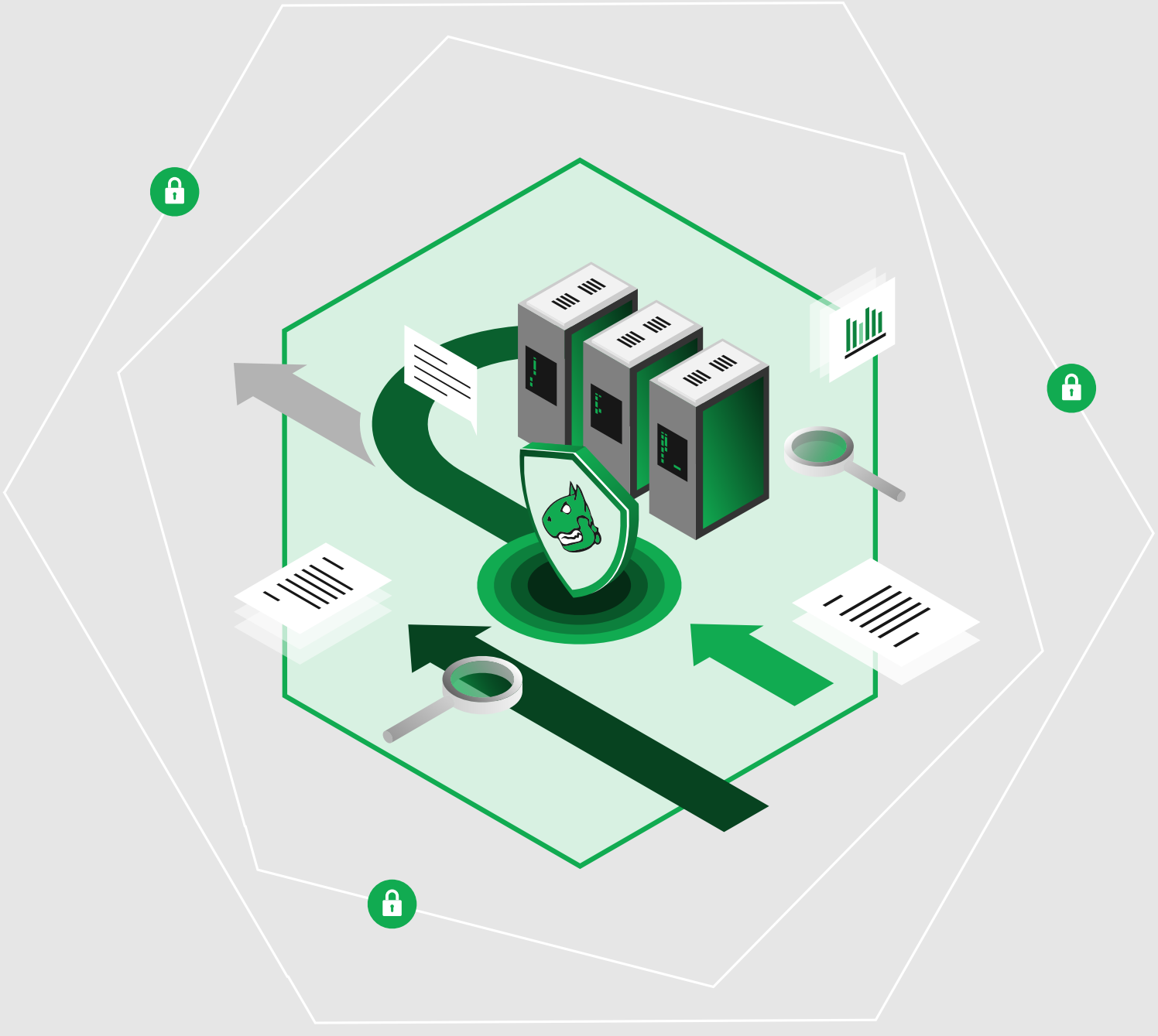
Greenbone

Manual

Greenbone Enterprise Appliance with Greenbone OS 22.04



Greenbone

Greenbone AG
Neumarkt 12
49074 Osnabrück
Germany
https://www.greenbone.net/en/

Greenbone OS version: GOS 22.04.18, 2024-02-20

This is the manual for the Greenbone Enterprise Appliance with Greenbone OS (GOS) version 22.04. Due to the numerous functional differences between GOS 22.04 and previous versions, this manual should not be used with older versions of GOS.
The Greenbone Enterprise Appliance is under constant development. This manual attempts to always document the latest software release. It is, however, possible that latest functionalities have not been captured in this manual.
Should you have additional notes or error corrections for this manual, contact the Greenbone Enterprise Support (https://www.greenbone.net/en/technical-support/).

Contents

CHAPTER 1

Introduction

1.1 Vulnerability Management

In IT security, the combination of three elements influence the attack surface of an IT infrastructure:

- Cyber criminals with sufficient experience, equipment and money to carry out the attack.
- Access to the IT infrastructure.
- Vulnerabilities in IT systems, caused by errors in applications and operating systems, or incorrect configurations.

If these three elements come together, a successful attack on the IT infrastructure is likely.

Since most vulnerabilities are known and can be fixed, the attack surface can be actively influenced using vulnerability management. Vulnerability management involves looking at the IT infrastructure from the outside – just as potential cyber criminals would. The goal is to find every vulnerability that could exist in the IT infrastructure.

Vulnerability management identifies weaknesses in the IT infrastructure, assesses their risk potential, and recommends concrete measures for remediation. In this way, attacks can be prevented through targeted precautionary measures. This process – from recognition to remedy and monitoring – is carried out continuously.

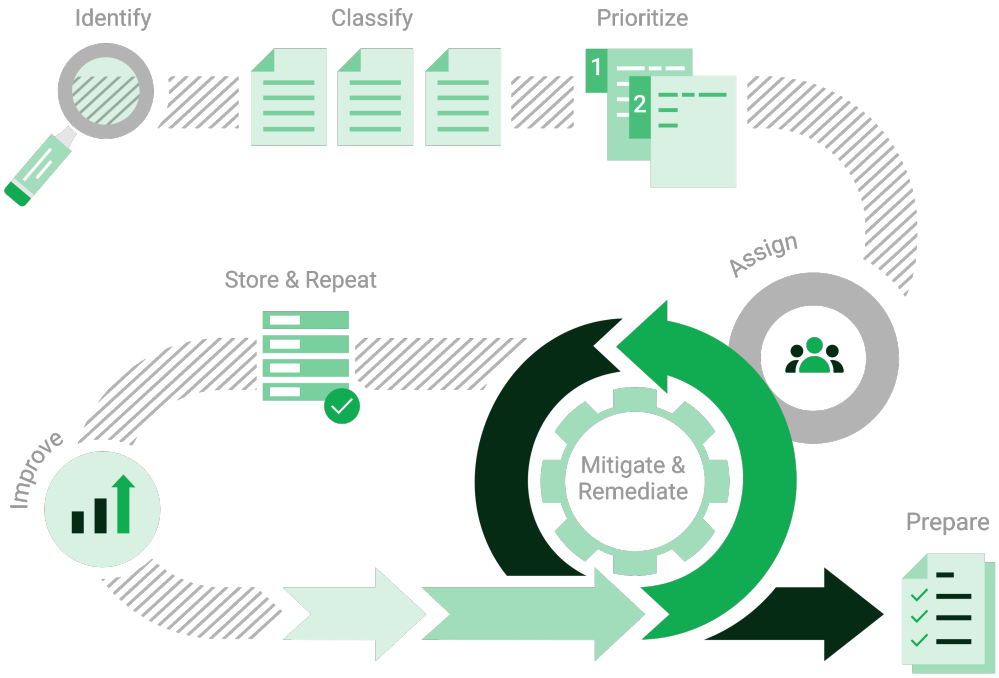


Fig. 1.1: Process of vulnerability management

1.2 Greenbone Enterprise Appliance

The Greenbone Enterprise Appliance is a vulnerability management appliance, available as hardware and virtual models. It assists companies and agencies with automated and integrated vulnerability assessment and management.

1.2.1 Components and Field of Application

The appliance consists of the Greenbone Operating System (GOS) on which the Greenbone Enterprise Feed is installed, a scan service, the web interface and, in case of a physical appliance, a special hardware. The feed provides the vulnerability tests (VTs) that the scan service uses to detect existing vulnerabilities on the inspected network.

As new vulnerabilities are discovered every day, new vulnerability tests must be added constantly. Greenbone analyzes CVE[1] messages and security advisories of vendors and develops new vulnerability tests. The feed is updated daily and thus always provides the latest vulnerability tests to reliably detect the newest vulnerabilities.

The appliance is flexible in use and can be utilized for large enterprises, for medium-sized and small companies as well as for special use cases like audits and trainings. Due to the master-sensor technology, the appliance can also be deployed in high-security sectors.

[1] The Common Vulnerability and Exposures (CVE) project is a vendor neutral forum for the identification and publication of new vulnerabilities.

1.2.2 Types of Scans

The appliance discovers vulnerabilities through different perspectives of cyber criminals:

External The appliance can simulate an external attack to identify outdated or misconfigured firewalls.

Demilitarized Zone (DMZ) The appliance can identify actual vulnerabilities that may be exploited by cyber criminals who get past the firewall.

Internal The appliance can also identify exploitable vulnerabilities in the internal network, for example those targeted by social engineering or computer worms. Due to the potential impact of such attacks, this perspective is particularly important for the security of any IT infrastructure.

DMZ and internal scans can be both unauthenticated and authenticated. When performing an authenticated scan, the appliance uses credentials and can discover vulnerabilities in applications that are not running as a service but have a high risk potential (e.g., web browsers, office applications or PDF viewers).

1.2.3 Vulnerability Classification and Elimination

The detected vulnerabilities are rated according to their severity using the Common Vulnerability Scoring System (CVSS). The severity can be used to determine which vulnerabilities to prioritize when executing remediation measures. The most important measures are those that protect the system against critical risks and eliminate the corresponding vulnerabilities.

Fundamentally, there are two options to deal with vulnerabilities:

- Eliminating the vulnerability by updating the software, removing the vulnerable component or changing the configuration.
- Implementing a rule in a firewall or in an intrusion prevention system (virtual patching).

  Virtual patching is the apparent elimination of the vulnerability through a compensating control. The real vulnerability still exists and the cyber criminals can still exploit the vulnerability if the compensating control fails or if an alternate approach is used.

An actual patch or update of the affected software is always preferred over virtual patching.

CHAPTER 2

Read Before Use

2.1 Using a Supported GOS Version

The Greenbone Enterprise Appliance should always be operated in a version supported by Greenbone (including patch level)[2]. Otherwise, the following problems/effects may occur:

- Incompatibilities in the feed
- Unfixed bugs
- Missing functionalities (e.g., ones that are required for VTs to work reliable or to work at all)
- Decreased scan coverage or missing vulnerability detection due to the issues mentioned above
- Unfixed security vulnerabilities in the used components (e.g., GOS)

2.2 Effects on the Scanned Network Environment

The Greenbone Enterprise Appliance includes a full-featured vulnerability scanner. While the vulnerability scanner has been designed to minimize any adverse effects on the network environment, it still needs to interact and communicate with the target systems being analyzed during a scan.

Note: It is the fundamental task of the Greenbone Enterprise Appliance to find and identify otherwise undetected vulnerabilities. To a certain extent, the scanner must behave like real cyber criminals would.

While the default and recommended settings reduce the impact of the vulnerability scanner on the environment to a minimum, unwanted side effects may still occur. By using the scanner settings, the side effects can be controlled and refined.

[2] https://www.greenbone.net/en/roadmap-lifecycle/

Note: Be aware of the following general side effects:

- Log and alert messages may show up on the target systems.
- Log and alert messages may show up on network devices, monitoring solutions, firewalls and intrusion detection and prevention systems.
- Firewall rules and other intrusion prevention measures may be triggered.
- Scans may increase latency on the target and/or the scanned network. In extreme cases, this may result in situations similar to a denial-of-service (DoS) attack.
- Scans may trigger bugs in fragile or insecure applications resulting in faults or crashes.
- Embedded systems and elements of operational technology with weak network stacks are especially subject to possible crashes or even broken devices.
- Logins (e.g., via SSH or FTP) are done against the target systems for banner-grabbing purposes.
- Probes via different protocols (e.g., HTTP, FTP) are done to all exposed services for service detection.
- Scans may result in user accounts being locked due to the testing of default user name/password combinations.

Since the behavior described above is expected, desired, or even required for vulnerability scanning, the scanner's IP address(es) should be added to the allow list of the affected system/service. Information on creating such an allow list is available from the documentation or support of the respective system/service.

Remember that triggering faults, crashes or locking with default settings means that cyber criminals can do the very same at unplanned times and to an unplanned extent. Finding out about it earlier than the cyber criminals is the key to resilience.

While the side effects are very rare when using the default and recommended settings, the vulnerability scanner allows the configuration of invasive behavior and thus will increase the probability of the effects listed above.

Note: Be aware of these facts and verify the required authorization to execute scans before using the Greenbone Enterprise Appliance to scan the target systems.

2.3 Scanning Through Network Equipment

2.3.1 General Information

Scanning through network equipment like an IDS (Intrusion Detection System)/IPS (Intrusion Prevention System), a WAF (Web Application Firewall), a proxy or a firewall should be avoided, as such devices may interfere with the scan, which may lead to the following unpredictable scan behavior or environmental impact:

- False-positive and false-negative results
- Slow scanning speed
- Too many ports reported as open on the scan target
- Dropped packets due to TCP connection limits, or reaching the maximum session limit
- Depending on the settings, logs can become very extensive, which can lead to an overload of the log server or – if they are completely deactivated – to a blind spot.

Note: Such behavior can also occur if the maximum number of checks per host is limited.

2.3.2 Firewall-Specific Information

Depending on the specific product, a firewall may have several additional modules such as deep packet inspection and denial-of-service (DoS) protection.

- These modules may have limited configurability like general on/off switching per interface and not per source/target IP address.
- Some of the modules may even be hidden or not configurable at all, so that the side effects as mentioned above may occur without any knowledge of why and where they occur.
- The load on the firewall will increase significantly. In a worst-case scenario, connections are not only interrupted for the scanner, but the entire firewall functionality can be impaired, which can lead to a denial of service.

CHAPTER 3

Greenbone Enterprise Appliance – Overview

The Greenbone Enterprise Appliance is a dedicated appliance for vulnerability scanning and vulnerability management. It is offered in different performance levels.

3.1 Hardware Appliances

3.1.1 Large Organizations – Greenbone Enterprise 5400/6500

The Greenbone Enterprise 5400 and Greenbone Enterprise 6500 are designed for the operation in large organizations.

Fig. 3.1: Greenbone Enterprise Appliance for large organizations

They can control other appliances as sensors and can also be controlled as remote scanners by other appliances.

The appliances come in a 2U 19” chassis for easy integration into the data center. For simple installation and monitoring, they are equipped with a two-line LC display with 16 characters per line. For uninterruptible operation, they have redundant, hot-swappable power supplies, 4 hard disk drives (HDDs) and fans.

The appliances use RAID (Redundant Array of Independent Disks) 6 as a software RAID. RAID is a data storage virtualization technology that combines multiple HDD components into one or more logical units for the purposes of data redundancy.

For managing the appliance, a serial port is available in addition to two out-of-band management Ethernet ports. The serial port is set up as a Cisco-compatible console port.

To connect to other systems, the appliances can be equipped with up to four modules. The following modules can be used in any order:

- Module(s) with 8 ports GbE-Base-TX (copper)
- Module(s) with 8 ports 1 GbE SFP (Small Form-factor Pluggable)
- Module(s) with 2 ports 10 GbE SFP+ (Enhanced Small Form-factor Pluggable)

3.1.2 Medium-Sized Organizations and Branches – Greenbone Enterprise 400/450/600/650

The Greenbone Enterprise 400, Greenbone Enterprise 450, Greenbone Enterprise 600 and Greenbone Enterprise 650 are designed for medium-sized organizations and larger branch offices.

Fig. 3.2: Greenbone Enterprise Appliance for medium-sized organizations

They can control other appliances as sensors and can also be controlled as remote scanners by other appliances.

The appliances come in a 1U 19” chassis for easy integration into the data center. For simple installation and monitoring, they are equipped with a two-line LC display with 16 characters per line. For uninterruptible operation, the appliances come with redundant fans.

For managing the appliance, a serial port is available in addition to a management Ethernet port. The serial port is set up as a Cisco-compatible console port.

To connect to other systems, the appliances are equipped with ten ports in total, pre-configured and set up as follows:

- 8 ports GbE-Base-TX (copper)
- 2 ports 10 GbE SFP+ (Enhanced Small Form-factor Pluggable)

A modular configuration of the ports is not possible. One of these ports is also used as management port.

3.1.3 Small Organizations and Branches – Greenbone Enterprise 150

The Greenbone Enterprise 150 is designed for small organizations as well as for small to medium-sized branch offices.

Controlling sensors in other security zones is not considered. However, the Greenbone Enterprise 150 itself can be controlled as a remote scanners by other appliances.

The appliance comes in a 1U steel chassis. For easy integration into the data center, an optional rackmount kit can be used. The appliance does not come with a display.

For managing the appliance, a serial port is available in addition to a management Ethernet port. The serial port is set up as a Cisco-compatible console port.

To connect to other systems, the appliance comes with four GbE-Base-TX (copper) ports in total. One of these ports is also used as management port.

Fig. 3.3: Greenbone Enterprise Appliance for small organizations

3.1.4 Sensor – Greenbone Enterprise 35

The Greenbone Enterprise 35 is designed as a sensor for distributed scan systems.

Fig. 3.4: Hardware sensor

The appliance can only be used in sensor mode and has to be managed via a master appliance. For this reason, it does not have a web interface itself. Appliances from Greenbone Enterprise 400/DECA can be utilized as masters for the Greenbone Enterprise 35.

The appliance comes in a 1U steel chassis. For easy integration into the data center, an optional rackmount kit can be used. The appliance does not come with a display.

For managing the appliance, a serial port is available in addition to a management Ethernet port. The serial port is set up as a Cisco-compatible console port.

To connect to other systems, the appliance comes with four GbE-Base-TX (copper) ports in total. One of these ports is also used as management port.

	Appliance							Sensor
	Greenbone Enterprise 6500	Greenbone Enterprise 5400	Greenbone Enterprise 650 Rev. 2	Greenbone Enterprise 600 Rev. 2	Greenbone Enterprise 450 Rev. 2	Greenbone Enterprise 400 Rev. 2	Greenbone Enterprise 150	Greenbone Enterprise 35
Class/use case	Large enterprises/ service providers	Large enterprises/ service providers	Medium enterprises/ branch offices	Medium enterprises/ branch offices	Medium enterprises/ branch offices	Medium enterprises/ branch offices	Small and medium enterprises/branch offices	Sensor for managed services/branch-office scans
Estimated scan capacity (IP addresses per 24 h)	Up to 15.000	Up to 8.000	Up to 4.000	Up to 2.000	Up to 1.000	Up to 300	Up to 100	Up to 100
Weight	22 kg	22 kg	7 kg	7 kg	7 kg	7 kg	4 kg	4 kg
Dimensions (BxTxH)	480x550x88 mm	480x550x88 mm	480x300x44 mm	480x300x44 mm	480x300x44 mm	480x300x44 mm	480x200x45 mm	480x200x45 mm
Networks								
Management/feed	2 out-of-band management	2 out-of-band management	1	1	1	1	1	1
Scan GbE-Base-TX	0–32 ports	0–32 ports	8 ports	8 ports	8 ports	8 ports	4 ports	4 ports
Scan 1 GbE SFP	0–32 ports	0–32 ports	√	√	√	√	×	×
Scan 10 GbE SFP+	0–8 ports	0–8 ports	2 ports	2 ports	2 ports	2 ports	×	×
Port roles	2 management, others dynamic	2 management, others dynamic	10 ports dynamic	10 ports dynamic	10 ports dynamic	10 ports dynamic	4 ports dynamic	4 ports dynamic
VLAN support	128 per Ethernet port	64 per Ethernet port	64 per Ethernet port	64 per Ethernet port	16 per Ethernet port	16 per Ethernet port	8 per Ethernet port	8 per Ethernet port
Max. routes per network interface	20	20	20	20	16	16	8	8
Hardware								
Fan speed control	×	×	√	√	√	√	√	√
Redundant fan	√	√	√	√	√	√	×	×
Redundant power supply	√	√	×	×	×	×	×	×
Redundant hard disk	√	√	×	×	×	×	×	×
Hot swap power supply	√	√	×	×	×	×	×	×
Hot swap hard disk	√	√	×	×	×	×	×	×
Hot swap fan	√	√	×	×	×	×	×	×
LCD	√	√	√	√	√	√	×	×
Power supplies/outlets	2	2	1	1	1	1	1	1
Max. power consumption per supply	500 W	500 W	300 W	300 W	300 W	300 W	40 W	40 W
Power operation								
Master mode (scan & management)	Up to 80 sensors	Up to 40 sensors	Up to 20 sensors	Up to 12 sensors	Up to 6 sensors	Up to 2 sensors	×	×
Sensor mode (managed via master)	√	√	√	√	√	√	√	√
Airgap master	USB, FTP	USB, FTP	USB, FTP	USB, FTP	USB, FTP	USB, FTP	×	×
Airgap sensor	USB, FTP	USB, FTP	USB, FTP	USB, FTP	USB, FTP	USB, FTP	FTP	×
Features								
SSH v2	√	√	√	√	√	√	√	√
NTP	√	√	√	√	√	√	√	√
GMP (API)	√	√	√	√	√	√	√	×
Web interface (G), report plugins (P), alerts (A), schedules (S)	G, P, A, S	G, P, A, S	G, P, A, S	G, P, A, S	G, P, A, S	G, P, A, S	G, P, A, S	×
LDAP/RADIUS	√	√	√	√	√	√	√	×
SNMP v2	√	√	√	√	√	√	√	√
Syslog (UDP/TCP/TLS)	√	√	√	√	√	√	√	√
IPv6 support	√	√	√	√	√	√	√	√
RAID6	√	√	×	×	×	×	×	×
Certificate management	√	√	√	√	√	√	√	×
Netzwork namespaces	√	√	√	√	√	√	×	×
Remediation workflow	√	√	√	√	√	√	×	×
Backup/restore	Remote/USB, periodic	Remote/USB, periodic	Remote/USB, periodic	Remote/USB, periodic	Remote/USB, periodic	Remote/USB, periodic	USB	×

* The actual achievable number depends on the scan pattern, the scan targets, the network infrastructure and the frequency of scans. The values given for the estimated scan capacity can only be understood as guide values and cannot be guaranteed. Further information can be found in Chapter *20.2* (page 416).

3.2 Virtual Appliances

3.2.1 Medium-Sized Organizations and Branches – Greenbone Enterprise DECA/TERA/PETA/EXA

The Greenbone Enterprise DECA, Greenbone Enterprise TERA, Greenbone Enterprise PETA and Greenbone Enterprise EXA are designed for medium-sized organizations and larger branch offices.

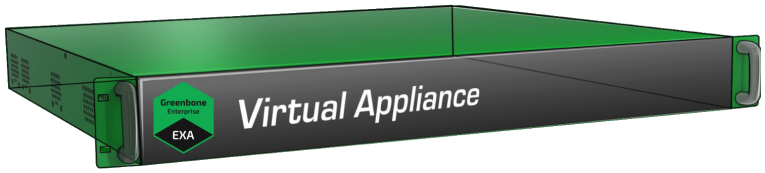


Fig. 3.5: Greenbone Enterprise Appliance for medium-sized organizations

They can control other appliances as sensors and can also be controlled as remote scanners by other appliances.

The appliances can be deployed using VMware ESXi on Microsoft Windows, MacOS and Linux systems.

To connect to other systems, the appliances come with eight dynamic, virtual ports in total in case of the Greenbone Enterprise TERA/PETA/EXA, or with four dynamic, virtual ports in total in case of the Greenbone Enterprise DECA.

One of these ports is also used as management port.

3.2.2 Small Organizations – Greenbone Enterprise CENO

The Greenbone Enterprise CENO is designed for small organizations as well as for small to medium-sized branch offices.

Controlling sensors in other security zones is not considered. However, the Greenbone Enterprise CENO itself can be controlled as a remote scanners by other appliances.

The appliance can be deployed using VMware ESXi on Microsoft Windows, MacOS and Linux systems.

To connect to other systems, the appliance comes with four dynamic, virtual ports in total.

One of these ports is also used as management port.

3.2.3 Sensor – Greenbone Enterprise 25V

The Greenbone Enterprise 25V is designed as a sensor for distributed scan systems.

The appliance can only be used in sensor mode and has to be managed via a master appliance. For this reason, it does not have a web interface itself. Appliances from Greenbone Enterprise 400/DECA can be utilized as masters for the Greenbone Enterprise 25V.

The appliance can be deployed using VMware ESXi on Microsoft Windows, MacOS and Linux systems.

To connect to other systems, the appliance comes with four dynamic, virtual ports in total.

One of these ports is also used as management port.

3.2.4 Training and Audit-via-Laptop – Greenbone Enterprise ONE

The Greenbone Enterprise ONE is designed for special use cases such as audit-via-laptop or trainings. It can neither control other sensors nor be controlled as a sensor by another appliance.

The appliance can be deployed using various virtualization environments. The recommended and supported environment is Oracle VirtualBox.

The appliance comes with one virtual port used for management, scan and updates.

The appliance has all the functions of the appliances for medium-sized and large organizations except for the following:

- Master mode: the Greenbone Enterprise ONE cannot control other appliances as sensors.
- Sensor mode: the Greenbone Enterprise ONE cannot be controlled as a remote scanner by other appliances.
- VLANs: the Greenbone Enterprise ONE does not support VLANs on the virtual port.

Note: The Greenbone Enterprise ONE is optimized for the usage on a mobile computer. Features required for enterprise vulnerability management like remote scan engines are only available on the full-featured appliances.

	Appliance						Sensor
	Greenbone Enterprise EXA	Greenbone Enterprise PETA	Greenbone Enterprise TERA	Greenbone Enterprise DECA	Greenbone Enterprise CENO	Greenbone Enterprise ONE	Greenbone Enterprise 25V
Class/use case	Medium enterprises/branch offices	Medium enterprises/branch offices	Medium enterprises/branch offices	Medium enterprises/branch offices	Small and medium enterprises/branch offices	Special use/training/ audit-via-laptop	Sensor for managed services/branch-office scans
Estimated scan capacity* (IP addresses per 24 h)	Up to 5.000	Up to 2.000	Up to 1.000	Up to 300	Up to 100	Up to 100	Up to 100
Required memory on hypervisor	24 GB	16 GB	8 GB	8 GB	8 GB	6 GB	6 GB
vCPUs	12	8	6	4	2	2	2
Networks							
Virtual ports	8	8	8	4	4	1	4
Port roles	8 ports dynamic	8 ports dynamic	8 ports dynamic	4 ports dynamic	4 ports dynamic	1 port management/ scan/update	4 ports dynamic
Max. routes per network interface	8	8	8	8	8	0	0
Remote operation							
Master mode (scan & management)	Up to 24 sensors	Up to 12 sensors	Up to 6 sensors	Up to 2 sensors	×	×	×
Sensor mode (managed via master)	√	√	√	√	√	×	√
Airgap master	×	×	×	×	×	×	×
Airgap sensor	FTP	FTP	FTP	FTP	FTP	×	×
Open VM tools	√	√	√	√	√	×	√
Supported hypervisors	Microsoft Hyper-V, VMware vSphere Hypervisor (ESXi), Huawei FusionCompute	Microsoft Hyper-V, VMware vSphere Hypervisor (ESXi), Huawei FusionCompute	Microsoft Hyper-V, VMware vSphere Hypervisor (ESXi), Huawei FusionCompute	Microsoft Hyper-V, VMware vSphere Hypervisor (ESXi), Huawei FusionCompute	Microsoft Hyper-V, VMware vSphere Hypervisor (ESXi)	Oracle VirtualBox, VMware Workstation Pro, VMware Workstation Player	Microsoft Hyper-V, VMware vSphere Hypervisor (ESXi), Huawei FusionCompute
Features							
SSH v2	√	√	√	√	√	√	√
NTP	√	√	√	√	√	×	√
GMP (API)	√	√	√	√	√	√	×
Web interface (G), report plugins (P), alerts (A), schedules (S)	G, P, A, S	G, P, A, S	G, P, A, S	G, P, A, S	G, P, A, S	G, P, A, S	×
LDAP/RADIUS	√	√	√	√	√	×	×
SNMP v2	√	√	√	√	√	×	√
Remediation workflow	√	√	√	√	×	×	×
Syslog (UDP/TCP/TLS)	√	√	√	√	√	×	×
IPv6 support	√	√	√	√	√	√	√
Certificate management	√	√	√	√	√	√	×
Backup/restore	Remote, periodic, VM snapshot	Remote, periodic, VM snapshot	Remote, periodic, VM snapshot	Remote, periodic, VM snapshot	Remote, periodic, VM snapshot	VM snapshot	VM snapshot

* The actual achievable number depends on the scan pattern, the scan targets, the network infrastructure and the frequency of scans. The values given for the estimated scan capacity can only be understood as guide values and cannot be guaranteed. Further information can be found in Chapter *20.2* (page 416).

CHAPTER 4

Guideline for Using the Greenbone Enterprise Appliance

The following steps are fundamental in using the Greenbone Enterprise Appliance:

- Setting up the Greenbone Enterprise Appliance → Chapter *5* (page 28)
- Upgrading the Greenbone Operating System to the latest version → Chapters *6* (page 60) and *7.3.4* (page 149)
- Updating the feed → Chapter *7.3.6* (page 150)
- Performing a scan → Chapter *10* (page 208)
- Reading and using a report → Chapter *11.2.1* (page 288)

The following steps are more advanced:

- Performing an authenticated scan → Chapter *10.3* (page 218)
- Using schedules and alerts to automate the scanning process → Chapters *10.10* (page 268) and *10.12* (page 272)
- Using overrides to manage false positives → Chapter *11.8* (page 307)
- Using a master-sensor setup for distributed scanning → Chapter *16* (page 371)

CHAPTER 5

Setting up the Greenbone Enterprise Appliance

5.1 Setup Requirements

5.1.1 Greenbone Enterprise 6500/5400

The Greenbone Enterprise 5400 and Greenbone Enterprise 6500 are 19-inch mountable and require two rack units (RU). Rack holders for the installation in a 19-inch rack are supplied.

For cabling, the Greenbone Enterprise 5400 and Greenbone Enterprise 6500 have corresponding connectors at the front and back:

- **Front**
  - 1 RS-232 serial port, Cisco compatible, suitable cable is enclosed
  - 2 USB 2.0 ports
  - 2 RJ45 Ethernet ports, labeled “MGMT”, for management
  - Up to 4 optional modules with additional Ethernet ports (RJ45, SFP, SFP+ or XFP)
- **Back**
  - 1 VGA port
  - 2 USB 3.0 ports
  - 2 USB 2.0 ports
  - 2 power supplies

The installation requires either a monitor and a keyboard or a serial console connection and a terminal application.

5.1.2 Greenbone Enterprise 650/600/450/400

The Greenbone Enterprise 400, Greenbone Enterprise 450, Greenbone Enterprise 600 and Greenbone Enterprise 650 are 19-inch mountable and require one rack unit (RU). Rack holders for the installation in a 19-inch rack are supplied.

For cabling, the Greenbone Enterprise 400, Greenbone Enterprise 450, Greenbone Enterprise 600 and Greenbone Enterprise 650 have corresponding connectors at the front and back:

- **Front**
  - 1 RS-232 serial port, Cisco compatible, suitable cable is enclosed
  - 2 USB 3.0 ports
  - 6 RJ45 Ethernet ports
  - 2 SFP Ethernet ports
- **Back**
  - 1 VGA port
  - 1 power supply

The installation requires either a monitor and a keyboard or a serial console connection and a terminal application.

5.1.3 Greenbone Enterprise 150

The Greenbone Enterprise 150 is 19-inch mountable and requires one rack unit (RU). The optional RACKMOUNT150 kit provides the rack holders for installing the appliance in a 19-inch rack.

For stand-alone appliances, four self-sticking rubber pads have to be mounted on the corresponding bottom side embossments.

For cabling, the Greenbone Enterprise 150 has corresponding connectors at the front and back:

- **Front**
  - 1 RS-232 serial port, Cisco compatible, suitable cable is enclosed
  - 2 USB 3.0 ports
  - 1 HDMI port
  - 4 RJ45 Ethernet ports
- **Back**
  - 1 power supply

The installation requires either a monitor and a keyboard or a serial console connection and a terminal application.

5.1.4 Greenbone Enterprise 35

The Greenbone Enterprise 35 is 19-inch mountable and requires one rack unit (RU). The optional RACKMOUNT35 kit provides the rack holders for installing the appliance in a 19-inch rack.

For stand-alone appliances, four self-sticking rubber pads have to be mounted on the corresponding bottom side embossments.

For cabling, the Greenbone Enterprise 35 has corresponding connectors at the front and back:

- **Front**
  - 1 RS-232 serial port, Cisco compatible, suitable cable is enclosed
  - 2 USB 3.0 ports
  - 1 HDMI port
  - 4 RJ45 Ethernet ports
- **Back**
  - 1 power supply

The installation requires either a monitor and a keyboard or a serial console connection and a terminal application.

5.1.5 Greenbone Enterprise DECA/TERA/PETA/EXA

This section lists the requirements for successfully deploying a Greenbone Enterprise DECA, Greenbone Enterprise TERA, Greenbone Enterprise PETA or Greenbone Enterprise EXA. All requirements have to be met.

The virtual appliances require and are limited to the following resources:

- Greenbone Enterprise DECA
  - 4 virtual CPUs
  - 8 GB RAM
  - 220 GB virtual hard disk
- Greenbone Enterprise TERA
  - 6 virtual CPUs
  - 8 GB RAM
  - 220 GB virtual hard disk
- Greenbone Enterprise PETA
  - 8 virtual CPUs
  - 16 GB RAM
  - 220 GB virtual hard disk
- Greenbone Enterprise EXA
  - 12 virtual CPUs
  - 24 GB RAM
  - 225 GB virtual hard disk

The following hypervisors are officially supported for running a Greenbone Enterprise DECA/TERA/PETA/EXA:

- Microsoft Hyper-V, version 5.0 or higher

- VMware vSphere Hypervisor (ESXi), version 6.0 or higher
- Huawei FusionCompute, version 8.0

For Microsoft Hyper-V, each Greenbone Enterprise CENO/DECA/TERA/PETA/EXA is delivered as a generation 2 virtual machine.

The required booting mode is the EFI/UEFI boot mode.

5.1.6 Greenbone Enterprise CENO

This section lists the requirements for successfully deploying a Greenbone Enterprise CENO. All requirements have to be met.

The virtual appliance requires and is limited to the following resources:

- 2 virtual CPUs
- 8 GB RAM
- 135 GB virtual hard disk

The following hypervisors are officially supported for running a Greenbone Enterprise CENO:

- Microsoft Hyper-V, version 5.0 or higher
- VMware vSphere Hypervisor (ESXi), version 6.0 or higher

For Microsoft Hyper-V, each Greenbone Enterprise CENO/DECA/TERA/PETA/EXA is delivered as a generation 2 virtual machine.

The required booting mode is the EFI/UEFI boot mode.

5.1.7 Greenbone Enterprise 25V

This section lists the requirements for successfully deploying a Greenbone Enterprise 25V. All requirements have to be met.

The virtual appliance requires and is limited to the following resources:

- 2 virtual CPUs
- 6 GB RAM
- 70 GB virtual hard disk

The following hypervisors are officially supported for running a Greenbone Enterprise 25V:

- Microsoft Hyper-V, version 5.0 or higher
- VMware vSphere Hypervisor (ESXi), version 6.0 or higher
- Huawei FusionCompute, version 8.0

For Microsoft Hyper-V, each Greenbone Enterprise 25V is delivered as a generation 2 virtual machine.

The required booting mode is the EFI/UEFI boot mode.

5.1.8 Greenbone Enterprise ONE

This section lists the requirements for successfully deploying a Greenbone Enterprise ONE. All requirements have to be met.

The virtual appliance requires and is limited to the following resources:

- 2 virtual CPUs
- 6 GB RAM
- 130 GB virtual hard disk

The following hypervisors are officially supported for running a Greenbone Enterprise ONE:

- Oracle VirtualBox, version 6.1 or higher
- VMware Workstation Player, version 16.0 or higher
- VMware Workstation Pro, version 16.0 or higher

The required booting mode is the EFI/UEFI boot mode.

5.2 Setting up a Hardware Appliance

Note: The requirements for installing the appliance can be found in Chapter *5.1* (page 28).

5.2.1 Utilizing the Serial Port

The enclosed console cable is used for utilizing the serial port. Alternatively, a blue Cisco console cable (rollover cable) can be used.

To access the serial port, a terminal application is required. The application must be configured to a speed of 9600 bits/s (Baud).

Under Linux, the command `screen` can be used in the command line to access the serial port. The device providing the serial port must be passed as a parameter:

```
screen /dev/ttyS0  #(for serial port)
screen /dev/ttyUSB0 #(for USB adapter)
```

Tip: After starting screen, it may be necessary to press `Enter` several times to see a command prompt.

To close the serial connection, press `Ctrl` + `a` and immediately afterwards `\`.

In Microsoft Windows, PuTTY[3] can be used. After starting it, the options as shown in Fig. 5.1 and the appropriate serial port must be selected.

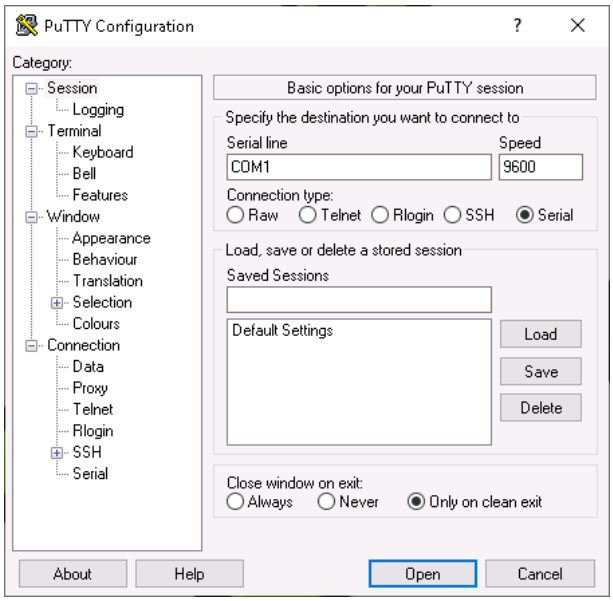


Fig. 5.1: Setting up the serial port in PuTTY

[3] https://www.chiark.greenend.org.uk/~sgtatham/putty/

5.2.2 Starting the Appliance

Once the appliance is fully wired, a connection to the appliance using the console cable is achieved and the terminal application (PuTTY, screen or similar) is set up, the appliance can be started.

The appliance will boot and after a short time – depending on the exact model – the login prompt is shown. The default login information is:

- User: `admin`
- Password: `admin`

Note: During the first setup, this password should be changed (see Chapter *7.2.1.1* (page 72)).

5.2.3 Performing a General System Setup

All appliances share the same way of basic configuration and readiness check.

When the appliance is delivered by Greenbone or after a factory reset, the GOS administration menu shows the first setup wizard after logging in to assist with the basic GOS configuration (see Fig. 5.2).

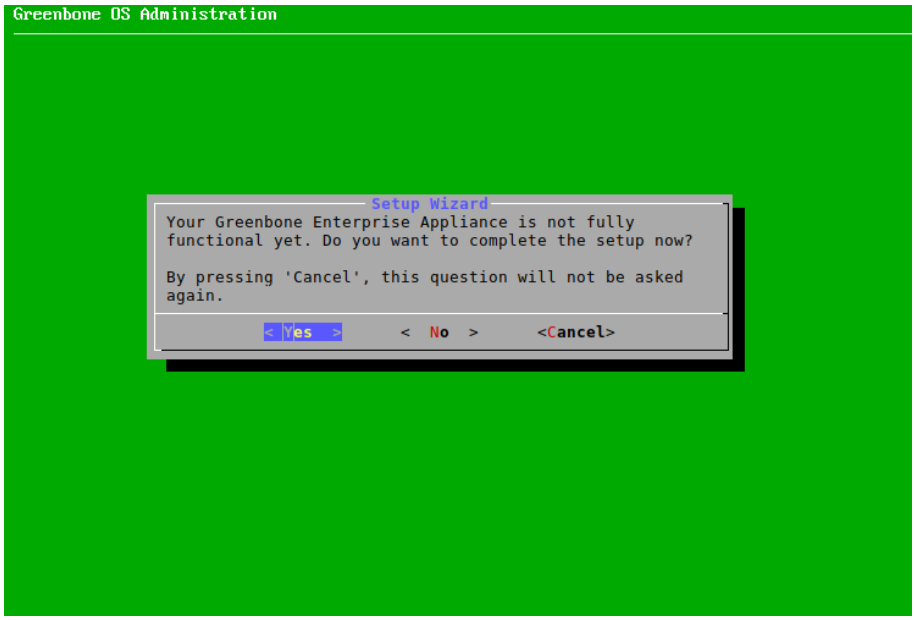


Fig. 5.2: Using the first setup wizard

By selecting *Yes* and pressing `Enter` the first setup wizard is opened.

Note: By selecting *No* and pressing `Enter` the wizard can be closed. Incomplete steps are displayed when logging in again.

By selecting *Cancel* and pressing `Enter` the wizard can be closed as well. However, in this case, incomplete steps are not displayed again.

The first setup wizard is dynamic and shows only those steps necessary to operate the used appliance model. In the following, all possible steps are mentioned but they may not appear in every case.

In case of a factory reset, all steps have to be carried out (see *20.10* (page 421)).

Every step can be skipped by selecting *Skip* or *No* and pressing `Enter`. Skipped steps are displayed when logging in again.

5.2.3.1 Configuring the Network

The network must be set up for the appliance to be fully functional. If there is no IP address configured, it is asked whether the network settings should be adjusted (see Fig. 5.3).

Note: When using DHCP, the appliance does not transmit the MAC address but a DHCP Unique ID (DUID). While this should not pose a problem with modern DHCP servers, some older DHCP servers (e.g., Windows Server 2012) may not be able to handle it.

One possible solution is to specify the DUID instead of the MAC address on the DHCP server. Alternatively, a static IP address can be used on the appliance.

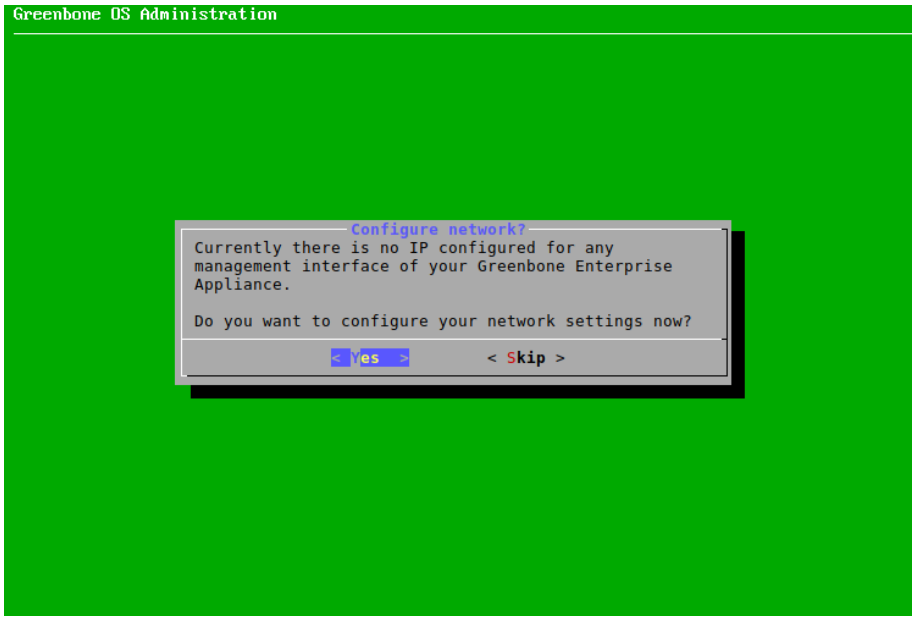


Fig. 5.3: Configuring the network settings

1. Select *Yes* and press `Enter`.
2. Select *Interfaces* and press `Enter`.

3. Select the desired interface and press `Enter`.

   → The interface can be configured.

4. If DHCP should be used, select *DHCP* (for IPv4 or IPv6) and press `Enter` (see Fig. 5.4).

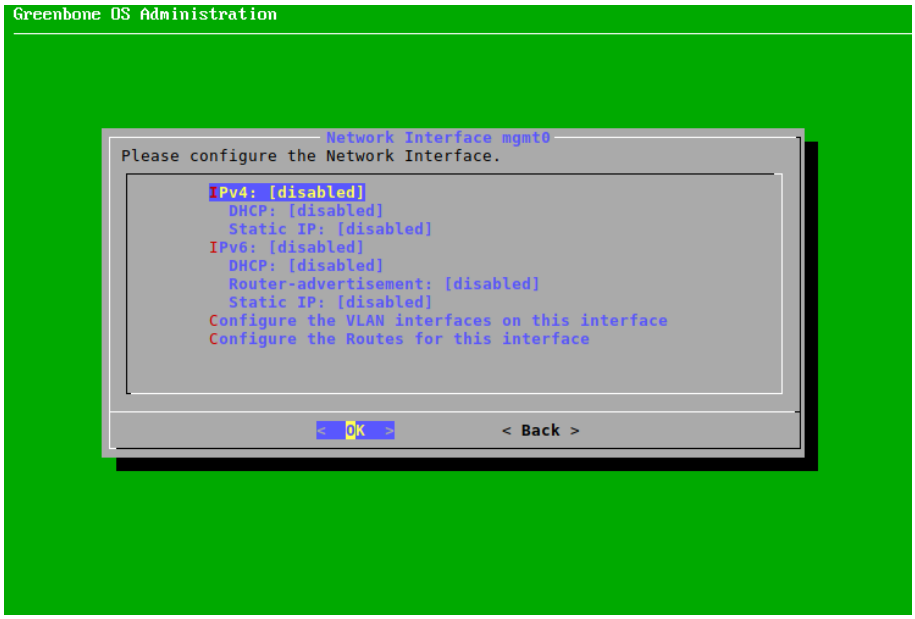


Fig. 5.4: Configuring the network interface

5. Select *Save* and press `Enter`.
6. Select *Back* and press `Enter`.
7. Select *Back* and press `Enter`.
8. Select *Ready* and press `Enter`.

   or

4. If a static IP address should be used, select *Static IP* (for IPv4 or IPv6) and press `Enter`.
5. Enter the IP address including the prefix length in the input box (see Fig. 5.5).
6. Press `Enter`.

   → A message informs that the changes have to be saved.

7. Press `Enter` to close the message.
8. Select *Save* and press `Enter`.
9. Select *Back* and press `Enter`.
10. Select *Back* and press `Enter`.
11. Select *Ready* and press `Enter`.

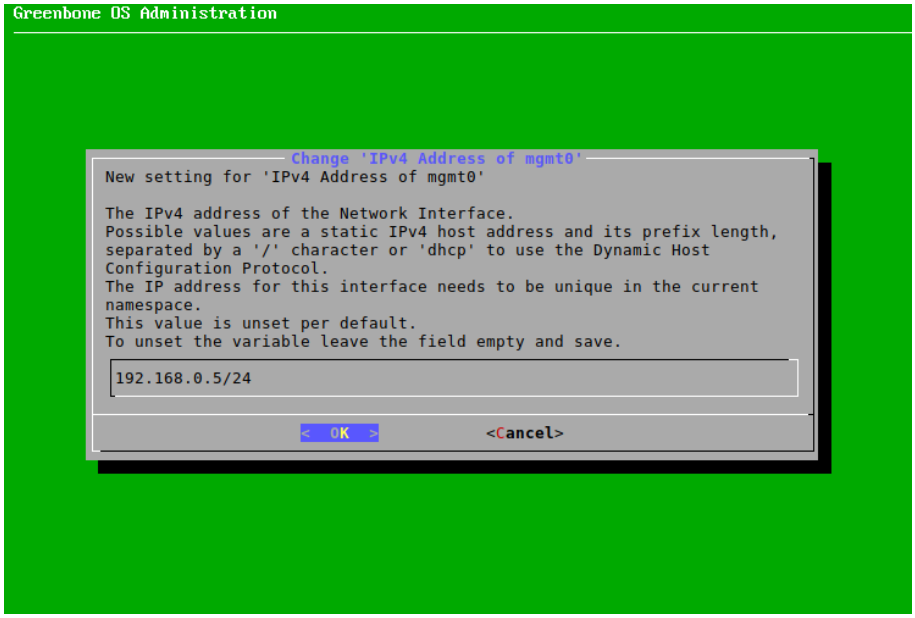


Fig. 5.5: Entering a static IP address

5.2.3.2 Importing or Generating an HTTPS Certificate

An HTTPS certificate must present on the appliance to use the web interface securely. The certificate can be imported or generated as follows:

1. Select *Import* and press `Enter` (see Fig. 5.6).

   → A message informs that a PKCS#12 file can be imported.

2. Select *Continue* and press `Enter`.
3. Open the web browser and enter the displayed URL.
4. Click *Browse...*, select the PKCS#12 file and click *Upload*.

   → When the certificate is retrieved by the appliance, the GOS administration menu displays the fingerprint of the certificate for verification.

5. Check the fingerprint and confirm the certificate by pressing `Enter`.

   or

1. Select *Generate* and press `Enter`.

   → A message informs that parameters have to be entered to generate the certificate.

2. Select *Continue* and press `Enter`.

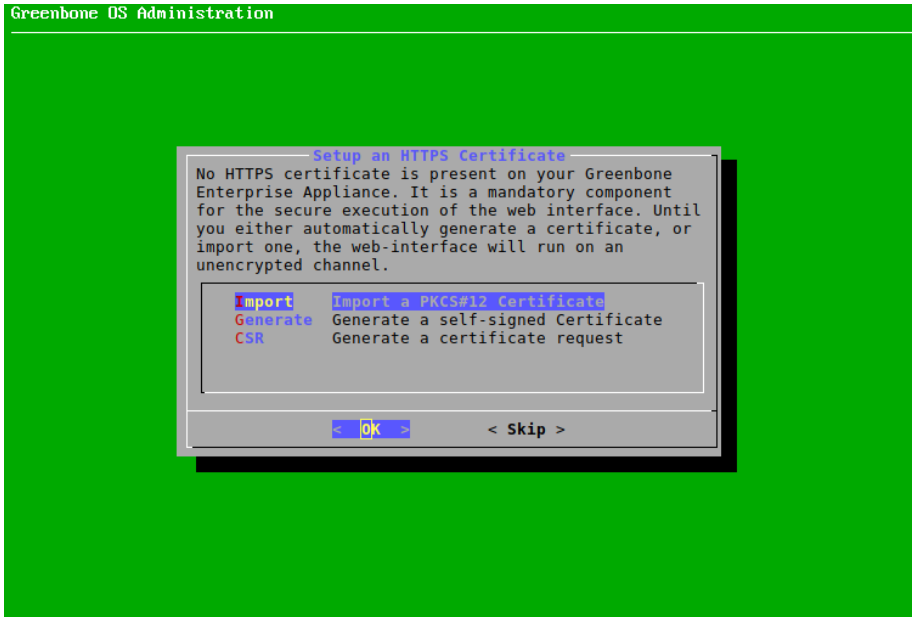


Fig. 5.6: Importing or generating an HTTPS certificate

3. Provide the settings for the certificate (see Fig. 5.7).

Note: It is valid to generate a certificate without a common name. However, a certificate should not be created without (a) Subject Alternative Name(s).

If a common name is used, it should be the same as one of the SANs.

---

4. Select *OK* and press `Enter`.

   → A message informs that the certificate is created and can be downloaded (see Fig. 5.8).

Note: The download is not done in the first setup wizard, but in the later GOS administration menu as described in Chapter *7.2.4.1.7.1* (page 102), steps 1–4 and 9–13.

