios

The article describes targets and test scenarios and how their attributes and specification works when the user runs test cases.

What are target attributes?

Target attributes define the properties of the system/device under test.

Target attribute helps the user to:

- alter the behavior of test cases
- add target-specific values, such as credentials or timing to test cases
- deliver target-specific data to test cases (which modify the test case behavior)

The user can also get information about the TAs from two different sources: test cases and targets.

How to use TAs?

The TAs are configured in the YAML structure.

The following example helps define the login credentials to be used within the Nessus scanner, as well as specific Nessus' settings.

```
credentials: &credentials
  Host:
    Windows:
    - auth_method: Password
      username: Administrator
      password: '123456789'
      domain: WORKGROUP

nessus:
  credentials: *credentials
  settings:
    start_remote_registry:       yes             # for Windows login
    enable_admin_shares:         yes             # for Windows login
```

The user can find more examples under most of the Test Case's descriptions on Web Interface.

Target specifications (TSpecs)

Target specifications help evaluate and specify the results, and not the behavior of the tests. TSpecs modify the behavior of the Result Checker.

How to use TSpecs?

The TSpecs is also set in the YAML structure. For more information on the YAML language, refer to YAML Basics.

The following example helps define the multiple ways to specify TSpecs.

- Specifying ports 22, 80, 443, and 161 as open

```
ports:
- port: 22
  protocol: tcp
  type: open
- port: 80
  protocol: tcp
  type: open
- port: 443
  protocol: tcp
  type: open
- port: 161
  protocol: udp
  type: open
```

- Specifying the allowed severity level for Nessus vulnerabilities, rating specific vulnerabilities as 'medium' or 'low' as well as whitelisting several vulnerabilities

```
vulnerabilities:
- tool: Nessus
type:
- allowed_severity_level:
  - value:
  - info
- rate_check_as_medium:
  - value, comment:
     - 10915, Microsoft Windows - Local Users Information : User
Has Never Logged In
     - 10916, Microsoft Windows - Local Users Information :
Passwords Never Expire
     - 11422, Web Server Unconfigured - Default Install Page Present
     - 11457, Microsoft Windows SMB Registry : Winlogon Cached
Password Weakness
     - 65821, SSL RC4 Cipher Suites Supported (Bar Mitzvah)
     - 83875, SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
     - 104743, TLS Version 1.0 Protocol Detection
     - 70544, SSL Cipher Block Chaining Cipher Suites Supported
```

```
- rate_check_as_low:
  - value, comment:
  - 10107, HTTP Server Type and Version
 - whitelist_check:
  - value, comment:
     - 10114, ICMP Timestamp Request Remote Date Disclosure
     - 10150, Windows NetBIOS / SMB Remote Host Information
Disclosure
     - 10287, Traceroute Information
     - 10394, Microsoft Windows SMB Log In Possible
     - 10395, Microsoft Windows SMB Shares Enumeration
     - 10396, Microsoft Windows SMB Shares Access
```

- Specifying components, services, and shares that may exist, must exist, or may not exist

```
components:
- detection_source: "*"
type:
- may_exist
  - name: ".*"
services:
- status: "*"
type:
- must_exist
  - name: "Update for Microsoft.*"
shares:
- type: must_not_exist
  - name: "Microsoft Baseline Security Analyzer 2.3"
```

- Specifying host tags

```
host_tags:
- host_tag: "s7-1500"
- host_tag: "PLC"
```

What are test scenarios?

Test scenarios (TSs) are an entire security test setup, comprised of Targets, Test Cases, STRs (configured inside the TCs), and RCs.

Inside a TS the user configures the scan to run.

Within TS, the user can add Test Scenario Attributes (TSAs) or Test Scenario Specifications (TSSpecs), to apply it to all the different targets.

Test Scenario Attributes (TSAs)

TSAs are used when the user has to specify multiple targets for test scenarios. The option that is configured by the user within TAs can also be configured in TSAs.

TSAs get automatically merged with TAs when the user runs the test.

However, if there is a contradiction amongst the attributes defined in TAs and TSAs, the TSAs attributes overwrite the TAs attributes and thus are applied to each target which is part of that corresponding Test Scenario.

The following are some examples of where TSAs can be used:

- giving the duration of a web application scan
- giving the same credentials to multiple targets
- TSAs can be used with the SiESTA OT Scanner

An example, where Test Scenario runs with multiple targets, TSAs, and TSSpecs are applied to all targets is explained below.

Test Scenario Specifications (TSSpecs)

Similar to TSAs; TSSpecs is used when the user has to specify multiple targets in one Test Scenario. The option that is configured by the user within TSpecs can also be configured in TSSpecs.

TSSpecs get automatically merged with TSpecs when the user runs the test.

However, if there is a contradiction amongst the attributes defined in TSpecs and TSSpecs, the TSSpecs attributes overwrite the TSpecs attribute and thus are applied to each target that is a part of that corresponding Test Scenario.

An example, where Test Scenario runs with multiple targets, TSAs, and TSSpecs are applied to all targets is explained below.

How to use TSSpecs?

The following example helps to specify port 80 to open for all targets which are part of the Test Scenario.

```
ports:
- port: 80
  protocol: tcp
  type: open
```

How to apply TAs, TSpecs, TSAs, and TSSpecs within SINEC Security Inspector?

As stated in the previous sections, TAs and TSAs are interrelated to each other, and so are the TSpecs and TSSpecs. The following are two examples to state the connection between TAs, TSpecs, TSAs, and TSSpecs.

Example 1: This displays how Test Scenario with one Target (where TAs and TSpecs are defined) merges with TSSpecs, where no TSAs are defined.

In the following example, the user can view that within one target we have specified Target Attributes (TAs) and Target Specifications (TSpecs) that are getting merged to TSAs with no values and TSSpecs with some values.

After the test is run, the result displays merged attributes (TAs and TSAs), and within Specifications, the user can view the merged results, in ports and vulnerabilities.

The user should notice that since there are no TSAs defined, the TAs gets populated as it is within the results.
But, since TSpecs and TSSpecs have values, the result gets merged (in this case, for vulnerabilities and ports).