---

or

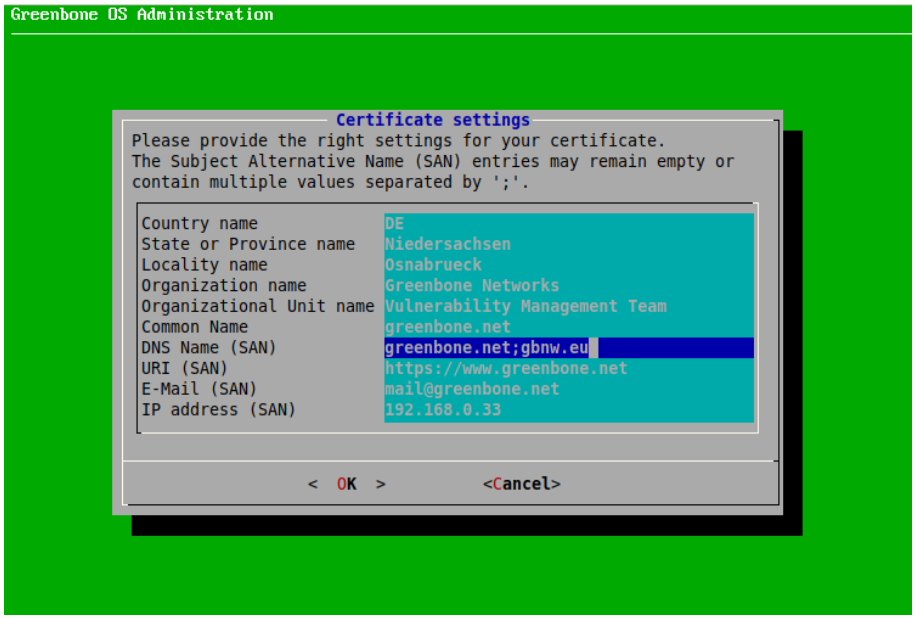


Fig. 5.7: Entering information for the certificate

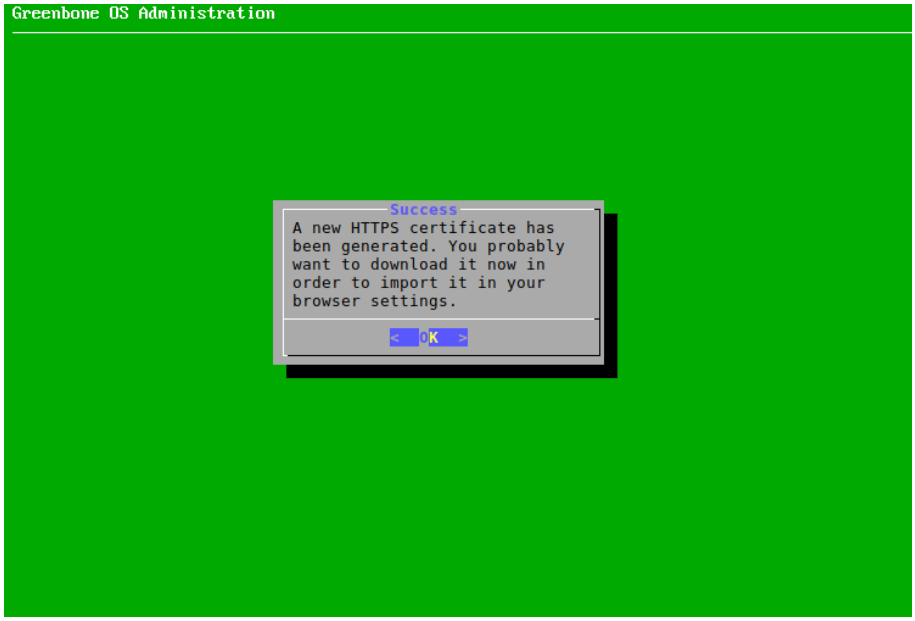


Fig. 5.8: Completing the HTTPS certificate

1. Select *CSR* and press `Enter`.

   → A message informs that a key pair and a certificate request are created.

2. Select *Continue* and press `Enter`.
3. Provide the settings for the certificate.

   Note: It is valid to generate a certificate without a common name. However, a certificate should not be created without (a) Subject Alternative Name(s).

   If a common name is used, it should be the same as one of the SANs.

4. Select *OK* and press `Enter`.
5. Open the web browser and enter the displayed URL.
6. Download the PEM file.

   → The GOS administration menu displays a message to verify that the CSR has not been tampered with.

7. Verify the information by pressing `Enter`.

   Note: When the certificate is signed, it has to be uploaded to the appliance. The upload is not done in the first setup wizard, but in the later GOS administration menu as described in Chapter *7.2.4.1.7.2* (page 104), steps 1–4 and 11–14.

5.2.3.3 Creating a Web Administrator

If there is no web administrator, it is asked whether such an account should be created (see Fig. 5.9).

Note: A web administrator is required to use the web interface of the appliance.

The first web administrator (web user) that is created is automatically the Feed Import Owner (see Chapter *7.2.1.10* (page 80)).

1. Select *Yes* and press `Enter`.
2. Enter the user name for the web administrator.

   Note: Only the following characters are allowed for the user name:

   - All alphanumeric characters
   - - (dash)
   - _ (underscore)
   - . (full stop)

3. Enter the password for the web administrator twice.

   Note: The password can contain any type of character and can be at most 30 characters long.

   When using special characters, note that these must be available on all used keyboards and correctly supported by all client software and operating systems. Copying and pasting special characters for passwords can lead to invalid passwords depending on these external factors.

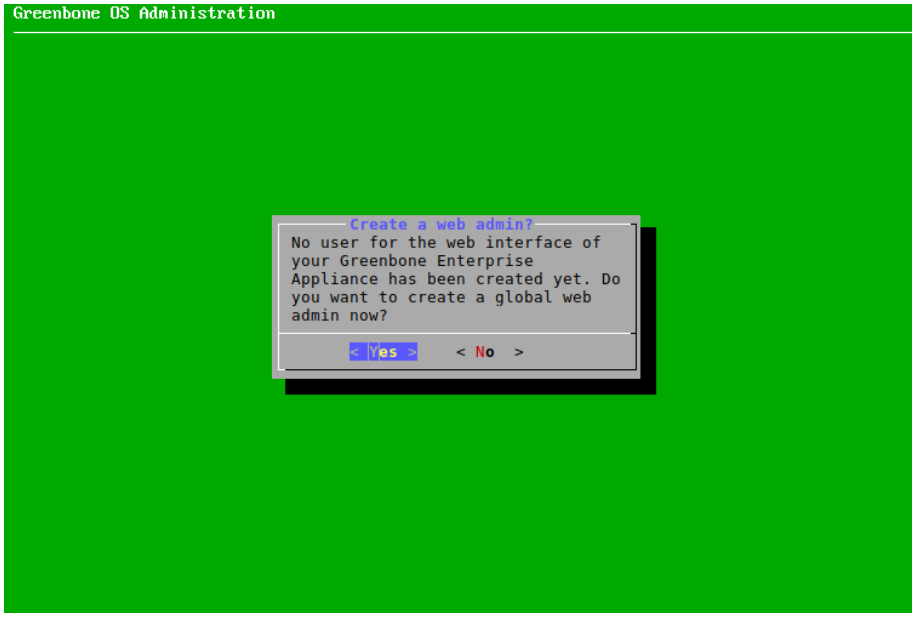


Fig. 5.9: Creating a web administrator

4. Select *OK* and press `Enter`.

   → A message informs that the web administrator has been created.

5. Press `Enter` to close the message.

5.2.3.4 Entering or Uploading a Greenbone Enterprise Feed Subscription Key

If no valid subscription key is stored on the appliance, the appliance only uses the public Greenbone Community Feed and not the Greenbone Enterprise Feed.

Note: It is not necessary to add a Greenbone Enterprise Feed subscription key on a newly delivered appliance since a key is already pre-installed.

A subscription key can be entered or uploaded as follows:

1. Select *Editor* and press `Enter` (see Fig. 5.10).

   → The editor is opened.

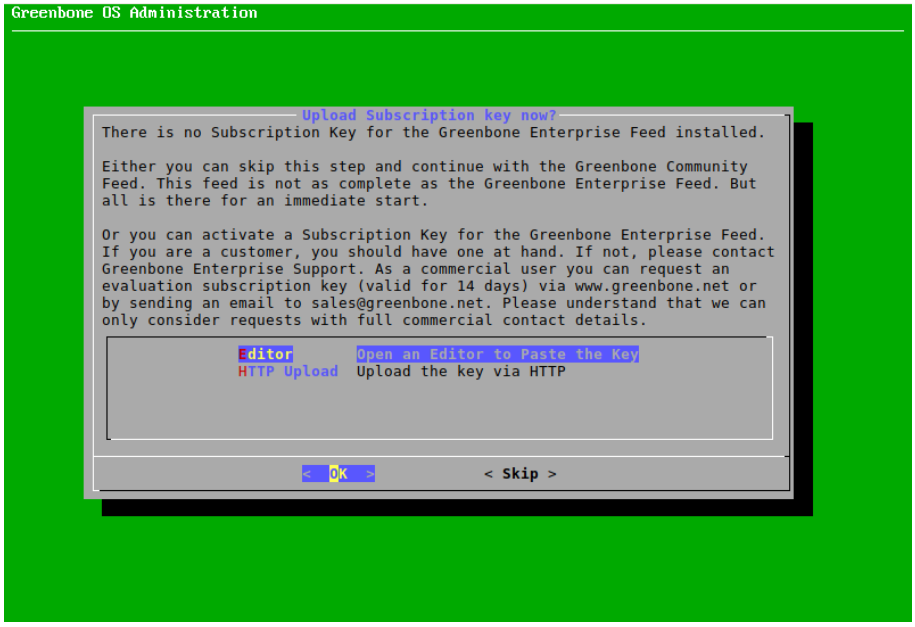


Fig. 5.10: Entering or uploading a subscription key

2. Enter the subscription key.
3. Press `Ctrl` + `S` to save the changes.
4. Press `Ctrl` + `X` to close the editor.

   or

1. Select *HTTP Upload* and press `Enter`.
2. Open the web browser and enter the displayed URL.
3. Click *Browse. . .*, select the subscription key and click *Upload*.

5.2.3.5 Downloading the Feed

If no feed is present on the appliance, the feed can be downloaded as follows:

1. Select *Yes* and press `Enter` (see Fig. 5.11).

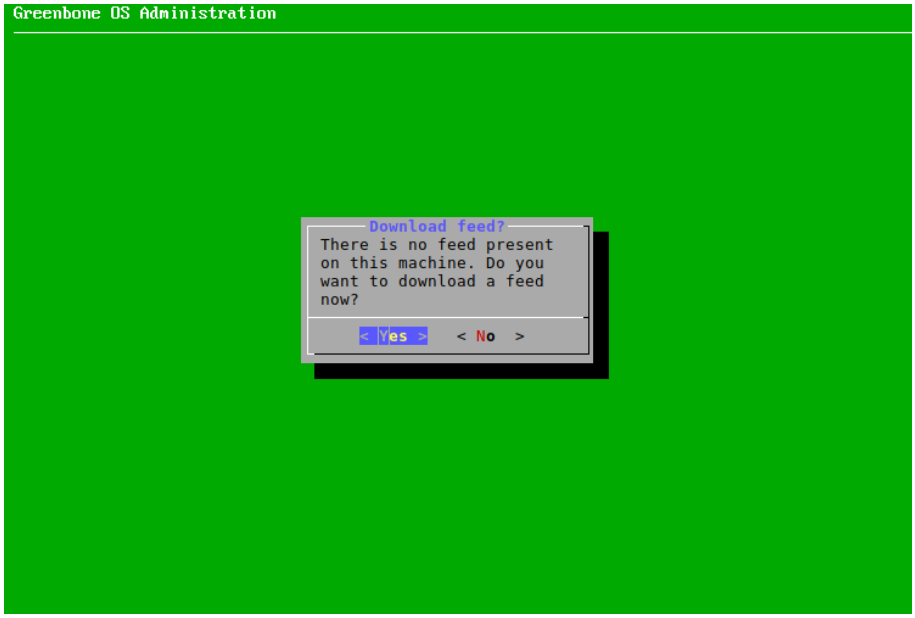


Fig. 5.11: Downloading the feed

   → A message informs that the feed update was started in the background (see Fig. 5.12).

2. Press `Enter` to close the message.

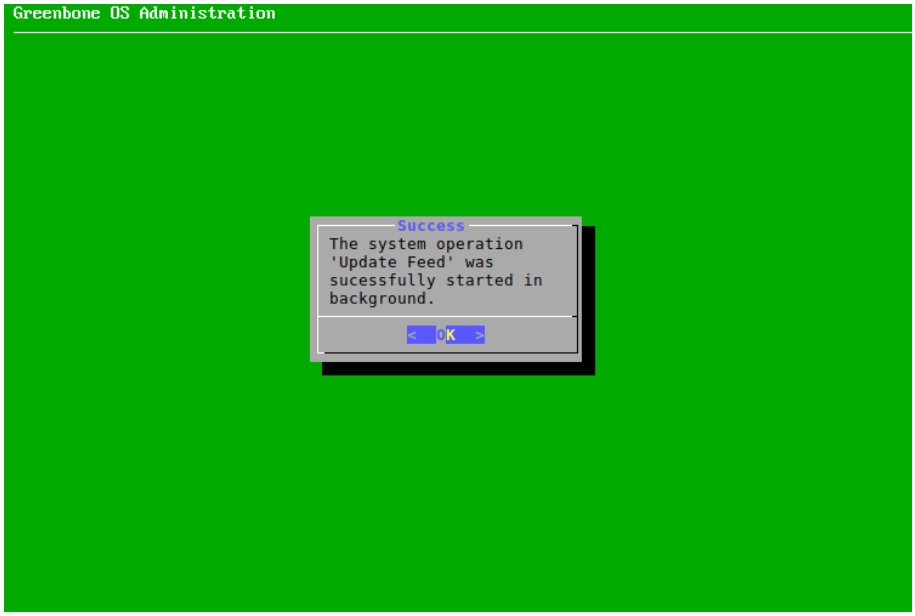


Fig. 5.12: Downloading the feed

5.2.3.6 Finishing the First Setup Wizard

Note: After the last step, a status check is performed.

1. When the check is finished, press `Enter`.

   → The results of the check are displayed (see Fig. 5.13).

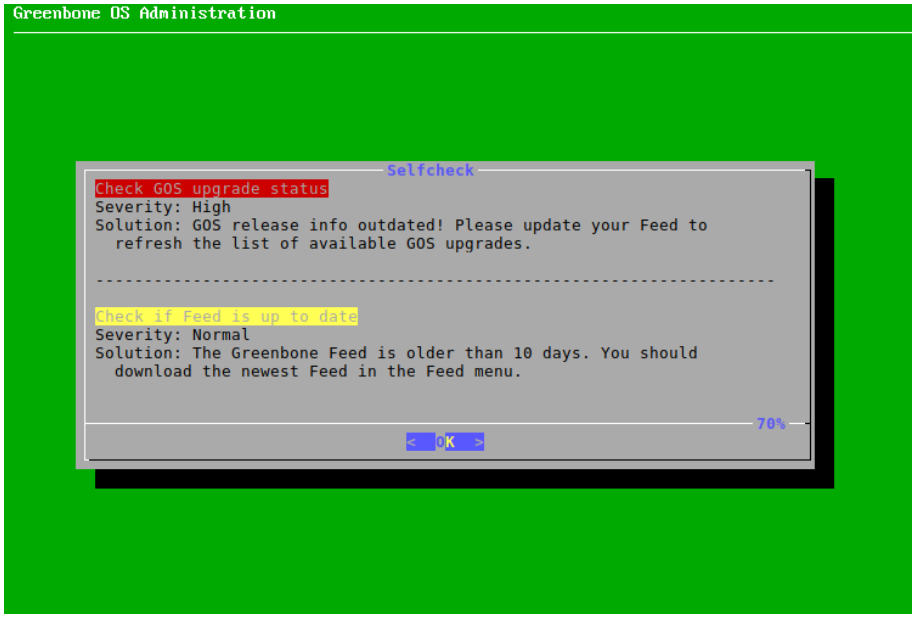


Fig. 5.13: Result of the status check

2. Press `Enter`.

   → The GOS administration menu can be used as described in Chapter *7* (page 67).

If there are any unfinished or skipped steps, the first setup wizard is shown when logging in again.

5.2.4 Logging into the Web Interface

Note: This step does not apply for the Greenbone Enterprise 35.

The main interface of the appliance is the web interface, also called Greenbone Security Assistant (GSA). The web interface can be accessed as described in Chapter *8.1* (page 163).

5.3 Setting up a Virtual Appliance

Note: The requirements for installing the appliance can be found in Chapter *5.1* (page 28).

5.3.1 Verification of Integrity

Note: The integrity of the virtual appliance can be verified. On request, the Greenbone Enterprise Support provides an integrity checksum.

To request the checksum, contact the Greenbone Enterprise Support[4] including the subscription number.

The integrity checksum can be provided via phone or via support portal[5].

The local verification of the checksum depends on the host operating system.

On Linux systems, the following command for calculating the checksum can be used:

```
sha256sum <file>
```

Note: Replace `<file>` with the name of the appliance's OVA file.

On Microsoft Windows systems, the following command for calculating the checksum can be used in the Windows PowerShell:

```
Get-Filehash 'C:\<path>\<file>' -Algorithm SHA256
```

Note: Replace `<path>` and `<file>` with the path and the name of the appliance's OVA file.

If the checksum does not match the checksum provided by the Greenbone Enterprise Support, the virtual appliance has been modified and should not be used.

5.3.2 Deploying the Appliance

5.3.2.1 VMware vSphere/ESXi

The virtual appliance is provided by Greenbone in the Open Virtualization Appliance (OVA) format.

Each appliance is activated using a unique subscription key.

Note: Cloning the appliance and using several instances in parallel is not permitted and can result in inconsistencies and unwanted side effects.

[4] https://www.greenbone.net/en/technical-support/
[5] https://jira.greenbone.net/servicedesk/customer/user/login?destination=portals

To deploy an appliance, it has to be imported into the hypervisor of choice as follows:

Note: The example features VMware ESXi, but is also applicable for VMware vCenter.

The figures show the installation of a Greenbone Enterprise TERA. The installation of another appliance model is carried out equivalently. File names used in the example differ based on the appliance model and the subscription key.

1. Open the web interface of the VMware ESXi instance and log in.
2. Click *Virtual Machines* in the *Navigator* column on the left.
3. Click *Create / Register VM*.
4. Select *Deploy a virtual machine from an OVF or OVA file* and click *Next* (see Fig. 5.14).

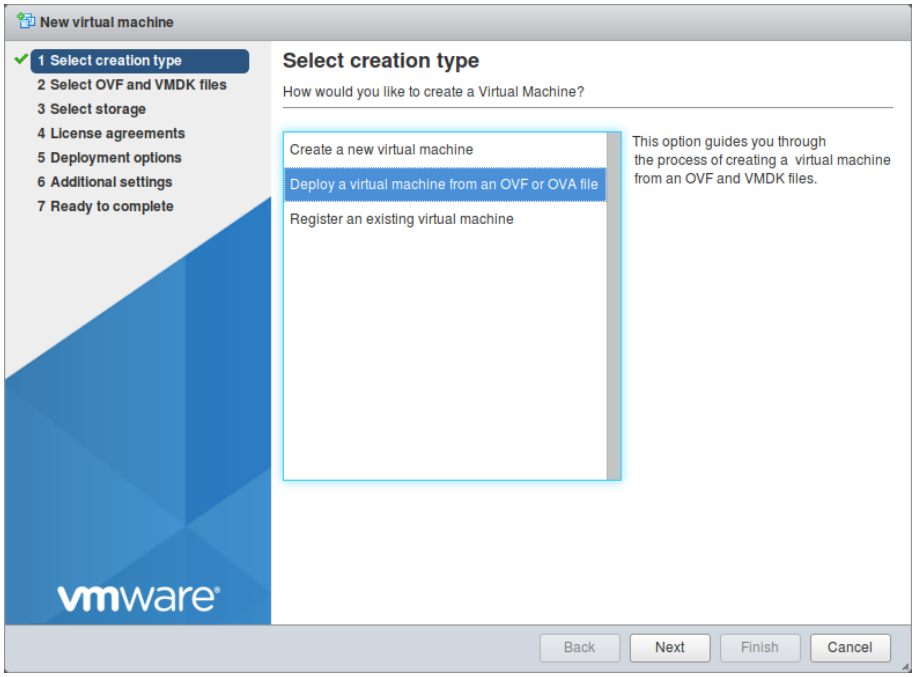


Fig. 5.14: Selecting the creation type

5. Enter a name for the virtual machine in the input box.
6. Click *Click to select files or drag/drop*, select the OVA file of the appliance and click *Next*.
7. Select the storage location in which to store the virtual machine files and click *Next*.
8. Adjust the deployment options as required and click *Next*.

Note: The default deployment settings may be used.

9. Check the configuration of the virtual machine (see Fig. 5.15).

Tip: Settings can be changed by clicking *Back* and adjusting them in the respective dialog.

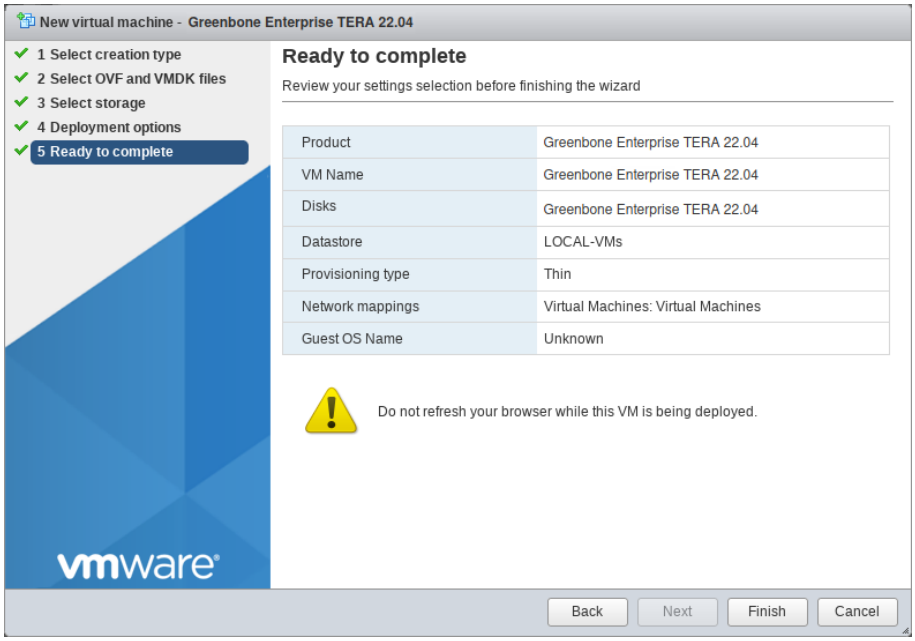


Fig. 5.15: Checking the configuration of the virtual machine

10. Click *Finish*.

    → The appliance is being imported. This can take up to 10 minutes.

Important: Do not refresh the browser while the virtual machine is being deployed.

11. When the appliance is imported, click *Virtual Machines* in the *Navigator* column on the left.
12. Select the appliance in the list and click *Power on* (see Fig. 5.16).

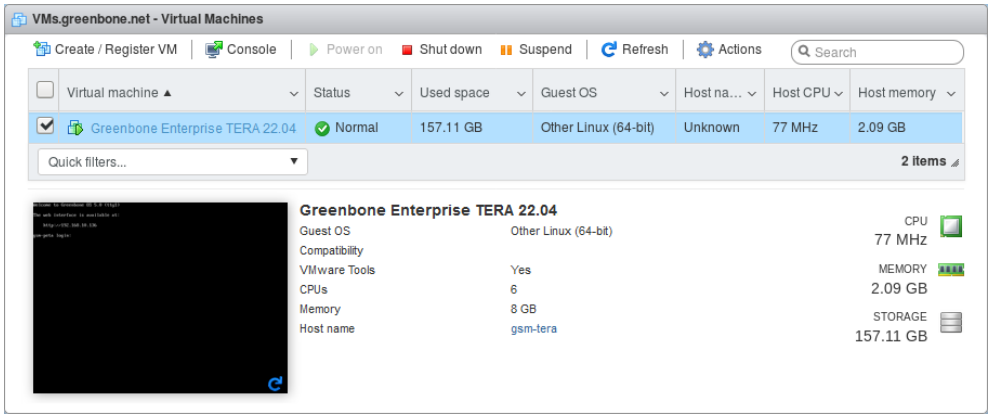


Fig. 5.16: Imported virtual machine

→ The appliance will boot and after a short time – depending on the exact model – the login prompt is shown.

13. Log in using the default login information:
    - User: `admin`
    - Password: `admin`

    Note: During the first setup, this password should be changed (see Chapter *7.2.1.1* (page 72)).

5.3.2.2 Oracle VirtualBox

The virtual appliance is provided by Greenbone in the Open Virtualization Appliance (OVA) format.

Each appliance is activated using a unique subscription key.

Note: Cloning the appliance and using several instances in parallel is not permitted and can result in inconsistencies and unwanted side effects.

To deploy an appliance, it has to be imported into the hypervisor of choice as follows:

Note: File names used in the example differ based on the subscription key.

1. Install Oracle VirtualBox for the current operating system.

   Note: VirtualBox is often included with Linux distributions.

   Should this not be the case and or a version of Microsoft Windows is used, VirtualBox is available at https://www.virtualbox.org/wiki/Downloads.

2. Start VirtualBox.
3. Select *File > Import Appliance...* in the menu bar.
4. Click and select the OVA file of the appliance (see Fig. 5.17).
5. Check the configuration of the virtual machine in the window *Appliance settings* (see Fig. 5.17).

   Values can be changed by double clicking into the input box of the respective value.
6. Click *Import*.

   → The appliance is being imported. This can take up to 10 minutes.

   When the appliance is imported, it is displayed in the left column in VirtualBox.

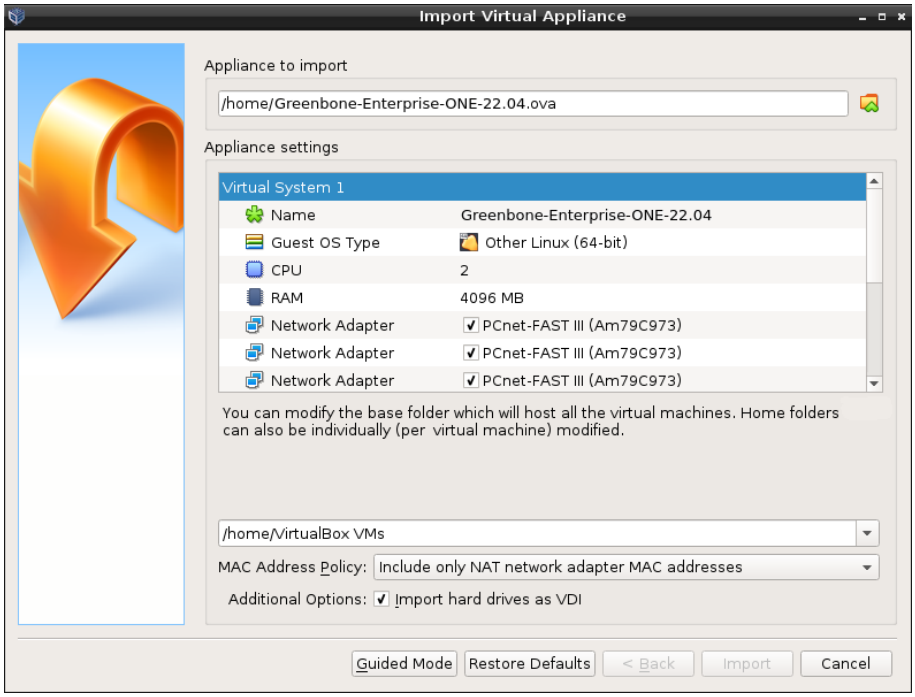


Fig. 5.17: Importing the OVA file of the appliance

7. Select the appliance in the list and click *Start*.

   → The appliance will boot and after a short time – depending on the exact model – the login prompt is shown.

8. Log in using the default login information:

   - User: `admin`
   - Password: `admin`

Note: During the first setup, this password should be changed (see Chapter *7.2.1.1* (page 72)).

5.3.3 Performing a General System Setup

All appliances share the same way of basic configuration and readiness check.

When the appliance is delivered by Greenbone or after a factory reset, the GOS administration menu shows the first setup wizard after logging in to assist with the basic GOS configuration (see Fig. 5.18).

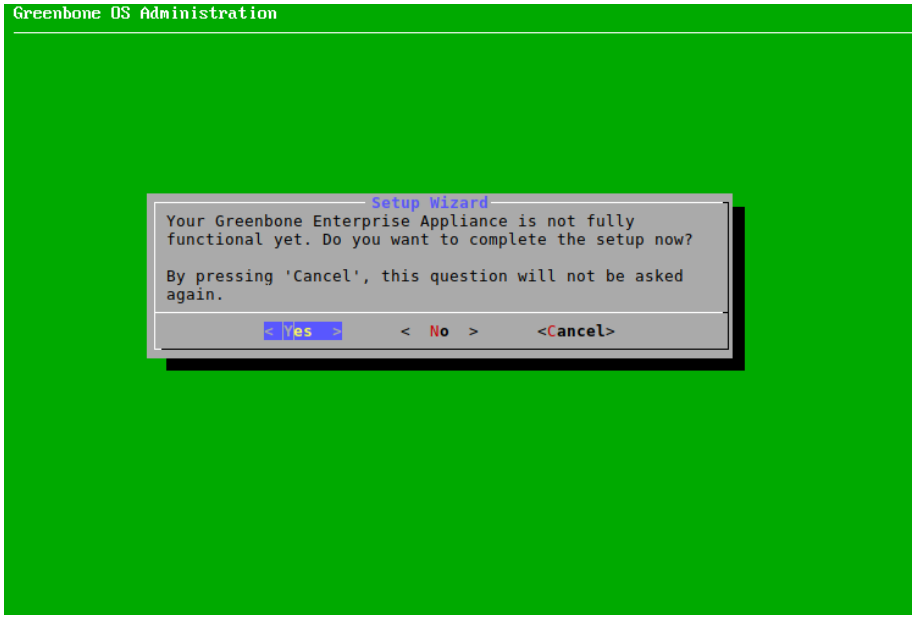


Fig. 5.18: Using the first setup wizard

By selecting *Yes* and pressing `Enter` the first setup wizard is opened.

Note: By selecting *No* and pressing `Enter` the wizard can be closed. Incomplete steps are displayed when logging in again.

By selecting *Cancel* and pressing `Enter` the wizard can be closed as well. However, in this case, incomplete steps are not displayed again.

The first setup wizard is dynamic and shows only those steps necessary to operate the used appliance model. In the following, all possible steps are mentioned but they may not appear in every case.

In case of a factory reset, all steps have to be carried out (see *20.10* (page 421)).

Every step can be skipped by selecting *Skip* or *No* and pressing `Enter`. Skipped steps are displayed when logging in again.

5.3.3.1 Configuring the Network

Note: Other than hardware appliances, virtual appliances have DHCP enabled for the eth0 interface as a factory setting. Therefore, the step of configuring the network is omitted here.

5.3.3.2 Importing or Generating an HTTPS Certificate

An HTTPS certificate must be present on the appliance to use the web interface securely. The certificate can be imported or generated as follows:

1. Select *Import* and press `Enter` (see Fig. 5.19).

   → A message informs that a PKCS#12 file can be imported.

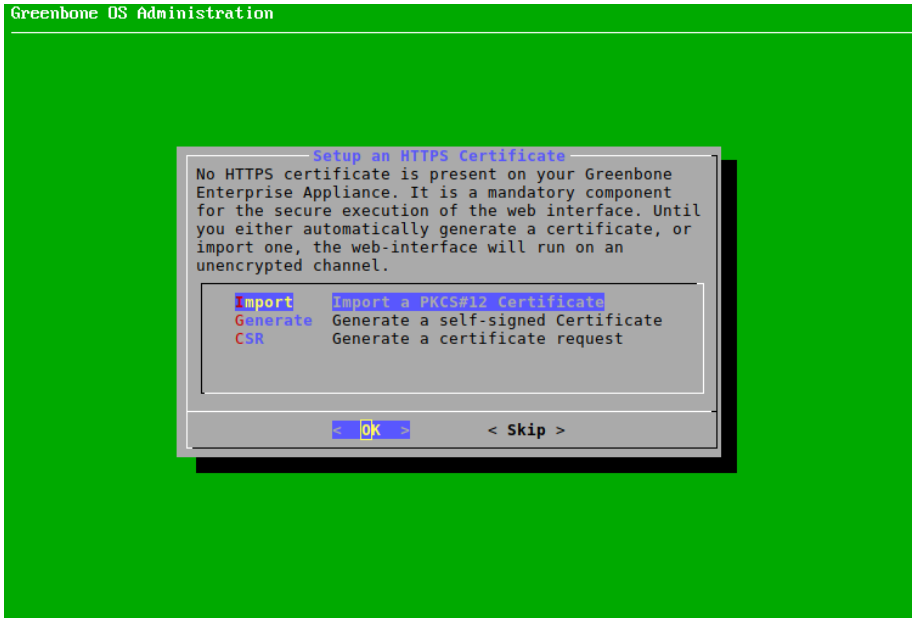


Fig. 5.19: Importing or generating an HTTPS certificate

2. Select *Continue* and press `Enter`.
3. Open the web browser and enter the displayed URL.
4. Click *Browse...*, select the PKCS#12 file and click *Upload*.

   → When the certificate is retrieved by the appliance, the GOS administration menu displays the fingerprint of the certificate for verification.

5. Check the fingerprint and confirm the certificate by pressing `Enter`.

   or

1. Select *Generate* and press `Enter`.

   → A message informs that parameters have to be entered to generate the certificate.

2. Select *Continue* and press `Enter`.
3. Provide the settings for the certificate (see Fig. 5.20).

Note: It is valid to generate a certificate without a common name. However, a certificate should not be created without (a) Subject Alternative Name(s).

If a common name is used, it should be the same as one of the SANs.

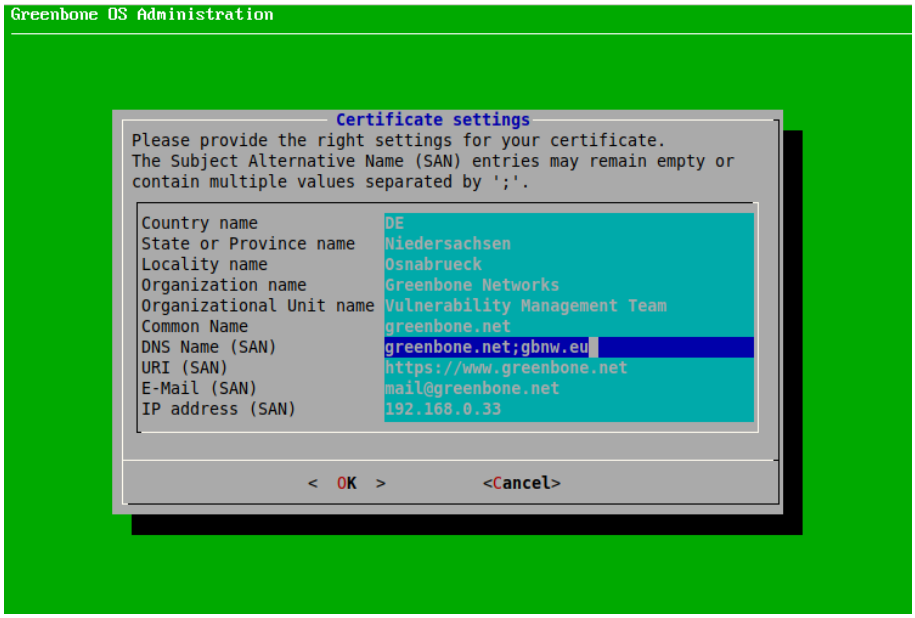


Fig. 5.20: Entering information for the certificate

4. Select *OK* and press `Enter`.

   → A message informs that the certificate is created and can be downloaded (see Fig. 5.21).

Note: The download is not done in the first setup wizard, but in the later GOS administration menu as described in Chapter *7.2.4.1.7.1* (page 102), steps 1 – 4 and 9 – 13.

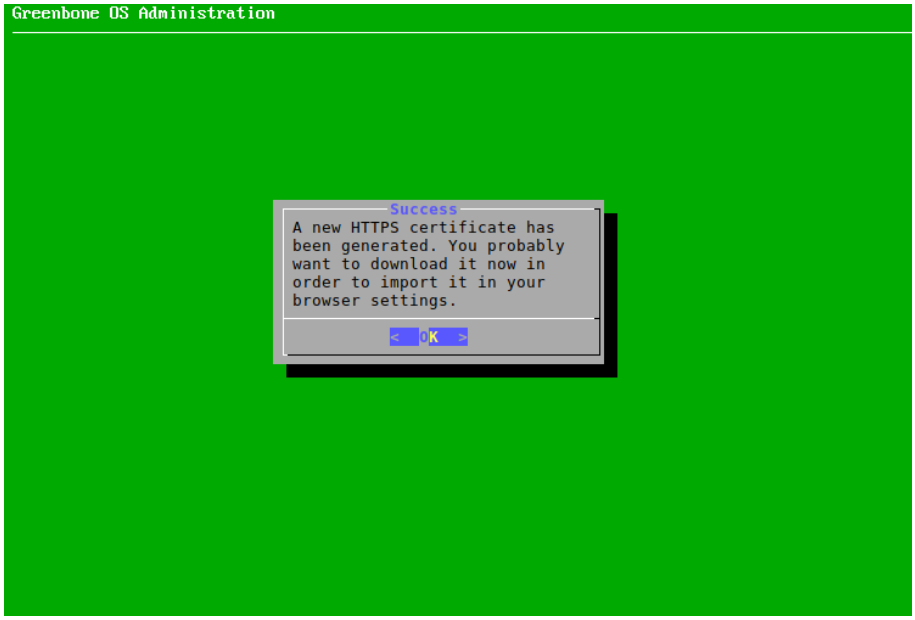


Fig. 5.21: Completing the HTTPS certificate

or

1. Select *CSR* and press `Enter`.

   → A message informs that a key pair and a certificate request are created.

2. Select *Continue* and press `Enter`.
3. Provide the settings for the certificate.

   Note: It is valid to generate a certificate without a common name. However, a certificate should not be created without (a) Subject Alternative Name(s).

   If a common name is used, it should be the same as one of the SANs.

4. Select *OK* and press `Enter`.
5. Open the web browser and enter the displayed URL.
6. Download the PEM file.

   → The GOS administration menu displays a message to verify that the CSR has not been tampered with.

7. Verify the information by pressing `Enter`.

   Note: When the certificate is signed, it has to be uploaded to the appliance. The upload is not done in the first setup wizard, but in the later GOS administration menu as described in Chapter *7.2.4.1.7.2* (page 104), steps 1 – 4 and 11 – 14.

5.3.3.3 Creating a Web Administrator

If there is no web administrator, it is asked whether such an account should be created (see Fig. 5.22).

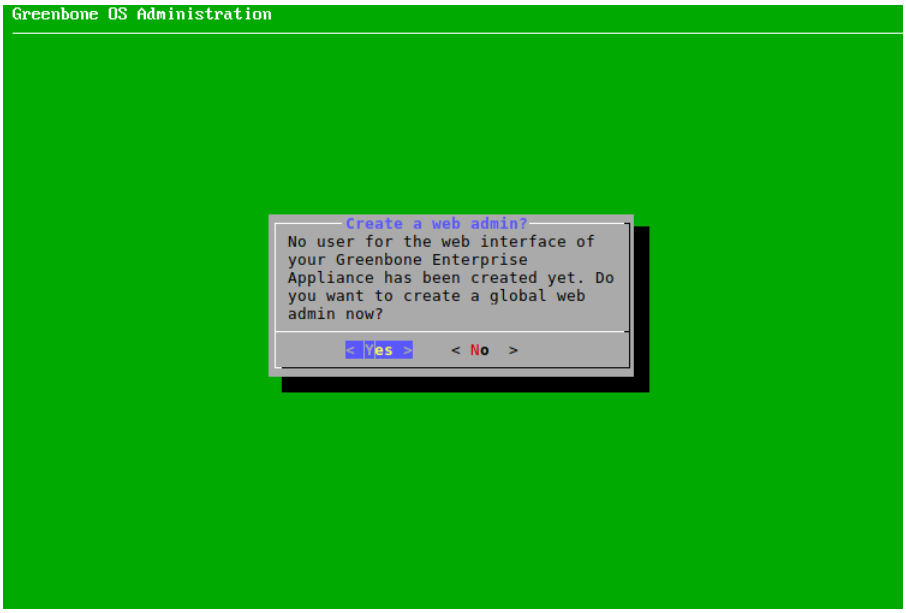


Fig. 5.22: Creating a web administrator

Note: A web administrator is required to use the web interface of the appliance.

The first web administrator (web user) that is created is automatically the Feed Import Owner (see Chapter *7.2.1.10* (page 80)).

---

1. Select *Yes* and press `Enter`.
2. Enter the user name for the web administrator.

   Note: Only the following characters are allowed for the user name:

   - All alphanumeric characters
   - - (dash)
   - _ (underscore)
   - . (full stop)

   ---

3. Enter the password for the web administrator twice.

   Note: The password can contain any type of character and can be at most 30 characters long.

   When using special characters, note that these must be available on all used keyboards and correctly supported by all client software and operating systems. Copying and pasting special characters for passwords can lead to invalid passwords depending on these external factors.

   ---

4. Select *OK* and press `Enter`.

   → A message informs that the web administrator has been created.

5. Press `Enter` to close the message.

5.3.3.4 Entering or Uploading a Greenbone Enterprise Feed Subscription Key

If no valid subscription key is stored on the appliance, the appliance only uses the public Greenbone Community Feed and not the Greenbone Enterprise Feed.

Note: It is not necessary to add a Greenbone Enterprise Feed subscription key on a newly delivered appliance since a key is already pre-installed.

A subscription key can be entered or uploaded as follows:

1. Select *Editor* and press `Enter` (see Fig. 5.23).

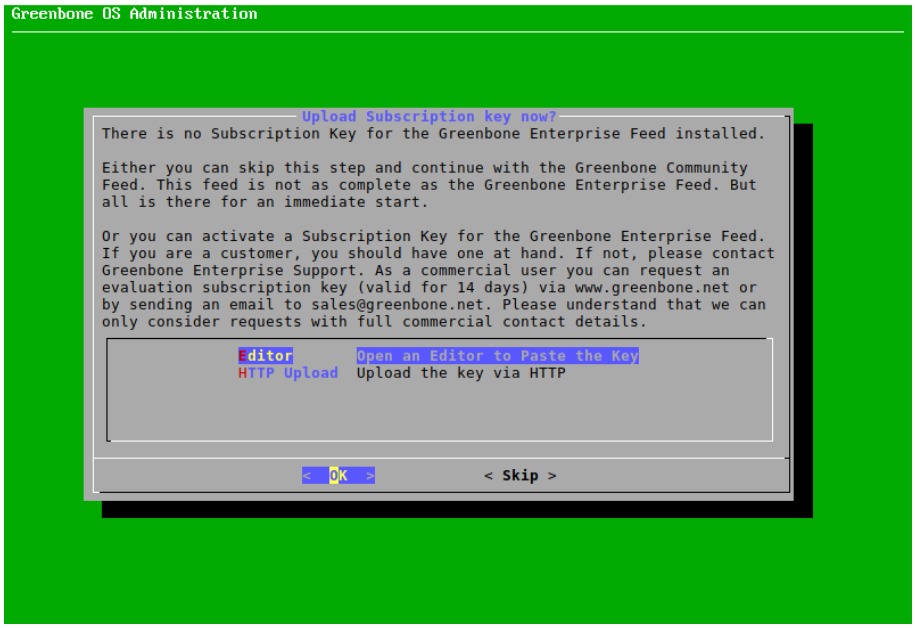


Fig. 5.23: Entering or uploading a subscription key

→ The editor is opened.

2. Enter the subscription key.
3. Press `Ctrl` + `S` to save the changes.
4. Press `Ctrl` + `X` to close the editor.

   or

1. Select *HTTP Upload* and press `Enter`.
2. Open the web browser and enter the displayed URL.
3. Click *Browse...*, select the subscription key and click *Upload*.

5.3.3.5 Downloading the Feed

If no feed is present on the appliance, the feed can be downloaded as follows:

1. Select *Yes* and press `Enter` (see Fig. 5.24).

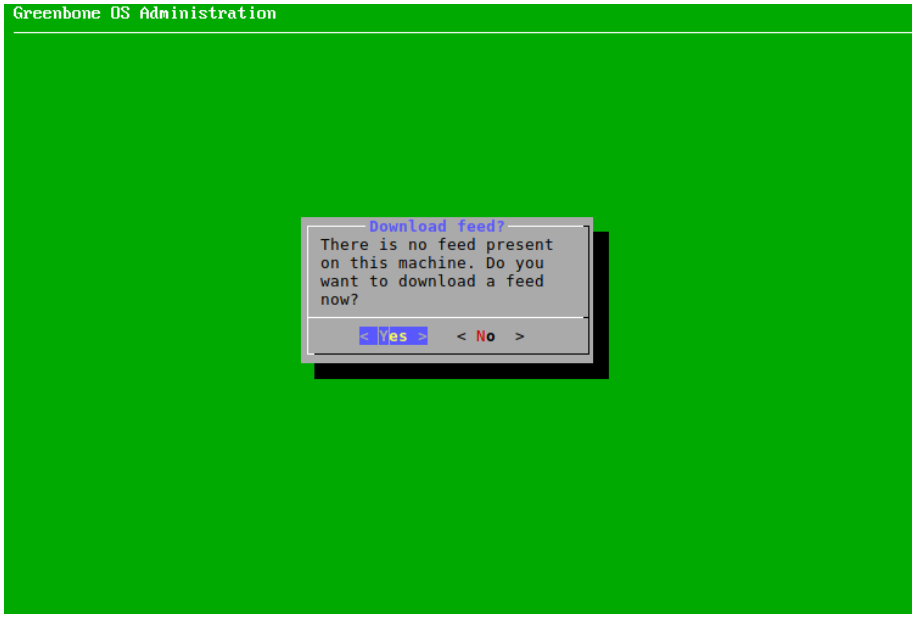


Fig. 5.24: Downloading the feed

   → A message informs that the feed update was started in the background (see Fig. 5.25).

2. Press `Enter` to close the message.

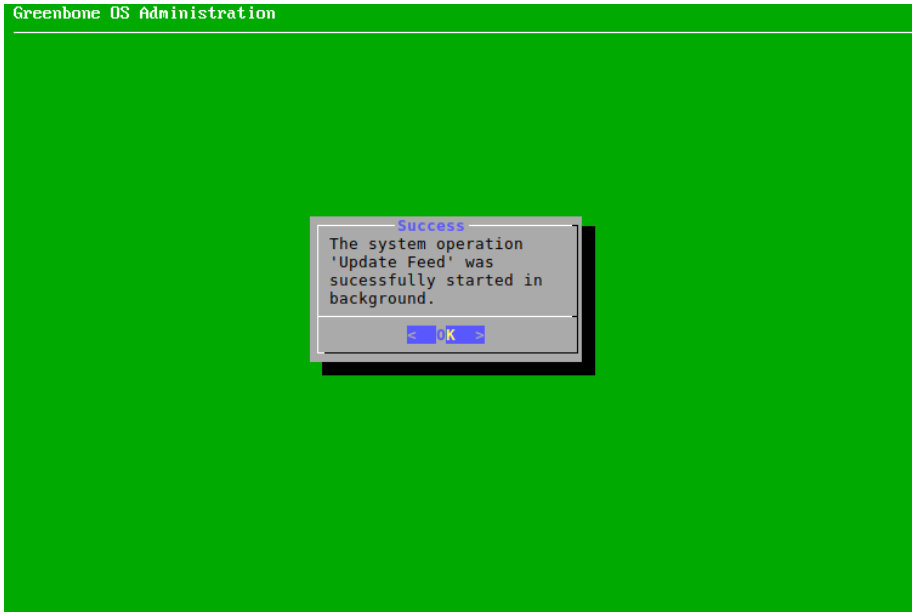


Fig. 5.25: Downloading the feed

5.3.3.6 Finishing the First Setup Wizard

Note: After the last step, a status check is performed.

1. When the check is finished, press `Enter`.

   → The results of the check are displayed (see Fig. 5.26).

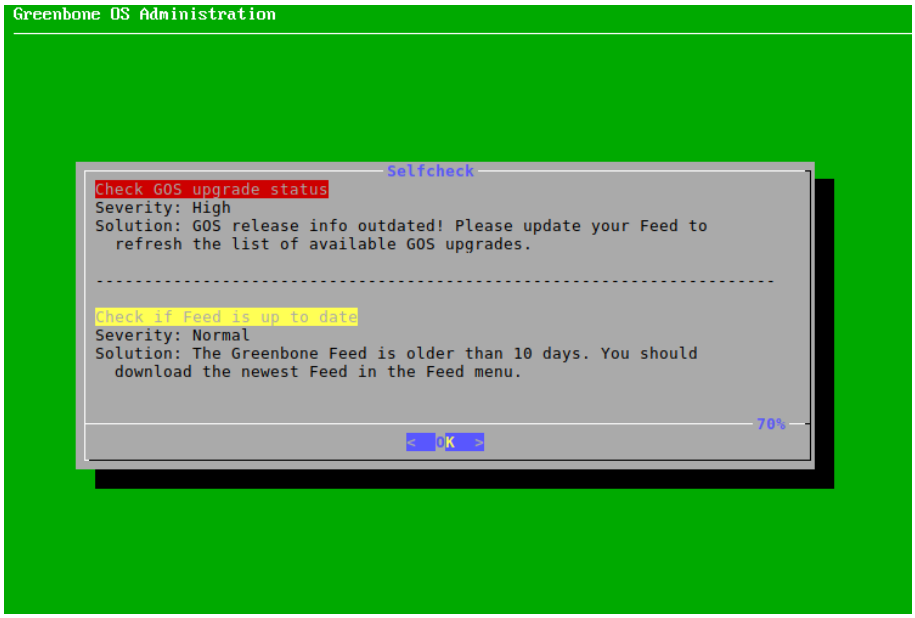


Fig. 5.26: Result of the status check

2. Press `Enter`.

   → The GOS administration menu can be used as described in Chapter *7* (page 67).

   If there are any unfinished or skipped steps, the first setup wizard is shown when logging in again.

5.3.4 Logging into the Web Interface

Note: This step does not apply for the Greenbone Enterprise 25V.

The main interface of the appliance is the web interface, also called Greenbone Security Assistant (GSA). The web interface can be accessed as described in Chapter *8.1* (page 163).

CHAPTER 6

Upgrading the Greenbone Enterprise Appliance to the Latest Major Version

GOS 21.04 provides seamless upgrades to the new major version GOS 22.04.

All system settings and user data are retained and automatically migrated to the new version unless a change in default behavior affects a specific setting or data. For a list of changes to the default behavior, see Chapter *6.5* (page 63).

6.1 Upgrading the Greenbone Operating System

Note: Before upgrading to GOS 22.04, some requirements must be met in GOS 21.04:

- The latest version of GOS 21.04 must be installed on the appliance.
- A Feed Import Owner must be set as described here[6].
- The data objects must be installed. For this, a feed update is required after setting the Feed Import Owner.

It is recommended to switch to the networking mode *gnm* before upgrading to GOS 22.04 (see Chapter *7.2.2.1* (page 83)).

The upgrade to GOS 22.04 can be carried out as follows:

1. Select *Maintenance* and press `Enter`.
2. Select *Upgrade* and press `Enter`.

   → A message informs that a new GOS release is available.
3. Press `Enter` to close the message.

[6] https://docs.greenbone.net/GSM-Manual/gos-21.04/en/managing-gos.html#changing-the-feed-import-owner

4. Select *Switch Release* and press `Enter`.

   → A warning informs that the appliance is upgraded to a major new version (see Fig. 6.1).

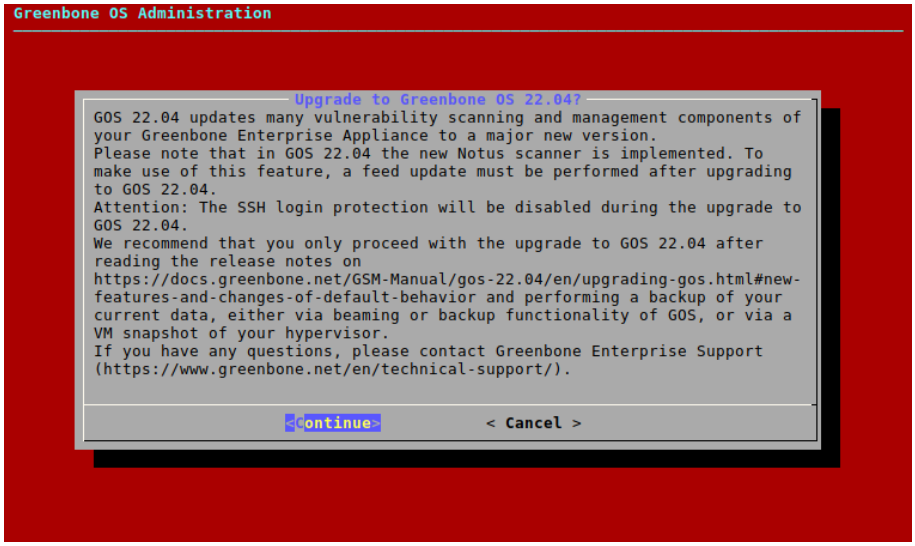


Fig. 6.1: Warning when upgrading to GOS 22.04

5. Select *Continue* and press `Enter`.

   → A warning informs that the appliance is locked during the upgrade to GOS 22.04 (see Fig. 6.2).

Note: No system operations can be run during the upgrade and all running system operations must be completed before upgrading.

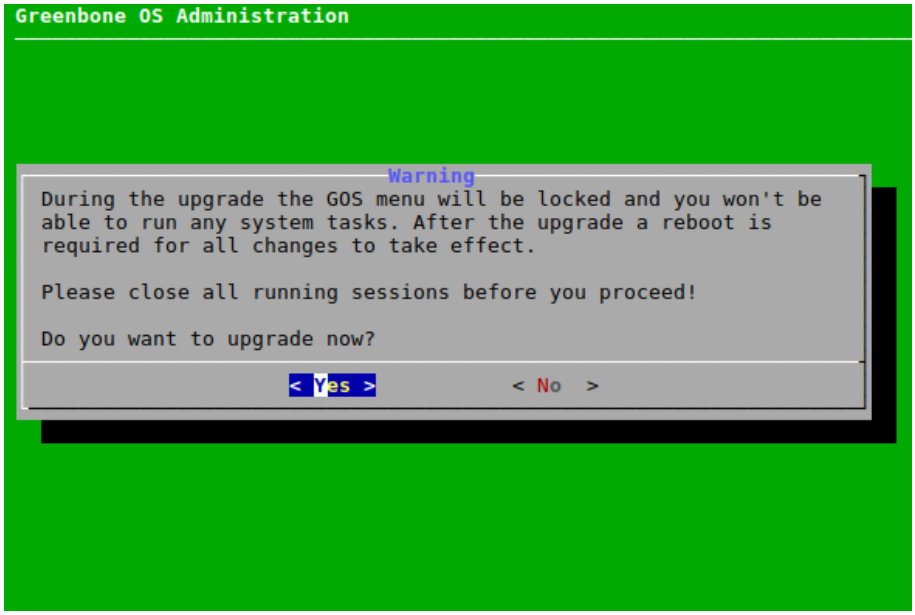


Fig. 6.2: Warning that system is locked during the upgrade

6. Select *Yes* and press `Enter`.

   → A message informs that the upgrade was started.

Note: When the upgrade is finished, a message informs that a reboot is required to apply all changes (see Fig. 6.3).

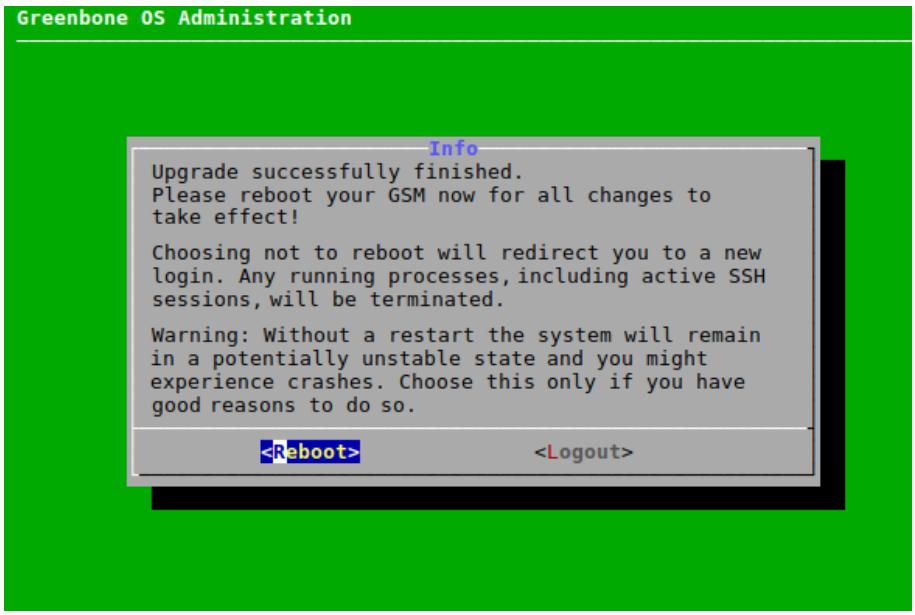


Fig. 6.3: Message after a successful upgrade

7. Select *Reboot* and press `Enter`.

   → After the reboot is finished, it is checked if there are any unfinished setup steps. If there are unfinished steps, a message asks whether they should be completed now.

Note: If the old legacy network mode was still used when upgrading from GOS 21.04 to GOS 22.04, a message offers to switch to the new network mode *GOS Network Manager (gnm)*. If the network mode is not switched directly after the upgrade, this can also be done at a later time (see Chapter *7.2.2.1* (page 83)).

A feed update must be performed after upgrading to GOS 22.04 in order to make use of new features such as the Notus Scanner (see Chapter *6.5* (page 63)).

6.2 Upgrading the Flash Partition to the Latest Version

The internal flash partition of the appliance contains a backup copy of GOS and is used in case of a factory reset.

Upgrading the GOS version stored on the flash partition is recommended (see Chapter *7.3.8* (page 152)).

6.3 Relogging into the GOS Administration Menu After an Upgrade

It is possible that a GOS upgrade changes the functionality available via the GOS administration menu. This changed functionality will only be available after reloading the GOS administration menu. Therefore, it is recommended to log out of the GOS administration menu and log back in after the GOS upgrade.

6.4 Reloading the Web Interface After an Upgrade

After an upgrade from one major version to another, the cache of the browser used for the web interface must be emptied. Clearing the browser cache can be done in the options of the used browser.

Alternatively, the page cache of every page of the web interface can be emptied by pressing `Ctrl` and `F5`.

Note: Clearing the page cache must be done for every single page.

Clearing the browser cache is global and applies to all pages.

6.5 New Features and Changes of Default Behavior

The following list displays the major additions and changes of default behavior between GOS 21.04 and GOS 22.04.

Depending on the currently used features, these changes may affect the currently deployed setup. For a full list of changes, see the Roadmap & Lifecycle page[7].

6.5.1 Notus Scanner

With GOS 22.04, the new Notus Scanner is implemented. It scans after every regular scan, so no user interaction is necessary.

The Notus Scanner offers better performance due to less system resource consumption and thus, faster scanning.

When creating a scan configuration manually and the Notus Scanner is supposed to work, the VT *Determine OS and list of installed packages via SSH login* (OID: 1.3.6.1.4.1.25623.1.0.50282) must be activated.

The Notus Scanner replaces the logic of potentially all NASL-based local security checks (LSCs). A comparison of installed software on a host against a list of known vulnerable software is done instead of running a VT script for each LSC.

The regular OpenVAS Scanner loads each NASL LSC individually and executes it one by one for every host. A single known vulnerability is then compared to the installed software. This is repeated for all LSCs.

With the Notus Scanner, the list of installed software determined during a scan is directly compared to all known vulnerabilities. This eliminates the need to run the LSCs because the information about the known vulnerable software is collected in one single list and not distributed in individual NASL scripts.

Currently, Notus data exists for the following LSC VT families:

- AlmaLinux Local Security Checks
- Amazon Linux Local Security Checks
- Debian Local Security Checks

[7] https://www.greenbone.net/en/roadmap-lifecycle/#gos-22-04

- EulerOS Local Security Checks
- Mageia Linux Local Security Checks
- Oracle Linux Local Security Checks
- Rocky Linux Local Security Checks
- Slackware Local Security Checks
- SuSE Local Security Checks
- Ubuntu Local Security Checks

The setting *Report vulnerabilities of inactive Linux kernel(s) separately* in the VT *Options for Local Security Checks* is deprecated. However, the setting is still visible, but no longer functional.

6.5.2 Appliance Feature Set

With GOS 22.04, the feature set for some appliances is extended:

- The SNMP service (GOS menu *Setup > Services > SNMP*) is made available for the appliance models Greenbone Enterprise 150, Greenbone Enterprise 35, Greenbone Enterprise CENO and Greenbone Enterprise 25V.
- The automatic time synchronization via NTP (GOS menu *Setup > Timesync*) is made available for the appliance models Greenbone Enterprise CENO and Greenbone Enterprise 25V.
- The remote and local backup functionality (GOS menus *Setup > Backup*, *Maintenance > Backup > Incremental Backup* and *Maintenance > Backup > List*) is made available for the appliance model Greenbone Enterprise CENO.

6.5.3 Virtual Appliances

With GOS 22.04, the virtual hard disk sizes for virtual appliances are changed.

The new sizes are:

- Greenbone Enterprise EXA: 225 GB
- Greenbone Enterprise DECA/PETA/EXA: 220 GB
- Greenbone Enterprise CENO: 135 GB
- Greenbone Enterprise ONE: 130 GB
- Greenbone Enterprise 25V: 70 GB

The new sizes are only relevant for newly installed virtual appliances. Upgraded appliances keep their partition layout and thus, their required disk size.

6.5.4 HTTP Web Interface Access

With GOS 22.04, unencrypted HTTP access for the web interface is not supported anymore. HTTPS must be used instead.

A valid HTTPS certificate (either self-signed, or signed by a CA) must now be configured on the appliance to use the web interface (see Chapter *7.2.4.1.7* (page 102)).

6.5.5 Backups

6.5.5.1 Password for Remote Backup Repository

With GOS 22.04, it is possible to change the password of the remote backup repository. For this, the menu option *Setup > Backup > Backup Password* is added to the GOS administration menu. The menu option is only visible if the backup location is configured as *remote*.

Changing the backup password is recommended.

If multiple appliances use the same remote backup repository, it is recommended that each appliance uses its own unique backup password.

6.5.5.2 *obnam*

With GOS 20.08, the backend for managing backups in GOS was changed from *obnam* to *restic*. However, *obnam* remained available in GOS 20.08 and 21.04 as did the backups created with *obnam* in GOS 6 or earlier.

With GOS 22.04, *obnam* and all backups created with *obnam* are removed. Incremental backups created with GOS 6 and earlier will be removed due to incompatibility and to reclaim disk space.

If these old backups should be kept, a copy of the files must be made before upgrading to GOS 22.04. If there are any questions, contact the Greenbone Enterprise Support[8].

6.5.6 Mailhub

With GOS 22.04, a new option for enforcing the usage of SMTPS for e-mails sent by a Greenbone Enterprise Appliance is added.

For this, the GOS administration menu contains the new menu *Setup > Mail > SMTP Enforce TLS*.

6.5.7 Web Interface

6.5.7.1 Business Process Map

With GOS 22.04, the Business Process Map (BPM) functionality is removed from the web interface. Existing Business Process Maps will be deleted and will not be recoverable. If the information contained in a Business Process Map is to be saved, this must be done in GOS 21.04.

6.5.7.2 Task/Audit Setting *Network Source Interface*

With GOS 22.04, the task/audit setting *Network Source Interface* is removed. If this setting was previously configured for a task or an audit, it will be ignored.

6.5.7.3 User Setting *Interface Access*

As the task/audit setting *Network Source Interface* is removed with GOS 22.04, the user setting *Interface Access* is removed as well. If this setting was previously configured for a user, it will be ignored.

[8] https://www.greenbone.net/en/technical-support/

6.5.7.4 OVAL Definitions

With GOS 22.04, the OVAL definitions are removed from the SecInfo management in the web interface. The previous OVAL definitions were outdated and no longer served any purpose.

6.5.7.5 OSP Scanners

With GOS 22.04, the scanner type *OSP Scanner* is removed. It is no longer possible to create OSP scanners and select them to run scans.

This only affects the scanner type *OSP Scanner*, not the OSP protocol in general. The scanner type *Greenbone Sensor* will continue to use OSP.

The credential type *Client Certificate* that was used for (custom) OSP scanners was removed as well. Existing credentials of this type will not be affected or removed. They can still be accessed, but they are of no use anymore, and can be deleted manually.

6.5.8 Quality of Detection (QoD)

With GOS 22.04, the new quality of detection (QoD) level *package_unreliable* is implemented with a QoD of 30 %. It is used for authenticated package-based checks which are not always fully reliable for, e.g., Linux(oid) systems.

6.5.9 Vulnerability References

With GOS 22.04, the tag *script_bugtraq_id();* which references a BID of Bugtraq is no longer supported. For VTs with such tag, the BID was displayed under *References* on the web interface. Since bugtraq.securityfocus.com is not maintained anymore, the reference only led to confusion.

All existing BID references were migrated to *Other* references and will appear there as URLs on the web interface. To access the contents of the URLs, common services such as archive.org can be used.

6.5.10 Greenbone Management Protocol (GMP)

The Greenbone Management Protocol (GMP) has been updated to version 22.04 and the API has been adjusted slightly. The usage of some commands has changed and several commands, elements and attributes have been deprecated. The complete reference guide and the list of changes are available here[9].

[9] https://docs.greenbone.net/API/GMP/gmp-22.04.html

CHAPTER 7

Managing the Greenbone Operating System

Note: This chapter documents all possible menu options.

However, not all appliance models support all of these menu options. Check the tables in Chapter *3* (page 20) to see whether a specific feature is available for the used appliance model.

7.1 General Information

7.1.1 Greenbone Enterprise Feed Subscription Key

When purchasing a Greenbone Enterprise Appliance, a unique Greenbone Enterprise Feed subscription key is pre-installed to grant the appliance access to the Greenbone feed service. The subscription key is used for authorization purposes only, not for billing or encryption.

The subscription key is individual for each appliance and cannot be installed on more than one appliance.

If the subscription key is compromised (e.g., gets into the hands of third parties), no damage will occur for the rightful owner of the subscription key. Greenbone will deactivate the compromised key, preventing further unauthorized use. A replacement key may be issued at no cost.

A factory reset will delete the subscription key from the appliance and the key has to be re-installed. If a factory reset is planned, contact the Greenbone Enterprise Support[10] to receive a copy of the subscription key.

[10] https://www.greenbone.net/en/technical-support/

7.1.2 Authorization Concept

The appliance offers two different levels of access:

- **User level – via web interface or GMP** The user level is available via the web interface or the Greenbone Management Protocol (GMP) API.
- **System level – via GOS administration menu** The system level is only available via console or secure shell protocol (SSH).

7.1.2.1 User-Level Access

The user level provides access to the scanning and vulnerability management functionalities and supports the administration of users, groups and permissions.

Accessing the user level is possible either via the web interface (see Chapters *8* (page 163) and *9* (page 182)) or via the Greenbone Management Protocol (GMP) API (see Chapter *15* (page 361)).

Note: By default, no user-level account is configured when the appliance is delivered by Greenbone or after a factory reset. It is necessary to create at least one such account, a so-called “web administrator”, via the GOS administration menu (see Chapter *7.2.1.3* (page 74)).

Besides the initial web administrator, there are two options for creating web users:

Via the web interface Web users with different roles and permissions can be created via the web interface. These users have an owner who is the user who created them. They can be managed via the web interface as well as via the GOS administration menu.

Via the GOS administration menu Users created via the GOS administration menu always have the *Admin* role. These users do not have an owner and are so-called “global objects”. Sometimes they are also referred to as “global web users”. They can only be managed via the GOS administration menu or by a super administrator.

Note: For the appliance models Greenbone Enterprise 35 and Greenbone Enterprise 25V, no user-level access is supported. These appliances have to be managed using a master appliance.

7.1.2.2 System-Level Access

The system level provides access to the administration of the Greenbone Operating System (GOS). Only a single system administrator account is supported. The system administrator cannot modify system files directly but can instruct the system to change configurations.

GOS is managed using a menu-based graphical interface (GOS administration menu). The command line (shell) does not have to be used for configuration or maintenance tasks. Shell access is provided for support and troubleshooting purposes only.

Accessing the system level requires either console access (serial, hypervisor or monitor/keyboard) or a connection via SSH. To use SSH, a network connection is required and the SSH service must be enabled (see Chapter *7.2.4.4* (page 108)).

When the appliance is delivered by Greenbone or after a factory reset, a default system administrator account and password is pre-configured. During the initial setup, the system administrator password should be changed (see Chapter *7.2.1.1* (page 72)).

Accessing the GOS Administration Menu Using the Console

Once turned on, the appliance boots. The boot process can be monitored via the console.

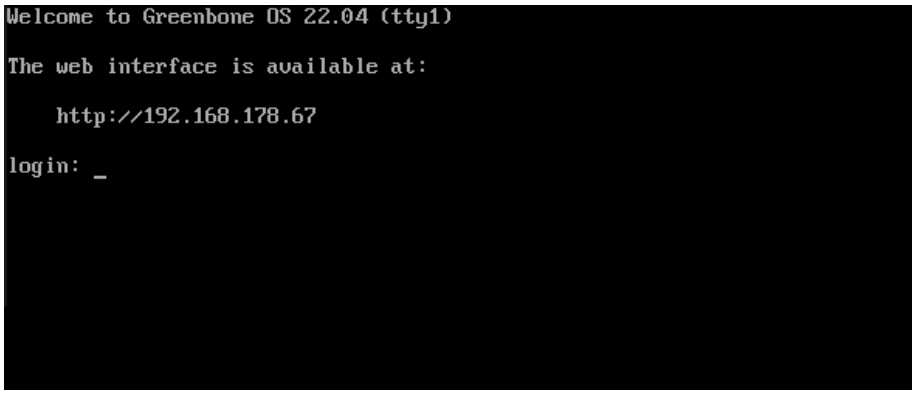


Fig. 7.1: Login prompt of the appliance

After the boot process is completed, the login prompt is shown (see Fig. 7.1). The default login information is:

- User: `admin`
- Password: `admin`

Note: During the first setup, this password should be changed (see Chapter *7.2.1.1* (page 72)).

When the appliance is delivered by Greenbone or after a factory reset, a setup wizard is shown after logging in to assist with the basic GOS configuration.

- By selecting *Yes* and pressing `Enter`, all mandatory settings can be configured.
- By selecting *No* and pressing `Enter`, the setup wizard is closed. Incomplete steps are displayed again when logging in the next time.
- By selecting *Cancel* and pressing `Enter`, the setup wizard is closed. Incomplete steps are **not** displayed again.

Accessing the GOS Administration Menu Using SSH

Note: When the appliance is delivered by Greenbone or after a factory reset, SSH access may be deactivated and must be enabled first using the console (see Chapter *7.2.4.4* (page 108)). A network connection is required for SSH (see Chapter *7.2.2.4* (page 85)).

Linux, macOS and Unix-Like Systems

To establish a SSH connection on Linux, macOS or Unix-like systems, the command line can be used as follows:

```
$ ssh admin@<appliance>
```

Replace `<appliance>` with the appliance's IP address or domain name.

The host key can be verified by displaying its fingerprint as follows:

1. Log in to the GOS administration menu.

2. Select *Setup* and press `Enter`.
3. Select *Services* and press `Enter`.
4. Select *SSH* and press `Enter`.
5. Select *Fingerprint* and press `Enter`.

   → The fingerprint is displayed.

Microsoft Windows

To establish an SSH connection on Microsoft Windows systems, the tools PuTTY or smarTTY can be used. On Microsoft Windows Server 2019, Microsoft Windows 10 Build 1809, or newer, the OpenSSH Client component can be installed to access SSH via the command line.

7.1.3 Using the GOS Administration Menu

The GOS administration menu can be navigated using a keyboard.

- The arrow keys of the keyboard are used for the menu selection.
- Pressing `Enter` is used to confirm the current menu selection and to continue.
- Pressing `Space` is used to toggle on/off switches.
- The current menu can be exited by pressing `Esc`.
- In most cases, changes made in the GOS administration menu are not activated immediately. Instead, the menu option *Save* is added below the other options (see Fig. 7.2). Select *Save* and press `Enter` to save changes.

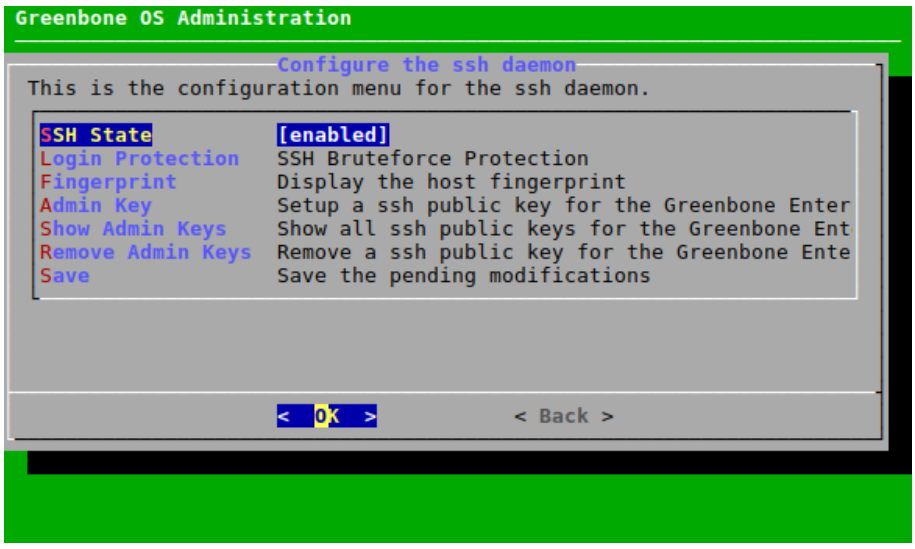


Fig. 7.2: New menu option for saving pending changes

If a menu is exited without saving the changes, a warning is displayed (see Fig. 7.3).

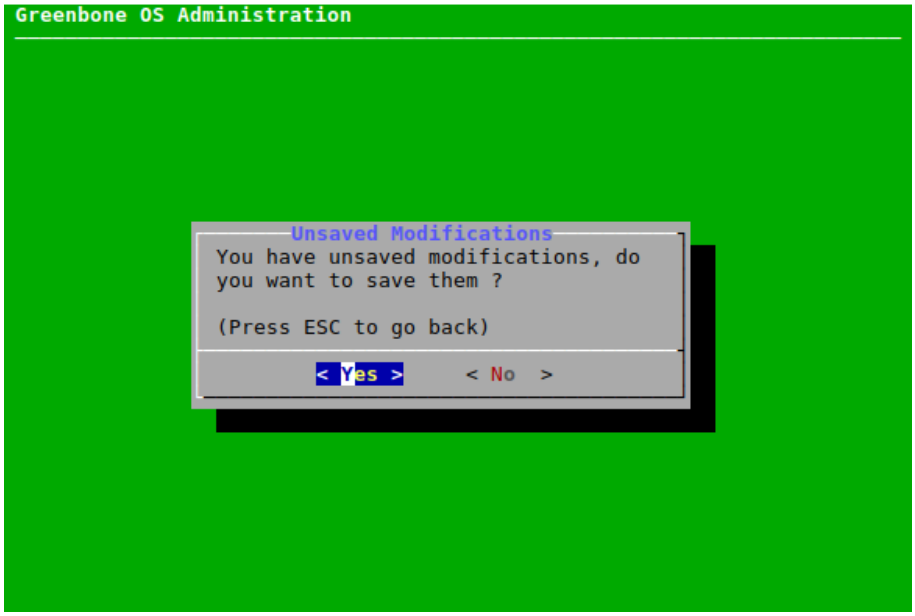


Fig. 7.3: Saving pending changes

7.2 Setup Menu

7.2.1 Managing Users

7.2.1.1 Changing the System Administrator Password

The password of the system administrator can be changed. This is especially important during the first basic configuration. The default setting is not suitable for a production environment.

The password can be changed as follows:

1. Select *Setup* and press `Enter`.
2. Select *User* and press `Enter`.
3. Select *Password* and press `Enter` (see Fig. 7.4).

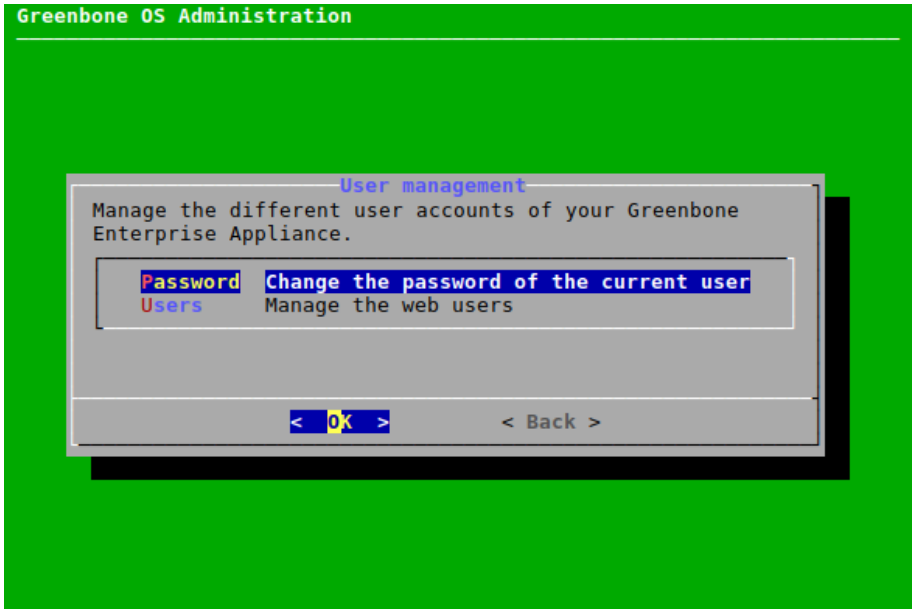


Fig. 7.4: Accessing the user management

4. Enter the current password and press `Enter` (see Fig. 7.5).

Fig. 7.5: Changing the system administrator password

5. Enter the new password and press `Enter`.

Note: Trivial passwords are rejected, including the default password `admin`.

6. Repeat the new password and press `Enter`.

Note: The change is effective immediately and a commit of the change is not required. A rollback is not possible either.

7.2.1.2 Managing Web Users

The GOS administration menu offers the possibility to manage web users (= user accounts for the appliance's web interface and GMP API).

Note: There is no web interface for the appliance models Greenbone Enterprise 35 and Greenbone Enterprise 25V.

For these appliance models, this chapter and its subchapters are not relevant.

Note: To use the appliance's web interface, at least one web administrator (= web user with the role *Admin*) must be created (see Chapter *7.2.1.3* (page 74)).

Web administrators which were created via the GOS administration menu do not have an owner and are so-called "global objects". Sometimes they are also referred to as "global web users". They can only be managed via the GOS administration menu or by a super administrator.

All web users can be displayed as follows:

1. Select *Setup* and press `Enter`.
2. Select *User* and press `Enter`.
3. Select *Users* and press `Enter`.
4. Select *List Users* and press `Enter` to display a list of all configured web users (see Fig. 7.6).

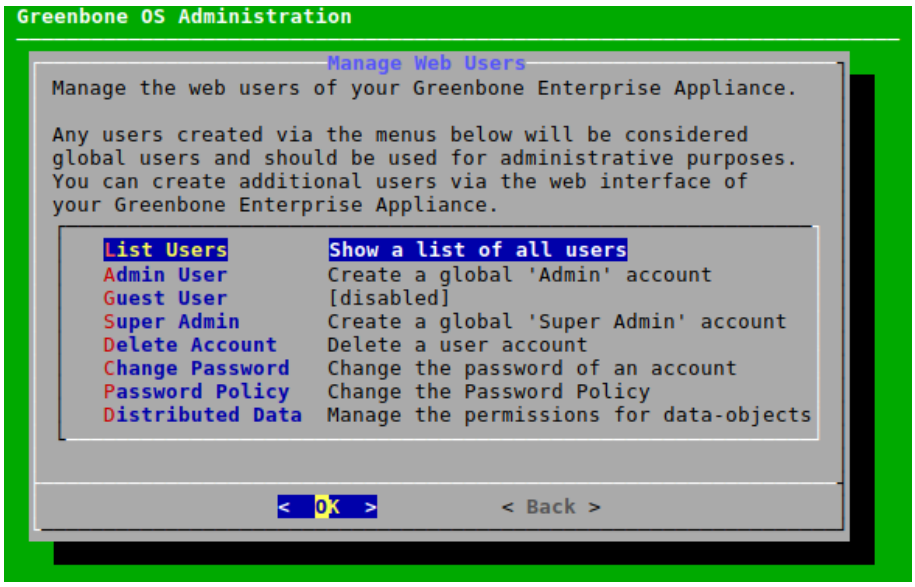


Fig. 7.6: Managing the web users

7.2.1.3 Creating a Web Administrator

To use the appliance's web interface, at least one web administrator (= web user with the role *Admin*) must be created.

Note: The creation of the first web administrator is only possible using the GOS administration menu.

A web administrator can be created as follows:

1. Select *Setup* and press `Enter`.
2. Select *User* and press `Enter`.
3. Select *Users* and press `Enter`.
4. Select *Admin User* and press `Enter`.
5. Enter the user name for the web administrator (see Fig. 7.7).

Note: Only the following characters are allowed for the user name:

- All alphanumeric characters
- - (dash)
- _ (underscore)
- . (full stop)

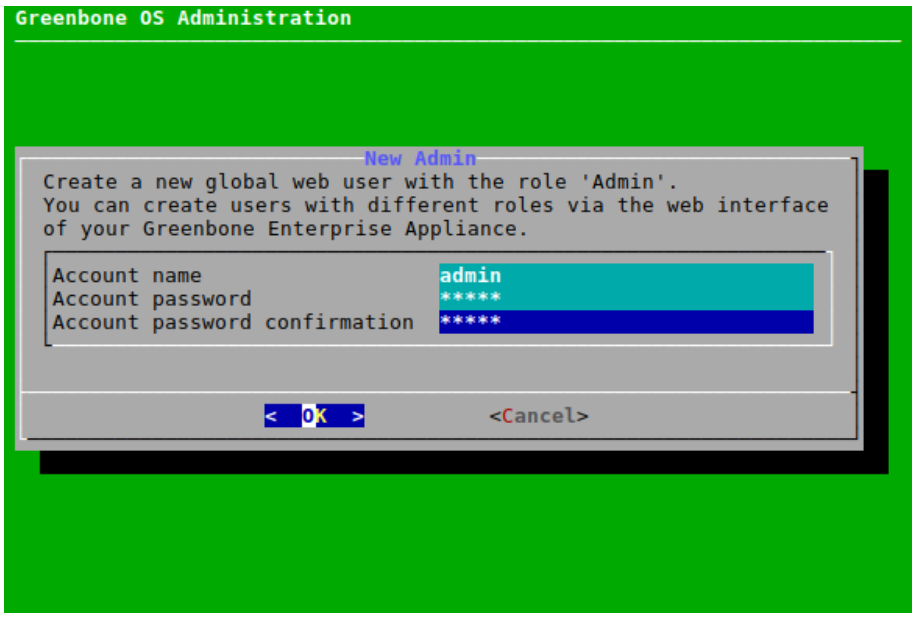


Fig. 7.7: Creating a new web administrator

6. Enter the password for the web administrator twice.

   Note: The password can contain any type of character and can be at most 30 characters long.

   When using special characters, note that these must be available on all used keyboards and correctly supported by all client software and operating systems. Copying and pasting special characters for passwords can lead to invalid passwords depending on these external factors.

7. Select *OK* and press `Enter`.

   → A message informs that the web administrator has been created.

8. Press `Enter` to close the message.

7.2.1.4 Enabling a Guest User

In order for a guest to log in without a password, the guest access must be enabled as follows:

1. Select *Setup* and press `Enter`.
2. Select *User* and press `Enter`.
3. Select *Users* and press `Enter`.
4. Select *Guest User* and press `Enter`.
5. Enter the user name and the password of an existing web user and press `Tab`.
6. Press `Enter`.

   → The web user is now allowed to log in to the web interface without needing the password (see Fig. 7.8).

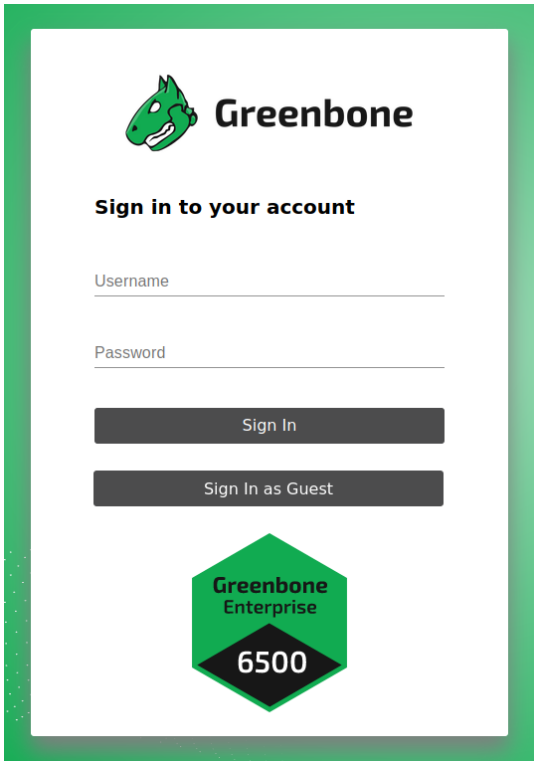


Fig. 7.8: Logging in as a guest user without password

7.2.1.5 Creating a Super Administrator

The role *Super Admin* is the highest level of access. A user with this role can be created as follows:

1. Select *Setup* and press `Enter`.
2. Select *User* and press `Enter`.
3. Select *Users* and press `Enter`.
4. Select *Super Admin* and press `Enter`.

   → A warning asks to confirm the process (see Fig. 7.9).

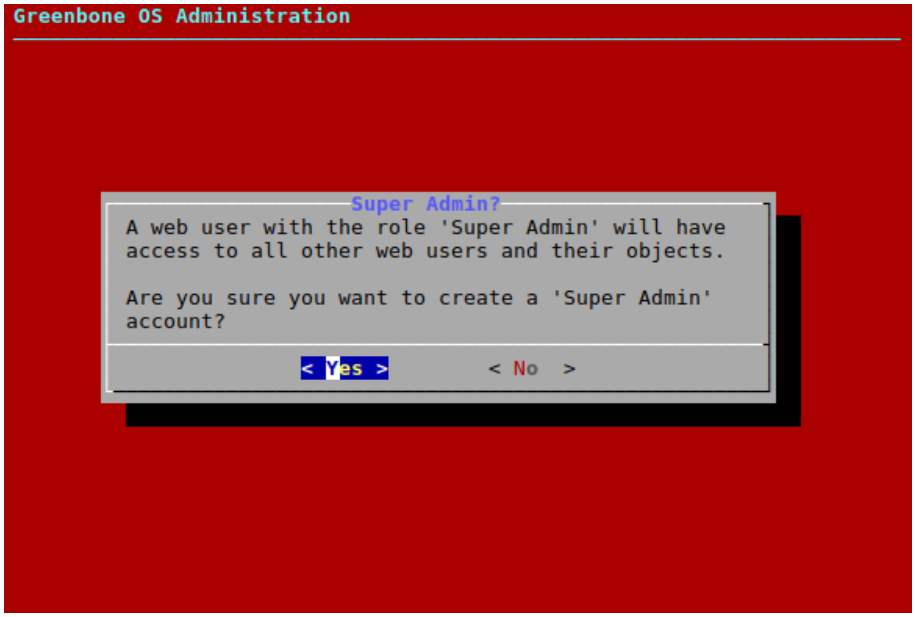


Fig. 7.9: Warning when creating a new super administrator

5. Select *Yes* and press `Enter`.
6. Enter the user name for the super administrator.

Note: Only the following characters are allowed for the user name:

- All alphanumeric characters
- - (dash)
- _ (underscore)
- . (full stop)

---

7. Enter the password for the super administrator twice.

Note: The password can contain any type of character and can be at most 30 characters long.

When using special characters, note that these must be available on all used keyboards and correctly supported by all client software and operating systems. Copying and pasting special characters for passwords can lead to invalid passwords depending on these external factors.

8. Select *OK* and press `Enter`.

   → A message informs that the super administrator has been created.

9. Press `Enter` to close the message.

Note: The super administrator can only be edited by the super administrator themself.

7.2.1.6 Deleting a User Account

Note: Super administrators can only be deleted as described here. Deleting a super administrator via the web interface is not possible.

The user who is Feed Import Owner cannot be deleted. Another Feed Import Owner must be set or the setting has to be unset first (see Chapter *7.2.1.10.1* (page 81))

A web user can be deleted as follows:

1. Select *Setup* and press `Enter`.
2. Select *User* and press `Enter`.
3. Select *Users* and press `Enter`.
4. Select *Delete Account* and press `Enter`.
5. Select the web user that should be deleted and press `Enter`.

   → A message asks whether an inheritor should be chosen.

6. If an inheritor should be defined, select *Yes* and press `Enter`.
7. Select the web user that should be the inheritor and press `Enter`.

   → The web user is deleted immediately.

   or

6. If no inheritor should be defined, select *No* and press `Enter`.

   → The web user is deleted immediately.

7.2.1.7 Limiting the Number of Concurrent Web Sessions

The same web user may log in to the web interface in multiple web sessions. It is possible to restrict the number of concurrent web sessions.

1. Select *Setup* and press `Enter`.
2. Select *User* and press `Enter`.
3. Select *Users* and press `Enter`.
4. Select *User sessions* and press `Enter`.

5. Enter the maximum number of concurrent web sessions in the input box (see Fig. 7.10).

Note: The value can be between `0` and `25`. The default value is `0`, which means that the number of web sessions is unlimited.

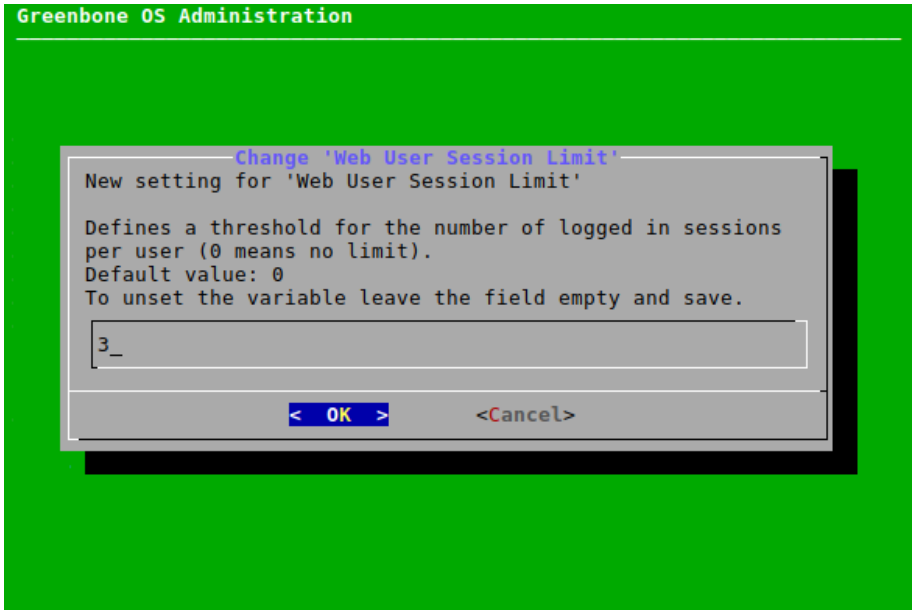


Fig. 7.10: Limiting the number of web sessions

6. Press `Enter`.

7.2.1.8 Changing a User Password

The password of a web user can be changed as follows:

1. Select *Setup* and press `Enter`.
2. Select *User* and press `Enter`.
3. Select *Users* and press `Enter`.
4. Select *Change Password* and press `Enter`.
5. Select the web user whose password should be changed and press `Enter`.
6. Enter the new password twice and press `Tab` (see Fig. 7.11).
7. Press `Enter`.

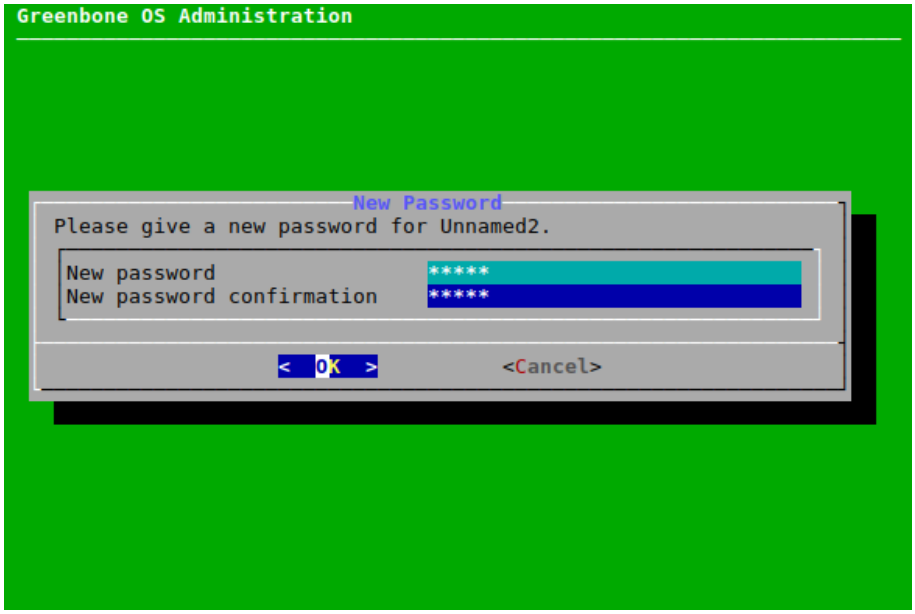


Fig. 7.11: Changing a user password

7.2.1.9 Changing the Password Policy

The requirements for passwords can be changed as follows:

1. Select *Setup* and press `Enter`.
2. Select *User* and press `Enter`.
3. Select *Users* and press `Enter`.
4. Select *Password Policy* and press `Enter`.
5. Select *Length* and press `Enter` to set the minimum length of a password.

   Note: The minimum length must be at least 10 characters.

   Select *Username* and press `Enter` to determine whether user name and password can be the same.

   Select *Complex* and press `Enter` to determine whether a password must contain at least one letter, one number and one symbol.

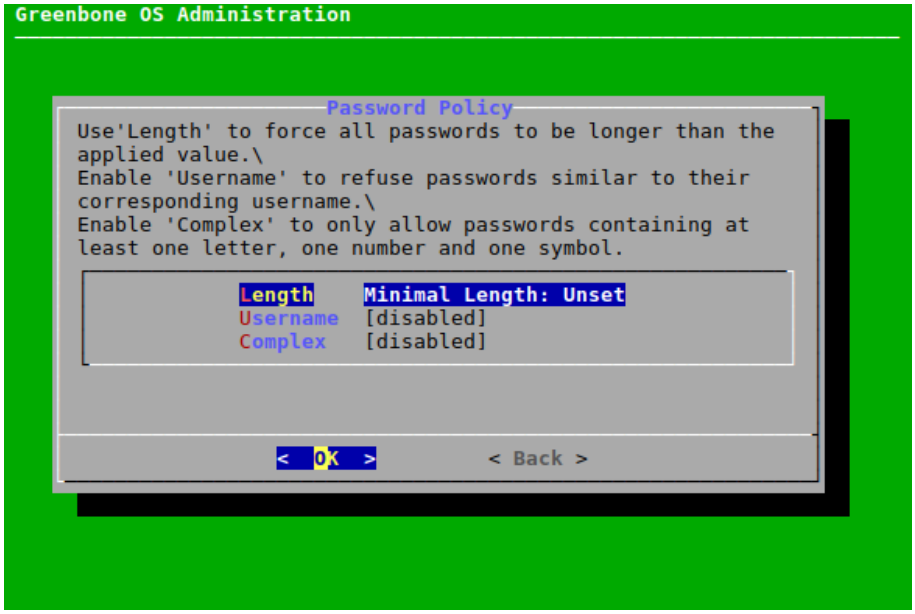


Fig. 7.12: Changing the password policy

7.2.1.10 Configuring the Settings for Data Objects

Scan configurations, compliance policies, report formats and port lists by Greenbone (hereafter referred to as “objects”) are distributed via the feed. These objects must be owned by a user, the Feed Import Owner.

The objects are downloaded and updated during a feed update if a Feed Import Owner has been set.

Only the Feed Import Owner, a super administrator and users who obtained respective rights are able to delete objects. If objects are deleted, they will be downloaded again during the next feed update.

Note: If the objects remain in the trashcan, they are not yet considered deleted and will not be downloaded again during the next feed update.

If no objects should be downloaded, the Feed Import Owner must be unset.

The Feed Import Owner, a super administrator (default role) and an administrator (default role) who currently has permissions for the objects may also grant additional permissions for the objects to other users (see Chapter *9.4.1.1* (page 194) or *9.4.1.2* (page 195)). Normally, this only applies to the default roles. Custom roles must be granted permissions manually first.

Changing the Feed Import Owner

The Feed Import Owner is set during the first appliance setup (see Chapters *6* (page 60) and *5* (page 28)). However, the Feed Import Owner can be changed at a later time.

Note: If the Feed Import Owner is changed, the ownership of the objects will be changed to the new Feed Import Owner the next time they are imported from the feed. The previous feed import owner continues to own the objects until then.

If the previous Feed Import Owner removes the objects, they will be imported during the feed update and owned by the new Feed Import Owner.

The Feed Import Owner can be changed as follows:

1. Select *Setup* and press `Enter`.
2. Select *User* and press `Enter`.
3. Select *Users* and press `Enter`.
4. Select *Distributed Data* and press `Enter` (see Fig. 7.13).

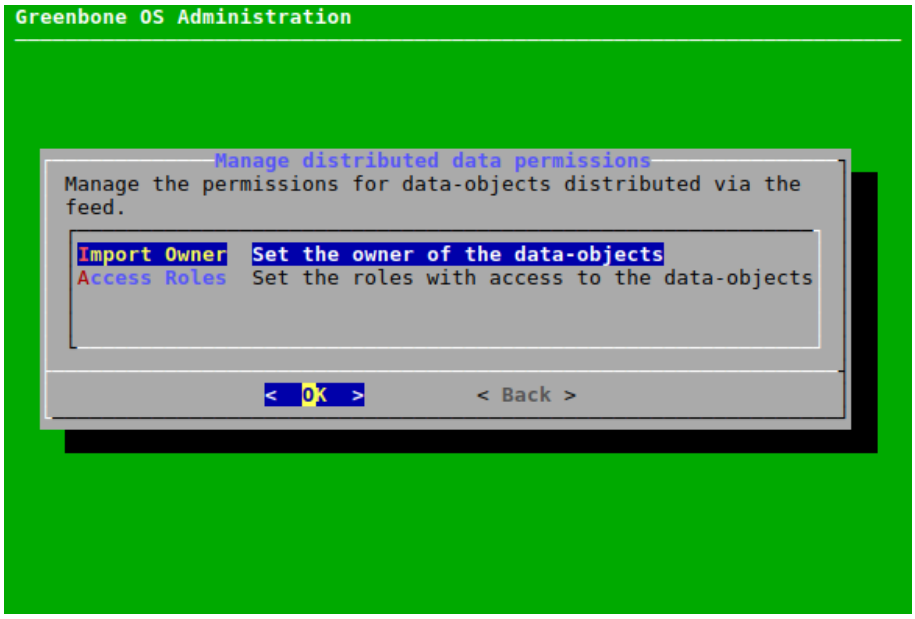


Fig. 7.13: Configuring the settings for the data objects

5. Select *Import Owner* and press `Enter`.
6. Select the user that should be Feed Import Owner and press `Space`.
7. Press `Enter`.

Note: The user who is Feed Import Owner cannot be deleted (see Chapter *7.2.1.6* (page 77)). Another Feed Import Owner or *(Unset)* must be selected.

Setting the Access Roles

By default, the roles *User*, *Admin* and *Super Admin* have read access to the objects, i.e., they can see and use them on the web interface.

However, the roles that should have read access to the objects can be selected as follows:

1. Select *Setup* and press `Enter`.
2. Select *User* and press `Enter`.
3. Select *Users* and press `Enter`.
4. Select *Distributed Data* and press `Enter`.
5. Select *Access Roles* and press `Enter`.
6. Select the roles that should be able to see and use the objects and press `Space` (see Fig. 7.14).

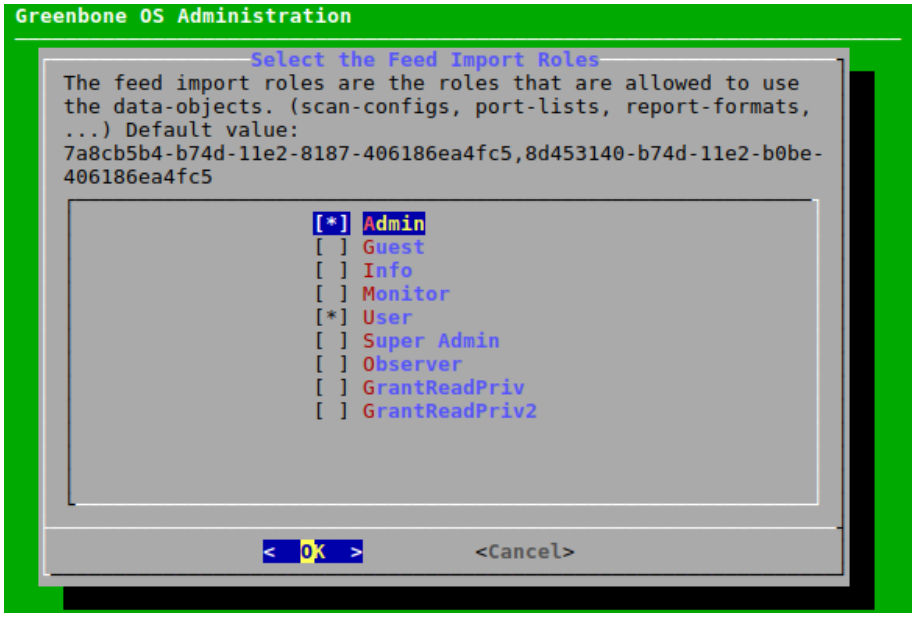


Fig. 7.14: Selecting the roles with read access to the objects

7. Press `Enter`.

7.2.2 Configuring the Network Settings

7.2.2.1 Updating the Networking Mode to *gnm*

If the old network mode is still active, a menu option for switching to the new network mode *GOS Network Manager (gnm)* is available. If the network mode *gnm* is already in use, the option is not displayed. Switching back to the old network mode is not possible.

The network mode can be switched as follows:

1. Select *Setup* and press `Enter`.
2. Select *Network* and press `Enter`.
3. Select *Switch Networking Mode* and press `Enter`.

   → A warning recommends to establish a console connection to the appliance before switching the network mode (see Fig. 7.15).

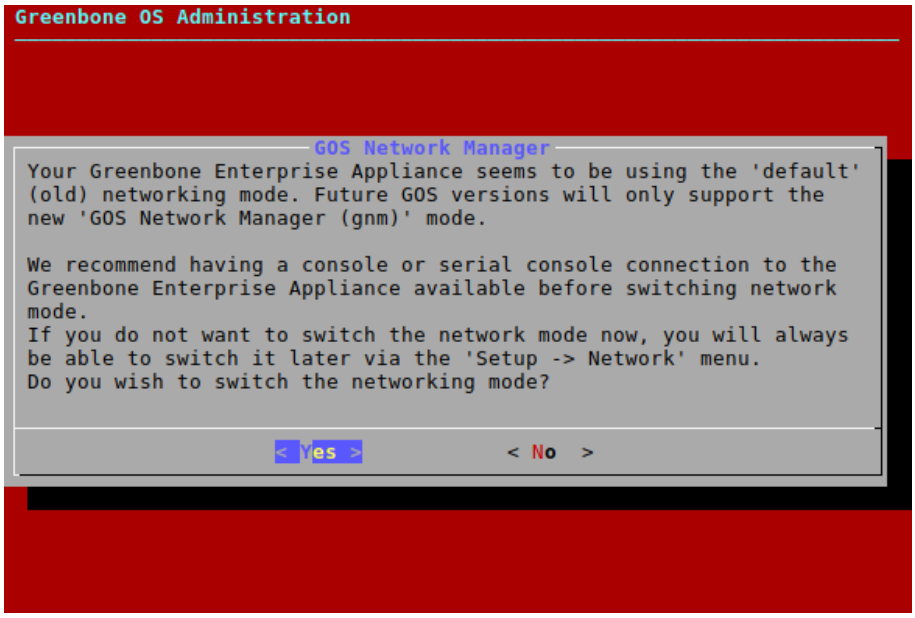


Fig. 7.15: Switching the network mode

4. Select *Yes* and press `Enter`.

   → When the process is finished, a message informs that the network mode was successfully updated to *gnm*.

7.2.2.2 General Information About Namespaces

Some appliance models (Greenbone Enterprise 5400/6500 and Greenbone Enterprise 400/450/600/650) have their network interfaces organized in different namespaces:

Management namespace

- This namespace includes all interfaces required for management activities.
- Only interfaces in the management namespace can handle management traffic. This includes accessing the GOS administration menu, the web interface, the Greenbone Feed Server, and configuring and operating master-sensor setups.

Scan namespace

- This namespace includes all interfaces required for vulnerability scanning activities.
- Interfaces in the scan namespace only handle scan traffic.

By default, all interfaces are in the management namespace. This enables both management and scan traffic on all interfaces. As soon as at least one interface is in the scan namespace, namespace separation goes into effect.

The namespaces are separated to connect only the interfaces in the scan namespace to networks accessible from the internet. In this way, attacks from the internet cannot reach the appliance's management interfaces.

Tip: Separating the namespaces is recommended.

7.2.2.3 Switching an Interface to Another Namespace

Interfaces can be moved to another namespace as follows:

1. Select *Setup* and press `Enter`.
2. Select *Network* and press `Enter`.
3. Select *Configure Namespaces* and press `Enter`.
4. Press `Enter`.

Note: Interfaces that are currently in the scan namespace are marked with * (see Fig. 7.16).

Interfaces that are currently in the management namespace are labeled accordingly.