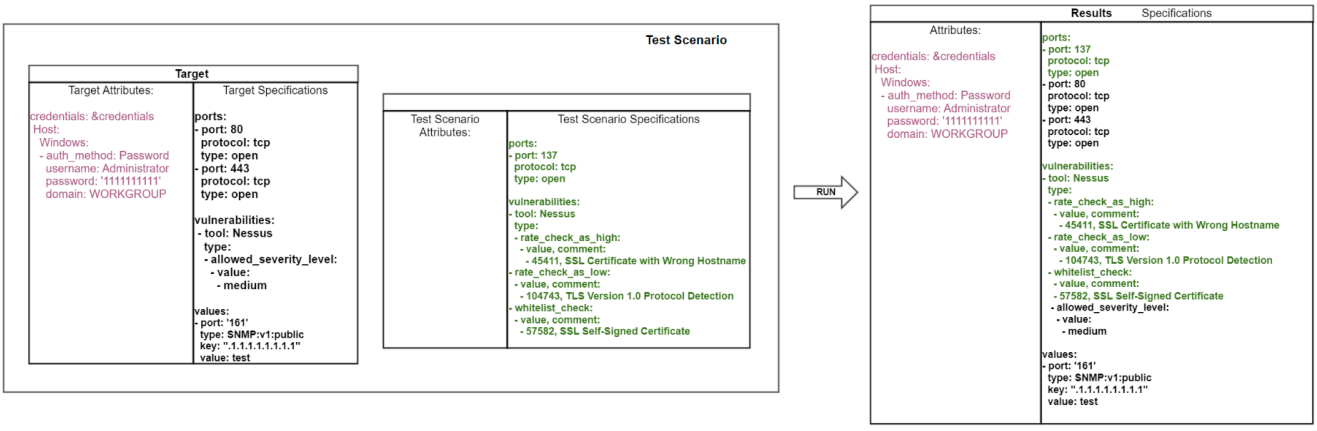


Figure 6-1 Example 1

Example 2: This displays how test scenario with multiple targets gets merged with TSAs and TSSpecs that are applied to all targets

In the following example, the user can view that there are multiple targets defined (that have TAs and TSpecs defined in them) that will be merged to TSAs and TSSpecs with some values.

After the test is run, the result displays merged Attributes (TAs and TSAs), and within specifications, the user can view the merged results, in ports.

The user should notice that since TSAs defined have the same key as TAs, hence in the result the TAs values get overwritten by TSAs.
And, TSpecs and TSSpecs resultant values get merged.

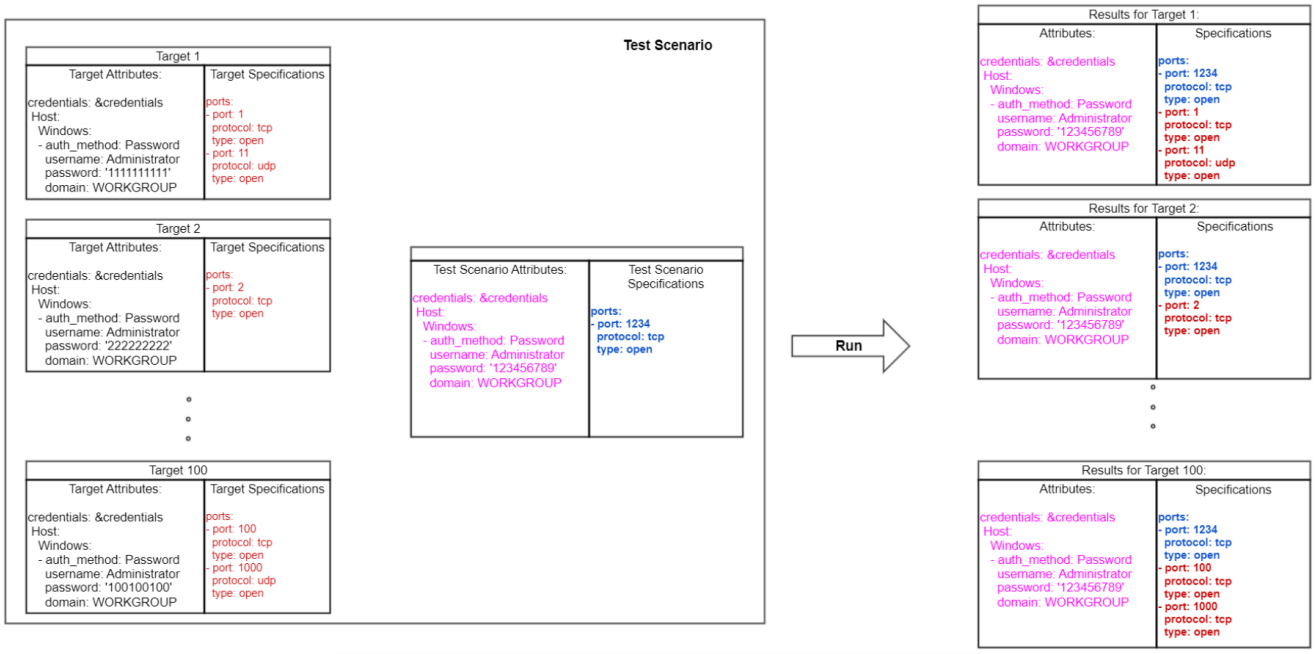


Figure 6-2 Example 2

Edge cases

The general rule is that:

1. Target attributes should never be used to define specifications.
2. Specifications should be defined under "Target Specifications" (or "Test Scenario Specifications", if we are defining specifications on a test scenario level).

There are only a few edge cases where the specifications can be given under "Target Attributes". But the user must ensure that those specifications will not be sent to the Result Checker, but will be sent to the corresponding test cases.

In other words, the user is using the 'specifications' key under "Target Attributes" to configure their test cases.

Please see the description of the above test cases for examples on how to configure them.

6.5.2 Importing and exporting a test scenario

Importing a Test Scenario

1. To import a Test Scenario (TS), follow these steps:
2. Navigate to the TS overview page.
3. Click the Import Test Scenario button located at the top of the page.
4. Select the TS you wish to import.

When importing a TS, you have three options:

Note

When importing a TS, it is recommended to install the latest versions of the included resources. Only use the fixed versions included if they are really needed.
If SINEC Security Inspector detects that some of the resources about to be imported are already available, it will assign them to the new TS by default instead of creating a copy.

- **Use as is**
  This option allows you to use the test scenario as it was originally created. All necessary resources will be installed or imported in the exact version included in the TS export. This ensures that the results of previous runs can be accurately reproduced.
- **Use latest**
  This option uses the latest resources available. It updates all necessary components for the test scenario to their most recent versions, allowing you to perform up-to-date scans.
- **Advanced**
  This option lets you configure the import settings as needed. Review the test scenario and complete any missing settings.

Security group:

When importing a TS, the following rules apply regarding security groups:

- If the TS being imported has an assigned security group that exists in SINEC Security Inspector, it will be preselected.
- If the importing user does not belong to the preselected security group or if the group does not exist in SINEC Security Inspector, the user will be prompted to choose a new one.
- If there is no security group assigned to the imported TS, '"None will be preselected.
- If a security group present in the exported TS matches an existing group in SINEC Security Inspector by name, the message "Security Group was matched by name, double-check" will be displayed during the import process.

Targets:

- A TS import includes one or more targets. SINEC Security Inspector will check if these targets are already present in the system:
- If the targets are present, their status is set to "Target already exists". You can choose to use these existing targets or not.
- If the targets are not present, they will be created and automatically assigned to the imported TS. You can change the settings of the newly imported targets, continue using them as they are, or decide not to import them independently.

Test cases

A TS import also includes one or more Test Cases (TCs). SINEC Security Inspector will check if these TCs are already present:

- If the TCs are present, their status is set to "Test Case already exists".
- If the TCs are not present, you have the following options:
  - Install the latest version of the TC: In the "Status" column, select "Install Test Case from update server immediately" from the drop-down menu. This option is available only for administrators.
  - Install the specific version included in the export: In the "Status" column, select "Import Test Case from export" from the drop-down menu.
  - Do not install the TC: Select the "Do not import" button.

A TC can only be executed with the original Security Tool Release (STR). If the original STR for a TC is not installed in SINEC Security Inspector, a message "No matching STR found" will be displayed.

Note

TC excecution is only possible with compatible STR

Every TC included in the imported TS can be installed. However, if there is at least one TC without a compatible installed STR, it will not be possible to execute it.

Result Checker and Specifications

SINEC Security Inspector checks if the Result Checkers (RCs) from the imported TS are already present in the system. If not, SINEC Security Inspector provides two options for installing the RC:

- Install Result Checker from Update Server immediately: Installs the latest version of the RC from the Update Server. Only administrators can install the RC.
- Import result checker from export: Installs the RC included in the zip file from the TS.

Test Scenario Attributes

Like Target Attributes (TA), Test Scenario Attributes (TSA) can modify the behavior of related Test Cases (TCs). In some cases, it may be beneficial to configure certain target attributes using the same values for all targets within a test scenario. For example, setting a uniform duration for a web application scan across all targets.

TSAs override the configured target attributes. For detailed documentation and examples on how TSAs operate, refer to section Target attributes, specifications and scenarios (Page 71).

To configure TSAs:

1. Navigate to "Configure Test Scenario Attributes" while creating a new test scenario or editing an existing one.
2. The TSAs are configured in YAML format. When you select "Configure Test Scenario Attributes", an empty field will appear where you can enter the TSAs.

Note

Test scenario attributes will overwrite any target attributes configured for the target.

Test Scenario Specifications

Similar to target specifications, test scenario specifications can modify the behavior of related Result Checkers (RCs).

TS specifications function like target attributes. To configure TS specifications:

Navigate to "Configure Test Scenario Specifications" when creating a new test scenario or editing an existing one.

The test scenario specifications are configured in YAML format. When you select "Configure Test Scenario Specifications YAML", an empty field will appear where you can enter the specifications.

Exporting a Test Scenario

To export a Test Scenario:

1. Locate the specific TS you want to export in the TS overview page.
2. Click the Export button situated behind the selected TS.

6.5.3 Creating a new test scenario

The creation of a Test scenario(TS) is divided into following five steps:

Step 1: Basics

Name and Description

- "Name" Field: Enter a unique name for the Test Scenario (TS). This field accepts free-text values.
- "Description" Field: Use this field to describe the purpose and intent of the TS.

Tags

- It is highly recommended to specify tags for better and faster sorting/filtering of the TS.
- Tags also help in obtaining more specific information.

Notification Emails

To activate notification emails and receive information about the relevant TS, the email address must be configured first. For more information, refer to section Email (Page 56).

Security Group

- Security Group Field (Optional): Restrict access to the TS by selecting an existing security group. Only users within the selected security group can manage or execute the TS.
- If a target added in step 2 uses a shared attribute, ensure the security group matches the one in the shared attribute. Mismatched selections will prevent the TS from being executed. Default value: "None" (no security group assigned).

Debugging Options

- Capture Network Traffic:
  - Recommended for a deeper analysis of test results.
  - Limited to TSs; not available for "Manual Mode" or "Edit Tool Configuration Mode".

Note

Traffic captures of long running TS may produce large capture files. Therefore, the traffic capture is limited to 1 Gigabyte (GB) and will terminate when it reaches that size.

- Enable Debug Log of Test Cases:
  - Changes the log level of the "Live Stream" output from "Info" (default) to "Debug".
  - Provides more detailed information about the test run in the "Live Stream".

Step 2: Select targets

1. Select Targets: Choose one or more targets to add to the TS.
2. Create New Targets: If you need to create a new target, click on "Create Target" within the "Add Selected Target(s)" dialog.
   You can select multiple targets by clicking on each one.
3. Confirm Selection: Once you have selected all the required targets, click on "Add Selected Target(s)" to confirm your choices.

Step 3: Associate test cases

Add one or more test cases (TCs) to the TS:

1. Open the "Associate Test Cases" dialog.
2. Use the search and filter options within the dialog to find the relevant test cases (TCs).
3. Select one or more test cases by clicking on each desired test case.
4. Click on "Add Selected Test Case(s)".
5. The "Original Security tool" for each selected test case will be automatically chosen.

   Note

   A TC can only be executed with the original Security Tool Release (STR). If the original STR for a TC is not installed in SINEC Security Inspector, a message "No matching STR found" will be displayed.

Step 4: Associate Result Checker [optional]

1. Select an appropriate RC from the drop-down list to obtain an automated analysis of the tool results. This step is optional.
2. Configure the RC to not generate a Word report by setting the option "Exclude docxplugin", if desired.
3. After selecting an RC, upload files such as the RC specification or Word report templates.
4. Select "Save and Exit" to store the changes made, or "Save and Start" to launch the TS right away.
5. If periodic execution is required, continue with the next step.

Step 5: Periodic Executions

To make the SINEC Security Inspector execute the TS periodically at fixed timeslots, click "Add new Periodic Execution" to configure one or multiple periodic executions.

Note

If a test scenario is scheduled to be executed periodically, it is not possible to simply delete it anymore.

Cloning an Existing Test Scenario

1. Select a TS that you want to clone.
2. Click on "Clone" in the Action column.
3. The cloned TS will have the same targets, test cases and result checker as the original TS. It is possible to change the configurations after cloning.

Note

Users are unable to clone test scenarios that are assigned to a security group they do not belong to. To check group membership, look for the green key symbol between the "Name" and "Tags" columns. This symbol indicates whether you are a member of the assigned security group.

6.5.4 SINEC Security Inspector test scenarios

A test scenario aggregates targets, STRs, TCs, and RCs to form an entire security test setup. In this way, it is easily possible to test a target with a certain tool, whether it is prone to one or more security vulnerabilities. It is possible to configure an email address at "Configuration" > "Email" (optional). The following options are available to create a SINEC Security Inspector test scenario (TS):

- Create a new TS from scratch
- Clone an existing TS
- Import a TS

6.6 Test execution

NOTICE
Device failure and network interruption possible Network interruptions and device failures can occur when executing test cases. Avoid performing tests in productive operation; instead, perform the test cases during maintenance periods.