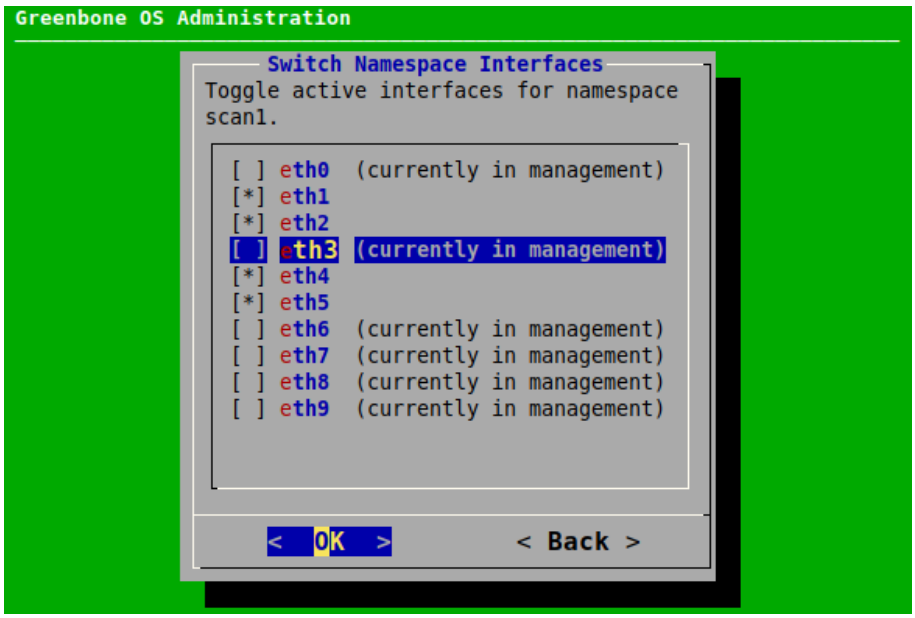


Fig. 7.16: Switching interfaces to another namespace

5. Select the interface that should be moved and and press `Space`.

Note: Not all interfaces may be moved to the scan namespace, otherwise the appliance will no longer be accessible.

6. Press `Enter`.

7.2.2.4 Configuring Network Interfaces

Note: At least one network interface must be configured to access the appliance via the network. Usually, the first network interface *eth0* is used for this purpose. The administrator must configure this network interface and connect the appliance to the network.

On all virtual appliances, the first network interface is preconfigured with IPv4 via DHCP.

Network interfaces can be configured as follows:

1. Select *Setup* and press `Enter`.
2. Select *Network* and press `Enter`.
3. Select the namespace of the desired interface and press `Enter`.
4. Select *Interfaces* and press `Enter`.
5. Select the desired interface and press `Enter`.

Note: If there is only one interface in this namespace, the configuration of the interface is opened directly.

→ The interface can be configured (see Fig. 7.17).

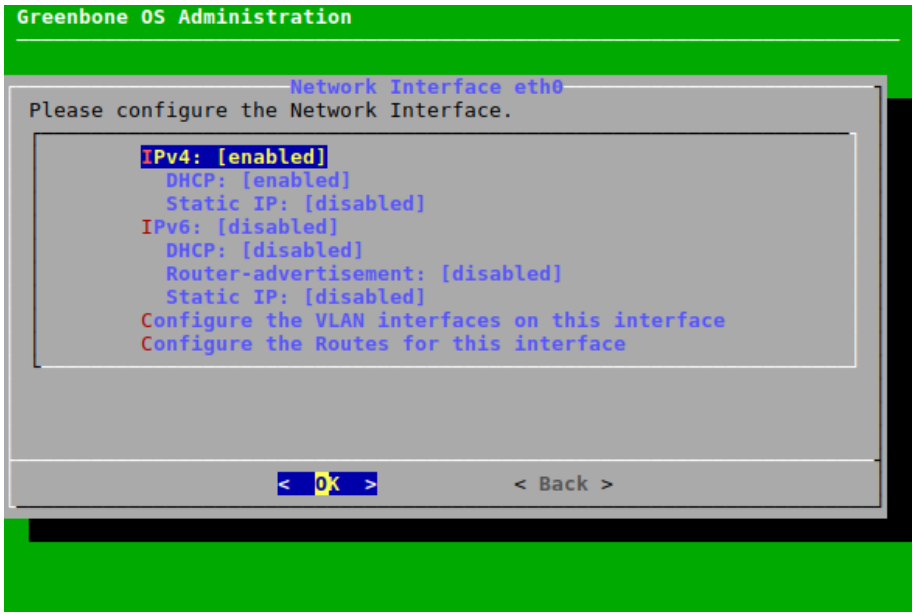


Fig. 7.17: Configuring the network interface

Setting up a Static IP Address

1. Select the desired interface (see Chapter *7.2.2.4* (page 85)).
2. Select *Static IP* (for IPv4 or IPv6) and press `Enter`.
3. Delete `dhcp` from the input box and replace it with the correct IP address including the prefix length (see Fig. 7.18).

Note: The static IP can be disabled by leaving the input box empty.

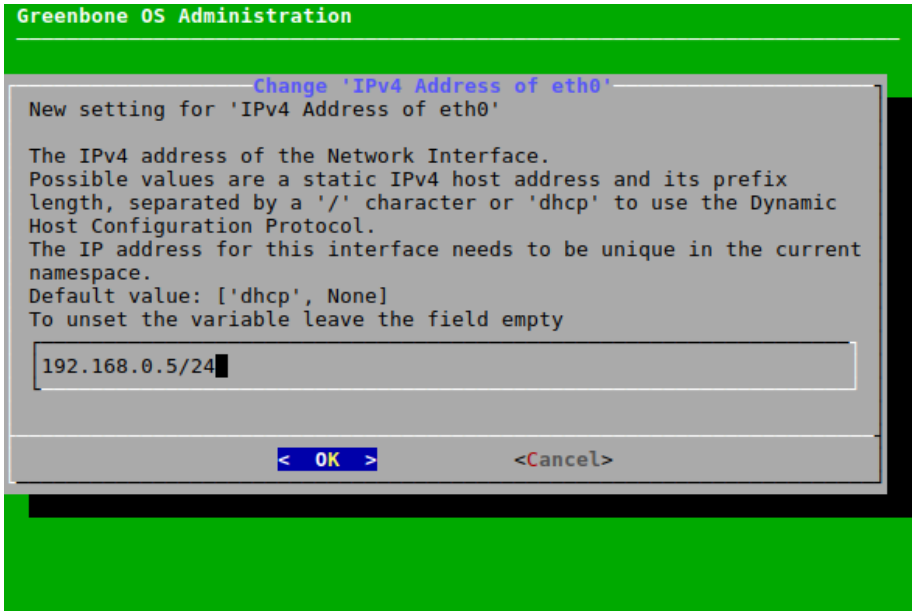


Fig. 7.18: Entering a static IP address

4. Press `Enter`.

   → A message informs that the changes must be saved.
5. Press `Enter` to close the message.

Configuring a Network Interface to Use DHCP

Note: When using DHCP, the appliance does not transmit the MAC address but a DHCP Unique ID (DUID). While this should not pose a problem with modern DHCP servers, some older DHCP servers (e.g., Windows Server 2012) may not be able to handle it.

One possible solution is to specify the DUID instead of the MAC address on the DHCP server. Alternatively, a static IP address can be used on the appliance.

A network interface can be configured to use DHCP as follows:

1. Select the desired interface (see Chapter *7.2.2.4* (page 85)).
2. Select *DHCP* (for IPv4 or IPv6) and press `Enter`.

Configuring the Maximum Transmission Unit (MTU)

Note: The configuration of the MTU is only possible if a static IP address is configured.

The MTU can be set as follows:

1. Select the desired interface (see Chapter *7.2.2.4* (page 85)).
2. Select *MTU* (for IPv4 or IPv6) and press `Enter`.
3. Enter the MTU in the input box.

   Note: If the input box is left empty, the default value is set.

4. Press `Enter`.

   → A message informs that the changes must be saved.
5. Press `Enter` to close the message.

Using the Router Advertisement for IPv6

If the configuration of IP addresses and a global gateway for IPv6 should be done automatically via SLAAC (Stateless Address Autoconfiguration), router advertisement can be enabled as follows:

1. Select the desired interface (see Chapter *7.2.2.4* (page 85)).
2. Select *Router-advertisement* and press `Enter`.

Configuring VLANs

Note: VLAN interfaces are currently not supported on virtual appliances. If the hypervisor supports virtual switches, those can be used to realize the functionality.

Creating a New VLAN

A new VLAN subinterface can be created as follows:

1. Select the desired interface (see Chapter *7.2.2.4* (page 85)).
2. Select *Configure the VLAN interfaces on this interface* and press `Enter`.
3. Select *Configure a new VLAN interface* and press `Enter`.
4. Enter the VLAN ID in the input box and press `Enter` (see Fig. 7.19).

   → A message informs that the changes must be saved.
5. Press `Enter` to close the message.

   → The new interface can be configured using IPv4 and IPv6 (see Fig. 7.20).

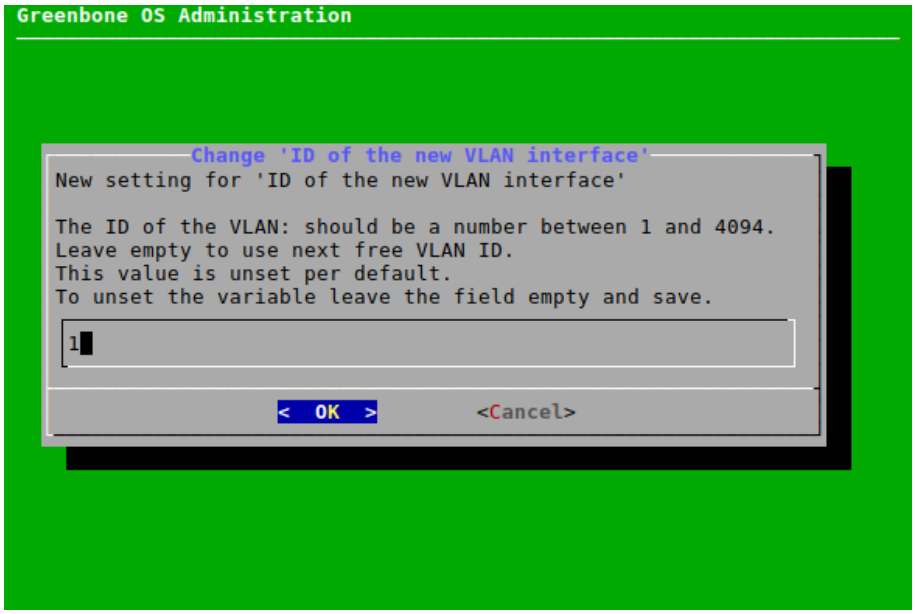


Fig. 7.19: Creating a new VLAN subinterface

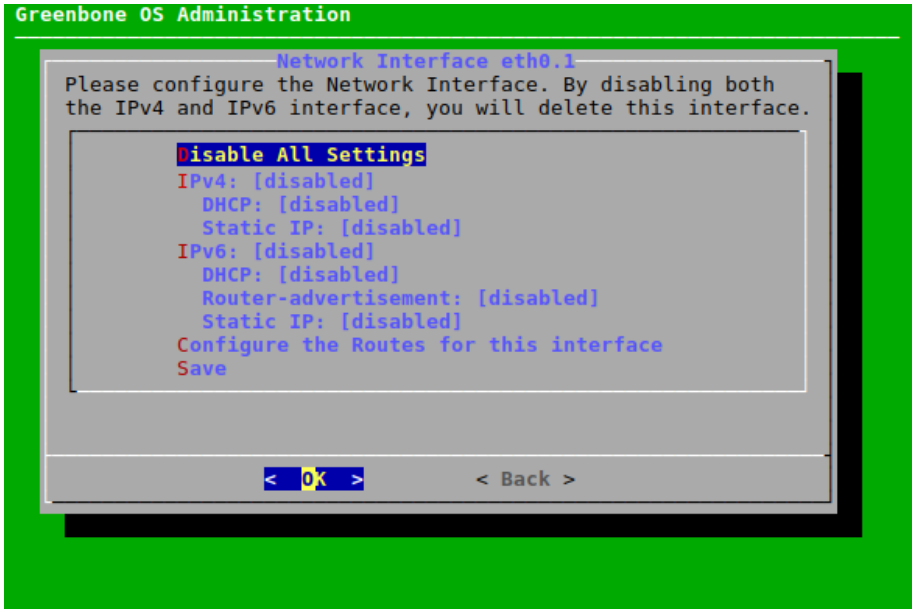


Fig. 7.20: Configuring the VLAN subinterface

Configuring a VLAN

All created subinterfaces can be configured as follows:

1. Select the desired interface (see Chapter *7.2.2.4* (page 85)).
2. Select *Configure the VLAN interfaces on this interface* and press `Enter`.
3. Select *Configure the VLAN interface . . .* for the desired subinterface.
4. Configure the subinterface as described in the subchapters of Chapter *7.2.2.4* (page 85).

Note: The VLAN can be deleted by selecting *Disable All Settings* and pressing `Enter`.

Configuring the Routes for an Interface

Adding a New Route

A new route for an interface can be configured as follows:

1. Select the desired interface (see Chapter *7.2.2.4* (page 85)).
2. Select *Configure the Routes for this interface* and press `Enter`.
3. Select *Configure IPv4 Routes* or *Configure IPv6 Routes* and press `Enter` (see Fig. 7.21).

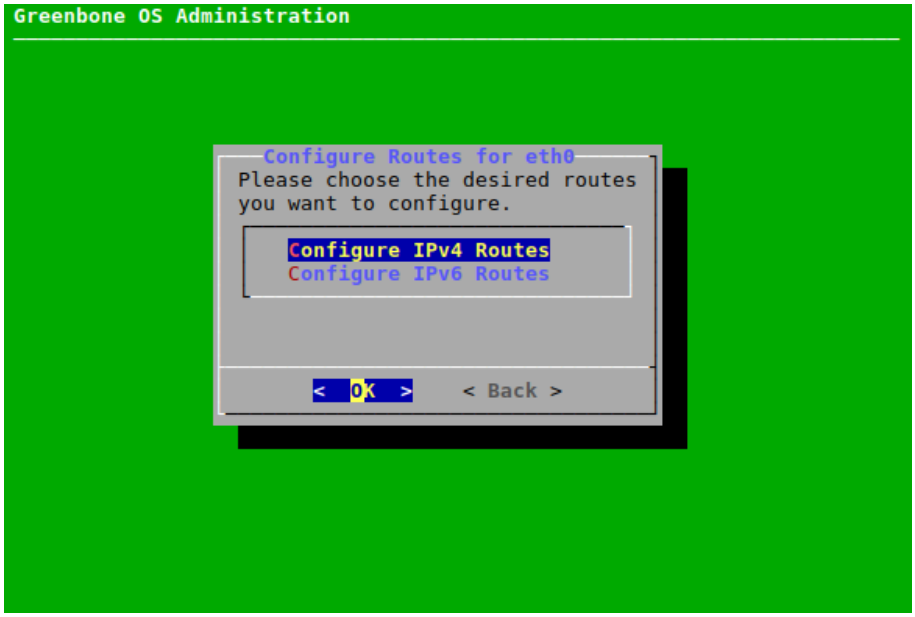


Fig. 7.21: Configuring routes for an interface

4. Select *Add a new route* and press `Enter`.
5. Enter the target network and the next hop in the input boxes, select *OK* and press `Enter`.

Configuring a Route

All created routes can be configured as follows:

1. Select the desired interface (see Chapter *7.2.2.4* (page 85)).
2. Select *Configure the Routes for this interface* and press `Enter`.
3. Select *Configure IPv4 Routes* or *Configure IPv6 Routes* and press `Enter`.

4. Select the desired route and press `Enter`.
5. Edit the route, select *OK* and press `Enter`.

7.2.2.5 Configuring the DNS Server

For receiving the feed and updates, the appliance requires a reachable and functioning DNS (Domain Name System) server for name resolution. This setting is not required if the appliance uses a proxy for downloading the feed and updates.

If DHCP is used for the configuration of the network interfaces, the DNS servers provided by the DHCP protocol are used.

The appliance supports up to three DNS servers. At least one DNS server is required. Additional servers will only be used if an outage of the first server occurs.

The DNS server can be configured as follows:

1. Select *Setup* and press `Enter`.
2. Select *Network* and press `Enter`.
3. Select *Namespace: Management* and press `Enter`.
4. Select *DNS* and press `Enter`.
5. Select the desired DNS server and press `Enter`.
6. Enter the IP address used as the DNS server in the input box and press `Enter` (see Fig. 7.22).

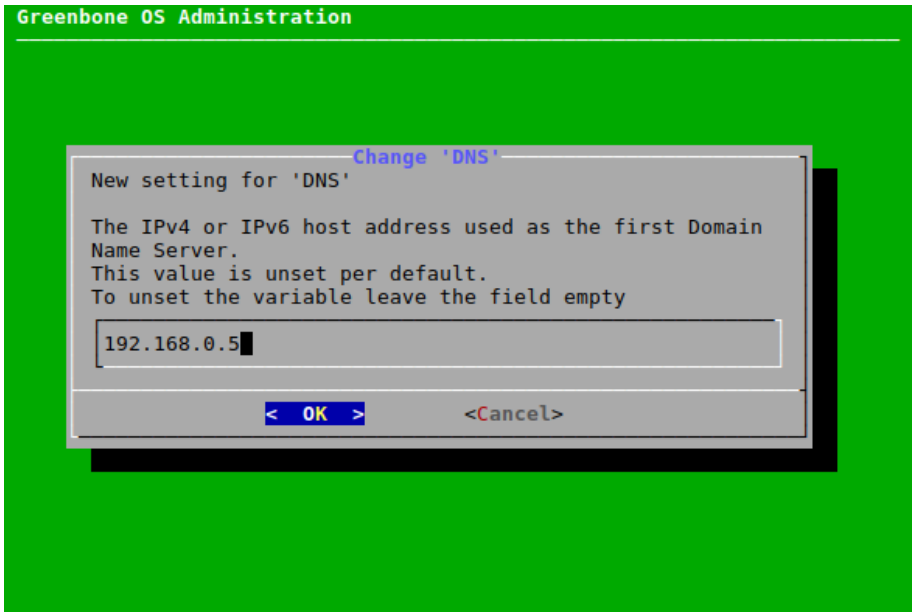


Fig. 7.22: Configuring the DNS server

→ A message informs that the changes must be saved.

7. Press `Enter` to close the message.

Note: Whether the DNS server can be reached and is functional can be determined by performing a self-check (see Chapter *7.3.1* (page 138)).

7.2.2.6 Configuring the Global Gateway

The global gateway is often called the default gateway.

It may be obtained automatically via DHCP or router advertisement.

- If using DHCP to assign IP addresses, the global gateway will be set via DHCP unless it was set explicitly.
- If SLAAC (Stateless Address Autoconfiguration) should be used with IPv6, router advertisement must be activated (see Chapter *7.2.2.4.4* (page 87)).

However, if the appliance is configured to use static IP addresses exclusively and access to other networks is desired, the gateway must be configured manually. Separate options are available for IPv4 and IPv6.

The global gateway can be configured as follows:

1. Select *Setup* and press `Enter`.
2. Select *Network* and press `Enter`.

   Note: If the appliance has namespaces (see Chapter *7.2.2.2* (page 83)), the desired namespace has to be selected first.

   If the appliance has no namespaces, continue with step 4.

3. Select the namespace for which the global gateway should be configured and press `Enter`.
4. Select *Global Gateway* for IPv4 or *Global Gateway (IPv6)* for IPv6 and press `Enter`.
5. Select the desired interface and press `Enter` (see Fig. 7.23).

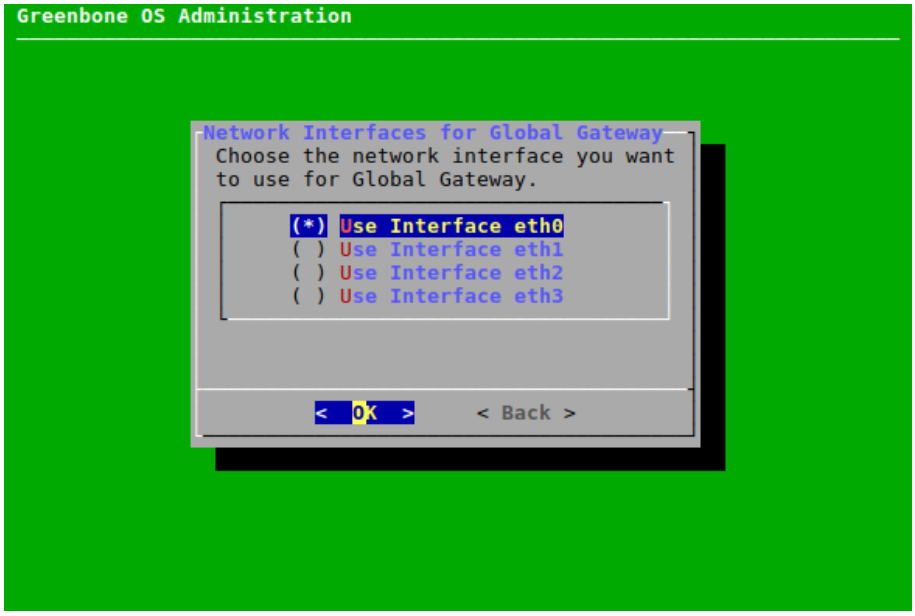


Fig. 7.23: Configuring the global gateway

6. Enter the IP address used as the global gateway in the input box and press `Enter`.

   → A message informs that the changes must be saved.

7. Press `Enter` to close the message.

7.2.2.7 Setting the Host Name and the Domain Name

When the appliance is delivered by Greenbone or after a factory reset, a default host and domain name are configured. Configuring a correct fully qualified domain name (FQDN) may be required depending on the setup in which the appliance is deployed, and is generally recommended.

The host name option is used to configure the short host name, and the domain name option is used for the domain name including its suffix. The two values combined form the FQDN. The default values are:

- Host name: gsm
- Domain name: gbuser.net

The currently configured domain name is always used as a search domain. DHCP servers can add search domains if DHCP is configured for at least one network interface of the appliance, and if the DHCP server is configured accordingly. GOS does not provide any further configuration options to add more custom search domains.

The host name and the domain name can be configured as follows:

1. Select *Setup* and press `Enter`.
2. Select *Network* and press `Enter`.
3. Select *Namespace: Management* and press `Enter`.
4. Select *Hostname* or *Domainname* and press `Enter`.
5. Enter the host name or the domain name in the input box and press `Enter` (see Fig. 7.24).

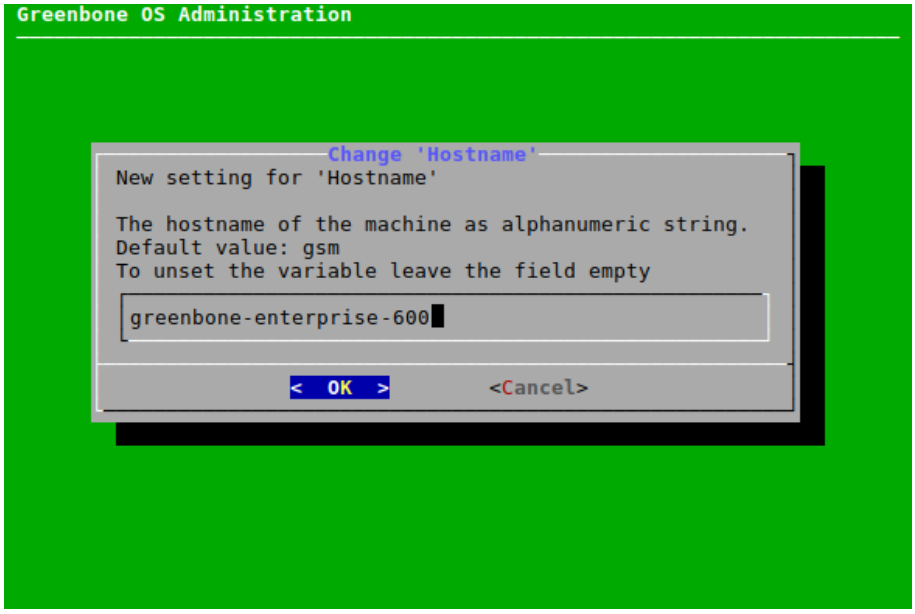


Fig. 7.24: Setting the host name/domain name

→ A message informs that the changes must be saved.

6. Press `Enter` to close the message.

7.2.2.8 Restricting the Management Access

The IP address under which the management interface is available can be set.

All administrative access (SSH, HTTPS, GMP) will be restricted to the respective interface and will not be available on the other interfaces.

Note: This feature overlaps with the namespace separation (see Chapter *7.2.2* (page 83)). Namespace separation is recommended.

If no IP address is set, the management interface will be available on all IP addresses of the interfaces in the management namespace.

The IP address for the management interface can be set as follows:

1. Select *Setup* and press `Enter`.
2. Select *Network* and press `Enter`.
3. Select *Namespace: Management* and press `Enter`.
4. Select *Management IP (v4)* or *Management IP (v6)* and press `Enter`.
5. Enter the IP address for the management interface in the input box and press `Enter` (see Fig. 7.25).

   Note: The IP address must be the IP address of one of the interfaces in the management namespace. If any other IP address is set, the management interface will not be available.

   Either the IP address or the name of the interface (e.g., `eth0`) can be entered.

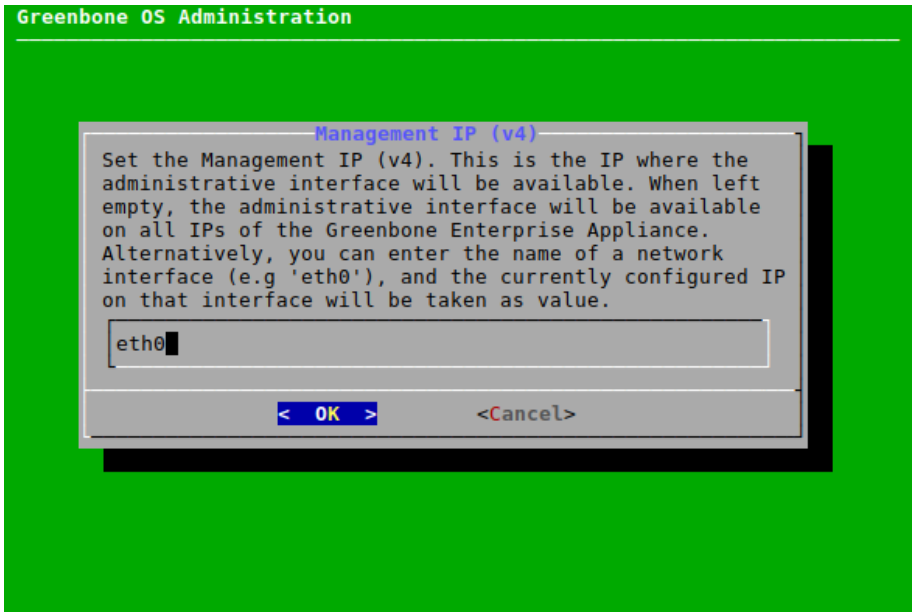


Fig. 7.25: Restricting the management access

7.2.2.9 Displaying the MAC and IP Addresses and the Network Routes

The used MAC addresses, the currently configured IP addresses and the appliance's network routes can be displayed in a simple overview.

Note: This does not support the configuration of the MAC addresses.

The MAC addresses, IP addresses or network routes can be displayed as follows:

1. Select *Setup* and press `Enter`.
2. Select *Network* and press `Enter`.
3. Select the namespace for which the IP addresses, MAC addresses or network routes should be displayed and press `Enter`.
4. Select *MAC*, *IP* or *Routes* and press `Enter`.

   → The MAC/IP addresses or the network routes of the selected namespace are displayed (see Fig. 7.26).

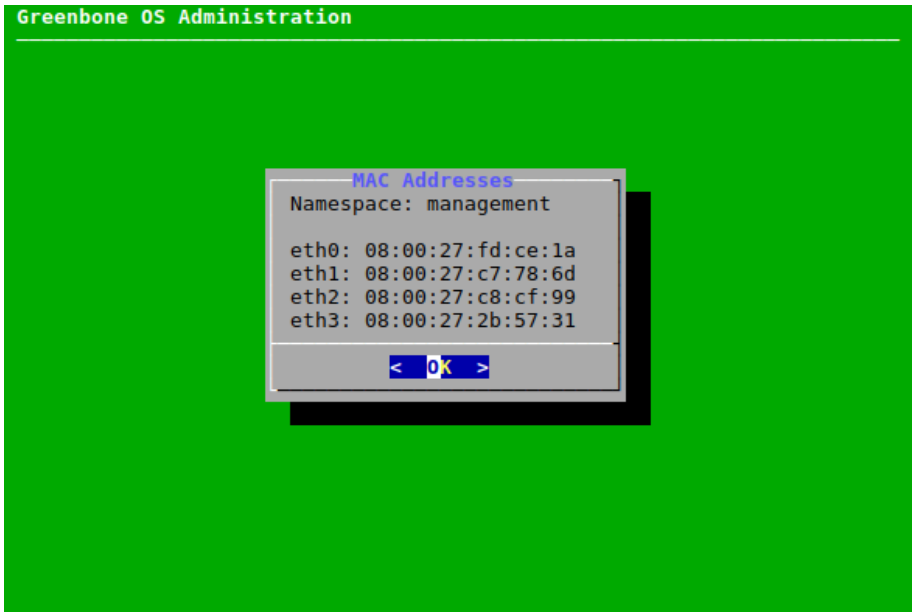


Fig. 7.26: Displaying the MAC/IP addresses or network routes

7.2.3 Configuring a Virtual Private Network (VPN) Connection

OpenVPN is integrated in GOS. The VPN feature allows scanning of targets reachable through the VPN tunnel, but has no effect on other targets, network settings, or master-sensor connections.

Note: Scanning through a VPN tunnel is only available for the appliance models Greenbone Enterprise DECA/TERA/PETA/EXA (see Chapter *3* (page 20)).

To run scans through a VPN tunnel, a VPN connection must be set up. The VPN tunnel is always initiated from the appliance side.

A PKCS#12 file with the following requirements is needed to authenticate the appliance in the VPN:

- The PKCS#12 file must contain the necessary certificate, and private key files.
- The PKCS#12 file may contain a certificate authority (CA) file. If it does not contain one, the CA file must be imported separately.
- The PKCS#12 file may be password protected or not.
- Password-protected private key files within the PKCS#12 file are not supported.

7.2.3.1 Setting up a VPN Connection

Note: Only one VPN connection can be set up at a time.

A new VPN connection can be set up as follows:

1. Select *Setup* and press `Enter`.
2. Select *VPN* and press `Enter`.
3. Select *Add a new VPN* and press `Enter` (see Fig. 7.27).

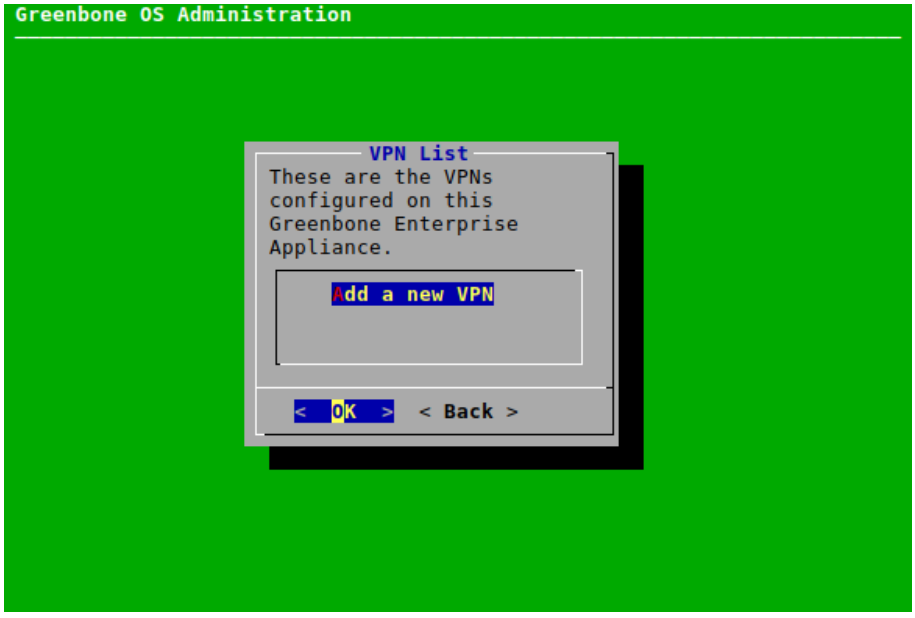


Fig. 7.27: Adding a VPN connection

4. Enter the VPN's IP address in the input box and press `Enter`.

5. Open the web browser and enter the displayed URL.
6. Click *Browse...*, select the PKCS#12 container and click *Upload*.
7. If an export password was used to protect the PKCS#12 container, enter the password and press `Enter`.

   → A message informs that the PKCS#12 file was successfully extracted.
8. Press `Enter`.

Note: If the PKCS#12 file does not contain a CA file, the CA file must be imported separately.

If the PKCS#12 file already contains a CA file, a CA file can also be imported separately, but this overwrites the CA file from the PKCS#12 file.

---

9. Select *Certificate Authority* and press `Enter`.
10. Open the web browser and enter the displayed URL.
11. Click *Browse...*, select the CA file and click *Upload*.

    → A message informs that the CA file was imported successfully.
12. Press `Enter`.

    → The VPN connection is established and targets reachable via the VPN can be scanned (see Chapter *10.2* (page 211)).

7.2.3.2 Editing or Deleting a VPN Connection

The VPN connection can be edited as follows:

1. Select *Setup* and press `Enter`.
2. Select *VPN* and press `Enter`.

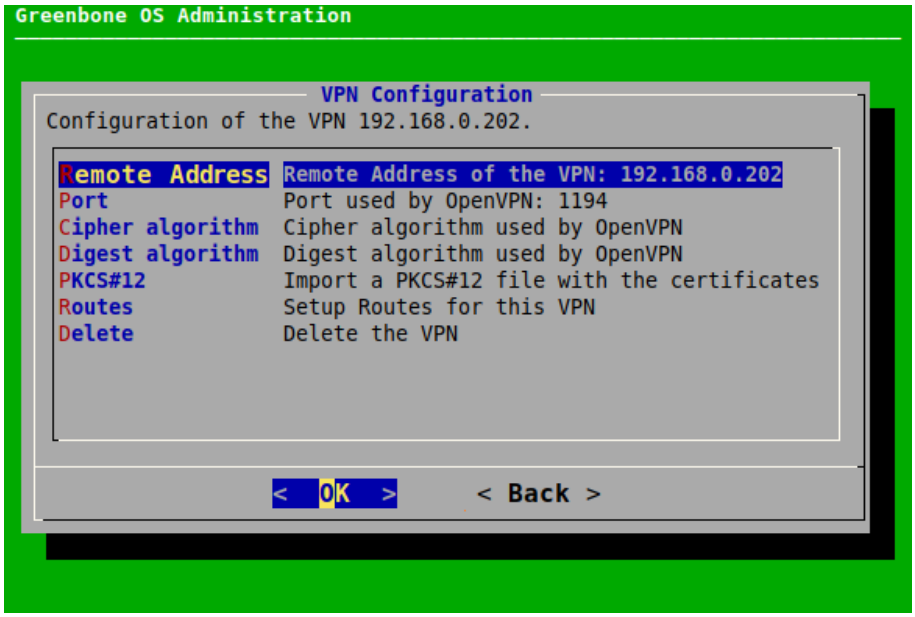


Fig. 7.28: Editing or deleting a VPN connection

The following actions are available:

Remote Address Define the VPN's IP address.

Port Define the port used by OpenVPN. By default, the port is 1194.

Cipher algorithm Select the cipher algorithm. By default, the default setting of OpenVPN is used.

Digest algorithm Select the digest algorithm. By default, the default setting of OpenVPN is used.

PKCS#12 Replace the PKCS#12 file.

Routes Add a route for the VPN connection. Target IP address, net mask and target gateway must be defined.

> **Note:** Only one route can be set up for the VPN connection.

Delete Delete the VPN connection.

7.2.4 Configuring Services

To access the appliance remotely, many interfaces are available:

- HTTPS, see Chapter *7.2.4.1* (page 97)
- Greenbone Management Protocol (GMP), see Chapter *15* (page 361)
- Open Scanner Protocol (OSP), see Chapter *7.2.4.3* (page 107)
- SSH, see Chapter *7.2.4.4* (page 108)
- SNMP, see Chapter *7.2.4.5* (page 111)

7.2.4.1 Configuring HTTPS

The web interface is the usual option for creating, running and analyzing vulnerability scans. It is enabled by default and cannot be disabled.

An HTTPS certificate is required for using the web interface.

The web interface is securely configured with the factory settings provided by Greenbone, but security can be further enhanced with the configuration options described in this chapter.

Configuring the Timeout of the Web Interface

If no action is performed on the web interface for a defined period of time, the user is logged out automatically. The timeout value can be set as follows:

1. Select *Setup* and press `Enter`.
2. Select *Services* and press `Enter`.
3. Select *HTTPS* and press `Enter`.
4. Select *Timeout* and press `Enter`.

5. Enter the desired timeout value in the input box and press `Enter` (see Fig. 7.29).

Note: The value can be between 1 and 1440 minutes (1 day). The default value is 15 minutes.

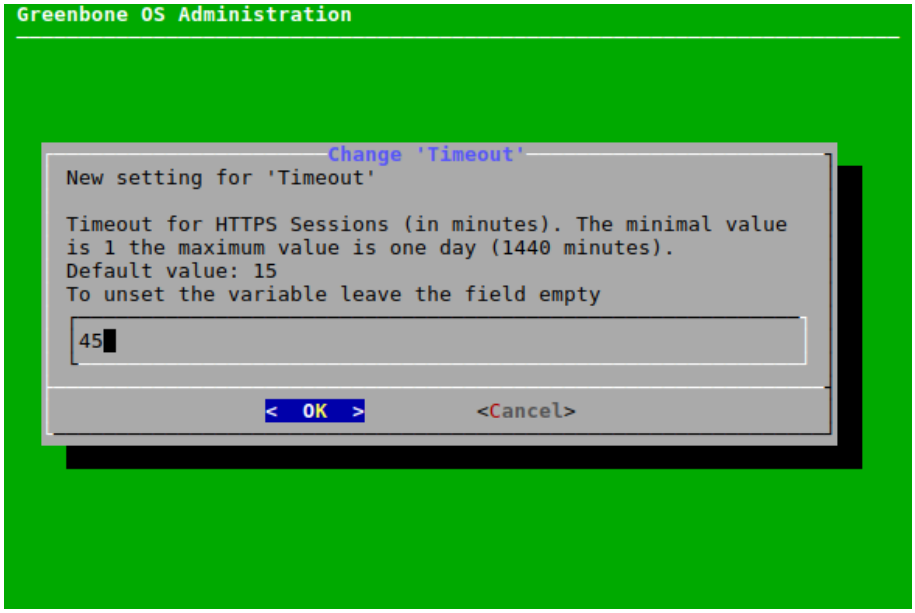


Fig. 7.29: Setting the timeout value

→ A message informs that the changes must be saved.

6. Press `Enter` to close the message.

Configuring the TLS Protocols

The TLS protocols for the HTTPS connection of the web interface can be configured as follows:

1. Select *Setup* and press `Enter`.
2. Select *Services* and press `Enter`.
3. Select *HTTPS* and press `Enter`.
4. Select *Protocols* and press `Enter`.
5. Select the desired protocol version and press `Space` (see Fig. 7.30).

Note: By default, both versions are selected.

If *TLSv1.2* is selected (either alone or in combination with version 1.3), the ciphers for the HTTPS connection can be configured (see Chapter *7.2.4.1.3* (page 99)).

If only *TLSv1.3* is selected, the default value for `-ciphersuites val` of OpenSSL[11] for the cipher suites is used. In this case, the menu option for configuring the ciphers is not available.

[11] https://www.openssl.org/docs/man1.1.1/man1/ciphers.html

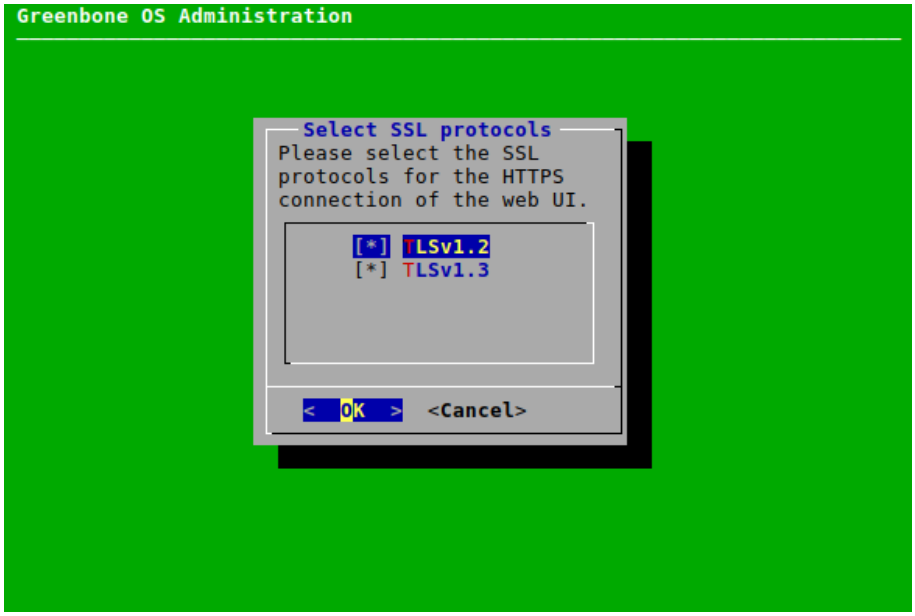


Fig. 7.30: Configuring the TLS protocols for the HTTPS connection

6. Select *OK* and press `Enter`.

Configuring the Ciphers

If TLS version 1.2 is used for the HTTPS connection of the web interface (either alone or in combination with version 1.3, see Chapter *7.2.4.1.2* (page 98)), the HTTPS ciphers can be configured to further enhance the security of the web interface.

Note: The current setting only allows secure ciphers using at least 128 bit key length, explicitly disallowing the cipher suites used by SSLv3 and TLSv1.0.

No ciphers exist for TLSv1.1.

The HTTPS ciphers can be configured as follows:

1. Select *Setup* and press `Enter`.
2. Select *Services* and press `Enter`.
3. Select *HTTPS* and press `Enter`.
4. Select *Ciphers* and press `Enter`.
5. Enter the desired value in the input box and press `Enter` (see Fig. 7.31).

   Note: The string used to define the ciphers is validated by OpenSSL and must comply with the syntax of an OpenSSL cipher list.

   More information about the syntax can be found here[12].

   → A message informs that the changes must be saved.

[12] https://www.openssl.org/docs/man1.1.1/man1/ciphers.html

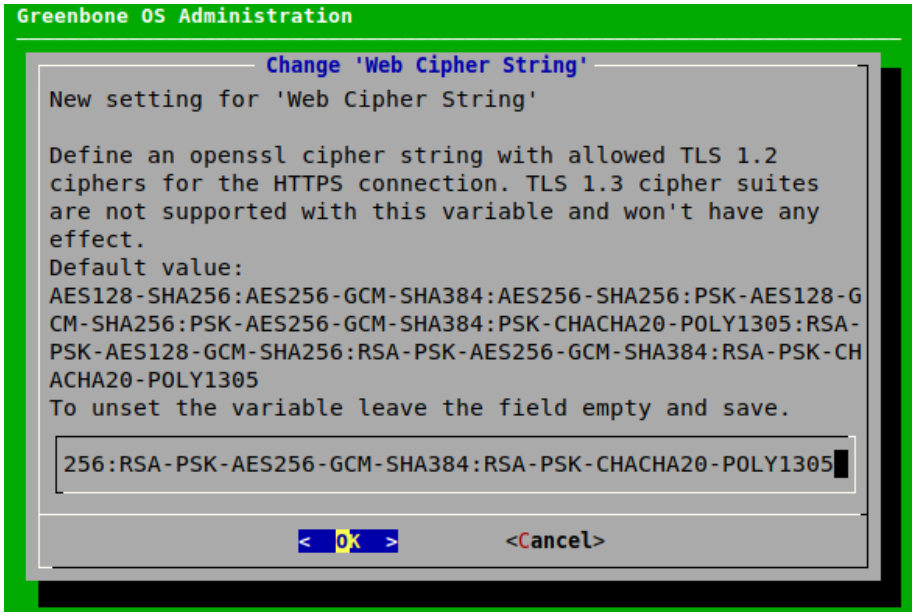


Fig. 7.31: Configuring the ciphers

6. Press `Enter` to close the message.

Configuring the Diffie-Hellman (DH) Parameters

DH parameters are used by the web server for establishing TLS connections. To further enhance the security of the web interface, new DH parameters can be generated as follows:

1. Select *Setup* and press `Enter`.
2. Select *Services* and press `Enter`.
3. Select *HTTPS* and press `Enter`.
4. Select *DH Parameters* and press `Enter`.
5. Select the desired key size and press `Space`.
6. Press `Enter`.

   → A message informs that the generation was started in the background.

Tip: The currently running system operation can be displayed by selecting *About* and pressing `Enter` in the GOS administration menu.

Configuring HTTP STS

To further enhance the security of the web interface, HTTP Strict Transport Security (HSTS) can be enabled. For HSTS to work, an HTTPS certificate signed by a certificate authority (CA) is required (see Chapter *7.2.4.1.7.2* (page 104)).

Enabling HSTS

HSTS can be enabled as follows:

1. Select *Setup* and press `Enter`.

2. Select *Services* and press `Enter`.
3. Select *HTTPS* and press `Enter`.
4. Select *HTTP STS* and press `Enter` to enable or disable HSTS.

Setting the Maximum Allowed Age of the HSTS Header

When HTTP STS is enabled, the maximum allowed age for the HSTS header can be set as follows:

1. Select *Setup* and press `Enter`.
2. Select *Services* and press `Enter`.
3. Select *HTTPS* and press `Enter`.
4. Select *HTTP STS max age* and press `Enter`.
5. Enter the maximum age in seconds in the input box and press `Enter` (see Fig. 7.32).

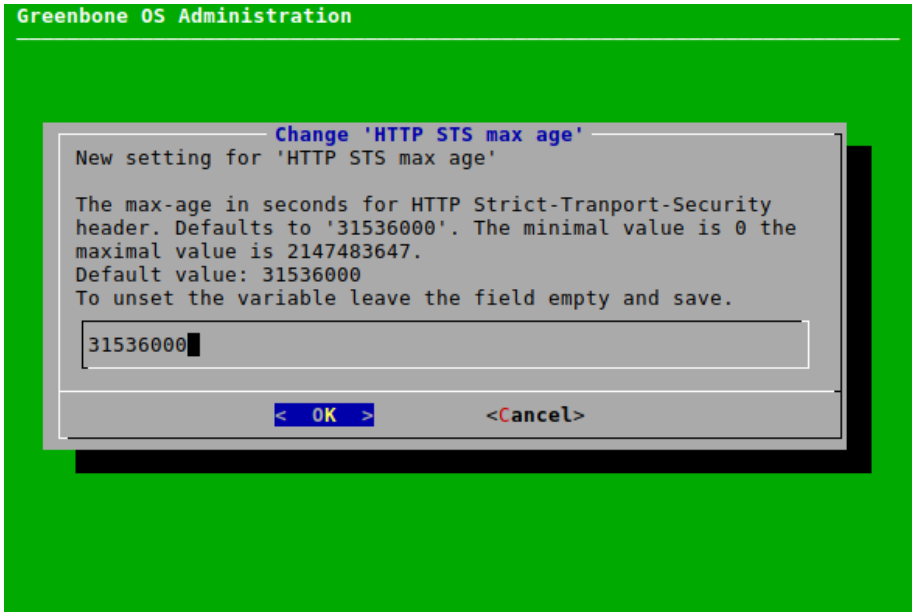


Fig. 7.32: Setting the maximum allowed age for the HTTP STS header

→ A message informs that the changes must be saved.

6. Press `Enter` to close the message.

Configuring OCSP Stapling

OCSP (Online Certificate Status Protocol) stapling is used for checking the validity status of X.509 digital certificates. It allows the certified party to perform the certificate validation by appending a time-stamped OCSP response signed by the certificate authority (CA) to the original TLS handshake (“stapling”).

OCSP stapling can be enabled as follows:

1. Select *Setup* and press `Enter`.
2. Select *Services* and press `Enter`.
3. Select *HTTPS* and press `Enter`.
4. Select *OCSP Stapling* and press `Enter` to enable or disable OCSP Stapling.

Managing Certificates

The appliance basically uses two types of certificates:

- Self-signed certificates
- Certificates issued by an external certificate authority (CA)

All modern operating systems support the creation and management of their own CA.

- Under Microsoft Windows Server, the Active Directory Certificate Services support the administrator in the creation of a root CA[13].
- For Linux systems, various options are available. One option is described in the IPSec-Howto[14].

Note: It must be verified how the systems are accessed later before creating the certificate.

The IP address or the DNS name is stored when creating the certificate.

Displaying the Current Certificate

The current certificate can be displayed as follows:

1. Select *Setup* and press `Enter`.
2. Select *Services* and press `Enter`.
3. Select *HTTPS* and press `Enter`.
4. Select *Certificate* and press `Enter`.
5. Select *Show* and press `Enter`.

   → The certificte is displayed.

Self-Signed Certificates

The use of self-signed certificates is the easiest way. It poses, however, the lowest security and more work for the user:

- The trustworthiness of a self-signed certificate can only be checked manually by the user through importing the certificate and examining its fingerprint.
- Self-signed certificates cannot be revoked. Once they are accepted by the user, they are stored permanently in the browser. If an attacker gains access to the corresponding private key, a man-in-the-middle attack on the connection protected by the certificate can be launched.

To support a quick setup, the appliance supports self-signed certificates.

- For most appliance models, such a certificate is not installed by default and must be created.
- Only the Greenbone Enterprise ONE already comes with a pre-installed certificate.

Creating a Self-Signed Certificate

Self-signed certificates can be created as follows:

1. Select *Setup* and press `Enter`.
2. Select *Services* and press `Enter`.
3. Select *HTTPS* and press `Enter`.

[13] https://learn.microsoft.com/en-us/windows-server/networking/core-network-guide/cncg/server-certs/install-the-certification-authority
[14] https://www.ipsec-howto.org/x600.html

4. Select *Certificate* and press `Enter`.
5. Select *Generate* and press `Enter`.

   → A message informs that the current certificate and private key will be overwritten.
6. Confirm the message by selecting *Yes* and pressing `Enter`.
7. Provide the settings for the certificate (see Fig. 7.33), select *OK* and press `Enter`.

Note: It is valid to generate a certificate without a common name. However, a certificate should not be created without (a) Subject Alternative Name(s) (SAN).

If a common name is used, it should be the same as one of the SANs.

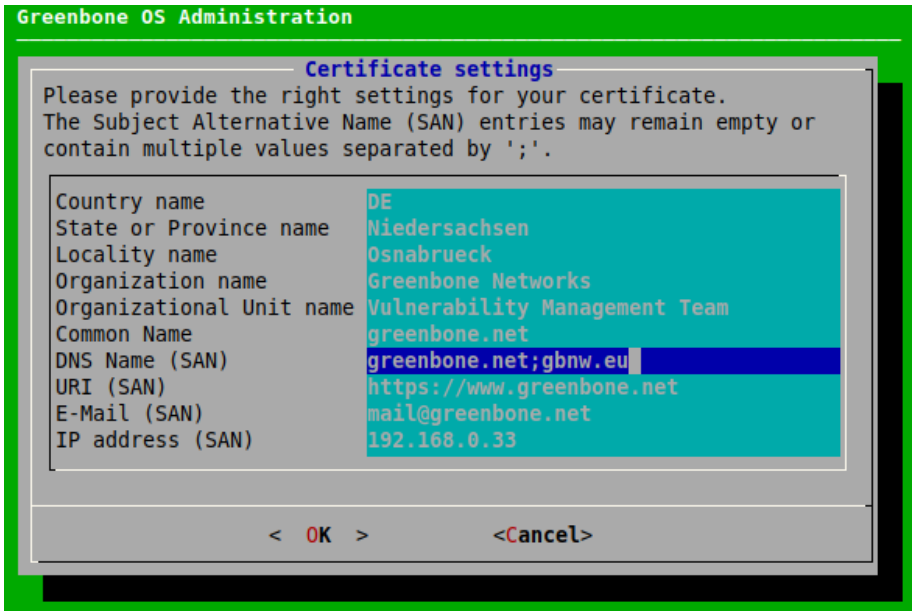


Fig. 7.33: Providing settings for the certificate

   → When the process is finished, a message informs that the certificate can be downloaded.
8. Press `Enter` to close the message.
9. Select *Download* and press `Enter`.
10. Open the web browser and enter the displayed URL.
11. Download the PEM file.
12. In the GOS administration menu, press `Enter`.

    → When the certificate is retrieved by the appliance, the GOS administration menu displays the fingerprint of the certificate for verification.
13. Check the fingerprint and confirm the certificate by pressing `Enter`.

Certificate by an External Certificate Authority (CA)

The use of a certificate issued by a CA has several advantages:

- All clients trusting the CA can verify the certificate directly and establish a secure connection. No warning is displayed in the browser.
- The certificate can be revoked easily by the CA. If the clients have the ability to check the certificate status, they can decline a certificate that may still be within its validity period but has been revoked. As mechanisms, the Certificate Revocation Lists (CRLs) or Online Certificate Status Protocol (OCSP) can be used.
- Especially if multiple systems within an organization serve SSL/TLS protected information, the use of an organizational CA simplifies the management drastically. All clients simply have to trust the organizational CA to accept all certificates issued by the CA.