6.6.1 Scheduling a task

A test scenario can be scheduled for execution as a task if all necessary components (targets and test cases) and configuration options are set properly. This is indicated with an existing blue "Start" button to the right of each item in the test scenario list.

If there is a "Cannot start" button instead of a "Start" button, the configuration options must be checked and adjusted. Hovering over the "Cannot start" button shows the reasons why the test scenario cannot be executed.

The "Start" button redirects the user to the "Schedule Task" screen. The start time of the task can be set. Tasks will be queued according to their scheduled time and are executed sequentially. In general, no tasks are executed in parallel by SINEC Security Inspector. Therefore, tasks might be pending until previous tasks are completed.

6.6.2 Task queue

Selecting the "Create Task" button queues the task. Depending on the state of the task execution engine, the created task will be marked as

- **Pending** (if another task is currently being executed or the "Not before" date is still in the future)
- **Running**

Selecting the "Abort" button cancels the task execution after confirmation.

Selecting the "Live Stream" button shows the current output of the ongoing task.

After selecting the "Create Task" button, a click on the test scenario's name will open the "Progress" tab.

This tab shows detailed progress information for each subtask. SINEC Security Inspector creates a subtask for each test case/target combination (called "test runs").

All test cases are executed on the first target before moving to the next target.

After the execution of all tests runs, the Result Checker will be executed. The Result Checker has access to all results of all test runs.

6.6.3 Test result evaluation

After execution, the task will be moved to the "Task History" tab.

The screen allows multiple task selections. The following actions are supported:

- **View task details** (click on task's name)
- **Remove tasks**
- **Export task results into a zip file** (including all tool results, result checker files, ...)
- **View generated live stream**

Result States

To indicate the evaluation outcome of a TS execution, the following result states are supported:

Result state	Description
compliant	The result evaluation was successful, and the results are compliant with the specification.
non-compliant	The results are non-compliant with the specification.The complete test is non-compliant if one result is non-compliant.
not checked	No result checker was assigned. Nothing was checked automatically.

Accessing Reports

The latest version of the Result Checker includes the generation of a PDF report available.

To access these reports:

Navigate to the "Task History" tab.

Open the executed task.

Under the verdict, you can export the different result formats:

- XLSX Report: An Excel comprehensive report where specifications can be configured.
- Short PDF Report: A PDF file containing all the scan findings organized by category.
- Long PDF Report: A PDF file containing all findings and associated details, organized by category.

6.6.4 Test result re-check

Test results can be re-evaluated with a (different) RC or a modified specification by selecting "Re-Check Results". The feature does not require re-running of all test runs. For further information, please refer to section Result Checkers (Page 70).

6.7 Manual modes

SINEC Security Inspector is intended for automated testing but provides the possibility of manual interaction with certain tools, like Nessus. SINEC Security Inspector can directly pass through and embed the user interface of the tool in its web interface – this functionality is called "Manual Mode" (MM).

Please keep in mind that the MM will be started in a non-persistent manner, which means all changes made in the tool, including the policies, configurations, and the scan results, will be lost after MM has been stopped. The only exception is that the user can export the results or policies with the tools functionality.

To start the MM, navigate to "Security Tools" and select "Manual Mode".

Note

Currently, only the security tool Nessus supports manual interaction.

6.7.1 Entering manual interaction for the first time

When entering the manual mode for the first time, there might be a trust issue with the self-signed certificate of SINEC Security Inspector. Before selecting "Click to import the SSL certificate", a window with a potential security issue warning appears.

To solve this issue, select "Click to import the SSL certificate" and follow the instructions of the web browser.

After importing the tools certificate, the interface redirects to the manual mode.

6.7.2 Starting manual mode

Selecting "Manual Mode" (MM) will open the "Start Manual Mode for tool" dialog. Make sure to select the right network profile which should be available in MM. It is also possible to schedule the start by selecting a date and time. By choosing "Schedule Manual Mode", the MM will be added to the "Task Queue". Keep in mind that all tasks in the "Task Queue" with prior schedule dates will still be executed before the MM.

6.7.3 Entering manual interaction

Booting up the "Security Tool" for "Manual Interaction" may take a while. After this, a dialog will appear at the top of every screen.

It is now possible to "Enter manual interaction". The screen provides SINEC Security Inspector controls at the top and the embedded web interface below. The tool's web interface can be used as usual.

Selecting "Switch to SINEC Security Inspector" does not stop the MM but switches the screen back to SINEC Security Inspector. The MM does not have a timeout and will not be stopped or canceled without further user interaction.

The MM can be stopped by selecting "Stop Manual Mode". A prompt message will appear which requires confirmation.

Be aware that stopping the MM will reset the used security tool. Changes will not be retained and all data, such as results or policies, will be lost.

Selecting "Reload tool" reloads the frame in which the MM was loaded and the main menu of the security tool is shown, regardless of which submenu the user is in at the time the button "Reload tool" is selected. The tool is not reset as in "Stop Manual Mode".

6.7.4 Configuring a test case interactively

Make sure to select the right network profile, which should be available in manual mode (MM), and confirm entry into MM by selecting "Schedule Edit Tool Config". It is also possible to schedule the test case and select a different Security Tool Release version.

When "Enter manual interaction" is selected in the following dialog, SINEC Security Inspector opens the tool in MM. This task may take a few seconds before the tool is displayed. After this, navigate to the "Policies" section.

Important to save a Nessus policy within SINEC Security Inspector:

- The Nessus policy's name must be set to "siesta-policy" ("Settings" > "BASIC"); otherwise, there will be an error.
- Select "Save" after editing the Nessus policy.

Choose "Save and exit tool" at the top of the screen to leave the MM and retain the edited test case. Otherwise, select "Abort" and the MM will be exited; Nessus will be shut down and the test case will remain unchanged.

Asset discovery and vulnerability detection in factories

7

Overview

This section describes how to prepare a scan with different targets and test scenarios. It also briefs about the asset scan and vulnerability detection scan to provide results.

Preparation for the scan

- Determine blacklisted devices.
- These devices will not be scanned by SINEC Security Inspector - this option should be used for very old and critical devices.
- Establish all network connections.
- The user must ensure that they have configured their network profiles correctly and that SINEC Security Inspector can reach the target network.

The list of blacklisted devices (devices which won't be scanned by SINEC Security Inspector can be given under the "Network Profile".

To view:

1. Log into SINEC Security Inspector, and navigate to "Configuration" > "Network.
2. On the screen, under "Network Profiles", click "Edit.
3. Under the "Editing Network Profile", click "Advanced Settings", and enter the list of devices to blacklist under "IP blacklist". Click "Save" and "Exit".