To import a certificate by an external CA, two options are available:

- Generate a certificate signing request (CSR) on the appliance, sign it via an external CA and import the certificate.
- Generate the CSR and the certificate externally and import both using a PKCS#12 file.

Generating a CSR and Importing a Certificate

Note: The appliance's web interface cannot be used while waiting for CA to process the CSR. Only after the signed certificate has been imported, the web interface is accessible again.

A new CSR can be created and the certificate can be imported as follows:

1. Select *Setup* and press `Enter`.
2. Select *Services* and press `Enter`.
3. Select *HTTPS* and press `Enter`.
4. Select *Certificate* and press `Enter`.
5. Select *CSR* and press `Enter`.

   → A message informs that the current certificate and private key will be overwritten.
6. Confirm the message by selecting *Yes* and pressing `Enter`.
7. Provide the settings for the certificate (see Fig. 7.34), select *OK* and press `Enter`.

   Note: It is valid to generate a certificate without a common name. A certificate should not be created without (a) Subject Alternative Name(s).

   If a common name is used, it should be the same as one of the SANs.
8. Open the web browser and enter the displayed URL.
9. Download the PEM file.

   → The GOS administration menu displays a message to verify that the CSR has not been tampered with.
10. Verify the information by pressing `Enter`.
11. When the certificate was signed by the CA, select *Certificate* and press `Enter`.
12. Open the web browser and enter the displayed URL.

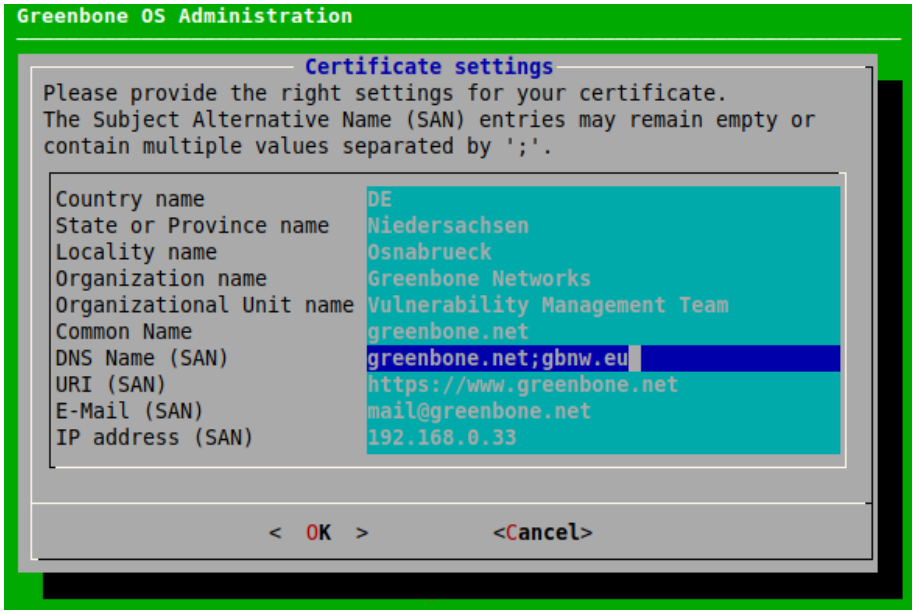


Fig. 7.34: Providing settings for the certificate

13. Click *Browse...*, select the signed certificate and click *Upload*.

    → When the certificate is retrieved by the appliance, the GOS administration menu displays the fingerprint of the certificate for verification.

14. Check the fingerprint and confirm the certificate by pressing `Enter`.

Importing an Already Existing Certificate

If a private key and a signed certificate already exist, they can be imported. The private key and the certificate must be formatted as a PKCS#12 file. The file can be protected with an export password.

The PKCS#12 file can be imported as follows:

1. Select *Setup* and press `Enter`.
2. Select *Services* and press `Enter`.
3. Select *HTTPS* and press `Enter`.
4. Select *Certificate* and press `Enter`.
5. Select *PKCS#12* and press `Enter`.

   → A message informs that the current certificate and private key will be overwritten.

6. Confirm the message by selecting *Yes* and pressing `Enter`.
7. Open the web browser and enter the displayed URL.
8. Click *Browse...*, select the PKCS#12 container and click *Upload*.

   Note: If an export password is used to protect the PKCS#12 container, the password must be entered.

   → When the certificate is retrieved by the appliance, the GOS administration menu displays the fingerprint of the certificate for verification.

9. Check the fingerprint and confirm the certificate by pressing `Enter`.

Displaying Fingerprints

The fingerprints of the used certificate can be displayed and checked as follows:

1. Select *Setup* and press `Enter`.
2. Select *Services* and press `Enter`.
3. Select *HTTPS* and press `Enter`.
4. Select *Fingerprints* and press `Enter`.

   → The following fingerprints of the currently active certificate are displayed:

   - SHA1
   - SHA256
   - BB

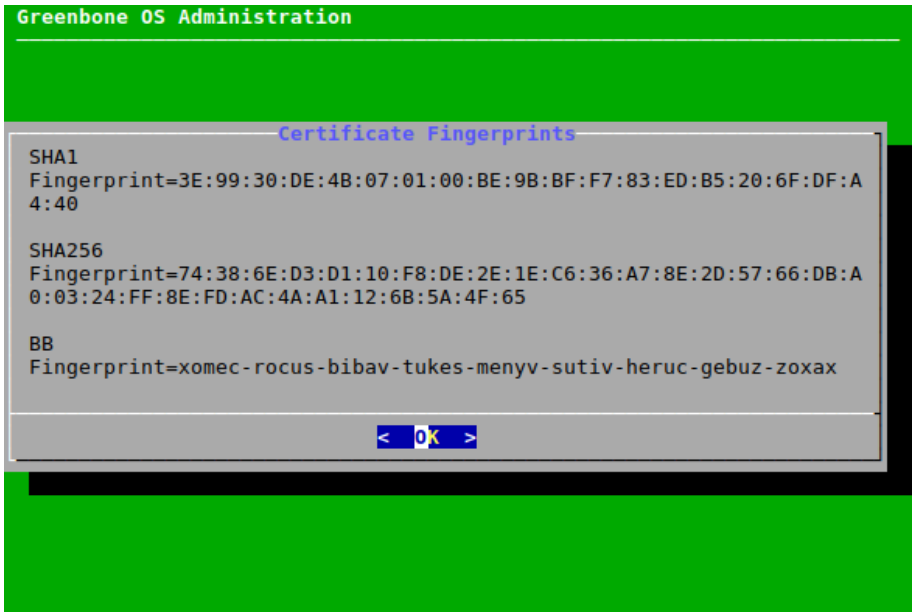


Fig. 7.35: Displaying the fingerprints

7.2.4.2 Configuring the Greenbone Management Protocol (GMP)

The Greenbone Management Protocol (GMP) can be used for the communication of in-house software with the appliance.

GMP can be activated using the GOS administration menu as follows:

Note: The SSH service must be enabled before GMP can be enabled (see Chapter *7.2.4.4* (page 108)).

1. Select *Setup* and press `Enter`.
2. Select *Services* and press `Enter`.
3. Select *GMP* and press `Enter`.
4. Press `Enter` to enable or disable GMP (see Fig. 7.36).

   → A message informs that the changes must be saved.
5. Press `Enter` to close the message.

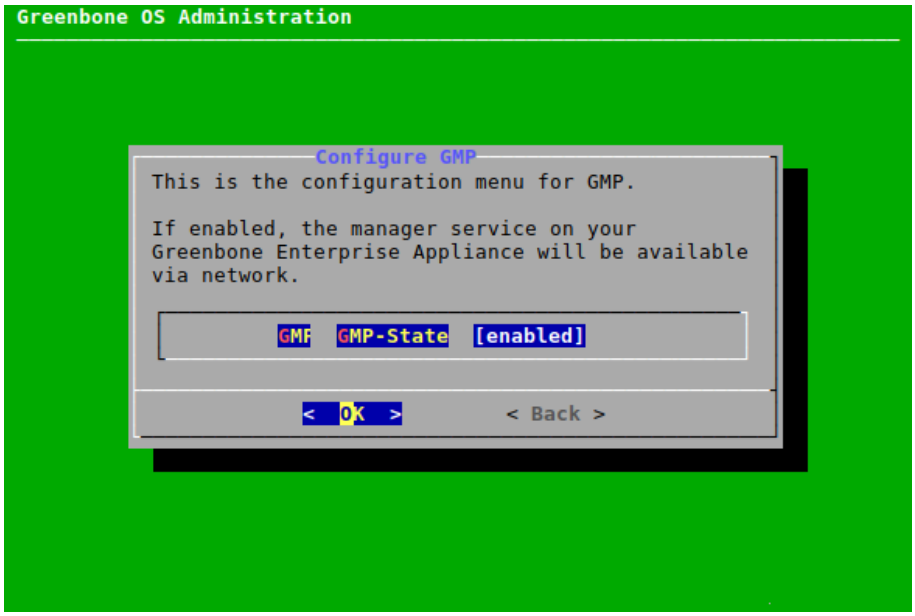


Fig. 7.36: Enabling GMP

7.2.4.3 Configuring the Open Scanner Protocol (OSP)

The Open Scanner Protocol (OSP) is required for the master-sensor communication (see Chapter *16* (page 371)).

OSP can be activated using the GOS administration menu as follows:

Note: The SSH service must be enabled before OSP can be enabled (see Chapter *7.2.4.4* (page 108)).

1. Select *Setup* and press `Enter`.
2. Select *Services* and press `Enter`.
3. Select *OSP* and press `Enter`.

4. Press `Enter` to enable or disable OSP.

   → A message informs that the changes must be saved.

5. Press `Enter` to close the message.

7.2.4.4 Configuring SSH

SSH allows secure and remote access to the appliance's GOS administration menu and command line over an unsecured network. Additionally, it is required for the master-sensor communication (see Chapter *16* (page 371)).

By default, SSH is disabled on the appliance and must be activated first, e.g., by using the serial console. In addition, an SSH client is required to connect to the appliance.

- When connecting *to* the appliance with an SSH client, the following key exchange methods are supported:
  - ecdh-sha2-nistp256
  - ecdh-sha2-nistp384
  - ecdh-sha2-nistp521
  - curve25519-sha256
  - curve25519-sha256@libssh.org
- When connecting *from* the appliance to another system, the supported methods depend both on the other system and the appliance. There are many possible combinations, which would go beyond the scope of this documentation.

Enabling the SSH State

The SSH server embedded in the appliance can be enabled as follows:

1. Select *Setup* and press `Enter`.
2. Select *Services* and press `Enter`.
3. Select *SSH* and press `Enter`.
4. Select *SSH State* and press `Enter` to enable SSH.

Enabling and Managing a Login Protection

A login protection can be enabled, i.e., if a number of consecutive login attempts fail, the user will be locked.

Note: A self-scan, i.e., a scan where the appliance is part of the scan target, may trigger the login protection.

The login protection does not block logging in via SSH admin key if such a key is set up (see Chapter *7.2.4.4.3* (page 110)).

Setting Up the Login Protection

The login protection can be enabled and managed as follows:

1. Select *Setup* and press `Enter`.
2. Select *Services* and press `Enter`.
3. Select *SSH* and press `Enter`.
4. Select *Login Protection* and press `Enter`.
5. Select *Login Protection* and press `Enter` (see Fig. 7.37).

Fig. 7.37: Setting a login protection

→ A message informs that the login protection can lead to a locked SSH access.

6. Select *Continue* and press `Enter` to enable the login protection.
7. Select *Login Attempts* and press `Enter`.
8. Enter the desired value and press `Enter`.

   → A message informs that the changes must be saved.
9. Press `Enter` to close the message.

Unlocking a Locked System

In case the system is locked after too many failed login attempts, it must be unlocked using console access (serial, hypervisor or monitor/keyboard) as follows:

1. Select *Setup* and press `Enter`.
2. Select *User* and press `Enter`.
3. Select *Unlock SSH* and press `Enter`.

   → The login attempt counter is reset.
4. Press `Enter` to close the message.

Adding an SSH Admin Key

SSH public keys can be uploaded to enable key-based authentication of administrators.

Note:

- SSH keys can be generated with OpenSSH using the command `ssh-keygen` on Linux or `puttygen.exe` if using PuTTY on Microsoft Windows.
- The following formats are supported:
  - Ed25519, e.g., `ssh-ed25519 AAAAB3NzaC1y...P3pCquVb admin@greenbone`
  - RSA, e.g., `ssh-rsa AAAAB3NzaC1y...P3pCquVb admin@greenbone`

An SSH admin key can be uploaded as follows:

1. Select *Setup* and press `Enter`.
2. Select *Services* and press `Enter`.
3. Select *SSH* and press `Enter`.
4. Select *Admin Key* and press `Enter`.
5. Open the web browser and enter the displayed URL (see Fig. 7.38).

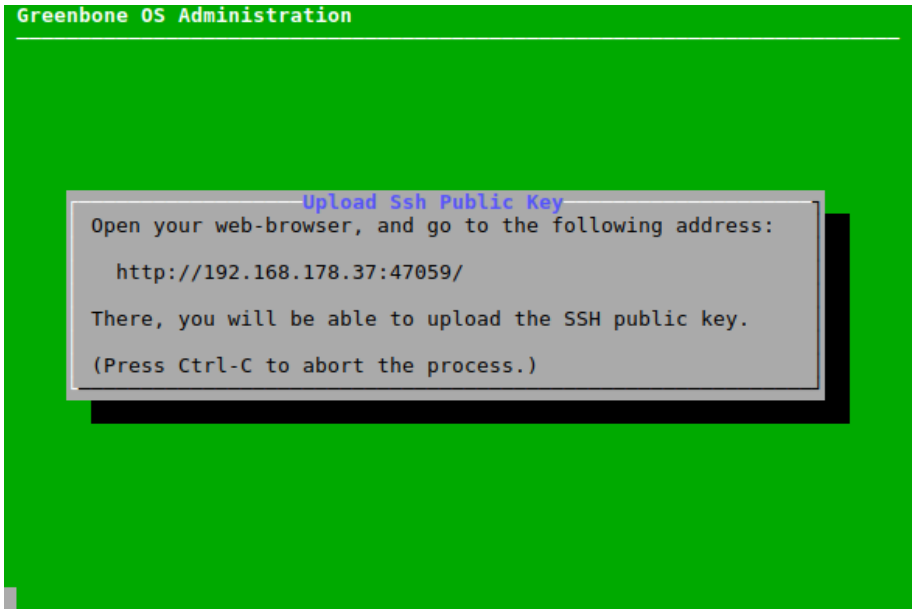


Fig. 7.38: Uploading an SSH public key

6. Click *Browse...*, select the SSH public key and click *Upload*.

   → When the upload is completed, a message informs that the login via SSH is possible.

Displaying Fingerprints

The appliance provides different host keys for its own authentication. The client decides which public key to use.

The fingerprints of the public keys used by the appliance's SSH server can be displayed as follows:

1. Select *Setup* and press `Enter`.
2. Select *Services* and press `Enter`.
3. Select *SSH* and press `Enter`.
4. Select *Fingerprint* and press `Enter`.

   → The SHA256 fingerprints of the following keys are displayed:

   - Ed25519
   - RSA

7.2.4.5 Configuring SNMP

The appliance supports SNMPv3 for read access, and SNMPv1 for sending traps through alerts and monitoring vital parameters of the appliance.

The supported parameters are specified in a Management Information Base (MIB) file. The current MIB is available in the Greenbone TechDoc Portal[15].

SNMPv3 can be configured as follows:

1. Select *Setup* and press `Enter`.
2. Select *Services* and press `Enter`.
3. Select *SNMP* and press `Enter`.
4. Select *SNMP* and press `Enter` to enable SNMP.

   → Several new options are displayed (see Fig. 7.39).
5. Select *Location* and press `Enter`.
6. Enter the location of the SNMP service in the input box and press `Enter`.
7. Select *Contact* and press `Enter`.
8. Enter the contact of the SNMP service in the input box and press `Enter`.
9. Select *Username* and press `Enter`.
10. Enter the SNMP user name in the input box and press `Enter`.

    Note: When configuring the authentication and privacy passphrase, note that the appliance uses SHA-1 and AES128 respectively.

11. Select *Authentication* and press `Enter`.
12. Enter the SNMP user authentication passphrase in the input box and press `Enter`.
13. Select *Privacy* and press `Enter`.

[15] https://docs.greenbone.net/API/SNMP/snmp-gos-22.04.en.html

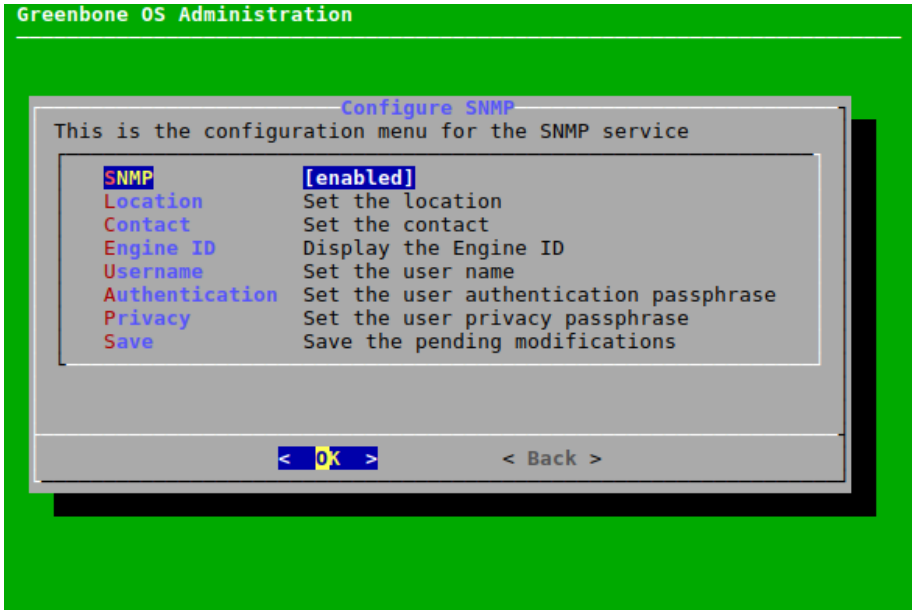


Fig. 7.39: Configuring SNMPv3

14. Enter the SNMP user privacy passphrase in the input box and press `Enter`.

> **Note:** After a user has been configured, the appliance's engine ID can be displayed by selecting *Engine ID* and pressing `Enter`.

15. Afterwards, test the read access of the SNMP service under Linux/Unix using `snmpwalk`:

```
$ snmpwalk -v 3 -l authPriv -u user -a sha -A password -x aes -X key 192.168.222.115
iso.3.6.1.2.1.1.1.0 = STRING: "Greenbone Enterprise Appliance"
iso.3.6.1.2.1.1.3.0 = Timeticks: (347275248) 40 days, 4:39:12.48
iso.3.6.1.2.1.1.4.0 = STRING: "Greenbone AG <info@greenbone.net>"
...
```

The following information can be gathered:

- Uptime
- Network interfaces
- Memory
- Harddisk
- Load
- CPU

7.2.4.6 Configuring a Port for the Temporary HTTP Server

By default, the port for HTTP uploads and downloads is randomly selected.

A permanent port can be configured as follows:

1. Select *Setup* and press `Enter`.
2. Select *Services* and press `Enter`.

3. Select *Temporary HTTP* and press `Enter`.
4. Select *Port* and press `Enter`.
5. Enter the port in the input box and press `Enter`.

   → A message informs that the changes must be saved.
6. Press `Enter` to close the message.

7.2.5 Configuring Periodic Backups

The appliance supports automatic daily backups. The following backups are stored locally or remotely:

- Last 7 daily backups
- Last 5 weekly backups
- Last 12 monthly backups

Backups older than one year will be deleted automatically.

7.2.5.1 Enabling Periodic Backups

Periodic backups can be enabled as follows:

1. Select *Setup* and press `Enter`.
2. Select *Backup* and press `Enter`.
3. Select *Periodic Backup* and press `Enter` (see Fig. 7.40).

   → Periodic backups are enabled.

Fig. 7.40: Configuring periodic backups

7.2.5.2 Setting up a Remote Backup Server

By default, backups are stored locally. To store them on a remote server, the server must be set up appropriately. The appliance uses the SSH File Transfer Protocol (SFTP) to securely transfer the backups.

The remote server can be set up as follows:

1. Select *Setup* and press `Enter`.
2. Select *Backup* and press `Enter`.
3. Select *Backup Location* and press `Enter`.

   → More options for the backup location are added (see Fig. 7.41).

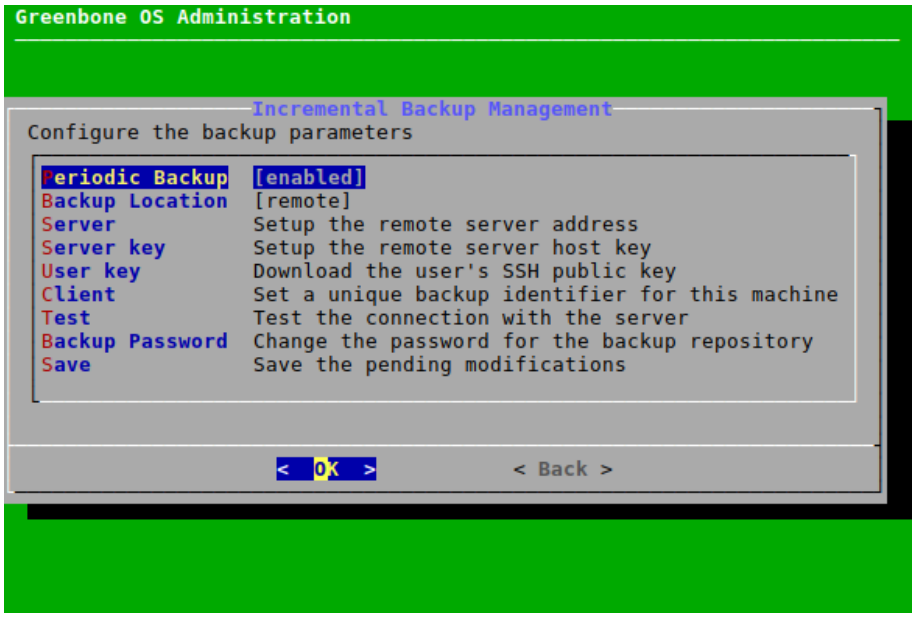


Fig. 7.41: Setting up the remote server

4. Select *Server* and press `Enter`.
5. Enter the remote server address in the following format:

   `username@hostname[:port]/directory`

   Note: The optional port may be omitted if the server uses port 22.

6. Select *OK* and press `Enter`.

   → A message informs that the changes must be saved.

7. Press `Enter` to close the message.

Note: The appliance uses an SSH host public key to identify the remote server.

- The key must be looked up on the remote backup server. On Linux and most Unix-like systems, it can be found under `/etc/ssh/ssh_host_*_key.pub`.
- The key must be in the OpenSSH Public Key Format.
- The expected structure is `<algorithm> <key> <comment>`.
  - The `<key>` section must be Base64 encoded.
  - The `<comment>` section is optional.
  - Example: `ssh-rsa AAAAB3NzaC1y...P3pCquVb`

8. Select *Server key* and press `Enter`.
9. Open the web browser and enter the displayed URL (see Fig. 7.42).

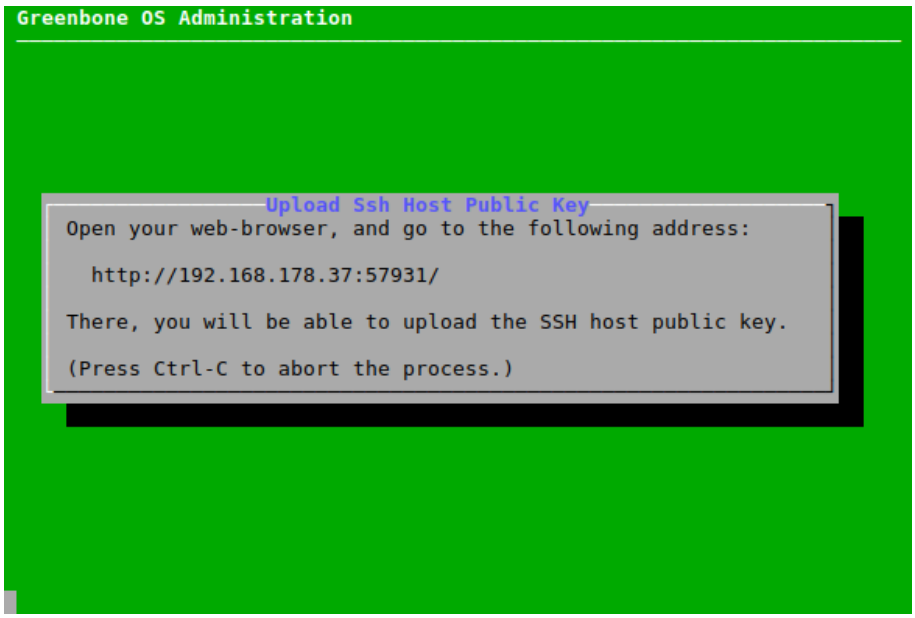


Fig. 7.42: Setting up the server key

10. Click *Browse...*, select the SSH host public key and click *Upload*.

Note: The appliance uses an SSH public key to log in on the remote server. To enable this login process, the SSH public key of the appliance must be enabled in the `authorized_keys` file on the remote server.

11. To download the public key, select *User key* and press `Enter`.
12. Open the web browser and enter the displayed URL.
13. Download the PUB file.

Note: If several appliances upload their backups to the same remote server, the files must be distinguishable. For this, a unique backup identifier must be defined. If this identifier is not set, the host name will be used.

14. Select *Client* and press `Enter`.
15. Enter the identifier and press `Enter`.

    Note: Since the setup of the remote backup including the keys is error-prone, a test routine is available. This option will test the successful login to the remote system.

16. Select *Test* and press `Enter`.

    → The login to the remote system is tested.

    Note: Optionally, the backup repository password can be changed, which is recommended.

    If multiple appliances use the same remote backup repository, it is recommended that each appliance uses its own unique backup password.

17. Select *Backup Password* and press `Enter`.
18. Enter the password in the input box and press `Enter`.

7.2.6 Configuring Special Upgrade Settings

7.2.6.1 Adding an Upgrade Key

This option is intended for possible recovery purposes. Uploading an upgrade key is not required for normal appliance operation and should only be done when instructed by Greenbone. Greenbone will provide the upgrade key in such a case.

Note: The key is automatically removed when GOS is upgraded successfully.

Adding an Upgrade Key Using the Editor

The key can be added using the editor as follows:

1. Select *Setup* and press `Enter`.
2. Select *Upgrade* and press `Enter`.
3. Select *New Upgrade Key (Editor)* and press `Enter` (see Fig. 7.43).

   → The editor is opened.
4. Enter the content of the upgrade key.

   Note: It is important to enter the content of the key and not the name of the key (e.g., `GBFeedSigningKeyUntil2024.gpg.asc`).

   The content of the key can be displayed with any text editor or under Linux using the program `less`. If the content is opened with a text editor, care must be taken to not change anything.

5. Press `Ctrl` + `S` to save the changes.
6. Press `Ctrl` + `X` to close the editor.

   → A message informs that the upgrade key was uploaded successfully.

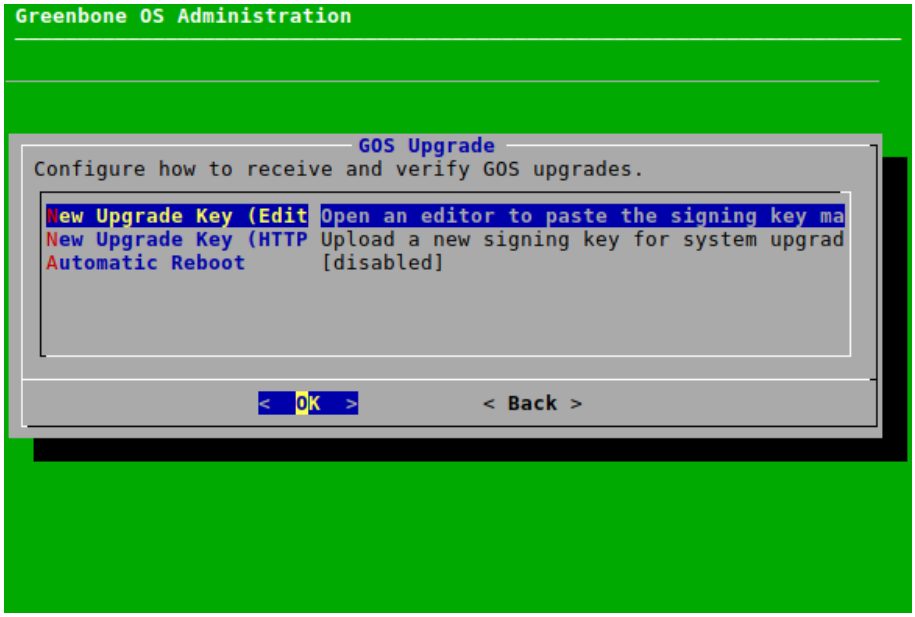


Fig. 7.43: Uploading an upgrade key

7. Press `Enter` to close the message.

   → Both menu options for uploading a key are hidden temporarily. Instead, the menu option *Delete Upgrade Key* is displayed (see Chapter *7.2.6.2* (page 117)).

Adding an Upgrade Key via HTTP

The key can be added via HTTP as follows:

1. Select *Setup* and press `Enter`.
2. Select *Upgrade* and press `Enter`.
3. Select *New Upgrade Key (HTTP)* and press `Enter` (see Fig. 7.43).
4. Open the web browser and enter the displayed URL.
5. Click *Browse...*, select the upgrade key and click *Upload*.

   → A message informs that the upgrade key was successfully uploaded.
6. Press `Enter` to close the message.

   → Both menu options for uploading a key are hidden temporarily. Instead, the menu option *Delete Upgrade Key* is displayed (see Chapter *7.2.6.2* (page 117)).

7.2.6.2 Deleting an Upgrade Key

An upgrade key can be deleted as follows:

1. Select *Setup* and press `Enter`.
2. Select *Upgrade* and press `Enter`.
3. Select *Delete Upgrade Key* and press `Enter`.

   → A message informs that the upgrade key was deleted.
4. Press `Enter` to close the message.

7.2.6.3 Configuring the Automatic Reboot

The appliance may reboot automatically after a successful GOS upgrade. However, a reboot is only performed when required, e.g., if the GOS Linux kernel is upgraded.

The automatic reboot is disabled by default. In this case, after a GOS upgrade that requires a reboot, a self-check warning is displayed asking to reboot manually.

Note: This setting applies only to the appliance on which it is configured. It does not apply to all sensors connected to the appliance. If sensors should reboot automatically, each sensor must be configured separately.

1. Select *Setup* and press `Enter`.
2. Select *Upgrade* and press `Enter`.
3. Select *Automatic Reboot* and press `Enter`.

   → A warning informs that the appliance will reboot immediately after a GOS upgrade (see Fig. 7.44).

   Note: All scans running at that time will be terminated. This can lead to the loss of unsaved data.

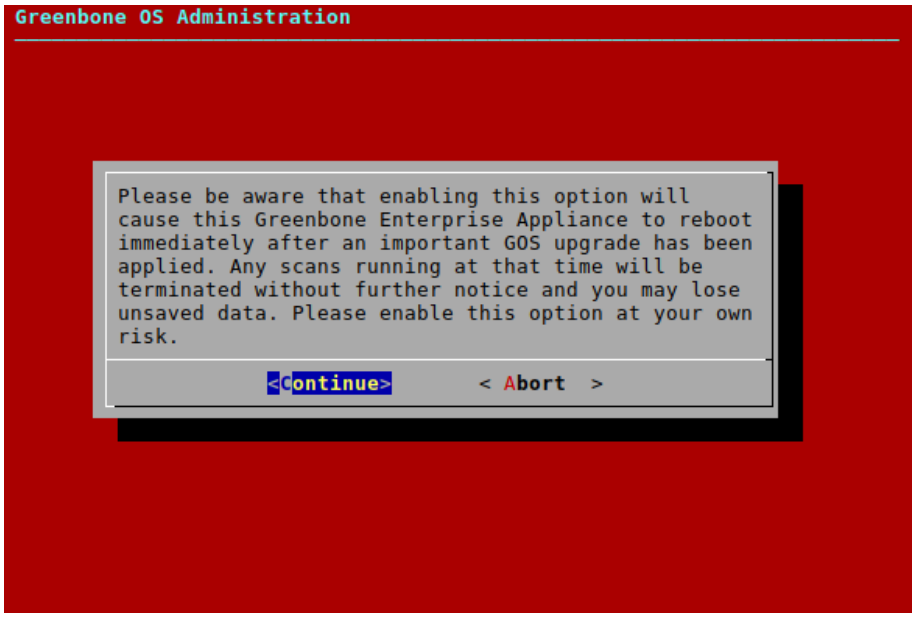


Fig. 7.44: Enabling automatic reboot

4. Select *Continue* and press `Enter`.

7.2.7 Configuring the Feed Synchronization

The Greenbone Enterprise Feed[16] provides updates to vulnerability tests (VT), SCAP data (CVE and CPE) and CERT-Bund and DFN-CERT advisories. Additionally, the feed provides upgrades for GOS as well as updates for scan configurations, compliance policies, port lists and report formats.

A subscription key is required to to download and use the Greenbone Enterprise Feed (see Chapter *7.1.1* (page 67)). If no valid key is stored on the appliance, the public Greenbone Community Feed is used instead of the Greenbone Enterprise Feed.

7.2.7.1 Adding a Greenbone Enterprise Feed Subscription Key

Note: It is not necessary to add a Greenbone Enterprise Feed subscription key on a newly delivered appliance since a key is already pre-installed.

Whether a subscription key is already present on the appliance can be displayed by selecting *About* and pressing `Enter` in the GOS administration menu.

A new subscription key can be stored on the appliance by either uploading it via HTTP or by copying and pasting it using an editor.

For information about the subscription key see Chapter *7.1.1* (page 67).

Note: The new key will overwrite any key already stored on the appliance.

When the subscription key is overwritten, the state of the feed on the appliance is reset to “No feed present”. A feed update must be performed after adding the new subscription key.

Adding a Subscription Key via HTTP

The key can be added via HTTP as follows:

1. Select *Setup* and press `Enter`.
2. Select *Feed* and press `Enter`.
3. Select *Key(HTTP)* and press `Enter`.

   → A message informs that the current subscription key will be overwritten (see Fig. 7.45).
4. Select *Yes* and press `Enter`.
5. Open the web browser and enter the displayed URL.
6. Click *Browse...*, select the subscription key and click *Upload*.

   → A message informs that the subscription key was uploaded successfully.
7. Press `Enter` to close the message.
8. Perform a feed update as described in Chapter *7.3.6* (page 150).

[16] https://www.greenbone.net/en/feed-comparison/

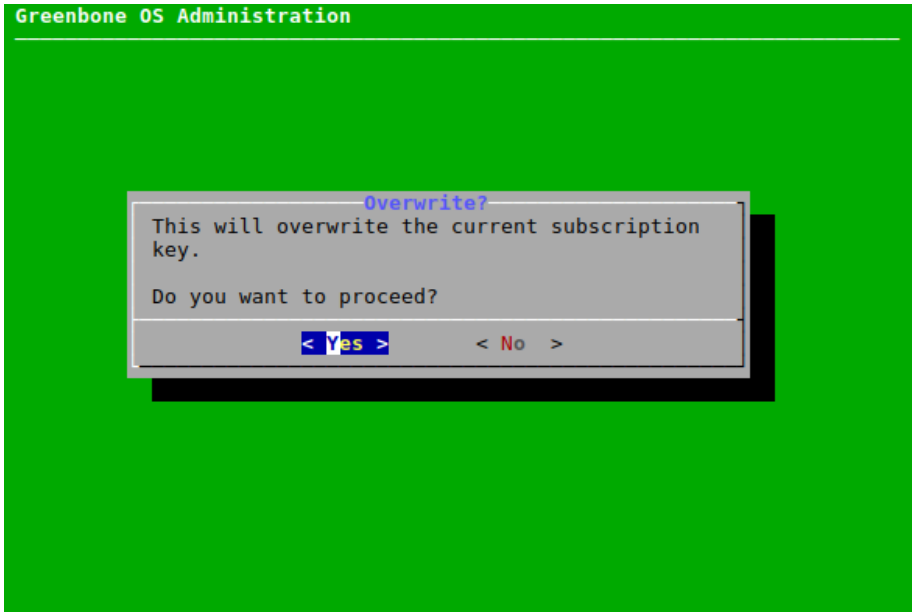


Fig. 7.45: Overwriting the current subscription key

Adding a Subscription Key Using the Editor

The key can be added using the editor as follows:

1. Select *Setup* and press `Enter`.
2. Select *Feed* and press `Enter`.
3. Select *Key(Editor)* and press `Enter`.

   → A message informs that the current subscription key will be overwritten (see Fig. 7.45).
4. Select *Yes* and press `Enter`.

   → The editor is opened.
5. Enter the content of the subscription key.

   Note: It is important to enter the content of the key and not the name of the key (e.g., `gsf2022122017`).

   The content of the key can be displayed with any text editor or under Linux using the program `less`. If the content is opened with a text editor, care must be taken to not change anything.
6. Press `Ctrl` + `S` to save the changes.
7. Press `Ctrl` + `X` to close the editor.

   → A message informs that the subscription key was uploaded successfully.
8. Press `Enter` to close the message.
9. Perform a feed update as described in Chapter *7.3.6* (page 150).

7.2.7.2 Enabling or Disabling Synchronization

The automatic synchronization of the Greenbone Enterprise Feed can be disabled in case the appliance does not have any internet access and should not try to access the Greenbone services on the internet. The synchronization can be enabled again.

The synchronization can be enabled or disabled as follows:

1. Select *Setup* and press `Enter`.
2. Select *Feed* and press `Enter`.
3. Select *Synchronisation* and press `Enter`.

   → The synchronization is enabled.
4. The synchronization can be disabled by selecting *Synchronisation* and pressing `Enter` again.

Note: The time of the automatic feed synchronization can be set by changing the maintenance time (see Chapter *7.2.13* (page 137)).

7.2.7.3 Configuring the Synchronization Port

The Greenbone Enterprise Feed is provided by Greenbone on two different ports:

- 24/tcp
- 443/tcp

While port 24/tcp is the default port, many firewall setups do not allow traffic to this port on the internet. Therefore, changing the port to 443/tcp is possible since this port is most often allowed.

Note: Port 443/tcp is usually used by HTTPS traffic. While the appliance uses this port, the actual traffic is not HTTPS but SSH since the appliance uses `rsync` embedded in SSH to retrieve the feed. Firewalls using deep inspection and application awareness may still reject the traffic.

The port can be configured as follows:

1. Select *Setup* and press `Enter`.
2. Select *Feed* and press `Enter`.
3. Select *Greenbone Server* and press `Enter`.
4. Select *Sync port* and press `Enter`.
5. Select the desired port and press `Enter` (see Fig. 7.46).

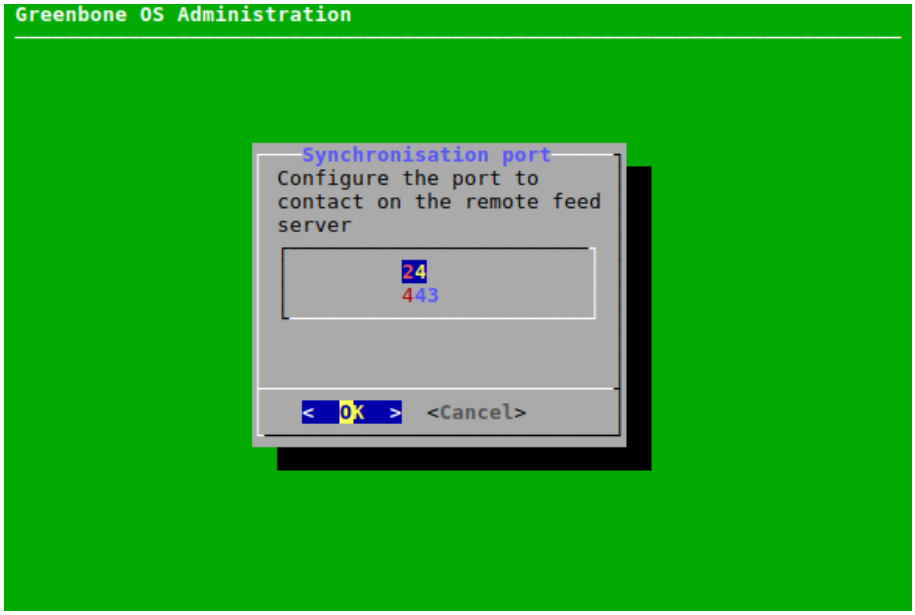


Fig. 7.46: Configuring the synchronization port

7.2.7.4 Setting the Synchronization Proxy

If a security policy does not allow for direct internet access, the appliance can use an HTTPS proxy service. This proxy must not inspect the SSL/TLS traffic but must support the CONNECT method. The traffic passing through the proxy is not HTTPS but SSH encapsulated in http-proxy.

The proxy can be set as follows:

1. Select *Setup* and press `Enter`.
2. Select *Feed* and press `Enter`.
3. Select *Greenbone Server* and press `Enter`.
4. Select *Sync proxy* and press `Enter`.
5. Enter the URL of the proxy in the input box (see Fig. 7.47).

Note: The URL must have the form `http://proxy:port`.

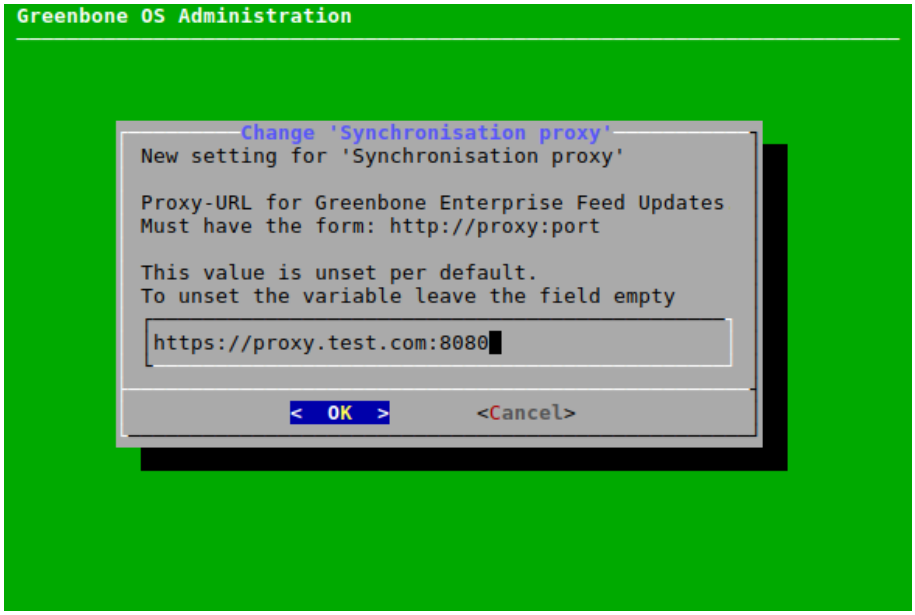


Fig. 7.47: Setting the synchronization proxy

7.2.7.5 Deleting the Greenbone Enterprise Feed Subscription Key

The subscription key can be removed. This is useful if an appliance has reached the end of its lifetime and is no longer in use. The cleanup ensures that there are no more licenses on the appliance. Without the subscription key, the appliance will only retrieve the Greenbone Community Feed.

The cleanup can be done as follows:

1. Select *Setup* and press `Enter`.
2. Select *Feed* and press `Enter`.
3. Select *Cleanup* and press `Enter`.

   → A warning informs that the synchronization with the Greenbone Enterprise Feed is no longer possible after the cleanup (see Fig. 7.48).
4. Select *Yes* and press `Enter`.

   → A message informs that the subscription key has been deleted.
5. Press `Enter` to close the message.

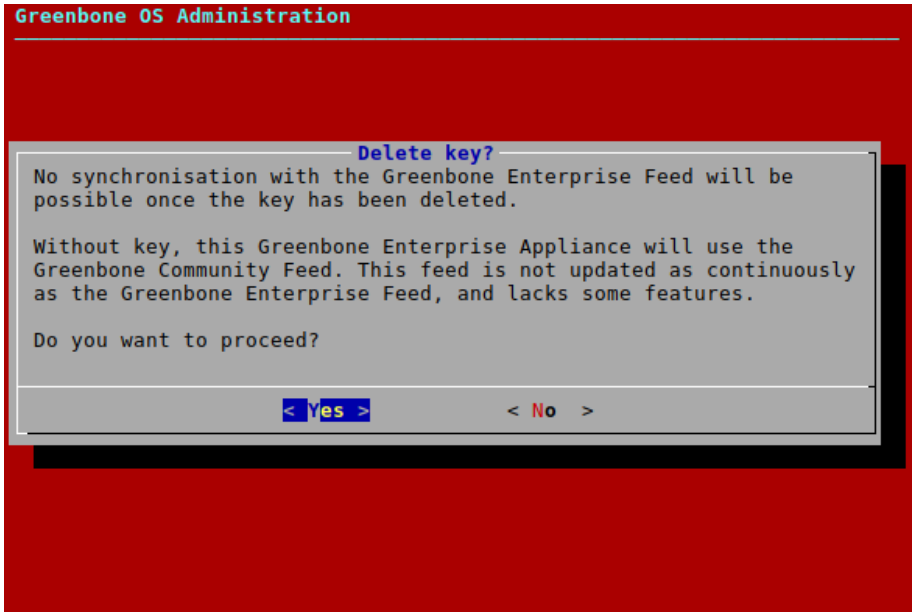


Fig. 7.48: Removing the subscription key

7.2.8 Configuring the Appliance as an Airgap Master/Sensor

The Airgap function allows an appliance that is not directly connected to the internet to obtain feed updates and GOS upgrades.

At least two appliances are required:

- Airgap sensor: situated in a secured area and not connected to the internet
- Airgap master: connected to the internet

Note: Airgap appliances may also be chained, i.e., one Airgap sensor becomes the Airgap master for another Airgap sensor.

Two options are available for the Airgap function:

- Greenbone Airgap USB stick
- Airgap FTP server

The following appliance models can be configured for USB Airgap:

- Greenbone Enterprise 400 and higher as Airgap USB master
- Greenbone Enterprise 400 and higher as Airgap USB sensor

The following appliance models can be configured for FTP Airgap:

- Greenbone Enterprise 400 and higher as Airgap FTP master
- Greenbone Enterprise 150 and higher as Airgap FTP sensor
- Greenbone Enterprise CENO and higher as Airgap FTP sensor

7.2.8.1 Using the Airgap USB Stick

The updates and upgrades are loaded from an appliance connected to the internet and copied to a USB stick. The USB stick can then can be used to update another appliance.

Note: The USB stick must be a specific Airgap USB stick provided by Greenbone. Contact the Greenbone Enterprise Support[17] providing the customer number to request a respective Airgap USB stick.

Tip: The USB stick can be checked for malware by a security gateway beforehand.

The data transfer using the Airgap USB stick is performed as follows:

1. In the GOS administration menu of the Airgap master, select *Setup* and press `Enter`.
2. Select *Feed* and press `Enter`.
3. Select *Airgap Master* and press `Enter`.
4. Select *USB Master* and press `Enter` (see Fig. 7.49).

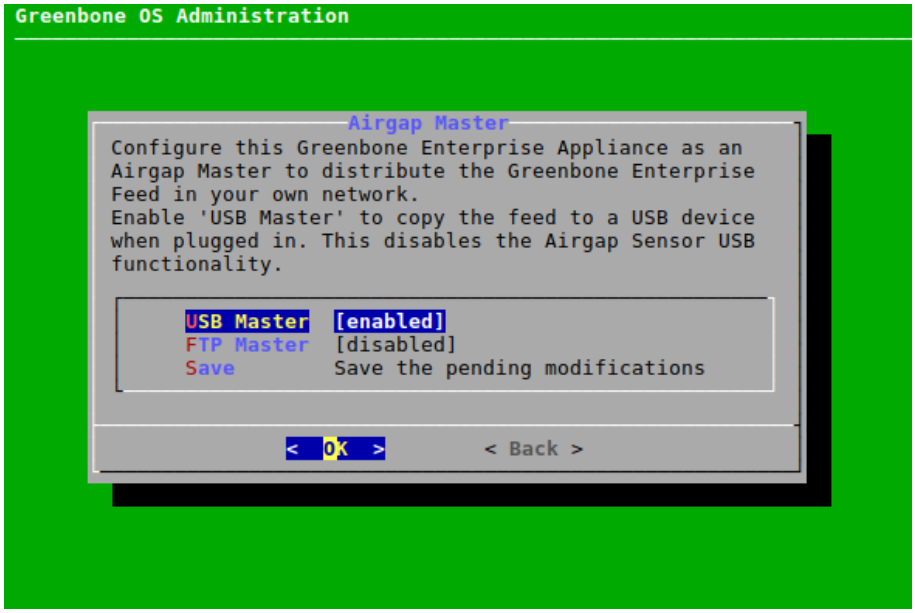


Fig. 7.49: Configuring the Airgap USB master

5. Select *Save* and press `Enter`.

   Note: Configuring an appliance as an Airgap USB master disables the possibility to configure the appliance as an Airgap USB sensor.

6. Connect the Airgap USB stick to the Airgap master.

   → The data transfer starts automatically.

7. When the data transfer is finished, connect the Airgap USB stick to the Airgap sensor.

   → The data transfer starts automatically.

[17] https://www.greenbone.net/en/technical-support/

7.2.8.2 Using the Airgap FTP Server

The updates and upgrades can be provided via an FTP server operating as a data diode. A data diode is a unidirectional security gateway allowing the data flow in only one direction.

The FTP Airgap update is performed when a manual (see Chapter *7.3.6* (page 150)) or an automatic feed update at maintenance time is performed.

Note: The Airgap master must have enough time to upload the Airgap FTP feed to the FTP server. For slower connections, it may be advisable to set the maintenance time of the Airgap sensor at least three hours behind that of the Airgap master (see Chapter *7.2.9* (page 128)).

The configuration of an Airgap FTP setup is performed as follows:

1. In the GOS administration menu of the Airgap master, select *Setup* and press `Enter`.
2. Select *Feed* and press `Enter`.
3. Select *Airgap Master* and press `Enter`.
4. Select *FTP Master* and press `Enter`.

   → Additional menu options for the configuration of the FTP server are shown (see Fig. 7.50).

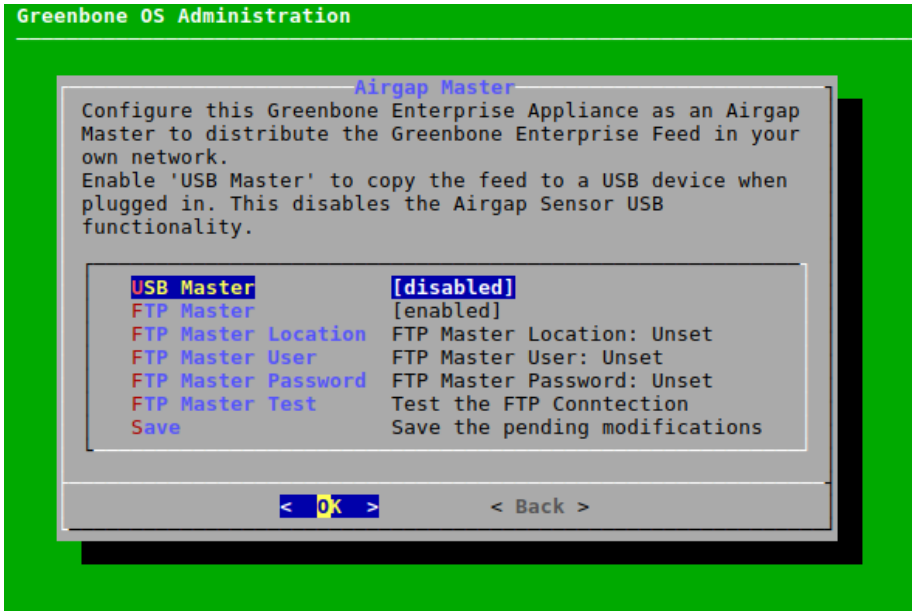


Fig. 7.50: Configuring the FTP server for the Airgap master

5. Select *FTP Master Location* and press `Enter`.
6. Enter the path of the FTP server in the input box and press `Enter`.
   - The required format for the path is `ftp://1.2.3.4` or `ftp://path.to.ftpserver`.
   - Optionally, a port can be configured, e.g., `ftp://1.2.3.4:21`.
   - If no port is configured, the default FTP port 21 is used. If a port other than 21 should be used, it must be configured explicitly.
7. Select *FTP Master User* and press `Enter`.
8. Enter the user used for logging into the FTP server in the input box and press `Enter`.

9. Select *FTP Master Password* and press `Enter`.
10. Enter the password used for logging into the FTP server in the input box and press `Enter`.
11. Select *FTP Master Test* and press `Enter`.

    → It is tested whether a login with the entered information works.
12. Select *Save* and press `Enter`.
13. In the GOS administration menu of the Airgap sensor, select *Setup* and press `Enter`.
14. Select *Feed* and press `Enter`.
15. Select *Airgap Sensor* and press `Enter`.
16. Execute steps 5 to 12 in the GOS administration menu of the Airgap sensor with the same entries as for the Airgap master.

Note: The menu options have slightly different names than in the GOS administration menu of the Airgap master (see Fig. 7.51).

→ The data transfer starts during the next feed update.

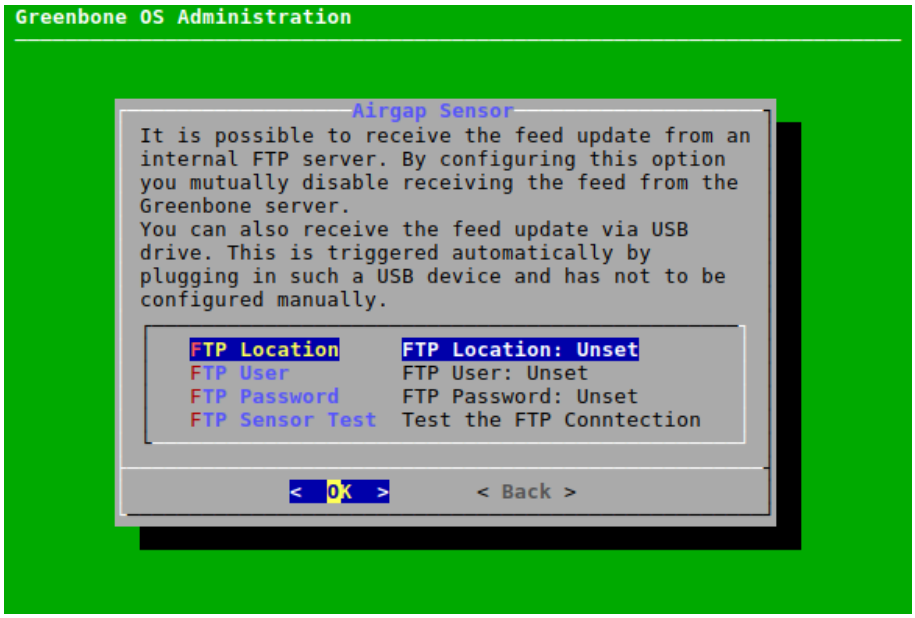


Fig. 7.51: Configuring the FTP server for the Airgap sensor

7.2.9 Configuring the Time Synchronization

To synchronize the appliance with central time servers, the appliance supports the Network Time Protocol (NTP). Up to four different NTP servers can be configured. The appliance will select the most suitable server. If a server fails, another server is used automatically.

Both IP addresses and DNS names are supported.

Note: Time zone and daylight saving time synchronization are not supported by NTP. The appliance's time zone is always UTC±00:00.

The NTP settings can be configured as follows:

1. Select *Setup* and press `Enter`.
2. Select *Timesync* and press `Enter`.
3. Select *Time synchronisation* and press `Enter`.

   → The time synchronization is enabled.
4. Select the desired time server and press `Enter` (see Fig. 7.52).

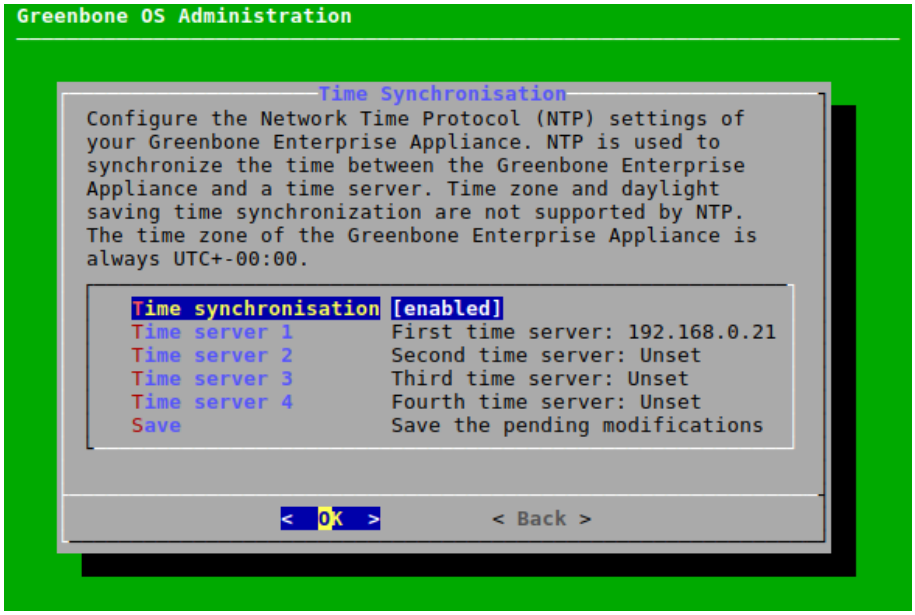


Fig. 7.52: Configuring the NTP settings

5. Enter the time server in the input box and press `Enter`.

   → A message informs that the changes must be saved.
6. Press `Enter` to close the message.

7.2.10 Selecting the Keyboard Layout

The appliance's keyboard layout can be modified as follows:

1. Select *Setup* and press `Enter`.
2. Select *Keyboard* and press `Enter`.

   → All available keyboard layouts are displayed. The current layout has the annotation *(selected)* (see Fig. 7.53).

Fig. 7.53: Selecting the keyboard layout

3. Select the desired keyboard layout and press `Enter`.

   → A message asks to confirm the change.

4. Select *Yes* and press `Enter`.

   → A message informs that the layout was changed.

7.2.11 Configuring the E-Mails Settings

If reports of vulnerability scans or compliance audits should be delivered via e-mail, the appliance must first be connected to a server that acts as a mailhub. Such a server is also called a "mail relay", "relay host" or "smart host". By default, the appliance does not deliver e-mails directly to the internet, but only indirectly via the mailhub, through which they must then be forwarded to the recipients' e-mail servers. The mailhub must support the Simple Mail Transfer Protocol (SMTP).

The appliance does not store e-mails in the event of delivery failure and no second delivery attempt is made.

Note: The appliance implements the Postfix mail transfer agent. The mailhub may need to be set up correctly to work with the appliance. Information about special configurations for this case can be found in the mailhub documentation.

In addition, any mailhub spam protection, such as the gray listing, must be disabled specifically for the appliance.

7.2.11.1 Configuring the Mailhub

The mailhub can be configured as follows:

1. Select *Setup* and press `Enter`.
2. Select *Mail* and press `Enter`.
3. Select *Mail* and press `Enter`.
4. Enter the mailhub's URL in the input box (see Fig. 7.54).

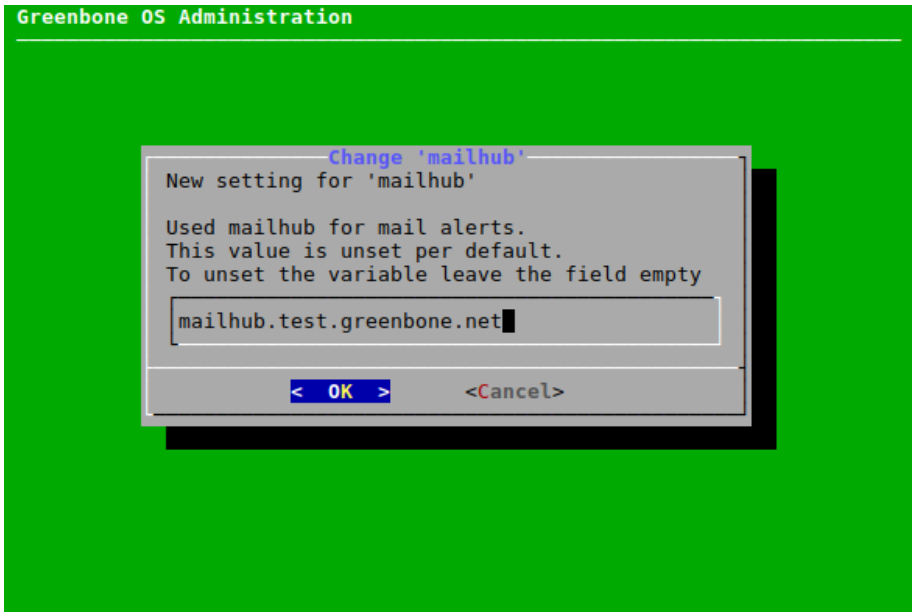


Fig. 7.54: Configuring the mailhub

5. Select *OK* and press `Enter`.

   → A message informs that the changes must be saved.
6. Press `Enter` to close the message.

Note: A port that is used for the mailhub can be configured if desired. However, a manual configuration is not necessary.

If no port is configured, the default ports for SMTP(S) are used automatically.

---

7. Select *Mailhub Port* and press `Enter`.
8. Enter the port in the input field and press `Enter`.

   → A message informs that the changes must be saved.
9. Press `Enter` to close the message.

7.2.11.2 Configuring SMTP Authentication for the Mailhub

Note: The appliance only supports authentication via the SMTP-Auth extension.

Setting up SMTP

Optionally, SMTP authentication can be configured for the used mailhub as follows:

1. Select *Setup* and press `Enter`.
2. Select *Mail* and press `Enter`.
3. Select *SMTP Authentication Requirements* and press `Enter` to enable SMTP authentication (see Fig. 7.55).

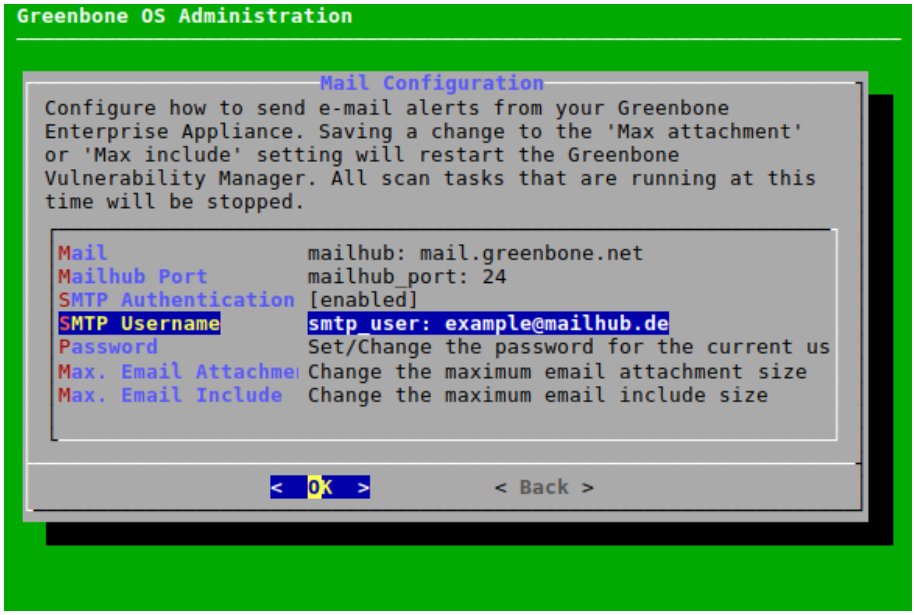


Fig. 7.55: Configuring SMTP authentication

4. Select *SMTP Username* and press `Enter`.
5. Enter the user name of the account used for authentication in the input field and press `Enter`.

   → A message informs that the changes must be saved.
6. Press `Enter` to close the message.
7. Select *Password* and press `Enter`.
8. Enter the password of the account used for authentication twice and press `Tab`.

   Note: Passwords must not be longer than 128 characters.
9. Press `Enter`.

Enforcing the Usage of SMTPS

SMTPS can be enabled to always secure e-mail traffic using TLS.

Note: If it is enabled, the mailhub must also support SMTPS, otherwise the e-mail sending will fail.

Even if SMTPS is not enforced, GOS will automatically try to use encryption via STARTTLS. Only if the mailhub does not support STARTTLS, e-mail traffic is unencrypted.

SMTPS can be enforced as follows:

1. Select *Setup* and press `Enter`.
2. Select *Mail* and press `Enter`.
3. Select *SMTP Enforce TLS* and press `Enter`.

7.2.11.3 Configuring the Size of Included or Attached Reports

The maximum size (in bytes) of reports included in or attached to an e-mail (see Chapter *10.12* (page 272)) can be limited as follows:

1. Select *Setup* and press `Enter`.
2. Select *Mail* and press `Enter`.
3. Select *Max. Email Attachment Size* or *Max. Email Include Size* and press `Enter`.

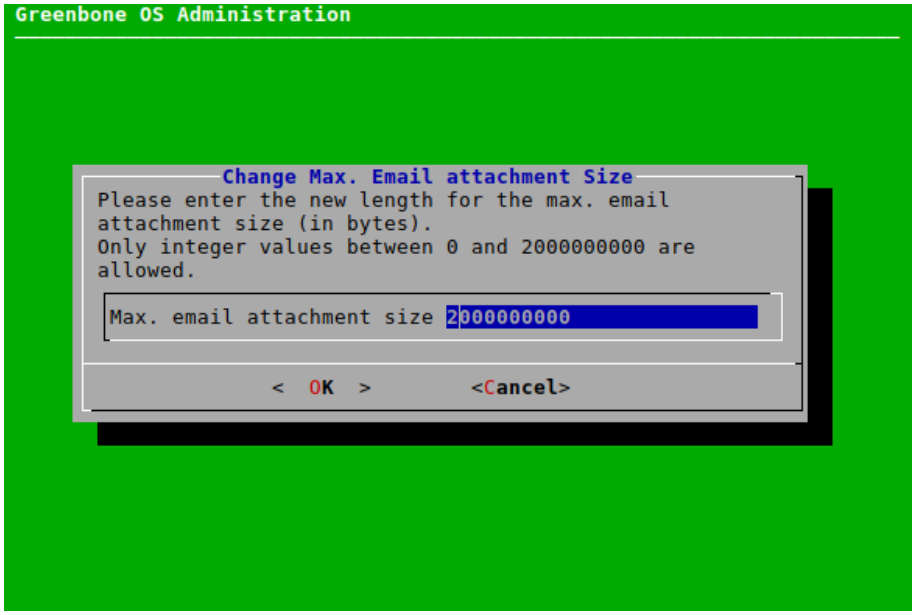


Fig. 7.56: Setting the maximum size of included or attached reports

→ A warning informs that changing the size requires a restart of the Greenbone Vulnerability Manager, which will cause all currently running scans to stop.

4. Enter the maximum size (in bytes) in the input box (see Fig. 7.56).
5. Select *OK* and press `Enter`.

   → A message informs that the changes must be saved.
6. Press `Enter` to close the message.

7.2.12 Configuring the Collection of Logs

The appliance supports the configuration of a central logging server for log collection. Either only the security-related logs or all system logs can be sent to a remote logging server.

The security-related logs contain only messages from the security and authentication logging facilities:

- *auth*
- *authpriv*
- *security*

Additionally, the full logs contain the following facilities:

- *cron*
- *daemon*
- *ftp*
- *kern*
- *lp*
- *lpr*
- *ntp*
- *mail*
- *news*
- *syslog*
- *user*
- *uucp*
- *console*
- *solaris-cron*
- *local0 – local7*

The appliance uses the syslog protocol. The central collection of logs allows central analysis, management and monitoring of the logs. Additionally, the logs are always stored locally as well.

A separate logging server can be configured for each type of log (security-related logs or all system logs).

UDP (default), TLS and TCP can be used for transmission.

- TCP ensures log delivery even if packet loss occurs.
- If a packet loss occurs during a transmission via UDP, the logs are lost.
- TLS allows optional authentication of the sender via TLS. Only TLS 1.2 and TLS 1.3 are supported. This process is not RFC 5425 compliant.

Note: The time zone of the appliance (UTC±00:00) is used for the log time stamps unless adjusted on the syslog server.

7.2.12.1 Configuring the Logging Server

The logging server can be set up as follows:

1. Select *Setup* and press `Enter`.
2. Select *Remote Syslog* and press `Enter`.
3. Select *Security Syslog* and press `Enter` to enable security-related logs (see Fig. 7.57).

   or

3. Select *Full Syslog* and press `Enter` to enable all system logs (see Fig. 7.57).

Note: Both logs can be enabled.

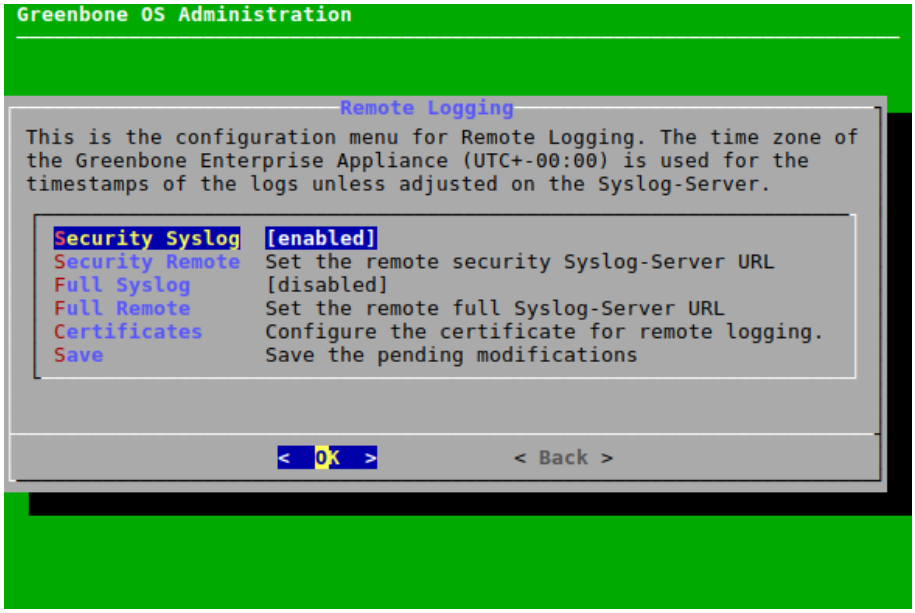


Fig. 7.57: Configuring the logs

4. Select *Security Remote* and press `Enter` to set the logging server URL for security-related logs.

   or

4. Select *Full Remote* and press `Enter` to set the logging server URL for all system logs.
5. Enter the logging server URL including the desired protocol in the input box (see Fig. 7.58).

Note: If no port is specified, the default port 514 is used.

If no protocol is specified, UDP is used.

If TLS is used, an HTTPS certificate must exist (see Chapter *7.2.12.2* (page 135)).

→ A message informs that the changes must be saved.

6. Press `Enter` to close the message.

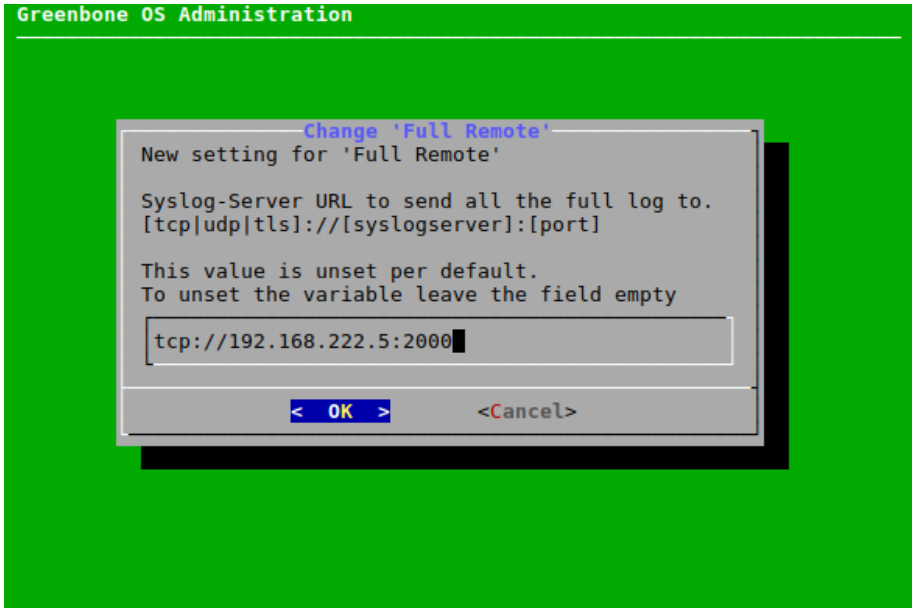


Fig. 7.58: Configuring the logging server

7.2.12.2 Managing HTTPS Certificates for Logging

Creating a Certificate

HTTPS certificates for logging can be managed as follows:

1. Select *Setup* and press `Enter`.
2. Select *Remote Syslog* and press `Enter`.
3. Select *Certificates* and press `Enter`.
4. Select *Generate* and press `Enter` to generate a certificate.

   → A message informs that the current certificate and private key will be overwritten.
5. Confirm the message by selecting *Yes* and pressing `Enter`.
6. Provide the settings for the certificate (see Fig. 7.59), select *OK* and press `Enter`.

   Note: It is valid to generate a certificate without a common name. However, a certificate should not be created without (a) Subject Alternative Name(s) (SAN).

   If a common name is used, it should be the same as one of the SANs.

   → When the process is finished, a message informs that the certificate can be downloaded.
7. Press `Enter` to close the message.
8. Select *Certificates* and press `Enter`.
9. Select *Download* and press `Enter`.
10. Open the web browser and enter the displayed URL.
11. Download the file.
12. In the GOS administration menu, press `Enter`.

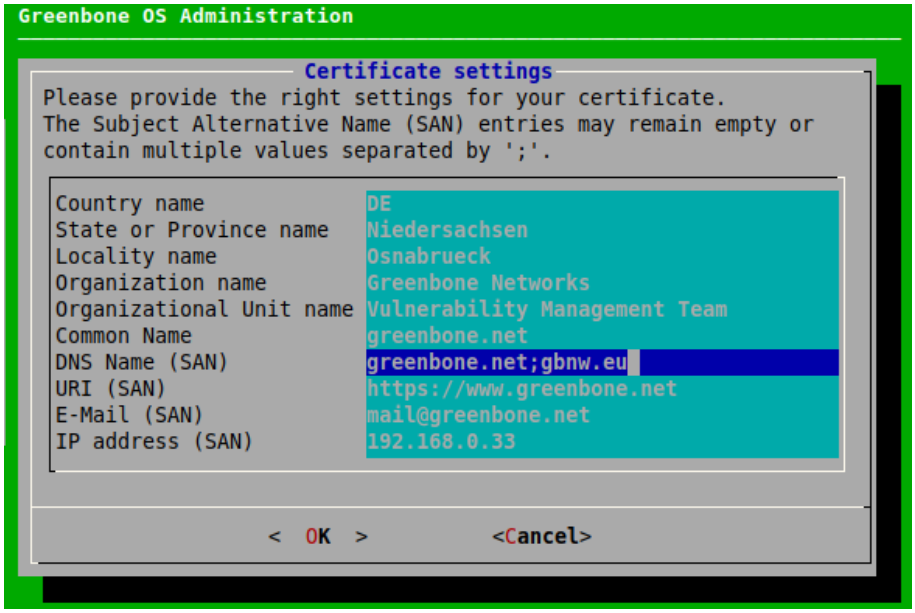


Fig. 7.59: Providing settings for the certificate

→ When the certificate is retrieved by the appliance, the GOS administration menu displays the fingerprint of the certificate for verification.

13. Check the fingerprint and confirm the certificate by pressing `Enter`.

Displaying the Current Certificate and the Fingerprints

The certificate and the according fingerprints can be displayed as follows:

1. Select *Setup* and press `Enter`.
2. Select *Remote Syslog* and press `Enter`.
3. Select *Certificates* and press `Enter`.
4. Select *Show* and press `Enter` to display the certificate.

   Select *Fingerprints* and press `Enter` to display the fingerprint.

   → The following fingerprints of the currently active certificate are displayed:

   - SHA1
   - SHA256

7.2.13 Setting the Maintenance Time

During maintenance, the daily feed synchronization takes place. Any time during the day can be selected, except for 10:00 a.m. to 1:00 p.m. UTC. During this time, Greenbone updates the feed and disables the synchronization services.

The default maintenance time is a random time between 3:00 a.m. and 5:00 a.m. UTC±00:00.

The maintenance time can be set as follows:

1. Select *Setup* and press `Enter`.
2. Select *Time* and press `Enter`.
3. Enter the desired maintenance time in the input box and press `Enter` (see Fig. 7.60).

Note: The time must be converted to UTC before entering it.

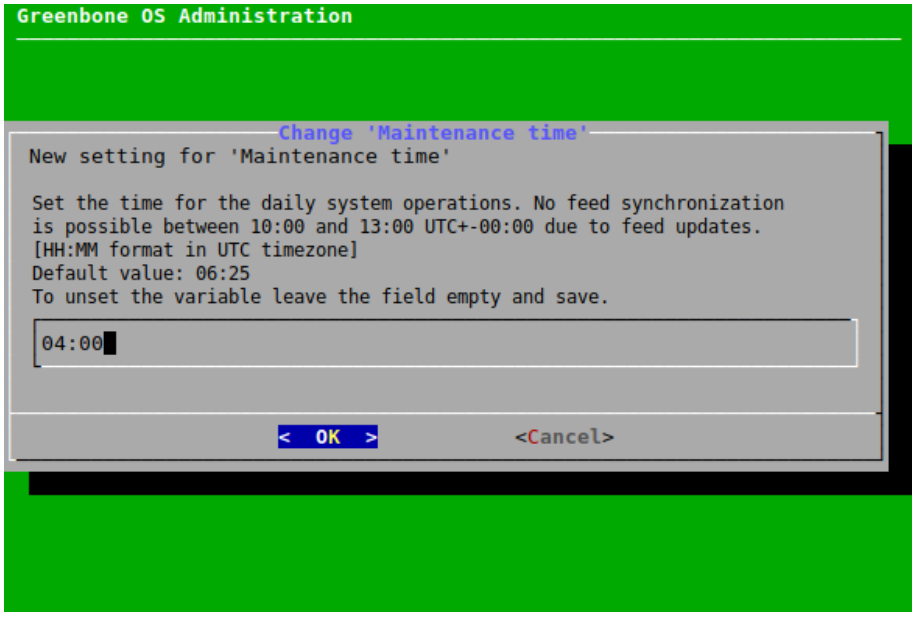


Fig. 7.60: Configuring the maintenance time

→ A message informs that the changes must be saved.

4. Press `Enter` to close the message.

7.3 Maintenance Menu

7.3.1 Performing a Self-Check

The self-check option checks the appliance setup. It displays wrong or missing configuration details that could prevent the appliance from functioning correctly. The following items are checked:

- Network connection
- DNS resolution
- Feed reachability
- Available updates
- User configuration

The self-check is performed as follows:

1. Select *Maintenance* and press `Enter`.
2. Select *Selfcheck* and press `Enter`.

   → The self-check is performed. When it is finished, the result is displayed.
3. Press `Enter` (see Fig. 7.61).

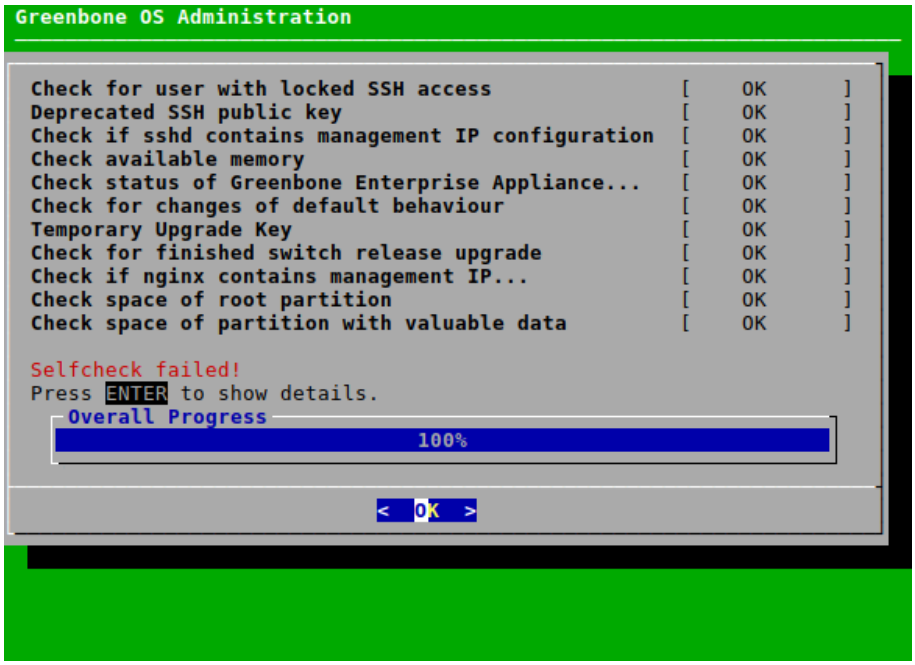


Fig. 7.61: Performing a self-check

7.3.2 Performing and Restoring a Backup

Note: Periodical, scheduled backups are configured in the menu *Setup* (see Chapter *7.2.5* (page 113)).

In addition to scheduled backups, backups can also be performed manually. There are two different backup types with different use cases:

- **Incremental backups**
  - Only data that was changed since the last backup is saved.
  - If no backup is present, a full backup will be performed.
  - The incremental backup can be stored remotely on a server or locally on the appliance.
  - By default, the last 7 daily backups, the last 5 weekly backups and the last 12 monthly backups are stored. Backups older than one year will be deleted automatically.
- **USB backups**
  - First, a separate, full (temporary) backup is created on the appliance and then copied to the USB flash drive.
  - The temporary backup on the hard disk is deleted afterwards.

7.3.2.1 Incremental Backups

Depending on the backup location configured in Chapter *7.2.5* (page 113), the incremental backups are stored remotely or locally.

The backups include user data (e.g., tasks, reports, results) and system settings, i.e., the GOS configuration.

Performing an Incremental Backup

A backup can be performed manually as follows:

1. Select *Maintenance* and press `Enter`.
2. Select *Backup* and press `Enter`.
3. Select *Incremental Backup* and press `Enter` (see Fig. 7.62).

   → A message informs that the backup was started in the background.

Tip: The currently running system operation can be displayed by selecting *About* and pressing `Enter` in the GOS administration menu.

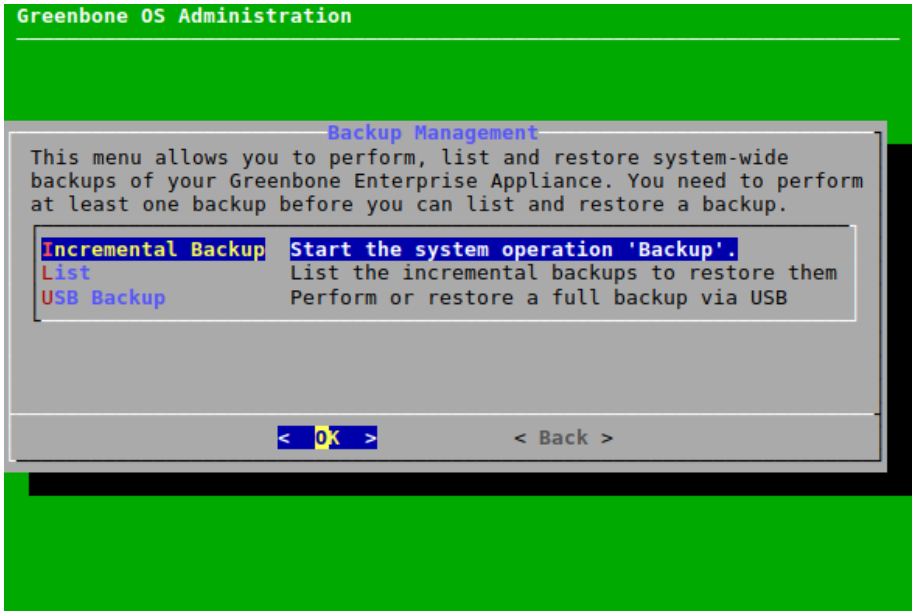


Fig. 7.62: Triggering a backup manually

Restoring an Incremental Backup

Note: Only backups created with the currently used GOS version or the previous GOS version can be restored. For GOS 22.04, only backups from GOS 21.04 or GOS 22.04 can be imported. If an older backup, e.g., from GOS 6 or GOS 20.08, should be imported, an appliance with a matching GOS version must be used.

Backups created with GOS versions newer than the currently used GOS version are also not supported. If a newer backup should be imported, an appliance with a matching GOS version must be used.

Only backups created with the same appliance model (see Chapter *3* (page 20)) can be restored.

It is checked whether the subscription keys of the backup and the appliance to which the backup should be restored are identical. If the keys do not match, a warning is displayed and the user must confirm that the key on the appliance should be overwritten. However, if a backup without a subscription key is restored, the key on the appliance is kept.

If a new backup password is configured (see Chapter *7.2.5.2* (page 114)), and a backup is restored that was created with a previous password, the previous password is not restored. The appliance will always use the newest backup password that was configured.

If there are any questions, contact the Greenbone Enterprise Support[18].

A backup can be restored as follows:

1. Select *Maintenance* and press `Enter`.
2. Select *Backup* and press `Enter`.
3. Select *List* and press `Enter`.
4. Select the desired backup and press `Enter`.
5. Select *Yes* and press `Enter` if both user data and system settings should be uploaded.

   or

[18] https://www.greenbone.net/en/technical-support/

5. Select *No* and press `Enter` if only user data should be uploaded.

Note: The system settings include all GOS configurations, e.g., the network settings.

The user data includes all vulnerability scanning and management information.

→ A warning informs that all local settings are lost if the backup is restored (see Fig. 7.63).

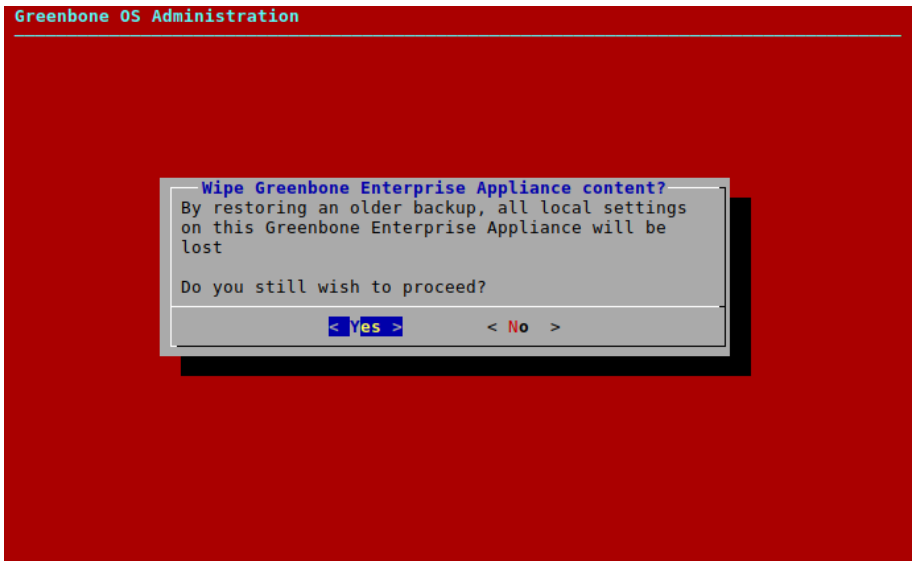


Fig. 7.63: Restoring a backup

6. Confirm the message by selecting *Yes* and pressing `Enter`.

   → A message informs that the restoration was started in the background.

Tip: The currently running system operation can be displayed by selecting *About* and pressing `Enter` in the GOS administration menu.

7.3.2.2 USB Backups

Performing a USB Backup

Backups can be performed on a USB flash drive as follows:

1. Connect a USB drive to the appliance.
2. Select *Maintenance* and press `Enter`.
3. Select *Backup* and press `Enter`.
4. Select *USB Backup* and press `Enter`.

   → If the used USB drive is not formatted for use as a GOS backup device yet, a message asks whether the USB drive should be formatted.

   If the USB drive is formatted for use as a GOS backup device already, no message is displayed. Continue with step 7.

5. Select *Yes* and press `Enter`.

   → A warning informs that the stored data is erased if the drive is formatted.

6. Select *Yes* and press `Enter`.

   → The USB drive is formatted for use as a GOS USB backup device.

7. Select *Backup* and press `Enter` (see Fig. 7.64).

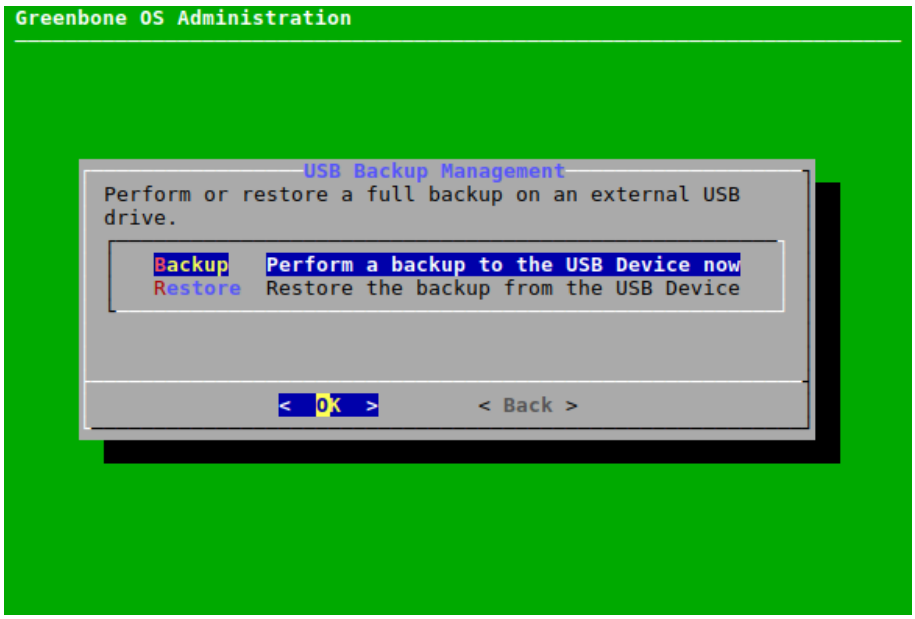


Fig. 7.64: Performing a backup using a USB drive

   → A message asks to confirm the backup.

8. Select *Yes* and press `Enter`.

   → A message informs that the backup was started in the background.

Tip: The currently running system operation can be displayed by selecting *About* and pressing `Enter` in the GOS administration menu.

Restoring a USB Backup

Note: Only backups created with the currently used GOS version or the previous GOS version can be restored. For GOS 22.04, only backups from GOS 21.04 or GOS 22.04 can be imported. If an older backup, e.g., from GOS 6 or GOS 20.08, should be imported, an appliance with a matching GOS version must be used.

Backups created with GOS versions newer than the currently used GOS version are also not supported. If a newer backup should be imported, an appliance with a matching GOS version must be used.

Only backups created with the same appliance model (see Chapter *3* (page 20)) can be restored.

It is checked whether the subscription keys of the backup and the appliance to which the backup should be restored are identical. If the keys do not match, a warning is displayed and the user must confirm that the key on the appliance should be overwritten. However, if a backup without a subscription key is restored, the key on the appliance is kept.

If a new backup password is configured (see Chapter *7.2.5.2* (page 114)), and a backup is restored that was created with a previous password, the previous password is not restored. The appliance will always use the newest backup password that was configured.

If there are any questions, contact the Greenbone Enterprise Support[19].

Backups can be restored from a USB drive as follows:

1. Connect the USB drive containing the desired GOS backup to the appliance.

   Note: In case of problems, another USB drive or another USB port on the appliance should be tried.

2. Select *Maintenance* and press `Enter`.
3. Select *Backup* and press `Enter`.
4. Select *USB Backup* and press `Enter`.
5. Select *Restore* and press `Enter` (see Fig. 7.64).
6. Select *Yes* and press `Enter` if both user data and system settings should be uploaded.

   or

6. Select *No* and press `Enter` if only user data should be uploaded.

   Note: The system settings include all GOS configurations, e.g., the network settings.

   The user data includes all vulnerability scanning and management information.

   → A warning informs that all local settings are lost if the backup is restored (see Fig. 7.65).

7. Confirm the message by selecting *Yes* and pressing `Enter`.

   → A message informs that the restoration was started in the background.

   Tip: The currently running system operation can be displayed by selecting *About* and pressing `Enter` in the GOS administration menu.

[19] https://www.greenbone.net/en/technical-support/

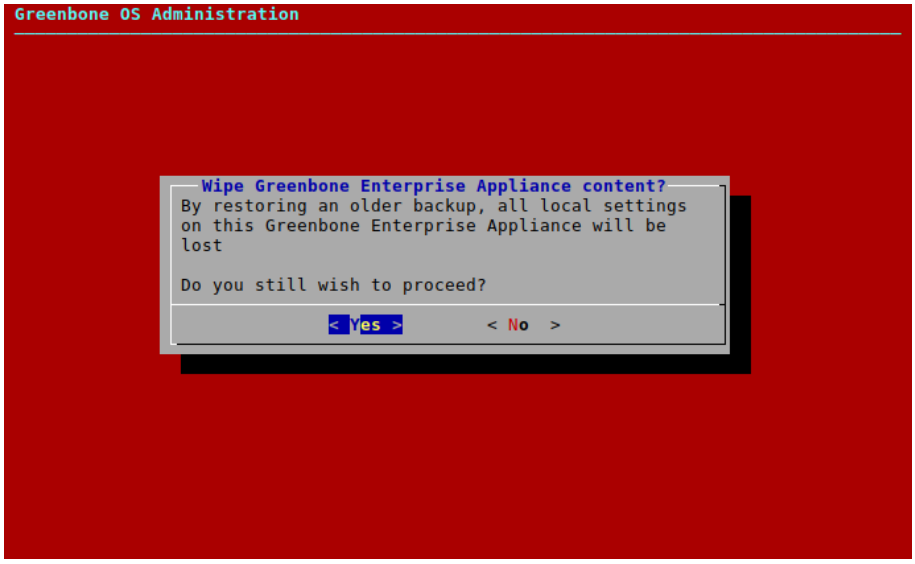


Fig. 7.65: Restoring a backup

7.3.3 Copying Data and Settings to Another Appliance with Beaming

The current state of an appliance can be copied to another appliance. This includes user data (e.g., tasks, reports, results) and system settings (i.e., the GOS configuration).

On the receiving appliance, the user can decide whether to import only the user data, or both the user data and the system settings.

Note: Only beaming images created with the currently used GOS version or the previous GOS version can be restored. For GOS 22.04, only beaming images from GOS 21.04 or GOS 22.04 can be imported. If an older beaming image, e.g., from GOS 20.08, should be imported, an appliance with a matching GOS version must be used.

It is only possible to import a beaming image to an appliance if the release information, i.e., the list of available GOS upgrades, on the corresponding appliance is up-to-date. To ensure this, a current Greenbone Enterprise Feed should be downloaded.

Beaming images created with GOS versions newer than the currently used GOS version are also not supported. If a newer beaming image should be imported, an appliance with a matching GOS version must be used.

Beaming is only allowed to an appliance of the same or of a higher class (see Chapter *3* (page 20)). Beaming to a Greenbone Enterprise TRIAL is not supported.

It is checked whether the subscription keys of the beaming image and the appliance to which the beaming image should be restored are identical. If the keys do not match, a warning is displayed and the user must confirm that the key on the appliance should be overwritten. However, if a beaming image without a subscription key is restored, the key on the appliance is kept.

If there are any questions, contact the Greenbone Enterprise Support[20].

---

[20] https://www.greenbone.net/en/technical-support/

7.3.3.1 Beaming Directly from Another Appliance

The beaming image can be created and copied directly as follows:

Note:

- Appliance A = Sending appliance
- Appliance B = Receiving appliance

1. In the GOS administration menu of Appliance A, select *Maintenance* and press `Enter`.
2. Select *Beaming* and press `Enter`.
3. Select *Download* and press `Enter` (see Fig. 7.66).

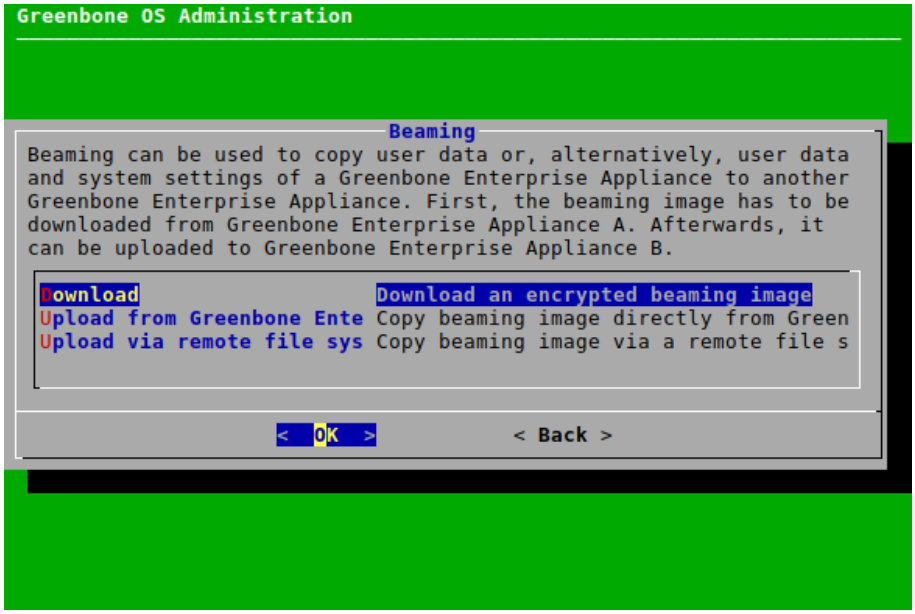


Fig. 7.66: Downloading a beaming image

→ A message informs that the beaming image creation was started in the background.

Tip: The currently running system operation can be displayed by selecting *About* and pressing `Enter` in the GOS administration menu.

When the creation is finished, a message informs that a password that must be noted will be shown.

4. Press `Enter`.
5. Note the password. It is needed in step 13.
6. Press `q` to close the editor.

Important: Do not close the message displaying the URL.

7. In the GOS administration menu of Appliance B, select *Maintenance* and press `Enter`.
8. Select *Beaming* and press `Enter`.

9. Select *Upload from Greenbone Enterprise Appliance A* and press `Enter`.
10. Enter the URL displayed in the GOS administration menu of Appliance A in the input box and press `Enter`.

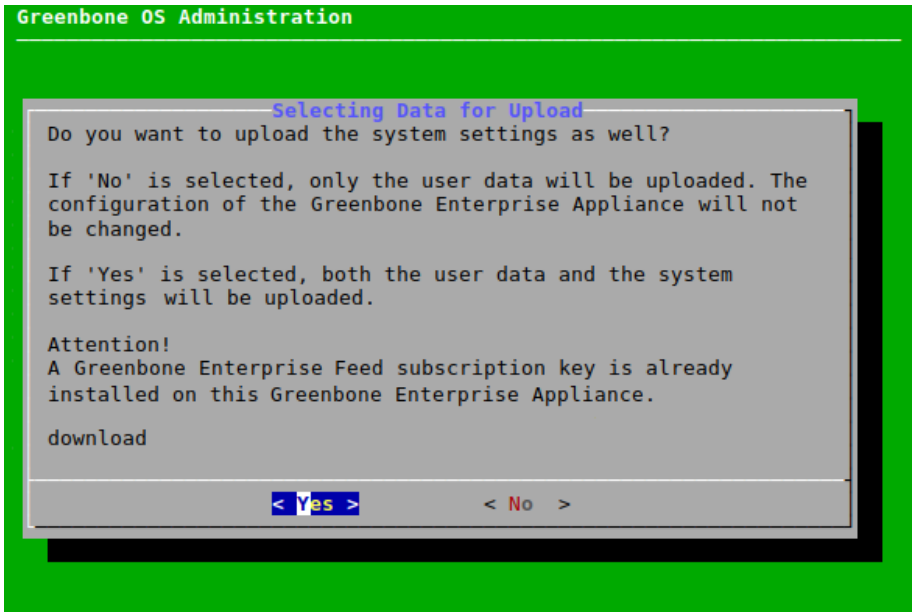


Fig. 7.67: Selecting the data and settings for uploading

11. Select *Yes* and press `Enter` if both user data and system settings should be uploaded.

    or

11. Select *No* and press `Enter` if only user data should be uploaded.

    → A warning asks to confirm the process.

12. Select *Yes* and press `Enter`.
13. Enter the password from step 5 in the input box and press `Enter` (see Fig. 7.68).

    → A message informs that the beaming image upload was started in the background.

    Tip: The currently running system operation can be displayed by selecting *About* and pressing `Enter` in the GOS administration menu.

    When the upload is finished, a message is displayed.

14. Press `Enter`.

7.3.3.2 Beaming via Remote File System

A beaming image can be created, downloaded, stored, and imported later via a remote file system as follows:

Note:

- Appliance A = Sending appliance
- Appliance B = Receiving appliance

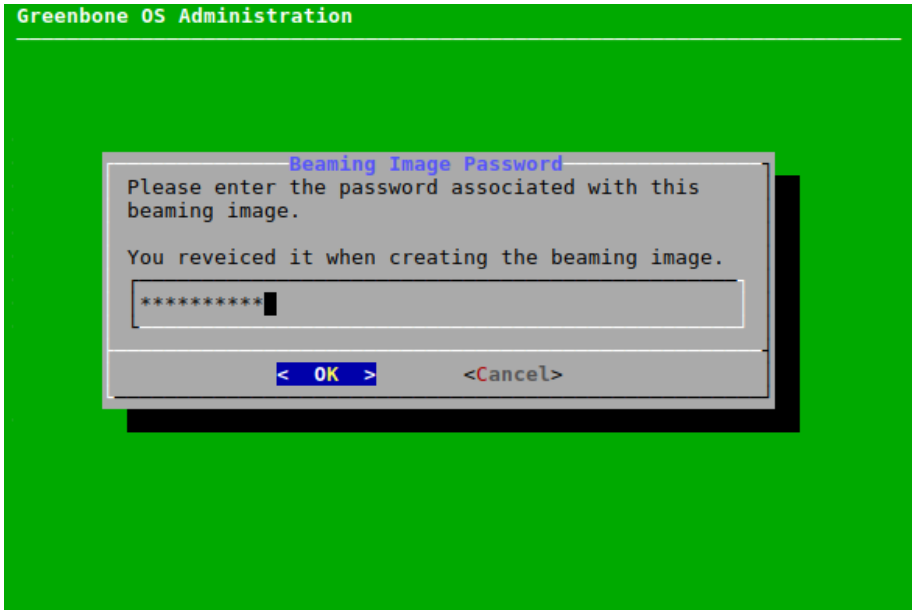


Fig. 7.68: Entering the password for the beaming image

1. In the GOS administration menu of Appliance A, select *Maintenance* and press `Enter`.
2. Select *Beaming* and press `Enter`.
3. Select *Download* and press `Enter` (see Fig. 7.69).

Fig. 7.69: Downloading a beaming image

→ A message informs that the beaming image creation was started in the background.

Tip: The currently running system operation can be displayed by selecting *About* and pressing `Enter` in the GOS administration menu.

When the creation is finished, a message informs that a password that must be noted will be shown.

4. Press `Enter`.
5. Note the password. It is needed in step 16.
6. Press `q` to close the editor.
7. Open the web browser and enter the displayed URL.
8. Download the GSMB file.
9. In the GOS administration menu of Appliance B, select *Maintenance* and press `Enter`.
10. Select *Beaming* and press `Enter`.
11. Select *Upload via remote file system* and press `Enter`.
12. Open the web browser and enter the displayed URL.
13. Click *Browse...*, select the GSMB file and click *Upload*.

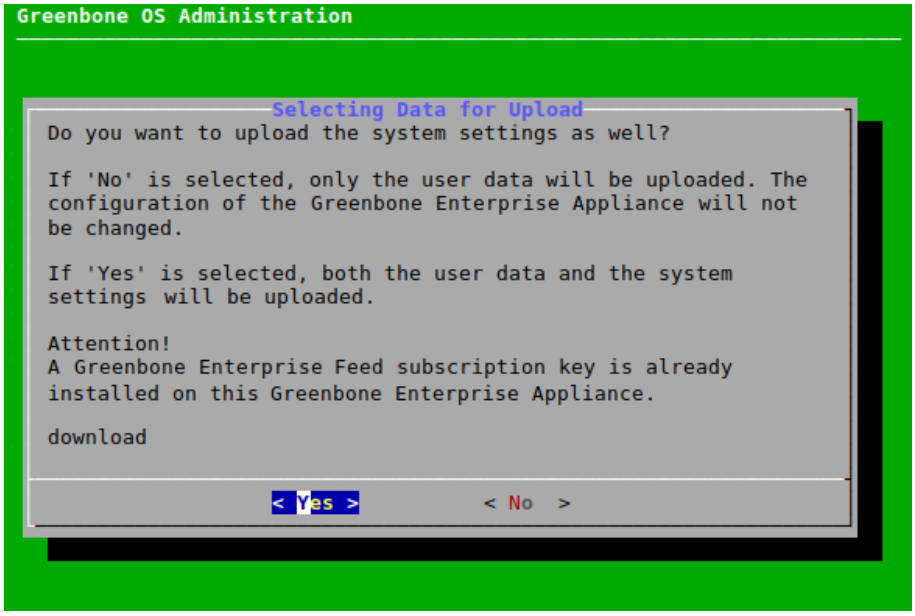


Fig. 7.70: Selecting the data and settings for uploading

14. Select *Yes* and press `Enter` if both user data and system settings should be uploaded.

    or

14. Select *No* and press `Enter` if only user data should be uploaded.

    → A warning asks to confirm the process.