Asset discovery

For asset discovery, the following SINEC Security Inspector resources are needed:

- Test Case: Asset and Vulnerability Discovery (OT Scanner)
- Result Checker: Security Inspector Check

The test case Asset and Vulnerability Discovery (OT Scanner), as the name indicates, is based on the OT Scanner (SOS) tool. It discovers assets using common ethernet-based ICS protocols and does passive detection of vulnerabilities for Siemens OT devices based on Siemens PSIRT Advisories.

OT Scanner:

- is very lightweight
- is fast
- discovers OT and IT assets

Supported Protocols

- ARP
- BACnet
- CDP
- CodeSys
- CSPv4
- DNP3
- EPL (Ethernet Powerlink / SDO via UDP)
- Ethernet/IPFinsHART-IPIEC 60870-5-104
- LLDP
- Modbus TCP
- Netbios
- Niagara Fo
- PCWorx
- ICMP PING
- ProConOS
- Profinet DCP
- Profinet-CM (I&M0 Data)
- Reverse DNS
- S7Comm
- SMB
- SNMP
- Web-IO (W&T GMBH)

Layer 2 vs Layer 3 Scanning

Note

If SINEC Security Inspector and the targets are in the same subnet then the communication will happen on Layer 2 of OSI model, which will possibly lead to more findings (such as more hosts are detected).

If SINEC Security Inspector and the targets are in different subnets, then the communication will happen on Layer 3, and if some traffic is filtered (for example, internal/external firewall) then some assets may not be detected.

Note

When adding DNS in the "Network Profile" the chances to get more host names are higher!

How to start an asset scan

Creating a target

- Log into SINEC Security Inspector, navigate to "Targets", and click "New Target".
- Enter the Name, Target IP, and Network Profile value with data specific to the user's (subnet) target that they would like to test

Target attributes (optional)

- Refer to the test case description on SINEC Security Inspector web interface to find possible options, which could be used in the target attributes.
- Sometimes usage of those options leads to the discovery of more assets!

Creating a test scenario

- Login to SINEC Security Inspector, navigate to "Test Scenarios", and click "New Test Scenario":
- Under Step 1: Enter a distinctive name for the test scenario.
- Under Step 2: Select "Targets", and add the (subnet) targets the user would like to scan
- Under Step 3 Associate "Test Cases", click "Add Test Case(s)" and select the "Asset and Vulnerability Discovery (OT Scanner)" test case. It is possible to choose a suitable Security Tool Release.
- Under Step 4: Associate "Result Checker", select the "Security Inspector Check" from the drop-down menu.
- Click "Save" and "Start" to start the scan.

Result evaluation

After the scan is completed, you can view the result.
On SINEC Security Inspector web interface, navigate to "Task History" and the user shall find the task that just ran.

Click it and scroll down to the bottom where the user would see the option to "Download Result Checker Files".

Here you can download the reports in desired format and analyze.

Security Inspector Check report example

In addition to the report formats, the Security Inspector Check is able to also generate an html based report.

The report contains information such as:

- Detailed device attributes
  Name, Siemens product number, and current software version.
- Lifecycle information
  Vulnerability overview and vulnerability details of the scanned device.

Vulnerability detection

For vulnerability detection, the following SINEC Security Inspector resources are needed:

- Test Case: Infrastructure Scan (Nessus, w/o UDP, safe checks)
- Result Checker: Security Inspector Check

Infrastructure scan (Nessus, w/o UDP, safe checks)

It is a policy for infrastructure scans that focus on speed and a reduction of false-positive results. This policy is well-suited to scan whole IT networks to get an overview of possible vulnerabilities.

How to start a vulnerability scan

Refer the above sections on how to create a target and how to create a test scenario.

To add the above test case to the test scenario:

1. On the Step 3: Associate "Test Cases" and select the "Infrastructure Scan (Nessus, w/o UDP, safe checks)" test case.

Note

Always use the latest tools and update the resources and the application. For more detailed information about how to keep SINEC Security Inspector and its tools updated, refer to the chapter Keeping SINEC Security Inspector up-to-date (Page 40).

Result evaluation

Refer to the above-mentioned section of the "Result Evaluation" under "How to Start an Asset Scan".

Merging results from multiple scan runs

SINEC Security Inspector supports merging of results from multiple test runs to create a consolidated report. This can be achieved in two ways:

- New test scenario
- Re-check

Option A: To merge results as new test scenario:

1. Export all results, which should be merged.
2. Click "New Test Scenario" to create a new test scenario.
   Within it, do not specify any target.
   Do not specify any test case.
3. Specify a Result Checker.
4. Upload all exported results as specification.
5. Click "Save" and "Start" to start the task.

Option B: Merge results as re-check

- Select a (base) task history item.
- Click on in the task details.
- Specify exported task history items.

More in depth scanning in factories

The test cases mentioned above are lightweight and do not use credentials to log into the targets.

If we want to perform more in-depth security testing in any of our detected assets (for example, configuration of crypto related settings, enumeration of running services, etc.), additional test cases could be executed.

Refer to the chapter Test cases (Page 66) for a list of all available test cases, and choose the appropriate ones depending on use-case and what the user would like to test.

Some of the recommended categories are:

- Generic Malware Scanning (for example, McAfee)
- Possibly adding also further OS specific compliance scans
- Security auditing - enumeration of important OS information
- The user should know that the current test case Discovery Scan (OS Enumerations) requires root/admin privileges.
- Choose additional test cases if it makes sense for the use-case.

For more details on what each test case does, refer to the description of the test cases on SINEC Security Inspector web interface.

Note

The user must read the description thoroughly of the test case and check its corresponding intrusiveness. OT devices tend to not deal well with intrusive scans.

See also

Link (https://en.wikipedia.org/wiki/OSI_model)

8 Security recommendations

8.1 Security functions

Security features

- **Different user roles**
  It is important to provide the minimum access necessary when creating users
  - Admin: An admin user can do all administrative tasks like reconfiguring the network or managing users. Admins have also more rights in managing test configurations.
  - User: A user is intended to just run scans.
  - ReadOnly: A user which only has read access to the UI.
- **Security Groups**
  Managing security groups can restrict the access of confidential information inside SINEC Security Inspector. More information can be found in the manual about the usage of these.
- **Password Policies**
  The password policies can be changed in "Configuration" > "General", see section General (Page 52). Some of the changes that can be applied are the following:
  - Minimum length of password
  - Minimum number of different character classes
  - Expire password after a given number of days
  - Password must differ from a given number of prior passwords
- **Secure protocols**
  SINEC Security Inspector uses the following protocols to secure data transmission:
  - HTTPS: for secure access ot the Web Interface
  - TLS Encryption: for encrypted data transmission
  - SSH: for connection to the SINEC Security Inspector
  - Certificates: SINEC Security Inspector is shipped with a self-signed SSL certificate. A custom certificate provided by your certificate authority can be uploaded to SINEC Security Inspector in "Configuration" > "SSL".
- **Protection against brute force attacks**
  - HTTPS: Login procedure is happening in a second to avoid brute force attacks
  - SSH: SSH login is configured with MaxAuthTries set to 6 tries by default.