15. Select *Yes* and press `Enter`.
16. Enter the password from step 5 in the input box and press `Enter` (see Fig. 7.71).

    → A message informs that the beaming image upload was started in the background.

    Tip: The currently running system operation can be displayed by selecting *About* and pressing `Enter` in the GOS administration menu.

    When the upload is finished, a message is displayed.

17. Press `Enter`.

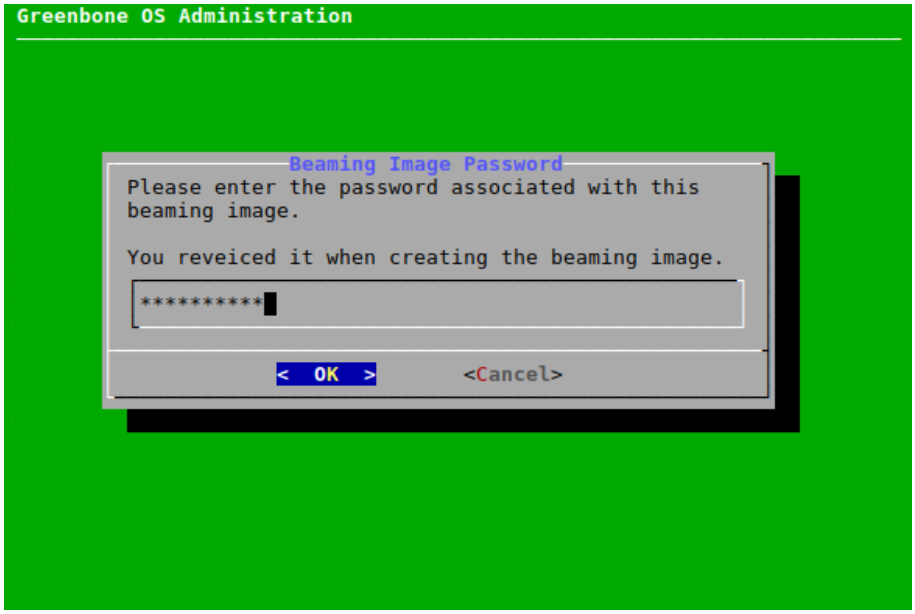


Fig. 7.71: Entering the password for the beaming image

7.3.4 Performing a GOS Upgrade

During the daily feed update at maintenance time (see Chapter *7.2.13* (page 137)), the appliance also downloads new GOS upgrades, if available. While the upgrades are downloaded automatically, they are not installed automatically.

Note: Because the upgrades can interrupt running scan tasks, they must be scheduled carefully.

Upgrades can be installed manually as follows:

1. Select *Maintenance* and press `Enter`.
2. Select *Upgrade* and press `Enter`.
3. Select *Upgrade* and press `Enter` to install an upgrade.

   or

3. Select *Switch Release* and press `Enter` to switch to a new release.

   → A message informs that the upgrade was started in the background.

   Tip: The currently running system operation can be displayed by selecting *About* and pressing `Enter` in the GOS administration menu.

Note: If errors occur when using the web interface after a GOS upgrade, the browser or page cache must be cleared (see Chapter *6.4* (page 63)).

It is possible that a GOS upgrade changes the functionality available via the GOS administration menu. This changed functionality will only be available after reloading the GOS administration menu. Therefore, it is recommended to log out of the GOS administration menu and log back in after the GOS upgrade.

Occasionally, a reboot of the appliance is required as well (see Chapter *7.3.9.1* (page 153)). The self-check displays a corresponding note if this is the case (see Chapter *7.3.1* (page 138)).

Note: By default, a successful GOS upgrade on the master will also start a GOS upgrade on the connected sensors. However, an upgrade can also be installed manually on the sensors (see Chapter *7.3.5* (page 150)).

7.3.5 Performing a GOS Upgrade on Sensors

A GOS upgrade on a sensor can be installed as follows:

1. Select *Maintenance* and press `Enter`.
2. Select *Upgrade* and press `Enter`.
3. Select *Sensors* and press `Enter`.
4. Select the desired sensor and press `Space`.

   → The sensor is marked with *. Multiple sensors can be selected at the same time.

   Sensors that are not ready for an upgrade are labelled accordingly.
5. Press `Enter`.

   → A message informs that the upgrade was started in the background.

Tip: The currently running system operation can be displayed by selecting *About* and pressing `Enter` in the GOS administration menu.

7.3.6 Performing a Feed Update

By default, the appliance tries to download feed updates and GOS upgrades daily at its maintenance time (see Chapter *7.2.13* (page 137)).

Additionally, a feed update can be triggered manually as follows:

1. Select *Maintenance* and press `Enter`.
2. Select *Feed* and press `Enter`.
3. Select *Update* and press `Enter` (see Fig. 7.72).

   → A message informs that the feed update was started in the background.

Tip: The currently running system operation can be displayed by selecting *About* and pressing `Enter` in the GOS administration menu.

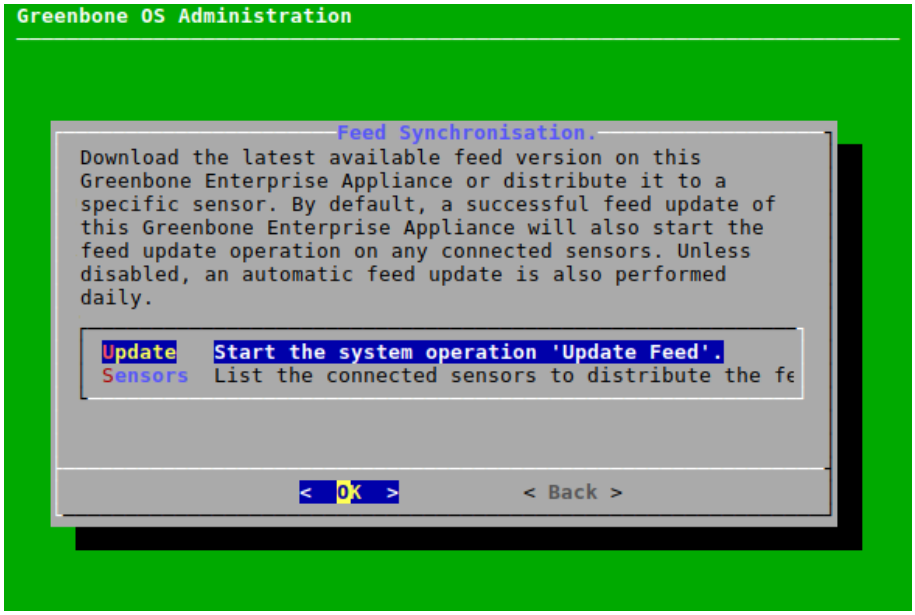


Fig. 7.72: Triggering a feed update manually

Note: By default, a successful feed update on the master will also start a feed update on the connected sensors. However, a feed update can also be pushed manually to the sensors (see Chapter *7.3.7* (page 151)).

7.3.7 Performing a Feed Update on Sensors

A feed update can be pushed to a sensor as follows:

1. Select *Maintenance* and press `Enter`.
2. Select *Feed* and press `Enter`.
3. Select *Sensors* and press `Enter`.
4. Select the desired sensor and press `Enter` (see Fig. 7.73).

   → A message informs that the feed update was started in the background.

Tip: The currently running system operation can be displayed by selecting *About* and pressing `Enter` in the GOS administration menu.

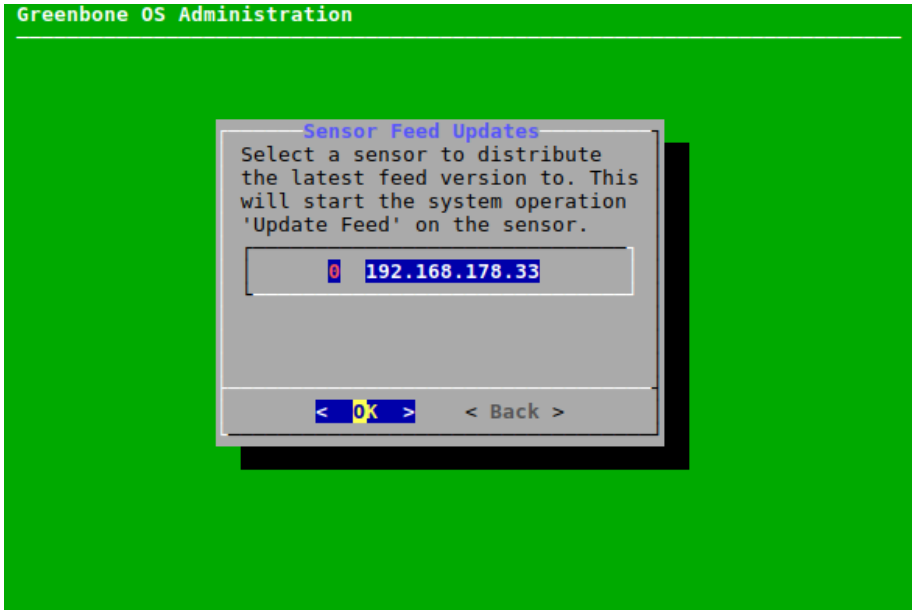


Fig. 7.73: Selecting the sensor

7.3.8 Upgrading the Flash Partition

The flash partition is used to perform factory resets of the appliance. To simplify factory resets, it should be upgraded to the latest GOS version regularly.

Note: Make sure that the appliance itself is able to connect to the Greenbone Feed Server.

It is not possible to upgrade the flash partition of sensors via the master.

The flash partition can be upgraded as follows:

1. Upgrade the appliance to the latest GOS version (see Chapter *7.3.4* (page 149)).
2. Select *Maintenance* and press `Enter`.
3. Select *Flash* and press `Enter`.
4. Select *Download* and press `Enter` (see Fig. 7.74).

   → The latest flash image is downloaded.

   Tip: The download status can be monitored in the live logs (*Advanced* > *Logs* > *Live*, see Chapter *7.4.1* (page 155)).

   ---

5. When the download is finished, select *Write* and press `Enter` (see Fig. 7.74) .

   → The image is written to the flash partition. The process may take up to 20 minutes.

   Tip: The currently running system operation can be displayed by selecting *About* and pressing `Enter` in the GOS administration menu.

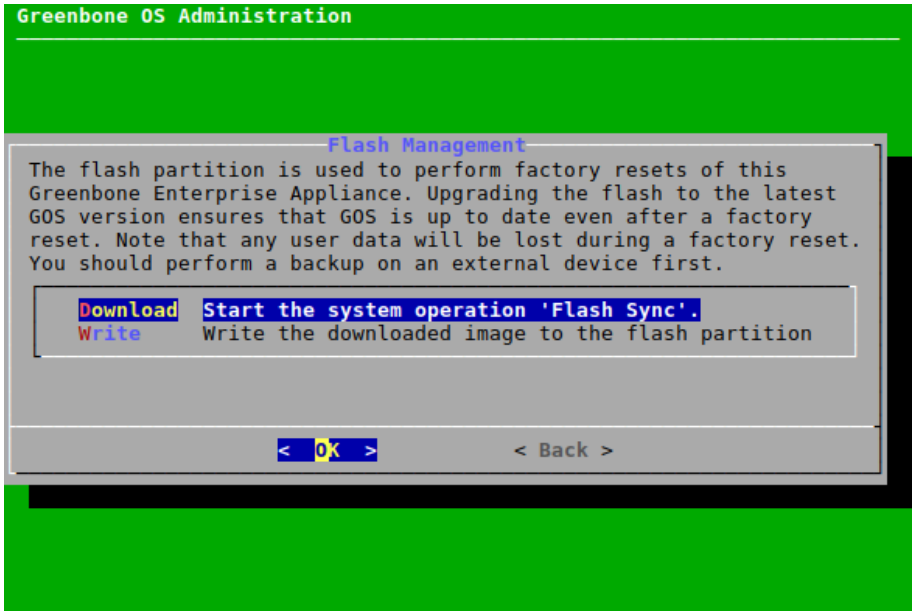


Fig. 7.74: Upgrading the flash partition

7.3.9 Shutting down and Rebooting the Appliance

Note: The appliance should not be turned off via the power switch.

Instead, the appliance should be shut down and rebooted via the GOS administration menu. This ensures that the mandatory cleanup processes are executed during shutdown and reboot.

7.3.9.1 Rebooting the Appliance

The appliance is rebooted as follows:

1. Select *Maintenance* and press `Enter`.
2. Select *Power* and press `Enter`.
3. Select *Reboot* and press `Enter`.

   → A message asks to confirm the reboot (see Fig. 7.75).
4. Select *Yes* and press `Enter`.

   → The appliance will reboot. The reboot process may take up to several minutes.

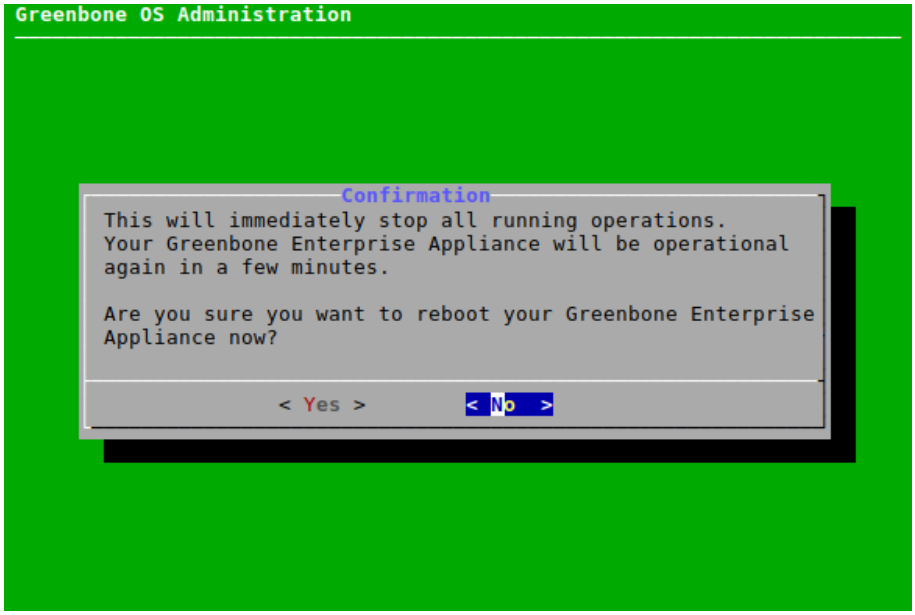


Fig. 7.75: Rebooting the appliance

7.3.9.2 Shutting down the Appliance

The appliance is shut down as follows:

1. Select *Maintenance* and press `Enter`.
2. Select *Power* and press `Enter`.
3. Select *Shutdown* and press `Enter`.

   → A message asks to confirm the shutdown (see Fig. 7.76).

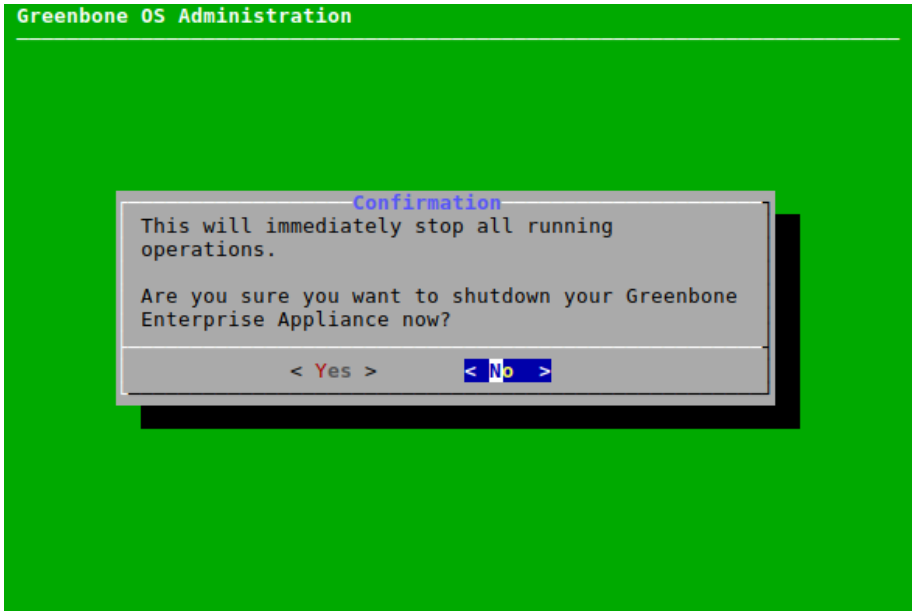


Fig. 7.76: Shutting down the appliance

4. Select *Yes* and press `Enter`.

   → The appliance will shutdown. The shutdown process may take up to several minutes.

7.4 Advanced Menu

7.4.1 Displaying the Log Files of the Appliance

The log files of the appliance can be displayed as follows:

1. Select *Advanced* and press `Enter`.
2. Select *Logs* and press `Enter`.
3. Select the desired logs and press `Enter` (see Fig. 7.77).

   → The log file is displayed in a viewer.
4. Press `q` or `Ctrl` + `C` to quit the viewer.

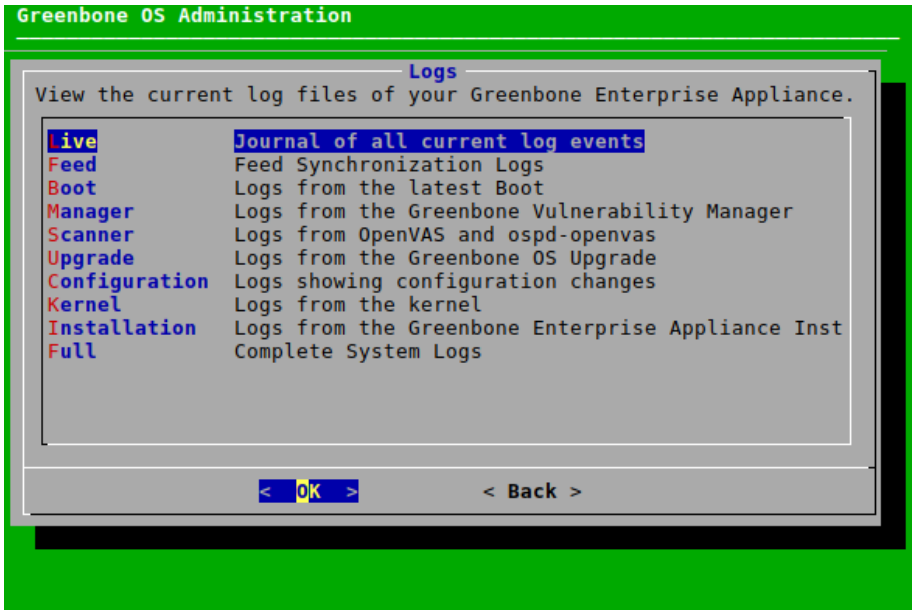


Fig. 7.77: Selecting the log files

7.4.2 Performing Advanced Administrative Work

7.4.2.1 Managing the Superuser Account

When the shell is accessed, a Linux command line is displayed with the unprivileged user *admin* (see Chapter *7.4.2.3* (page 159)). Any Debian GNU/Linux command can be executed, however some commands may be limited to the privileged user *root*.

Note: The privileged account *root* (superuser) should only be used in consultation with the Greenbone Enterprise Support[21].

If changes are made without consultation, the claim for support by the Greenbone Enterprise Support expires.

To obtain root privileges on the appliance, the command `su -` must be entered in the shell. The use of `su -` to switch from the *admin* user to the *root* user is disabled by default.

The superuser must be enabled and provided with a password as follows:

1. Select *Advanced* and press `Enter`.
2. Select *Support* and press `Enter`.
3. Select *Superuser* and press `Enter`.
4. Select *Superuser State* and press `Enter` (see Fig. 7.78).

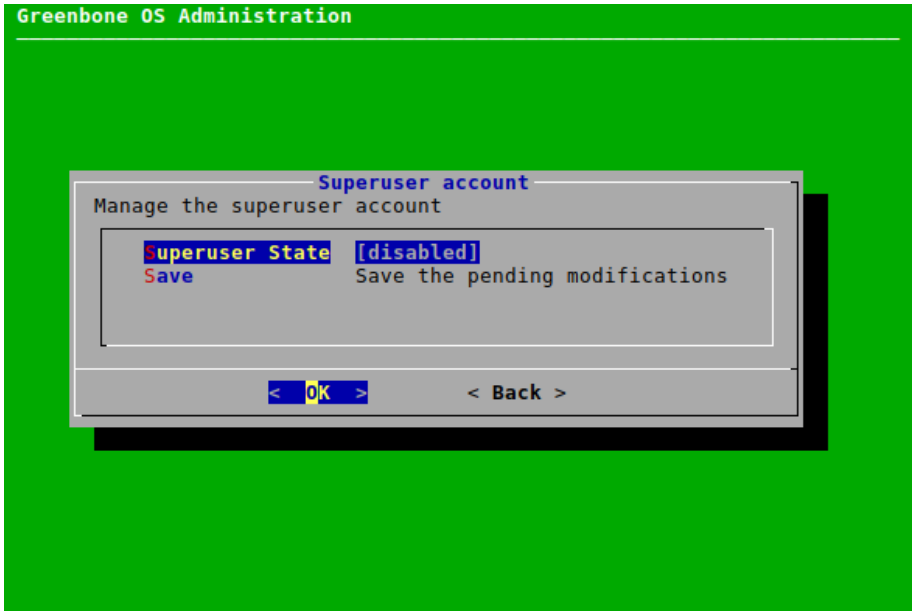


Fig. 7.78: Enabling the superuser

→ A warning informs that root privileges should only be obtained by exception and while consulting the Greenbone Enterprise Support.

5. Select *Yes* and press `Enter`.

   → A message informs that the changes must be saved.

6. Press `Enter` to close the message.
7. Select *Password* and press `Enter`.

[21] https://www.greenbone.net/en/technical-support/

8. Enter the password twice, select *OK* and press `Enter` (see Fig. 7.79).

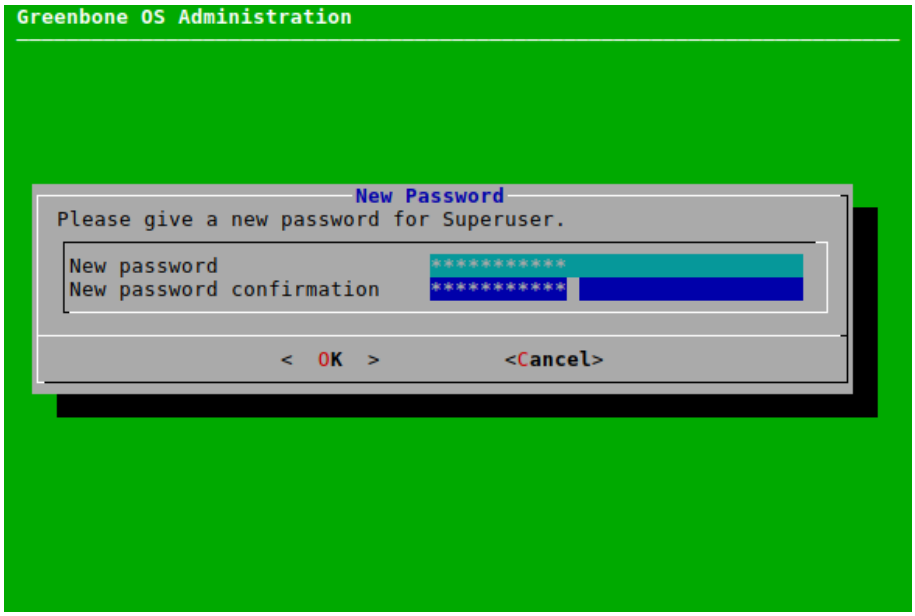


Fig. 7.79: Defining the superuser password

7.4.2.2 Generating and Downloading a Support Package

Sometimes the Greenbone Enterprise Support needs additional information to troubleshoot and support customers. The required data is collected in the form of an (encrypted) support package that contains all configuration data of the appliance.

The package can be encrypted using the Greenbone Enterprise Support GPG public key. The support package is stored on the appliance.

A support package can be created as follows:

1. Select *Advanced* and press `Enter`.
2. Select *Support* and press `Enter`.
3. Select *Support Package* and press `Enter`.

   → A message asks to confirm the generation of the support package.
4. Select *Yes* and press `Enter`.

   → A message asks whether the support package should be encrypted (see Fig. 7.80).
5. Select *Yes* and press `Enter` to encrypt the support package.

   or
5. Select *No* and press `Enter` to not encrypt the support package.

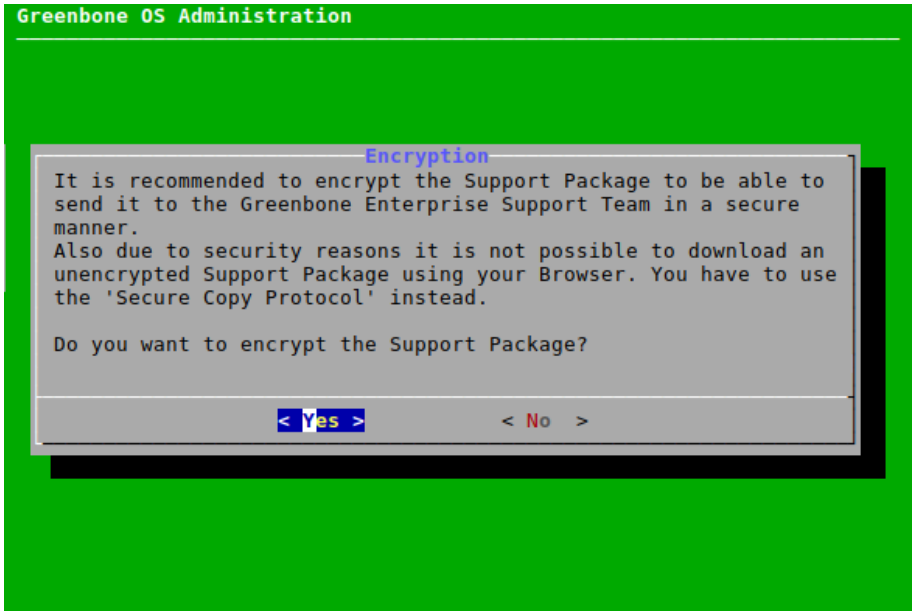


Fig. 7.80: Downloading a support package

6. If an encrypted support package was chosen, open the web browser, enter the displayed URL and download the GPG file (encrypted ZIP folder).

   or

   Note: If the support package is not encrypted, the download must be done via the Secure Copy Protocol (SCP). To do so, SSH must be enabled first (see Chapter *7.2.4.4* (page 108)).

6. If an unencrypted support package was chosen, enter the displayed command using SCP (see Fig. 7.81) and download the support package (ZIP folder).

   Note: The "." at the end can be replaced by a path. If the "." is kept, the current folder will be chosen.

7. Send the ZIP folder to the Greenbone Enterprise Support[22].

On Microsoft Windows systems, the support package can be downloaded using either `pscp`, a command line tool included in PuTTY, or smarTTY, a graphical tool implementing SCP.

[22] https://www.greenbone.net/en/technical-support/

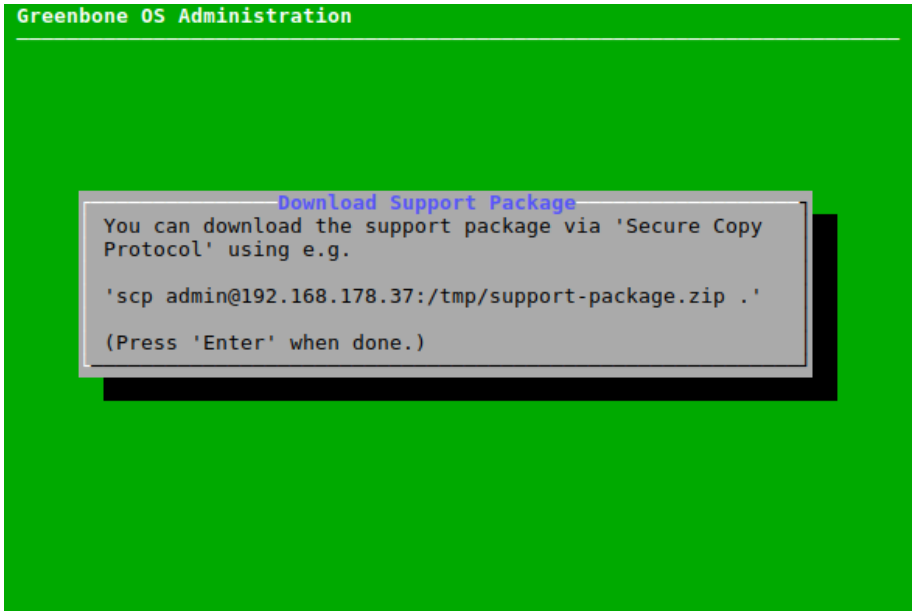


Fig. 7.81: Downloading an unencrypted support package

7.4.2.3 Accessing the Shell

Shell access is not required for any administrative work but can be requested by the Greenbone Enterprise Support for diagnostics and support.

The shell can be accessed as follows:

1. Select *Advanced* and press `Enter`.
2. Select *Support* and press `Enter`.
3. Select *Shell* and press `Enter`.

   → A warning informs that the shell level is undocumented and should not be used for administrative settings (see Fig. 7.82).
4. Select *Continue* and press `Enter`.

   → A Linux shell is opened with the unprivileged user *admin* (see Fig. 7.83).

   Note: Accessing as *root* requires enabling the superuser and setting a password (see Chapter *7.4.2.1* (page 156)). Afterwards, switching to *root* is possible using the command `su -`.
5. Enter `exit` or press `Ctrl` + `D` to quit the shell.

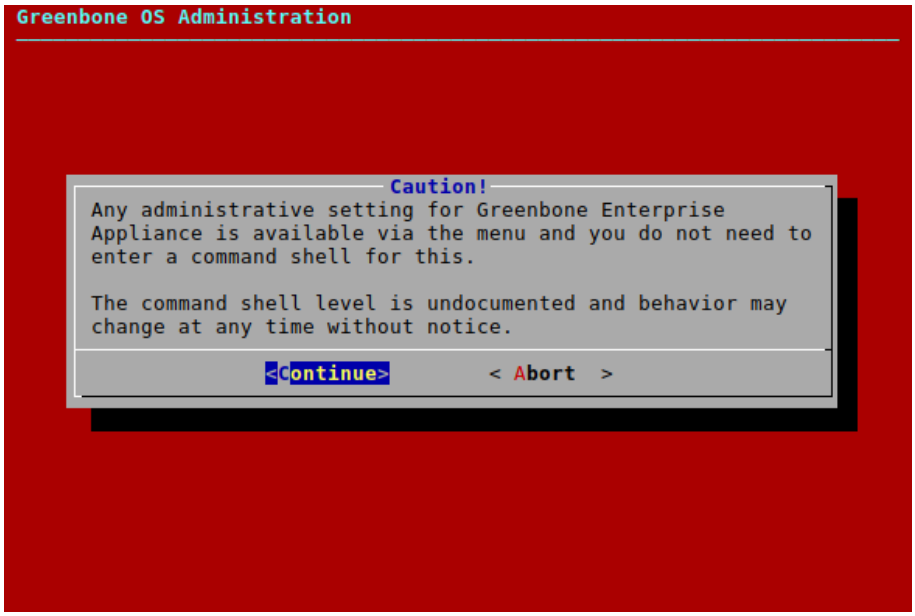


Fig. 7.82: Warning when accessing the shell

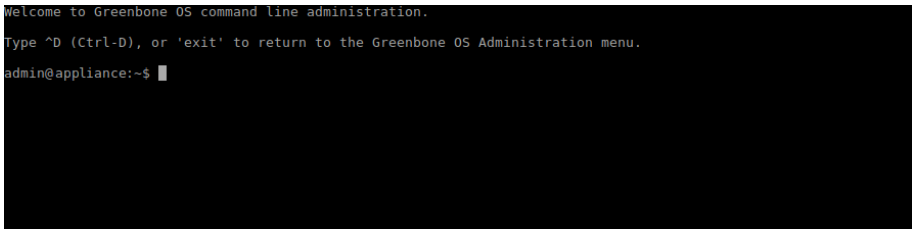


Fig. 7.83: Accessing the local shell

7.4.3 Displaying the Greenbone Enterprise Feed Subscription Key

The subscription key (see Chapter *7.2.7.1* (page 119)) can be displayed as follows:

1. Select *Advanced* and press `Enter`.
2. Select *Subscription* and press `Enter` (see Fig. 7.84).

   → The subscription key is displayed in a viewer.
3. Press `q` to quit the viewer.

7.4.4 Displaying the Copyright and License Information

The copyright file can be displayed as follows:

1. Select *Advanced* and press `Enter`.
2. Select *Copyright and Licenses* and press `Enter` (see Fig. 7.84).

   → The copyright file is displayed in a viewer.
3. Press `q` to quit the viewer.

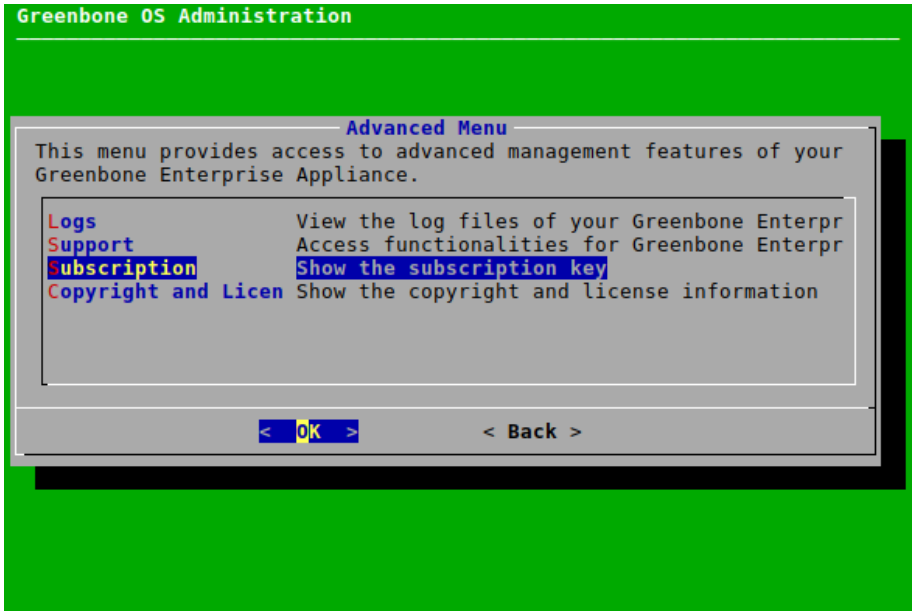


Fig. 7.84: Displaying the subscription key or the copyright file

7.5 Displaying Information about the Appliance

Information about the appliance can be displayed by selecting *About* and pressing `Enter`.

The following information is displayed:

- Appliance model
- GOS version
- Feed version
- Name of the subscription key
- IP address of the web interface
- Configured sensors
- Currently running system operations

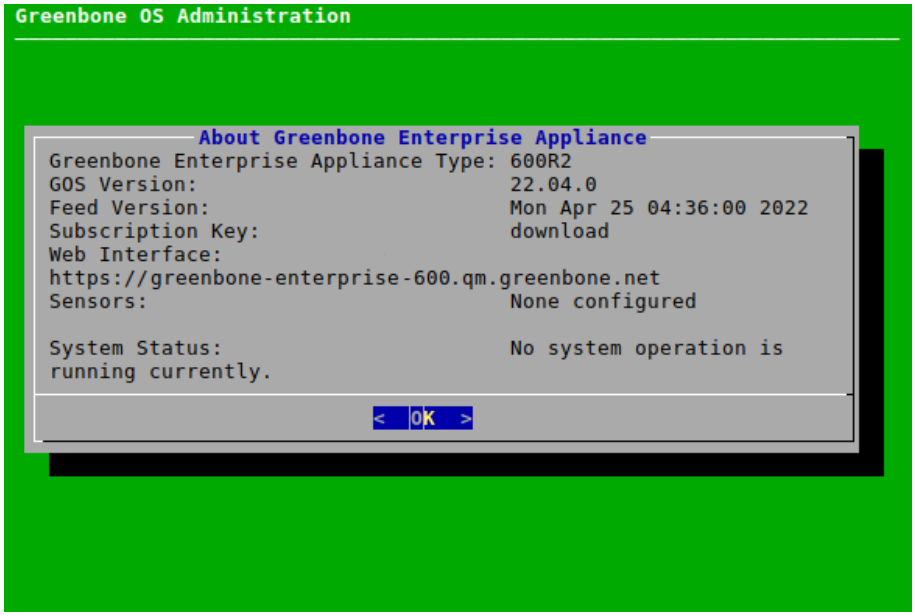


Fig. 7.85: Displaying information about the appliance

CHAPTER 8

Getting to Know the Web Interface

8.1 Logging into the Web Interface

The main interface of the appliance is the web interface, also called Greenbone Security Assistant (GSA). The web interface can be accessed as follows:

1. Open the web browser.
2. Enter the IP address of the appliance's web interface.

   Tip: The appliance's IP address is displayed on the login prompt of the console or in the GOS administration menu after selecting *About* and pressing `Enter`.

3. Log in using the web administrator created during the setup (see Chapter *5* (page 28)).

8.2 Dashboards and Dashboard Displays

Many pages of the web interface show dashboard displays on the top of the page depending on the page content.

There are two types of dashboard displays: charts and tables.

For each page there is a default setting of displays. The default setting can be restored by clicking ↻ on the right side above the displays.

8.2.1 Adding and Deleting Dashboard Displays

A new display can be added as follows:

1. Click ✚ on the right side above the displays.
2. Select the desired display in the drop-down list (see Fig. 8.1).

Tip: The input box above the selectable options can be used to filter the options.

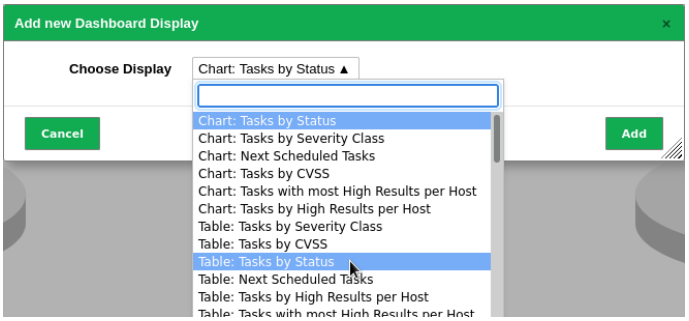


Fig. 8.1: Adding a display

3. Click *Add*.

A display can be deleted by clicking × in the upper right corner of the display (see Fig. 8.2).

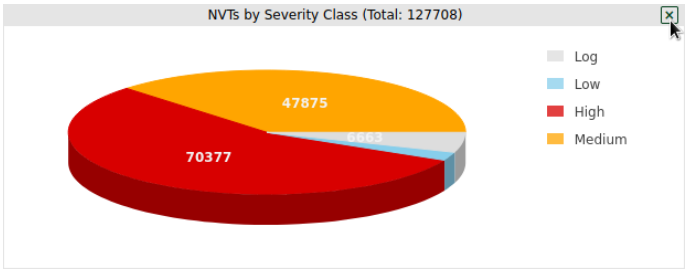


Fig. 8.2: Deleting a display

8.2.2 Editing a Dashboard Display

Depending on the display there are several options which can be selected by moving the mouse to the right edge of a display (see Fig. 8.3):

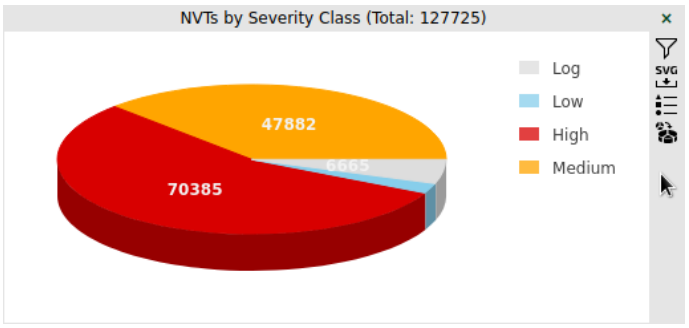


Fig. 8.3: Choosing further options for a display

- Apply a filter to the display. The filter has to be configured for the object type shown in the display.
- Download the chart as an SVG file (only for charts).
- Download the table as a CSV file (only for tables).
- Hide or show a legend (only for charts).

- Switch between 2D and 3D presentation (only for charts).

8.2.3 Organizing Displays in Dashboards

Dashboard displays can be summarized to dashboards. They can be individual compilations of displays but there are predefined dashboards which can be chosen as well.

There can be up to 10 dashboards.

By default, there is only the overview dashboard giving a short overview of tasks, CVEs and VTs (see Fig. 8.4).

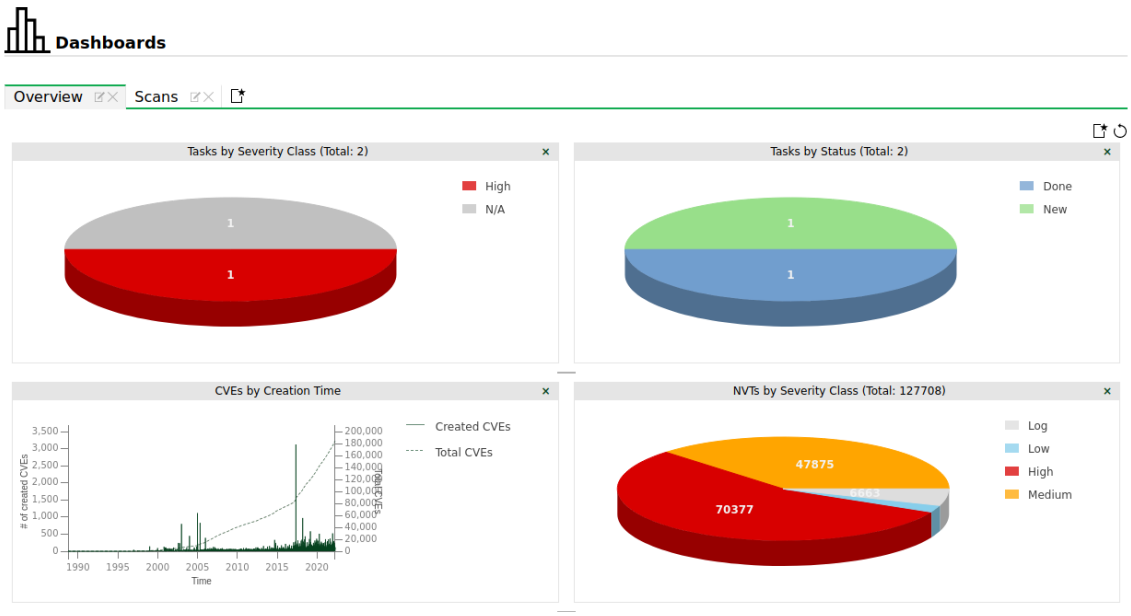


Fig. 8.4: Overview dashboard

The dashboards are displayed by selecting *Dashboards* in the menu bar.

8.2.3.1 Adding a New Dashboard

A new dashboard can be created as follows:

1. Click in the register bar above the dashboard (see Fig. 8.5).

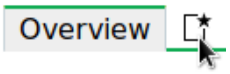


Fig. 8.5: Adding a new dashboard

2. Enter the name of the dashboard in the input box *Dashboard Title*.
3. Select the displays that should be shown by default in the drop-down list *Initial Displays* (see Fig. 8.6).

   The following default settings for the shown displays are possible:

   - Default: the dashboard contains the same displays as the overview dashboard.
   - Scan Displays: the dashboard contains displays concerning tasks, results and reports.
   - Asset Displays: the dashboard contains displays concerning hosts and operating systems.

- SecInfo Displays: the dashboard contains displays concerning VTs, CVEs, and CERT-Bund Advisories.
- Empty: the dashboard contains no displays.

Additionally, already existing dashboards can be chosen.

Tip: The displays can later be edited as well (see Chapters *8.2.1* (page 163) and *8.2.2* (page 164)).

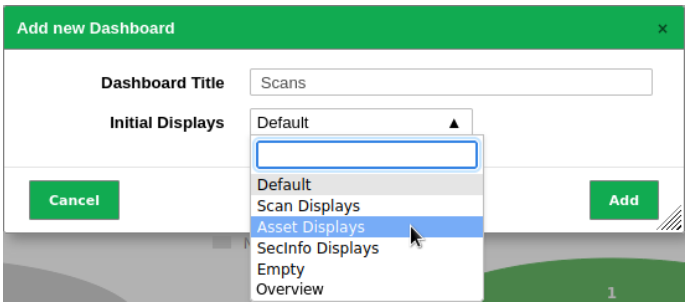


Fig. 8.6: Adding a new dashboard

4. Click *Add*.

   → The dashboard is added and shown in the register bar (see Fig. 8.7).

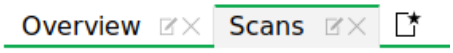


Fig. 8.7: Registers of available dashboards

8.2.3.2 Editing a Dashboard

Displays can be added to or deleted from a dashboard as described in Chapter *8.2.1* (page 163).

The displays in a dashboard can be edited as described in Chapter *8.2.2* (page 164).

A dashboard can be renamed as follows:

1. Click ✎ in the register of the dashboard in the register bar (see Fig. 8.8).

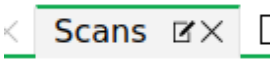


Fig. 8.8: Renaming or deleting a dashboard

2. Change the name in the input box *Dashboard Title*.
3. Click *Save*.

8.2.3.3 Deleting a Dashboard

A dashboard can be deleted by clicking ✕ in the register of the dashboard in the register bar (see Fig. 8.8).

8.3 Filtering the Page Content

Almost every page in the web interface offers the possibility to filter the displayed content.

8.3.1 Adjusting the Filter Parameters

Fig. 8.9: Filter bar at the top of the page

Multiple filter parameters are combined to form the Powerfilter.

Note: The filter is context aware which means that the filter parameters depend on the currently opened page.

The filter parameters can be entered in the input box in the filter bar (see Fig. 8.9) using the specific syntax of the filter (see Chapter *8.3.2* (page 169)) or be modified as follows:

1. Click in the filter bar (see Fig. 8.9).
2. Select and modify the filter parameters (see Fig. 8.10).

   Keywords which should be searched for can be entered in the input box *Filter*.

   Note: The Powerfilter is not case-sensitive. All uppercase letters are transformed to lowercase letters before applying the filter.

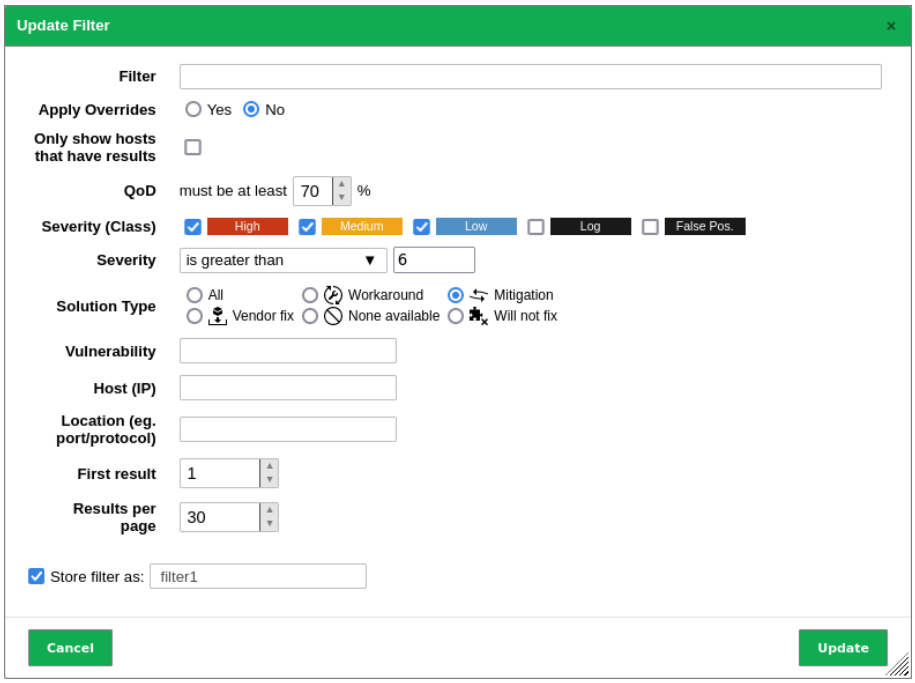


Fig. 8.10: Adjusting the filter

3. Activate the checkbox *Store filter as* if the filter should be stored for reuse.
4. Enter the name for the filter in the input box *Store filter as*.

5. Click *Update*.

   → The filter parameters are applied.

Next to the input box in the filter bar the following actions are available:

- Remove the currently applied filter.
- Update the filter with the current input.
- Reset the filter parameters to the default settings.
- A saved Powerfilter can be applied by selecting it in the drop-down list (see Fig. 8.11).

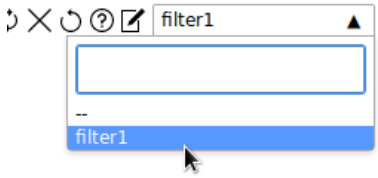


Fig. 8.11: Selecting a saved Powerfilter

Tip: If a specific filter should always be activated on a page, it can be set as the default filter in the user settings (see Chapter *8.7* (page 178)).

Powerfilters can also be created using the page *Filters* as follows:

1. Select *Configuration* > *Filters* in the menu bar.
2. Create a new filter by clicking .
3. Define the name of the filter.
4. Define the filter criteria in the input box *Term* (see Chapter *8.3.2* (page 169)).
5. Select the object type for which the filter should by applied in the drop-down list *Type* (see Fig. 8.12).

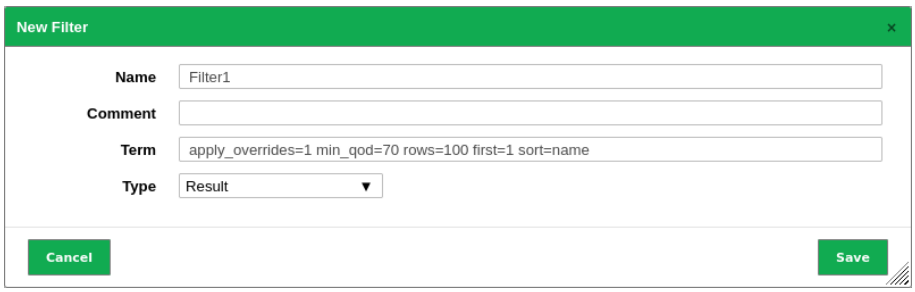


Fig. 8.12: Creating a new filter

6. Click *Save*.

   → The filter can be used for the object type for which it was created.

8.3.2 Filter Keywords

When applied, the filter parameters are shown in the lower left corner of the page (see Fig. 8.13).

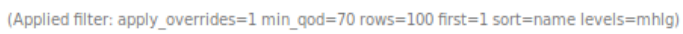


Fig. 8.13: Applied filter parameters

The filter uses a specific syntax which has to be considered when entering the filter keywords directly in the input box in the filter bar.

Tip: A full list of all filter keywords with possible values sorted by page/object type can be found here[23].

8.3.2.1 Global Keywords

In general, the specification of the following keywords is always possible:

Note: These keywords apply to the whole filter request and should only be mentioned once.

Example: filter requests like `name~test and rows=20 or name~def and rows=30` are not allowed. In this case, only `rows=30` would be applied.

- ***rows*:** Number of rows that are displayed per page. Per default the value is *rows=10*. Entering a value of `-1` will display all results. Entering a value of `-2` will use the value that was pre-set in *My Settings* under *Rows Per Page* (see Chapter *8.7* (page 178)).

  Note: Using `rows=-1` may cause performance issues if large amounts of data have to be processed.

  If long page loading times are encountered, another filter for the rows should be used.

- ***first*:** Determination of the first object displayed. Example: if the filter returns 50 results, *rows=10 first=11* displays the results 11 to 20.
- ***sort*:** Determination of the column used for sorting the results. The results are sorted ascending. Example: *sort=name* sorts the results by name. The sorting can also be done by clicking the title of the column. After applying the filter, upper cases of the column names are changed to lower cases and spaces are changed to underscores. Typical column names are:
  - *name*
  - *severity*
  - *host*
  - *location*
  - *qod* (quality of detection)
  - *comment*
  - *modified*
  - *created*

[23] https://www.greenbone.net/wp-content/uploads/Filterkeywords_EN.pdf

Note: *sort* is not applicable for report details pages (see Chapter *11.2.1* (page 288)).

- ***sort-reverse*:** Determination of the column used for sorting the results (see above). The results are sorted descending.

  Note: *sort-reverse* is not applicable for report details pages (see Chapter *11.2.1* (page 288)).

- ***tag*:** Selection of results with a specific tag (see Chapter *8.4* (page 174)). It can be filtered by a specific tag value (*tag="server=mail"*) or only by the tag (*tag="server"*). Regular expressions are also allowed.