- **Audit Logs**
  - There is an audit log with an overview of all executed tasks on SINEC Security Inspector that can be found on "Configuration" > "Audit Log", see section Audit Log (Page 52).
- **Syslog**
  - SINEC Security Inspector can be configured to send its internal logs to a syslog server via UDP in order to consolidate logs at a central server.

Antivirus software available for SINEC Security Inspector

At the time of product release, SINEC Security Inspector was scanned with McAfee which is available as a Security Tool and it can be used to scan itself. The SINEC Security Inspector team scans the software delivered to the users in a daily basis.

Certain directories must be excluded from the malware scanning, as some security tools and security tests might be flagged as malware, but they are safe to use. These are the exclusions that should be added to the target attributes:

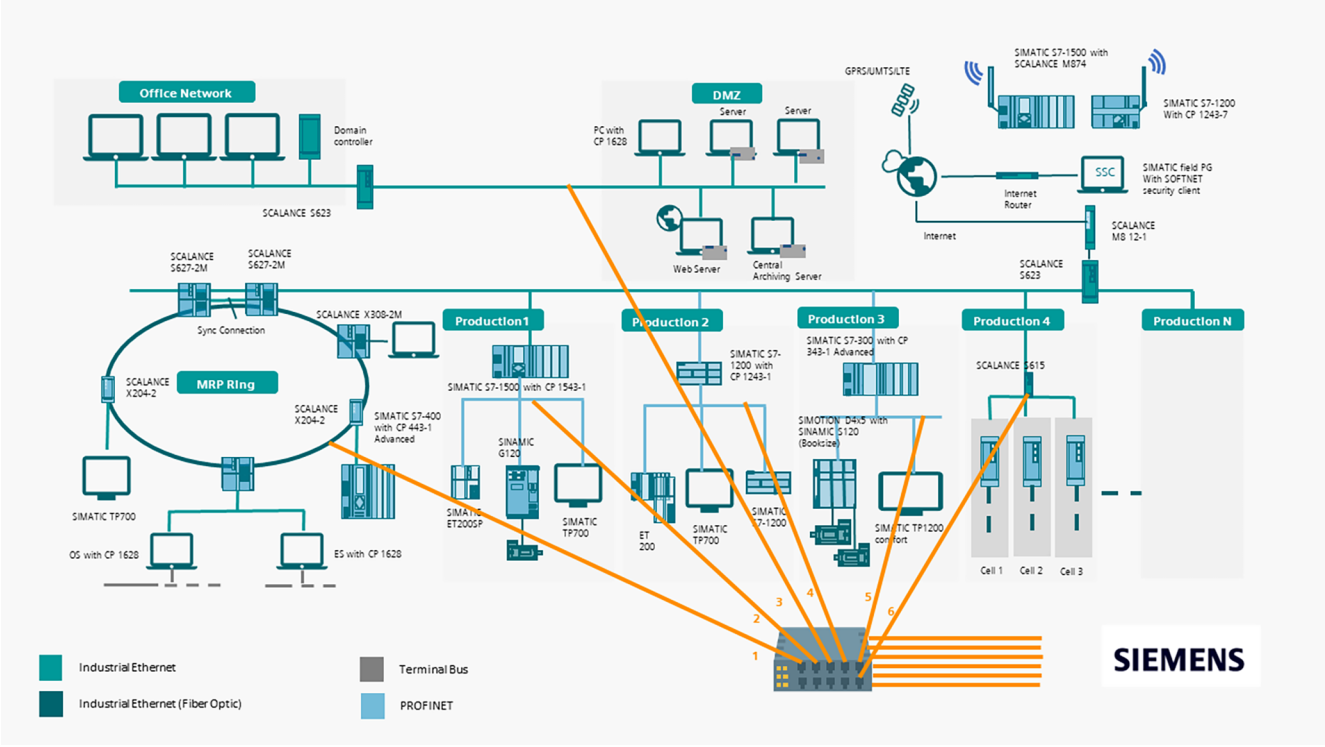
```
mcafee:
    paths:
    - /
    exclude:
    - /dev
    - /proc
    - /sys
    - /var/lib/docker
    - /opt/siesta/code/appliance/webcc/uploads
    - /opt/siesta/webcc_data/uploads/environment_production
```

Security Advisories

If Siemens detects and eliminates security incidents in the product, a Security Advisory would be published. The documents for SINEC Security Inspector can be found under the following site of the Siemens AG: https://new.siemens.com/global/en/products/services/cert.html?s=SINEC%20Security%20Inspector#SecurityPublications (https://new.siemens.com/global/en/products/services/cert.html?s=SINEC%20Security%20Inspector#SecurityPublications)

8.2 Intended operational environment

SINEC Security Inspector is designed to be operated in test networks as well as operative environments like a factory. The scan and the management parts of SINEC Security Inspector are separated and offered on different network interfaces. The scan interfaces are only active (accessible) if a scan is running, otherwise they are switched off. The management interface requires access to SINEC Security Inspector update server on port 443 to fetch updates. The scan interfaces can be directly connected to a target, connected to a switch, or connected via VLANs.



8.3 Security recommendations

General information

- Restrict access to SINEC Security Inspector to qualified and authorized personnel only.
- Provide a separate user for each authorized user and remove the admin user as soon as other users are created.
- Regularly ensure that the users with access are accurate, and that offboarding SINEC Security Inspector users always conclude with deleting the user from the system.
- Ensure that SINEC Security Inspector is up to date, especially security updates and SINEC Security Inspector application.
- Run periodic malware inspection using the Malware Scan available in SINEC Security Inspector.
- Consider running security verification for SINEC Security Inspector, see section Security verification (Page 96).

- Use the security user groups accordingly to provide the minimum permission necessary to the users to prevent unauthorized users from leaking confidential data.
- Define rules for assigning passwords.
- Do not use the same password for different users or systems.
- Do not update the settings on the Debian OS inside SINEC Security Inspector, it may break the SINEC Security Inspector functionality.
- Do not install any external package that comes out of the Security Inspector repository. All the security updates are done through the update server.
- The integrity of the SINEC Security Inspector installer can be verified with SHA-256 Secure Hash Algorithm comparing the sha256 of the ISO against the one provided using the following commands:
  - Windows: certutil –hashfile <file> SHA256
  - Linux: sha256sum <file>
- When decommissioning a SINEC Security Inspector, wipe the disk with the tool of your choice following the same procedure as if it was a Linux client decommissioning.

8.4 Hardening

These are the hardening measures that an admin must configure on top of the security measures that SINEC Security Inspector has built-in to completely fulfill the hardening requirements:

- Install BIOS/UEFI setup password.
- Configure boot sequence to primary hard disk first (only authorized personnel are allowed to change the boot sequence, or the host can be booted from an external interface which can introduce security issues on the host).
- Disable built-in remote management interface (ensure that existing remote management interfaces are either disabled or not connected to any network).
- Ensure physical access protection to the SINEC Security Inspector (e.g., it requires physical permission like a keycard to access the server room).
- Encrypt hard disk during installation.
- Configure a syslog server in SINEC Security Inspector web interface.
- Configure NTP in SINEC Security Inspector web interface for time synchronization.
- Configure SINEC Security Inspector to automatically update, see section How to update (Page 41).

8.5 Security verification

Despite SINEC Security Inspector is a pre-hardened system, some parts must be configured by the administrator of SINEC Security Inspector, see section Hardening (Page 96). It is recommended that a security verification is done periodically to ensure that SINEC Security Inspector remains compliant. In case there are some unexpected findings please contact the SINEC Security Inspector support.

Currently, the SINEC Security Inspector team is performing a nightly security verification to ensure no new findings are impacting SINEC Security Inspector. In future versions we will be providing the means for allowing the users doing a self-check on their own environment.

8.6 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**
  - Open
    The port is always open and cannot be closed.
  - Open after configuration
    The port is open if it has been configured.
- **Authentication**
  Specifies whether the protocol authenticates the communication partner during access.
- **Encryption**
  Specifies whether the transfer is encrypted.

Protocol / Function	Protocol / Port number	Port Status	Authentication	Encryption
SSH	TCP / 22	Open	Yes	Yes
HTTPS	TCP / 443	Open	Yes	Yes
HTTPS	TCP / 8443	Closed (used on demand for "Manual Modes")	Yes	Yes
Postgres	TCP / 5432	Open (internal)	Yes	No
Puma	TCP / 3000	Open (internal)	No	No
AutoSSH	TCP / dynamic	Open (internal)	Yes	Yes
Containerd	TCP / dynamic	Open (internal)	Yes	No
DHCP	UDP / 67 and 68	Open (internal)	No	No
Chrony	UDP / 123	Open (to NTP server only)	No	No
Chrony	UDP / 323	Open (internal)	No	No

8.7 Syslog messages

8.7.1 Structure of the Syslog messages

The Syslog server collects log information of the devices and informs you about specific events. The Syslog messages are output according to RFC 5424 or RFC 5426 via the set UDP port (standard: 514).

Syslog messages record information on the connected devices. This can be status information such as the origin of the message or a time stamp. The Syslog protocol prescribes a fixed sequence and structure of the possible parameters.

Syslog messages have the following structure:

Part / Parameter	Explanation
HEADER	
PRI	PRI contains the coded priority of the Syslog message, broken down into Severity (severity of the message) and Facility (origin of the message).
VERSION	Version number of the Syslog specification.
TIMESTAMP	The device sends the time stamp in the format "2010-01-01T02:03:15.0003+02:00" as the local time including the time zone and correction for daylight saving / standard time if needed.
HOSTNAME	References the source computer with its name or the IP address. IPv4 address according to RFC1035: Bytes in decimal representation: XXX.XXX.XXX.XXX IPv6 address according to RFC4291 Section 2.2 "-" is output if information is missing. Example in the product: The station name configured in the "System" tab for the RTU.
APP-NAME	Device or application from which the message originates. "-" is output if information is missing.
PROCID	The process ID serves to clearly identify the individual processes, for example during analysis and troubleshooting. "-" is output if information is missing.
MSGID	ID to identify the message. "-" is output if information is missing.
STRUCTURED-DATA	
timeQuality	The structured data element "timeQuality" provides information on system time. Example: [timeQuality tzKnown="0" isSynced="0"] The "tzKnown" parameter indicates whether the sender knows its time zone (value "1" = known; value "0" = unknown). The "isSynced" parameter indicates whether the sender is synchronized with a reliable external time source, e.g. via NTP (value "1" = synchronized; value "0" = not synchronized).
sysUpTime	The "sysUpTime" parameter is metainformation about the message. It specifies the time (in hundredths of seconds) since the last re-initialization of the network management part of the system.
MSG	
MESSAGE	Message as ASCII string (English)

Note

Additional information

You can read more detailed information on the structure of the Syslog messages and on the meaning of the parameters in the RFCs:

https://tools.ietf.org/html/rfc5424

https://tools.ietf.org/html/rfc5426

8.7.2 Explanation of the messages

This section describes the Syslog messages. The structure of the messages is based on IEC 62443-3-3.

{Local interface}: Service account logged in.

Example	Nov 23 15:36:44 siesta-box78 sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Explanation	The service-account logged in successfully via a local interface to the device.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

{Local interface}: Service account failed to log in.

Example	Nov 23 14:31:14 siesta-box78 sshd[25871]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=139.25.19.73 user=root
Explanation	Unsuccessful service-account login attempt via a local interface to the device.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

{Protocol}: User {User name} logged in from {IP address}.

Example	Nov 23 15:36:44 siesta-box78 sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Explanation	A user logged in successful via a network interface to the device.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

{Protocol}: Service account logged in from {IP address}.

Example	Nov 21 14:30:57 siesta-box78 sshd[4800]: Accepted publickey for root from 139.25.19.73 port 38399 ssh2: RSA SHA256:Msqlj6LaV5VOPSLE9pDJ7HNVqILl-qeUOwlFYybB/Cpc
Explanation	The service-account logged in successfully via a network interface to the device.

Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

{Protocol}: User {User name} failed to login from {IP address}.

Example	Nov 23 14:31:14 siesta-box78 sshd[25871]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=139.25.19.73 user=root
Explanation	Unsuccessful login attempt via a network interface to the device.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

{Protocol}: Service account failed to login from {IP address}.

Example	Nov 23 14:31:14 siesta-box78 sshd[25871]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=139.25.19.73 user=root
Explanation	Unsuccessful service-account login attempt via a network interface to the device.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

{Local interface}: User {User name} logged out.

Example	Nov 23 15:36:44 siesta-box78 sudo: pam_unix(sudo:session): session closed for user root
Explanation	A user logged out either manually or automatically due to a timeout via a local interface.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

{Protocol}: User {User name} logged out from {IP address}.

Example	Nov 23 15:36:44 siesta-box78 sudo: pam_unix(sudo:session): session closed for user root
Explanation	A user logged out either manually or automatically due to a timeout via a network interface.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

{Local interface}: Service account logged out.

Example	Nov 23 14:31:14 siesta-box78 sshd[25871]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=139.25.19.73 user=root
Explanation	The service-account logged out either manually or automatically due to a timeout via a local interface.
Severity	Info

Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

{Protocol}: Service account logged out from {IP address}.

Example	Nov 23 14:31:14 siesta-box78 sshd[25871]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=139.25.19.73 user=root
Explanation	The service-account logged out either manually or automatically due to a timeout via a network interface.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

{Protocol}: User {User name} has changed the password.

Example	2022-11-04 12:13:19 <acting user> Updated User '<user subject to change>'.
Explanation	An authenticated user changed its own password.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

{Protocol}: User {User name} has changed the password of user {Destination user name}.

Example	2022-11-04 12:13:19 <acting user> Updated User '<user subject to change>'.
Explanation	An authenticated user changed the password of another user.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

{Protocol}: User {User name} disabled user-account {Destination user name}.

Example	2022-11-23 15:48:00 xy@siemens.com Created User 'testasdf@asdf.at'.
Explanation	An authenticated user disabled the account of another user.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

{Protocol}: User {User name} disabled the service account.

Example	2022-11-23 15:48:00 xy@siemens.com Created User 'testasdf@asdf.at'.
Explanation	An authenticated user disabled the service account.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

{Protocol}: User {User name} changed user-account {Destination user name} with role {Role}.

Example	2022-11-04 12:13:19 <acting user> Updated User '<user subject to change>'.
Explanation	User account modified or assigned to another role.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

{Protocol}: User {User name} deleted user-account {Destination user name}.

Example	2022-11-23 15:48:17 xy@siemens.com Deleted User 'testasdf@asdf.at'.
Explanation	A user has deleted an existing user account. In the example, the "xy@siemens.com" user deleted the "testasdf@asdf.at" user account.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

{Protocol}: The access for User {User name} with role {Role} was denied.

Example	Nov 23 15:36:44 siesta-box78 sudo: pam_unix(sudo:session): session closed for user root
Explanation	Access (for system accounts, not web) denied for user with assigned role.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.1

{Protocol}: The session of user {User name} was closed after {Time second} seconds of inactivity.

Example	Nov 23 15:36:44 siesta-box78 sudo: pam_unix(sudo:session): session closed for user root
Explanation	Session was locked after some time of inactivity.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.5

{Protocol}: Remote session {Config detail} was closed after {Time second} seconds of inactivity.

Example	Nov 23 15:36:44 siesta-box78 sudo: pam_unix(sudo:session): session closed for user root
Explanation	Remote seesion closed after some time of inactivity.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.6

{Protocol}: User {User name} logged in from {IP address}.

Example	Nov 23 15:36:44 siesta-box78 sudo: pam_unix(sudo:session): User admin logged in from 192.168.1.105.
Explanation	The user has successfully logged in to the remote device.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.13

{Protocol}: User {User name} failed to login from {IP address}.

Example	Nov 23 14:31:14 siesta-box78 sshd[25871]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=139.25.19.73 user=root
Explanation	The user cannot log in to the remote device.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.13

{Protocol}: User {User name} has logged out.

Example	Nov 23 15:36:44 siesta-box78 sudo: pam_unix(sudo:session): session closed for user root
Explanation	User has logged out.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.13

{Protocol}: User {User name} created backup file.

Example	2022-09-22 17:27:08 karl@siemens.com Scheduled Task 'Backup create: creating a backup of Security Inspector'.
Explanation	The user created successful a backup at the device.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.3

{Protocol}: User {User name} activated the Software {Version}.

Example	Unpacking siesta-appliance (1.16.2.12+g4eda773~xenial) over (1.16.2.11+g6f71d55~xenial)
Explanation	The user updated and activated the software successful.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

{Protocol}: Software {Version} was activated.

Example	Unpacking siesta-appliance (1.16.2.12+g4eda773~xenial) over (1.16.2.11+g6f71d55~xenial)
Explanation	The software is updated and activated successful.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

{Protocol}: Software activation failed.

Example	dpkg: error processing package siesta-<package name>
Explanation	The software update and activation failed.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

{Protocol}: User {User name} failed to activate Software {Version}.

Example	dpkg: error processing package siesta-<package name>
Explanation	The user failed to update and activate the software.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

8.8 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

Table 8-1 HTTPS

CATEGORY	NAME	Hex Value
Cipher Suite	TLS_AES_128_GCM_SHA256	0x1301
Cipher Suite	TLS_AES_256_GCM_SHA384	0x1302
Cipher Suite	TLS_CHA-CHA20_POLY1305_SHA256	0x1303

Cipher Suite	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	0xc02f
Cipher Suite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	0xc030
Cipher Suite	TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256	0xc060
Cipher Suite	TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384	0xc061
Cipher Suite	TLS_ECDHE_RSA_WITH_CHA-CHA20_POLY1305_SHA256	0xcca8
Extension	application layer protocol negotiation/#16	------
Extension	EC point formats/#11	------
Extension	extended master secret/#23	------
Extension	key share/#51	------
Extension	max fragment length/#1	------
Extension	renegotiation info/#65281	------
Extension	session ticket/#35	------
Extension	signature algorithms cert/#50	------
Extension	signature algorithms/#13	------
Extension	supported versions/#43	------
Extension	supported_groups/#10	------
Named Group	ffdhe2048	0x0100
Named Group	ffdhe3072	0x0101
Named group	ffdhe4096	0x0102
Named group	ffdhe6144	0x0103
Named group	ffdhe8192	0x0104
Named group	secp256r1	0x0017
Named group	secp384r1	0x0018
Named group	secp521r1	0x0019
Named group	X448	0x001e
Named group	X25519	0x001d
Server Protocol	HTTP2/ALPN	------
Server Protocol	TLSv1.2	------
Server Protocol	TLSv1.3	------
Signature Algorithm	RSASSA-PSS (rsaEncryption) with SHA256 (FS)	0x0804
Signature Algorithm	RSASSA-PSS (rsaEncryption) with SHA256 (FS)	0x0804
Signature Algorithm	RSASSA-PSS (rsaEncryption) with SHA384 (FS)	0x0805
Signature Algorithm	RSASSA-PSS (rsaEncryption) with SHA384 (FS)	0x0805
Signature Algorithm	RSASSA-PSS (rsaEncryption) with SHA512 (FS)	0x0806

Signature Algorithm	RSASSA-PSS (rsaEncryption) with SHA512 (FS)	0x0806
Signature Algorithm	SHA224 with RSA (FS)	0

Table 8-2 SSH

Category	Name
Key exchange	curve25519-sha256
Key exchange	curve25519-sha256@libssh.org
Key exchange	diffie-hellman-group16-sha512
Key exchange	diffie-hellman-group18-sha512
Key	ssh-ed25519
Key	ssh-rsa
Encryption	aes128-ctr
Encryption	aes128-gcm@openssh.com
Encryption	aes192-ctr
Encryption	aes256-ctr
Encryption	aes256-gcm@openssh.com
Encryption	chacha20-poly1305@openssh.com
MAC	hmac-sha2-256-etm@openssh.com
MAC	hmac-sha2-512-etm@openssh.com
MAC	umac-128-etm@openssh.com

Index