  Note: By filtering using tags custom categories can be created and used in the filters. This allows for versatile and granular filter functionality.

- ***tag_id*:** Selection of results with a specific tag (see Chapter *8.4* (page 174)). It is filtered by the UUID of the tag. The UUID of a tag can be found on the tag's details page (see Chapter *8.4.4* (page 175)). The filter stays valid, even if the name of the tag is changed.

8.3.2.2 Operators

When specifying the components the following operators are used:

- = equals, e.g., *rows=10*
- ~ contains, e.g., *name~admin*
- < less than, e.g., *created<-1w* → older than a week
- > greater than, e.g., *created>-1w* → younger than a week
- `regexp` regular expression, e.g., *regexp 192.168.[0-9]+.[0-9]*

The following operators are **not** supported:

- <=
- >=
- `( )`

There are a couple of special features:

- If no value follows =, all results without this filter parameter are displayed. This example shows all results without a comment:

```
comment=
```

- If a keyword should be found but it is not defined which column to scan, all columns will be scanned. This example searches whether at least one column contains the stated value:

```
=192.168.15.5
```

- The data is usually or-combined. This can be specified with the keyword `or`. To achieve an and-combination the keyword `and` needs to be specified:

```
modified>2019-01-01 and name=services
```

- `and` is resolved before `or`, i. e., `x and y or a and b` → `(x and y) or (a and b)`

  Expressions like `x and (a or b)` have to be written as `x and a or x and b`.

- Using `not` negates the filter. This example shows all results that do not contain "192.168.81.129":

```
not ~192.168.81.129
```

8.3.2.3 Text Phrases

In general, text phrases that are being searched for can be specified.

The following examples show the differences:

`overflow` Finds all results that contain the word *overflow*. This applies to *Overflow* as well as to *Bufferoverflow*. Also, *192.168.0.1* will find *192.168.0.1* as well as *192.168.0.100*.

`remote exploit` Finds all results containing *remote* or *exploit*. Of course, results that contain both words will be displayed as well.

`remote and exploit` Finds all results containing both *remote* and *exploit*. The results do not have to be found in the same column.

`"remote exploit"` The exact string is being searched for and not the individual words.

`regexp 192.168.[0-9]+.[0-9]` The regular expression is being searched for.

8.3.2.4 Time Specifications

Time specifications in the Powerfilter can be absolute or relative.

Absolute time specification An absolute time specification has the following format:

```
2023-04-21T13h50
```

If the time is left out, a time of 12:00 am will be assumed automatically. The time specification can be used in the search filter, e.g., *created>2023-04-21*.

Relative time specification Relative time specifications are always calculated in relation to the current time. Time specification in the past are defined with a preceding minus (-). Time specification without a preceding character are interpreted as being in the future. For time periods the following letters can be used:

- *s* second
- *m* minute
- *h* hour
- *d* day
- *w* week
- *m* month (30 days)
- *y* year (365 days)

For example, entering *created>-5d* shows the results that were created within the past 5 days. A combination such as *5d1h* is not permitted but has to be replaced with *121h*.

To limit the time period, e.g., month for which information should be displayed, the following expression can be used:

```
modified>2023-03-01 and modified<2023-03-31
```

8.3.3 Examples for Powerfilters

Here are some examples for powerfilter:

- `127.0.0.1` shows any object that has “127.0.0.1” anywhere in the text of any column.
- `127.0.0.1 iana` shows any object that has “127.0.0.1” or “iana” anywhere in the text of any column.
- `127.0.0.1 and iana` shows any object that has “127.0.0.1” and “iana” anywhere in the text of any column.
- `regexp 192.168.[0-9]+.[0-9]` shows any object that has an IP style string starting with “192.168” anywhere in the text of any column.
- `name=localhost` shows any object with the exact name “localhost”.
- `name~local` shows any object with “local” anywhere in the name.
- `name:^local` shows any object with a name starting with “local”.
- `port_list~tcp` shows any object that has “tcp” anywhere in the port list name.
- `modified>2023-04-03 and modified<2023-04-05` shows any object that was modified between 2023-04-03 0:00 and 2023-04-05 0:00.
- `created>2023-04-03T13h00` shows any object that was created after 13:00 on 2023-04-03.
- `rows=20 first=1 sort=name` shows the first twenty objects sorted by the column *Name*.
- `created>-7d` shows any object that was created within the past 7 days.
- `=127.0.0.1` shows any object that has “127.0.0.1” as the exact name in any column.
- `tag="geo:long=52.2788` shows any object that has a tag named “geo:long” with the value “52.2788”.
- `tag~geo` shows any object that has a tag with a name containing “geo”.

8.3.4 Managing Powerfilters

List Page

All existing Powerfilters can be displayed by selecting *Configuration* > *Filters* in the menu bar (see Fig. 8.14).

For all Powerfilters the following information is displayed:

Name Name of the filter.

Term Filter terms that form the Powerfilter (see Chapter *8.3.2* (page 169)).

Type Object type for which the Powerfilter can be applied.

For all Powerfilters the following actions are available:

- Move the Powerfilter to the trashcan.
- Edit the Powerfilter.
- Clone the Powerfilter.
- Export the Powerfilter as an XML file.

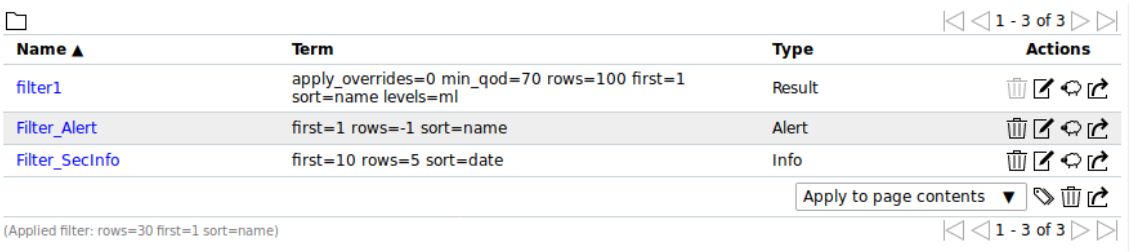


Fig. 8.14: Managing Powerfilters

Note: By clicking or below the list of filters more than one filter can be moved to the trashcan or exported at a time. The drop-down list is used to select which filters are moved to the trashcan or exported.

Details Page

Click on the name of a filter to display the details of the filter. Click to open the details page of the filter.

The following registers are available:

Information General Information about the Powerfilter.

User Tags Assigned tag (see Chapter *8.4* (page 174)).

Permissions Assigned permissions (see Chapter *9.4* (page 193)).

The following actions are available in the upper left corner:

- Open the corresponding chapter of the user manual.
- Show the list page of all Powerfilters.
- Create a new Powerfilter (see Chapter *8.3.1* (page 167)).
- Clone the Powerfilter.
- Edit the Powerfilter.
- Move the Powerfilter to the trashcan.
- Export the Powerfilter as an XML file.

8.4 Using Tags

Tags are information that can be linked to any object. Tags are created directly with the objects and can only be linked to the object type they are created for.

Tags can be used to filter objects (see Chapter *8.3* (page 167)).

Example: when filtering for `tag=target` the specific tag must be set. Otherwise, the desired result would not be found. With `tag="target=mailserver"` the exact tag with the respective value must be set (see Fig. 8.15).

Fig. 8.15: Tag for the object type *Target*

8.4.1 Linking a Tag to a Single Object

A tag for a single object can be created as follows:

1. Open the details page of the object by clicking on the object's name and clicking .
2. Click on the register *User Tags*.
3. Click in the opened section *User Tags*.
4. Define the tag (see Fig. 8.15).
5. Click *Save*.

8.4.2 Linking a Tag to Multiple Objects

A tag can be added to multiple objects of the same type (e.g., tasks, targets, scanners) as follows:

1. Open the list page of an object type.
2. Filter the list so that only the objects that should have the tag are displayed.
3. In the drop-down list below the list of objects select to which objects the tag should be added (see Fig. 8.16).

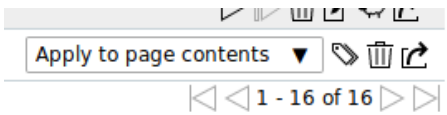


Fig. 8.16: Selecting the objects

Note: *Apply to page contents* links the tag to all objects which are visible on the current page.

Apply to all filtered links the tag to all objects which are affected by the filter even if they are not visible on the current page.

or

2. In the drop-down list below the list of objects select *Apply to selection*.
3. Activate the checkboxes of the objects that should have the tag in the column *Actions*.
4. Click below the list of objects.
5. Select the tag in the drop-down list *Choose Tag* (see Fig. 8.17).

Note: Only tags which are created for the chosen object type can be selected.

Additionally, a new tag can be created by clicking .

Fig. 8.17: Selecting a tag for multiple objects

6. Click *Add Tag*.

8.4.3 Creating a Tag

In addition to linking tags directly to an object, tags can be created on the page *Tags* and assigned afterwards.

1. Select *Configuration* > *Tags* in the menu bar.
2. Create a new tag by clicking .
3. Define the tag. Select the object type for which the tag can be assigned in the drop-down list *Resource Type*.
4. Click *Save*.

8.4.4 Managing Tags

List Page

All existing tags can be displayed by selecting *Configuration* > *Tags* in the menu bar.

For all tags the following actions are available:

- Disable the tag if it is enabled.
- Enable the tag if it is disabled.

- Move the tag to the trashcan.
- Edit the tag.
- Clone the tag.
- Export the tag as an XML file.

Note: By clicking or below the list of tags more than one tag can be moved to the trashcan or exported at a time. The drop-down list is used to select which tags are moved to the trashcan or exported.

Details Page

Click on the name of a tag to display the details of the tag. Click to open the details page of the tag.

The following registers are available:

Information General information about the tag.

Assigned Items Objects to which the tag is assigned. The objects are only displayed if the tag is enabled.

Permissions Assigned permissions (see Chapter *9.4* (page 193)).

The following actions are available in the upper left corner:

- Open the corresponding chapter of the user manual.
- Show the list page of all tags.
- Create a new tag (see Chapter *8.4.3* (page 175)).
- Clone the tag.
- Edit the tag.
- Move the tag to the trashcan.
- Export the tag as an XML file.
- Disable the tag if it is enabled.
- Enable the tag if it is disabled.

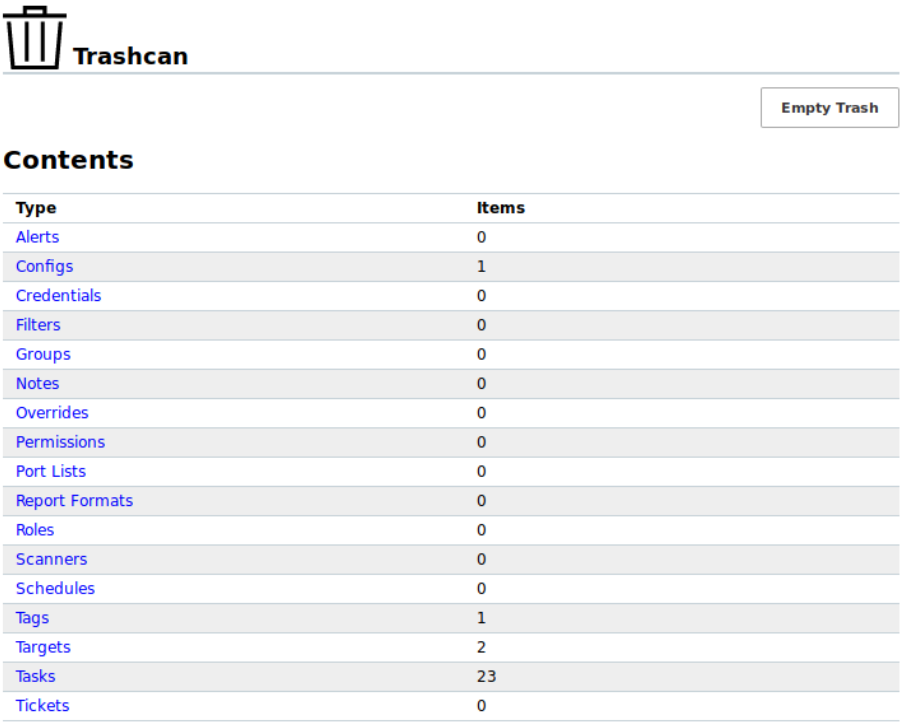
8.5 Using the Trashcan

The page *Trashcan* is opened by selecting *Administration* > *Trashcan* in the menubar. The page lists all objects that are currently in the trashcan, grouped by object type.

Note: Objects in the trashcan do not count as deleted yet. They are only finally deleted when manually deleting them from the trashcan, or when emptying the whole trashcan.

The summary table *Content* shows all possible types of deleted objects with object counts. By clicking on an object name the corresponding section is shown (see Fig. 8.18).

The trashcan can be emptied by clicking *Empty Trash*.



Trashcan

Empty Trash

Contents

Type	Items
Alerts	0
Configs	1
Credentials	0
Filters	0
Groups	0
Notes	0
Overrides	0
Permissions	0
Port Lists	0
Report Formats	0
Roles	0
Scanners	0
Schedules	0
Tags	1
Targets	2
Tasks	23
Tickets	0

Fig. 8.18: Contents of the trashcan

In the section of the respective object type the single objects can be managed (see Fig. 8.19):

- Clicking moves the object out of the trashcan and back to its regular page. The object cannot be restored if it depends on another object in the trashcan.
- Clicking removes the object entirely from the system. The object cannot be deleted if another object in the trashcan depends on it.

File Content Violation	File Content	Any	10.0 (High)	yes	
Error on File System	File Content: Errors	Any	5.0 (Medium)	yes	
File Content Violation	File Content: Violations	Any	5.0 (Medium)	yes	
OS End of Life Detection	OS End Of Life Detection	Any	2.0 (Low)	no	
TCP Timestamps	TCP timestamps	Any	5.0 (Medium)	yes	

Fig. 8.19: Restoring or deleting a trashcan object

8.6 Displaying the Feed Status

The synchronization status of all SecInfo can be displayed by selecting *Administration* > *Feed Status* in the menu bar.

The following information is displayed (see Fig. 8.20):

Type Feed type (*NVT*, *SCAP*, *CERT* or *GVMD_DATA*).

Content Type of information provided by the feed.

Origin Name of the feed service that is used to synchronize the SecInfo.

Version Version number of the feed data.

Status Status information of the feed, e.g., time since the last update.

If a feed update is currently being performed, *Update in progress...* is displayed. This status is displayed for all feeds, even if only one feed is currently being updated.

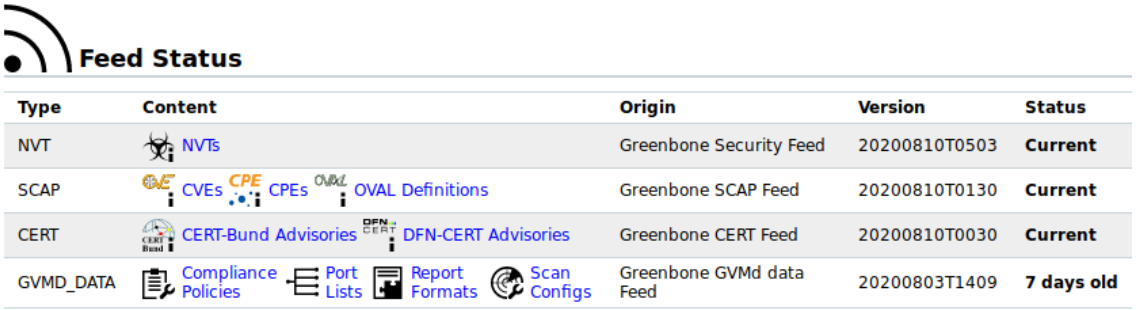


Fig. 8.20: Displaying the feed status

8.7 Changing the User Settings

Every user of the appliance can manage their own settings for the web interface. These settings can be accessed by moving the mouse over in the upper right corner and clicking *My Settings* (see Fig. 8.21).

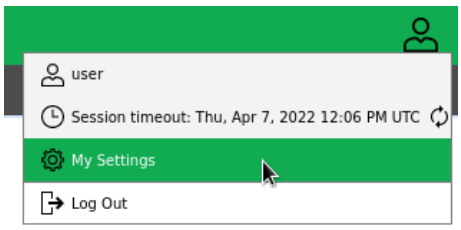


Fig. 8.21: Accessing the user settings

The settings can be modified by clicking .

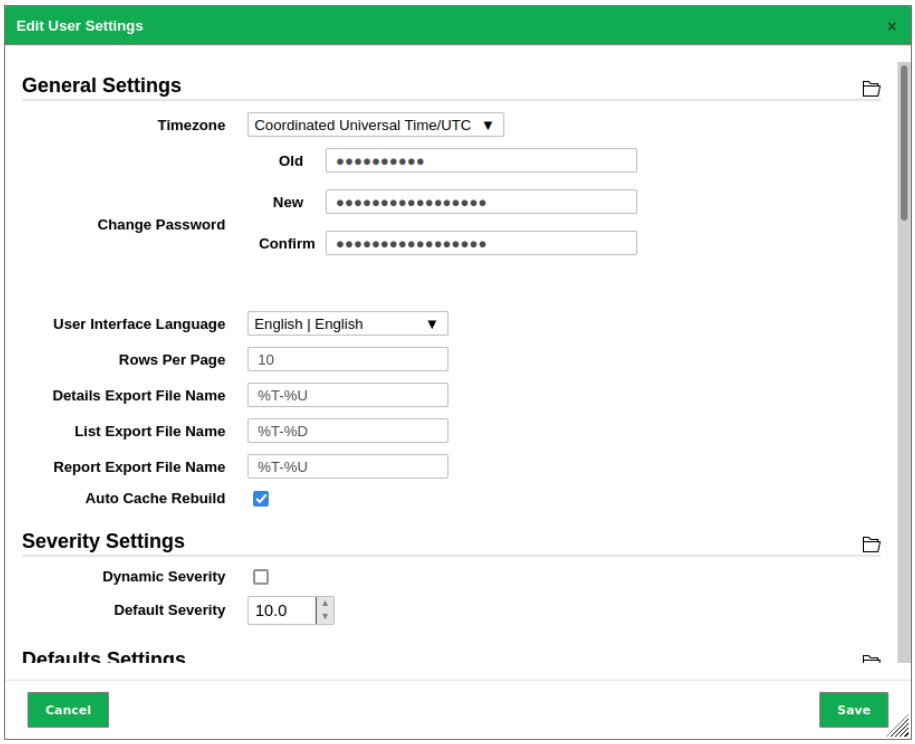


Fig. 8.22: Managing user settings

Important settings are:

Timezone The appliance saves all information in the time zone UTC±00:00 internally. In order to display the data in the time zone of the user the respective selection is required.

Change Password The user password can be changed here.

User Interface Language The language can be defined here. The browser setting are used per default.

Rows Per Page This defines the default number of objects shown per list page on the web interface. A high number of rows per page increases loading times. Custom user filters may override this setting (see Chapter *8.3* (page 167)).

Details Export File Name This defines the default name of the file for exported object details. For the file name the following placeholders can be used:

- %C: the creation date in the format YYYYMMDD. Changed to the current date if a creation date is not available.
- %c: the creation time in the format HHMMSS. Changed to the current time if a creation time is not available.
- %D: the current date in the format YYYYMMDD.
- %F: the name of the used report format (XML for lists and types other than reports).
- %M: the modification date in the format YYYYMMDD. Changed to the creation date or to the current date if a modification date is not available.
- %m: the modification time in the format HHMMSS. Changed to the creation time or to the current time if a modification time is not available.
- %N: the name for the object or the associated task for reports. Lists and types without a name will use the type (see %T).

- %T: the object type, e.g., “task”, “port_list”. Pluralized for list pages.
- %t: the current time in the format HHMMSS.
- %U: the unique ID of the object or “list” for lists of multiple objects.
- %u: the name of the currently logged in user.
- %%: the percent sign (%).

List Export File Name This defines the default name of the file for exported object lists (see above).

Report Export File Name This defines the default name of the file for exported reports (see above).

Auto Cache Rebuild The automatic cache rebuild can be enabled or disabled here. If many actions are performed in a row (e.g., deleting of multiple objects) with enabled automatic cache rebuild, each action triggers the cache rebuild leading to a slowed down process. For such cases, the automatic cache rebuild can be disabled temporarily.

Dynamic Severity This defines whether the severity of an existing result is changed if the severity of the underlying VT changes. Otherwise, the new severity only affects future scans.

Default Severity The default severity can be specified here. In case no severity is assigned to a VT, the default severity is used.

Defaults Settings The default selections or entries for various settings can be specified here.

Filter Settings Specific default filters for each page can be specified here. The filters are then activated automatically when the page is loaded.

8.8 Opening the Manual

The manual can be opened by selecting *Help > User Manual* in the menu bar.

Additionally, the manual can be opened on any page by clicking ⓘ in the upper left corner. The chapter related to the page content is opened.

8.9 Logging Out of the Web Interface

Logging out of the web interface can be done by moving the mouse over in the upper right corner and clicking *Log Out* (see Fig. 8.23).

If no action is performed on the web interface for a defined period of time, the user is logged out automatically (see Chapter *7.2.4.1.1* (page 97)). The default timeout is 15 minutes.

The remaining time until the user is automatically logged out can be displayed by moving the mouse over . By clicking the timeout can be reset.

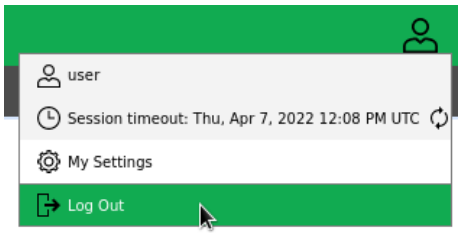


Fig. 8.23: Logging out of the web interface

CHAPTER 9

Managing the Web Interface Access

Note: This chapter documents all possible menu options.

However, not all appliance models support all of these menu options. Check the tables in Chapter *3* (page 20) to see whether a specific feature is available for the used appliance model.

9.1 Users

The Greenbone Enterprise Appliance allows for the definition and management of multiple users with different roles and permissions. When initializing the appliance, the first user – the web/scan administrator – is already created in the GOS administration menu. With this user, additional users can be created and managed.

Roles The appliance's user management supports a role-based permission concept when accessing the web interface. Various roles are already set up by default. Additional roles can be created and used by an administrator. The role defines which options of the web interface can be viewed and modified by the user. The role enforcement is not implemented in the web interface but rather in the underlying Greenbone Management Protocol (GMP) and so affects all GMP clients. Read and write access can be assigned to roles separately.

Groups In addition to roles, the appliance's user management supports groups as well. This serves mainly for logical grouping.

Groups and roles may be used to assign permissions to several users at once.

Each user is assigned an IP address range containing the allowed or denied targets. The appliance will refuse to scan any other IP addresses than the ones specified. Similarly, the access to specific interfaces of the appliance can be allowed or denied.

The user management is completely done with the appliance. External sources for the user management are not supported. However, to support central authentication and to allow password synchronization, the appliance can be integrated with a central LDAPS or RADIUS server (see Chapter *9.5* (page 203)). The server will only be used to verify the password during the login process of the user. All other settings are performed in the appliance's user management.

9.1.1 Creating and Managing Users

9.1.1.1 Creating a User

Users can be created as follows:

Note: Only administrators are allowed to create and manage additional users.

1. Log in as an administrator.
2. Select *Administration* > *Users* in the menu bar.
3. Create a new user by clicking .
4. Define the user (see Fig. 9.1).

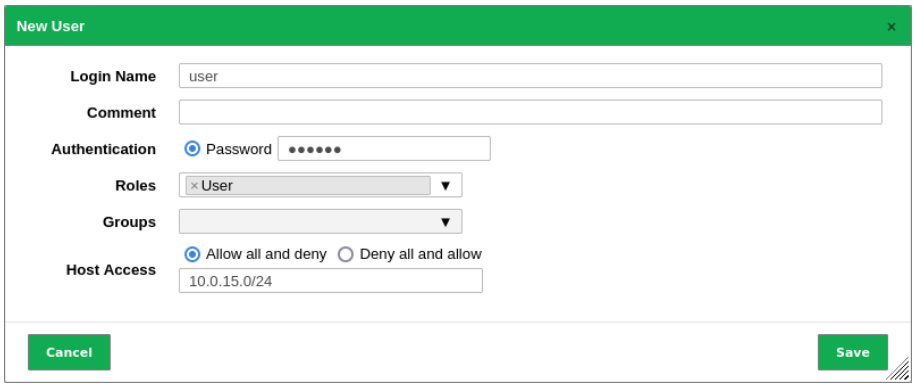


Fig. 9.1: Creating a new user

5. Click *Create*.

   → The user is created and displayed on the page *Users*.

The following details of the user can be defined:

Login Name This is the name used for logging in. Only the following characters are allowed for the login name:

- All alphanumeric characters
- - (dash)
- _ (underscore)
- . (full stop)

Note: When using a central user management (see Chapter *9.5* (page 203)), limitations to the length and character types may apply, based on the LDAP or RADIUS server. Additionally, the user must be created with the exact same name (rDN) as used by the server.

Authentication This is the method used for logging in.

- **Password** For using local authentication with the login name and a password.

  The password can contain any type of character and has practically no length limit.

  When using special characters, note that these must be available on all used keyboards and correctly supported by all client software and operating systems. Copying and pasting special characters for passwords can lead to invalid passwords depending on these external factors.

- **LDAP Authentication Only** For using a central user management, see Chapter *9.5* (page 203).
- **RADIUS Authentication Only** For using a central user management, see Chapter *9.5* (page 203).

Roles Each user can have multiple roles. The roles define the permissions of a user when using GMP. The roles *Admin*, *User*, *Info*, *Observer*, *Guest* and *Monitor* are available. Additionally, it is possible to add and configure custom roles (see Chapter *9.2.2* (page 188)).

If a user with a custom role should be able to use the web interface, at least the following permissions are necessary for that role:

- *authenticate*
- *get_settings*
- *help*

For further details see Chapter *9.2* (page 187).

Groups Each user can be a member of multiple groups. Permissions management can be performed using groups as well (see Chapter *9.4* (page 193)).

Host Access Hosts on which the user is allowed to run scans. The restrictions also apply to administrators but they are allowed to remove them themselves. Normal users (*User*) and roles without access to the user management cannot circumvent the restrictions. Basically either a whitelist (deny all and allow) or a blacklist (allow all and deny) is possible.

- **Whitelist** The scanning of all systems is denied in general. Only explicitly listed systems are allowed to be scanned.
- **Blacklist** The scanning of all systems is allowed in general. Only explicitly listed systems are not allowed to be scanned.

Tip: In general the whitelist methodology should be used. This ensures that users do not scan systems lying beyond their responsibility, located somewhere on the Internet or reacting to malfunctioning scans by accident.

System names as well as IPv4 and IPv6 addresses can be entered. Individual IP addresses as well as address ranges and network segments can be specified. The following listing shows some examples:

- 192.168.15.5 (IPv4 address)
- 192.168.15.5-192.168.15.27 (IPv4 address range long form)
- 192.168.15.5-27 (IPv4 address range short form)
- 192.168.15.128/25 (IPv4 address range, CIDR notation)
- 2001:db8::1 (IPv6 address)
- 2001:db8::1-2001:db8::15 (IPv6 address range long form)
- 2001:db8::1-15 (IPv6 address range short form)
- 2001:db8::/120 (IPv6 address range, CIDR notation)

All options can be mixed and matched, and entered as a comma-separated list. By default, the subnet mask in the CIDR notation is restricted to a maximum of 20 for IPv4 and 116 for IPv6. The reason for this is that the maximum number of IP addresses per target is 4096 for most appliances. If the maximum number of IP addresses is higher, e.g., for the Greenbone Enterprise 6500, correspondingly larger subnet masks can be configured.

9.1.1.2 Managing Users

List Page

All existing users can be displayed by selecting *Administration > Users* in the menu bar when logged in as an administrator.

For all users the following information is displayed:

Name Name of the user. Global users are users who are created in the GOS administration menu (see Chapter *7.2.1* (page 72)) and are marked with 👓.

Roles Role of the user (see Chapter *9.2* (page 187)).

Groups Groups to which the user belongs (see Chapter *9.3* (page 191)).

Host Access Hosts on which the user is allowed to run scans.

Authentication Type Type of authentication: *Local* if a password is used, *RADIUS* or *LDAP* if a central user management is used (see Chapter *9.5* (page 203)).

For all users the following actions are available:

- ✕ Delete the user. Only users which are currently not logged in and which are not super administrator can be deleted.
- Edit the user.
- Clone the user.
- Export the user as an XML file.

Note: By clicking ✕ or below the list of users more than one user can be deleted or exported at a time. The drop-down list is used to select which users are deleted or exported.

Details Page

Click on the name of a user to display the details of the user. Click to open the details page of the user (see Fig. 9.2).

The following registers are available:

Information General information about the user.

User Tags Assigned tags (see Chapter *8.4* (page 174)).

Permissions Permissions of the user or of other users/roles/groups to the resources of the user (see Chapter *9.4* (page 193)).

The following actions are available in the upper left corner:

- Open the corresponding chapter of the user manual.
- Show the list page of all users.
- Create a new user (see Chapter *9.1.1.1* (page 183)).
- Clone the user.
- Edit the user.
- Delete the user. Only users which are currently not logged in and which are not super administrator can be deleted.
- Export the user as an XML file.

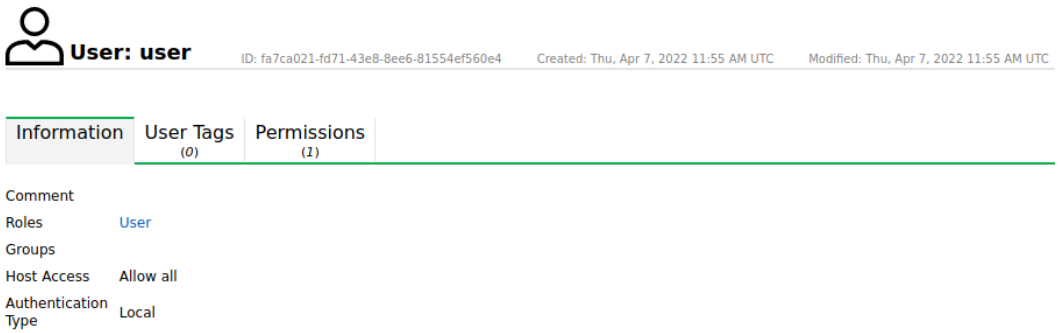


Fig. 9.2: Details of a user

9.1.2 Simultaneous Login

It is possible that two users are logged in at the same time.

If the same user wants to log in more than once at the same time, the login must be performed from a different PC or with a different browser. Another login in the same browser invalidates the first login.

9.1.3 Creating a Guest Login

The guest user is only allowed restricted access to the web interface.

To allow the guest access, a user can be created and assigned the role *Guest* (see Chapter *9.1.1* (page 183)).

Having knowledge of the password the guest user can now log in and is presented with the page *Dashboards*.

To allow a guest to log in without needing a password, this feature has to be activated in the GOS administration menu (see Chapter *7.2.1.4* (page 75)).

9.2 Roles

The web interface supports the creation and configuration of own user roles.

The following roles are available by default:

- **Admin** This role has all permissions by default. It is especially allowed to create and manage other users, roles and groups.
- **User** This role has all permissions by default except for user, role and group management. This role is not allowed to synchronize and manage the feeds. In the web interface there is no access to the page *Administration*.
- **Info** This role (Information Browser) has only read access to the VTs and SCAP information. All other information is not accessible. The role can modify personal setting, e.g., change the password.
- **Guest** This role corresponds with the role *Info* but is not allowed to change the user settings.
- **Monitor** This role has access to system reports of the appliance (see Chapter *17.1* (page 379)).
- **Observer** This role has read access to the system but is not allowed to start or create new scans. It has only read access to the scans for which it has been set as an observer.
- **Super Admin** This role has access to all objects of all users. It has no relation to the super user (*su/root*) in the GOS administration menu. This role cannot be configured in the web interface and users with this role cannot be deleted using the web interface. Users with this role should be managed using the GOS administration menu (see Chapter *9.2.5* (page 191)).

Note: Only administrators are allowed to create and manage additional roles.

Note: Modifying the default roles is not possible but they can be copied (cloned) and subsequently modified.

This ensures consistent behavior when updating the software.

9.2.1 Cloning an Existing Role

When an existing role closely reflects the demands, a new role can be created by cloning the existing role:

1. Log in as an administrator.
2. Select *Administration* > *Roles* in the menu bar.
3. In the row of an existing role, click .
4. In the row of the clone, click .
5. Enter the name of the role in the input box *Name* (see Fig. 9.3).
6. Select the users that should have the role in the drop-down list *Users*.
7. Add a permission by selecting it in the drop-down list *Name* and clicking *Create Permission*.
8. Add a super permission by selecting the respective group in the drop-down list *Group* and clicking *Create Permission*.

   Delete a permission by clicking in the list *General Command Permissions*.
9. Click *Save*.

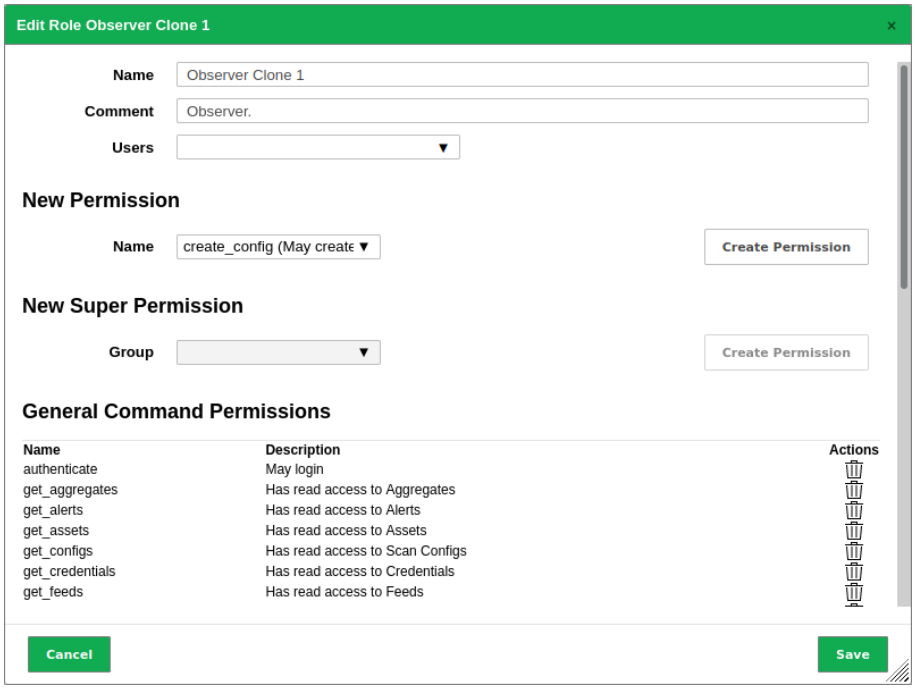


Fig. 9.3: Editing a cloned role

9.2.2 Creating a Role

When a role with only limited functionality should be created, it can be started with a new, empty role:

1. Log in as an administrator.
2. Select *Administration* > *Roles* in the menu bar.
3. Create a new role by clicking .

4. Define the role.

   The following details of the role can be defined:

   Name The name of the role can contain letters and numbers and can be at most 80 characters long.

   Comment (optional) A comment describes the role in more detail.

   Users The users with this role can be selected in the drop-down list *Users*. Alternatively, roles can be managed in the user profile (see Chapter *9.1.1* (page 183)).

5. Click *Save*.

   → The role is created and displayed on the page *Roles*.

6. In the row of the newly created role, click ✎.

7. Add a permission by selecting it in the drop-down list *Name* and clicking *Create Permission*.

   Note: If users with the role should be able to use the web interface, at least the following permissions are necessary:

   - *authenticate*
   - *get_settings*
   - *help*

   The permission *write_settings* allows users to change their own password, time zone and other personal settings.

8. Add a super permission by selecting the respective group in the drop-down list *Group* and clicking *Create Permission*.

   Delete a permission by clicking 🗑 in the list *General Command Permissions*.

9. Click *Save*.

9.2.3 Managing Roles

List Page

All existing roles can be displayed by selecting *Administration > Roles* in the menu bar.

For all roles the following information is displayed:

Name Name of the role. All default roles are global roles and are marked with 👓.

For all roles the following actions are available:

- 🗑 Move the role to the trashcan. Only self-created roles can be moved to the trashcan.
- ✎ Edit the role. Only self-created roles can be edited.
- Clone the role.
- Export the role as an XML file.

Note: By clicking 🗑 or below the list of roles more than one role can be moved to the trashcan or exported at a time. The drop-down list is used to select which roles are moved to the trashcan or exported.

Details Page

Click on the name of a role to display the details of the role. Click 🔍 to open the details page of the role.

The following registers are available:

Information General information about the role.

General Command Permissions GMP commands that can be executed by this role.

User Tags Assigned tags (see Chapter *8.4* (page 174)).

Permissions Permissions of the role or of other users/roles/groups to the role's resources (see Chapter *9.4* (page 193)).

The following actions are available in the upper left corner:

- Open the corresponding chapter of the user manual.
- Show the list page of all roles.
- Create a new role (see Chapter *9.2.2* (page 188)).
- Clone the role.
- Edit the role. Only self-created roles can be edited.
- Move the role to the trashcan. Only self-created roles can be moved to the trashcan.
- Export the role as an XML file.

9.2.4 Assigning Roles to a User

A user can have more than one role to group permissions.

The roles are assigned when creating a new user (see Fig. 9.4, see Chapter *9.1.1* (page 183)). If more than one role is assigned to a user, the permissions of the roles will be added.

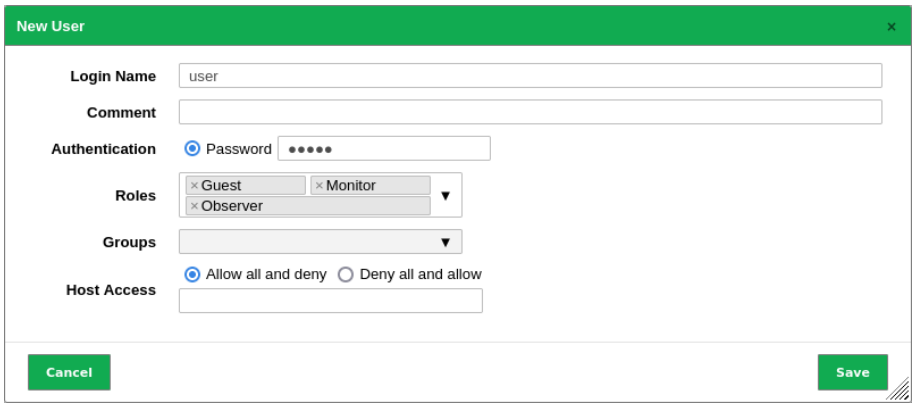


Fig. 9.4: Creating a new user with multiple roles

9.2.5 Creating a Super Administrator

The role *Super Admin* is the highest level of access.

The role *Admin* is allowed to create, modify and delete users. Additionally, it can view, modify and delete permissions but is subordinated to those permissions as well. If any user creates a private scan configuration but does not share it, the administrator cannot access it.

The role *Super Admin* is more suited for diagnostic purposes. The super administrator is excluded from permission restrictions and allowed to view and edit any configuration settings of any user.

The super administrator must be created in the GOS administration menu (see Chapter *7.2.1.5* (page 76))

Note: The super administrator can only be edited by the super administrator.

9.3 Groups

Groups are used to logically assemble users. An unlimited number of groups can be created.

Permissions can be assigned for the groups (see Chapter *9.4* (page 193)). By default, no groups are set up.

9.3.1 Creating a Group

A group can be created as follows:

Note: Only administrators are allowed to create and manage groups.

1. Log in as an administrator.
2. Select *Administration* > *Groups* in the menu bar.
3. Create a new group by clicking .
4. Define the group (see Fig. 9.5).

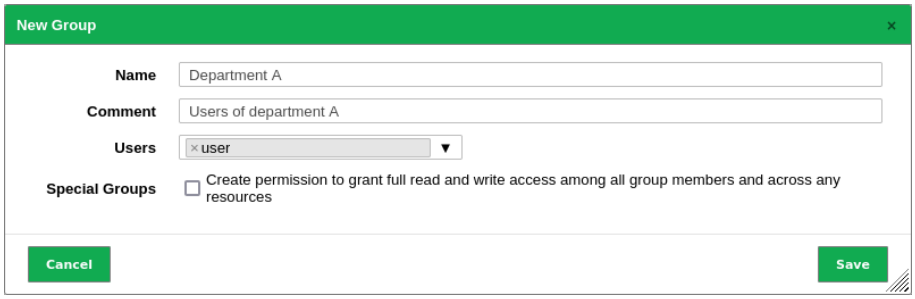


Fig. 9.5: Creating a new group

5. Click *Save*.

   → The group is created and displayed on the page *Groups*.

The following details of the group can be defined:

Name The name of the group can contain letters and numbers and can be at most 80 characters long.

Comment (optional) A comment describes the group in more detail.

Users The members of the group can be selected in the drop-down list *Users*. Alternatively, group memberships can be managed in the user profile (see Chapter *9.1.1* (page 183)).

Special Groups Activate the checkbox if all group members should have read and write access to all resources of the group.

9.3.2 Managing Groups

List Page

All existing groups can be displayed by selecting *Administration* > *Groups* in the menu bar.

For all groups the following information is displayed:

Name Name of the group.

For all groups the following actions are available:

- Move the group to the trashcan.
- Edit the group.
- Clone the group.
- Export the group as an XML file.

Note: By clicking or below the list of groups more than one group can be moved to the trashcan or exported at a time. The drop-down list is used to select which groups are moved to the trashcan or exported.

Details Page

Click on the name of a group to display the details of the group. Click to open the details page of the group.

The following registers are available:

Information General information about the group.

User Tags Assigned tags (see Chapter *8.4* (page 174)).

Permissions Permissions of the group or of other users/roles/groups to the resources of the group (see Chapter *9.4* (page 193)).

The following actions are available in the upper left corner:

- Open the corresponding chapter of the user manual.
- Show the list page of all groups.
- Create a new group (see Chapter *9.3.1* (page 191)).
- Clone the group.
- Edit the group.
- Move the group to the trashcan.
- Export the group as an XML file.

9.4 Permissions

Select *Administration* > *Permissions* to display all permissions assigned on the system. If multiple roles are created, there can easily be hundreds of permissions.

Each permission relates to exactly one subject. A permission enables a subject to perform an associated action.

Subjects can be of the following types:

- Users
- Roles
- Groups

There are two types of permissions:

- **Command permissions** Command permissions are linked to the Greenbone Management Protocol (GMP). Each command permission applies to a specific GMP command. The name of the permission is the relevant command.

  A command permission is either a command level permission or a resource level permission.

  - **Command level** When no resource is specified, a command level permission is created. A command level permission allows the subject to run the given GMP command.
  - **Resource level** When a resource is specified, a resource level permission is created. A resource level permission allows the subject to run the given GMP command on a specific resource.
- **Super permissions** (see Chapter *9.4.2* (page 197))

9.4.1 Creating and Managing Permissions

Note: Usually, permissions are assigned in the web interface using the role management (see Chapter *9.2* (page 187)).

Creating and managing permissions using the page *Permissions* is only recommended to experienced users looking for a specific permission.

9.4.1.1 Creating a Permission

A new permission can be created as follows:

1. Select *Administration* > *Permissions* in the menu bar.
2. Create a new permission by clicking .
3. Define the permission (see Fig. 9.6).

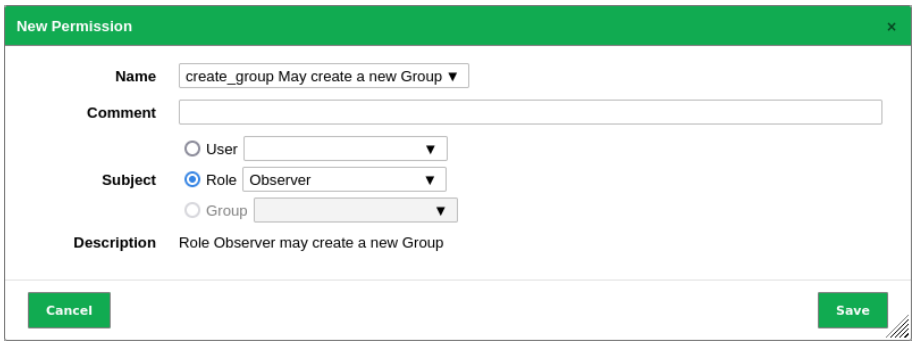


Fig. 9.6: Creating a new permission

4. Click *Save*.

   → The permission is created and displayed on the page *Permissions*.

The following details of the permission can be defined:

Name Permission that should be granted.

Comment (optional) A comment describes the permission in more detail.

Subject Subject (user, role or group) that should be granted with the permission.

Note: The subjects for which permissions can be assigned depend on the role of the currently logged in user. Users can grant permissions to other users, whereas administrators can grant permissions to users, roles and groups.

Resource Type (only for the permission *Super (Has super access)*) Resource type (user, role or group) to which the user/role/group has super access.

User/role/group ID (only for the permission *Super (Has super access)*) ID of the user/role/group to which the user/role/group has super access.

Description Textual description of the permission.

9.4.1.2 Creating Permissions from the Resource Details Page

When accessing a resource details page, e.g., the detail page of a task, permissions for the resource can be granted directly on the details page as follows:

1. Open the details page of a resource.

   Example: Select *Scans* > *Tasks* in the menu bar.
2. Click on the name of a task.
3. Click to open the details page of the task.
4. Click on the register *Permissions*.
5. Click in the opened section *Permissions*.
6. Define the permission (see Fig. 9.7).

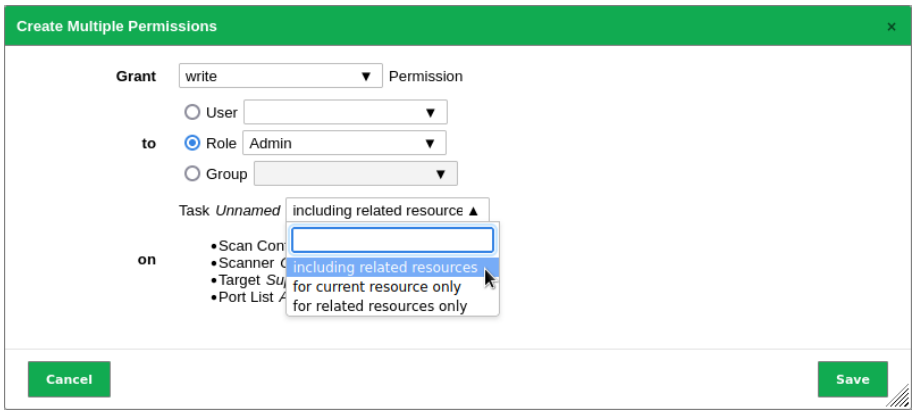


Fig. 9.7: Creating a permission from the resource details page

7. Click *Save*.

   → The permission is created and displayed in the section *Permissions* on the resource details page.

There are two types of permissions that can be granted directly on the resource details page:

- ***read*** Granting the permission *read* means allowing to view the resource on list pages and on its details page.
- ***write*** Granting the permission *write* means allowing to view and modify (but not delete) the resource.

Some resource types include additional permissions:

- **Tasks** When granting the permission *write* for a task, the permissions to start (*start_task*), stop (*stop_task*) and resume (*resume_task*) the task are added automatically.
- **Alerts** When granting the permission *write* for an alert, the permission to test the alert (*test_alert*) is added automatically.
- **Report formats and scanners** When granting the permission *write* for a report format or a scanner, the permissions to verify the report format (*verify_report_format*) or the scanner (*verify_scanner*) is added automatically.

For some resource types it can be selected whether the permissions should also be granted for related resources (see Fig. 9.7).

- **Tasks** For tasks this includes alerts and their filters, the target as well as its related credentials and port list, the schedule, the scanner and the scan configuration.
- **Targets** For targets this includes credentials and the port list.

- **Alerts** For alerts this includes the filter that is used on the report.

Note: Permissions can also be created only for the related resources.

The details of the related resources are displayed below the drop-down list.

9.4.1.3 Managing Permissions

List Page

All existing permissions can be displayed by selecting *Administration > Permissions* in the menu bar.

For all permissions the following information is displayed:

Name Name of the permission. A global permission is marked with .

Description Textual description of the permission.

Resource Type Resource type to which the user/role/group has access.

Resource Name of the resource to which the user/role/group has access.

Subject Type Subject type (user/role/group) that is granted with the permission.

Subject Subject that is granted with the permission.

For all permissions the following actions are available:

- Move the permission to the trashcan. Only self-created permissions can be moved to the trashcan.
- Edit the permission. Only self-created permissions can be edited.
- Clone the permission. Only self-created permissions can be cloned.
- Export the permission as an XML file.

Note: By clicking or below the list of permissions more than one permission can be moved to the trashcan or exported at a time. The drop-down list is used to select which permissions are moved to the trashcan or exported.

Details Page

Click on the name of a permission to display the details of the permission. Click to open the details page of the permission.

The following registers are available:

Information General information about the permission.

User Tags Assigned tags (see Chapter *8.4* (page 174)).

The following actions are available in the upper left corner:

- Open the corresponding chapter of the user manual.
- Show the list page of all permissions.
- Create a new permission (see Chapter *9.4.1.1* (page 194)).
- Clone the permission. Only self-created permissions can be cloned.
- Edit the permission. Only self-created permissions can be edited.
- Move the permission to the trashcan. Only self-created permissions can be moved to the trashcan.

- Export the permission as an XML file.

9.4.2 Granting Super Permissions

Any resource on the appliance (e.g., a user, a task, a target) is either global or owned by a specific user. Global resources are identified by .

Non-global resources can only be viewed and used by their owner. Individual permissions are necessary to make the resources available to other users which is quite tedious.

To avoid that, users, roles and groups can be assigned with super permissions. This makes all objects of other users, roles or groups accessible.

A user can get super permissions for:

- User
- Role
- Group
- Any

These super permissions allow complete access to any resource of the respective user, role, group or effectively all resources.

Note: The super permission *Any* cannot be set explicitly. It is restricted to the super administrator (see Chapter *9.2.5* (page 191)) and can only be set by creating such.

A user can only set super permissions for self-created objects. Only the super administrator can grant super permissions to any other user, role or group.

1. Click on the name of the user/role/group on the page *Users*/*Roles*/*Groups* for which super permissions should be assigned.

2. Open the details page by clicking .

   → The resource ID can be found in the upper right corner (see Fig. 9.8).

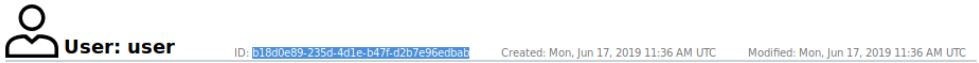


Fig. 9.8: ID of a resource

3. Note or copy the ID.
4. Select *Administration* > *Permissions* in the menu bar.
5. Create a new permission by clicking .
6. In the drop-down list *Name* select *Super (Has super access)* (see Fig. 9.9).
7. Select the radio button of the subject type that should have super permissions.
8. In the according drop-down list select the user/role/group that should have super permissions.
9. Select the resource type for which super permissions should be assigned in the drop-down list *Resource Type*.
10. Enter or paste the previously determined resource ID into the input box *ID*.

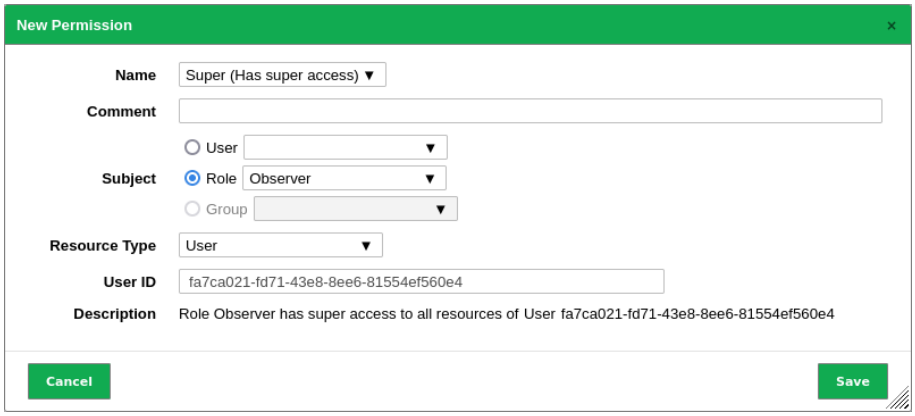


Fig. 9.9: Creating a new super permission

11. Click *Save*.

    → The super permission is created and displayed on the page *Permissions*.

Tip: Super permissions simplify the permission management on the appliance. They can easily be assigned for entire groups. This allows all users of a group to access all resources that are created by other members of the group.

9.4.3 Granting Read Access to Other Users

9.4.3.1 Requirements for Granting Read Access

Every user can share indefinite self-created resources. To do so, the user requires the **global** *get_users* permission as well as the **specific** *get_users* permission for the respective user who should obtain read access.

Note: The easiest and recommended way to share self-created resources is to use an administrator account and to create the user accounts that should receive read access with this administrator account.

All other ways described here are cumbersome and time-consuming.

Requirements for Administrators

By default, administrators already have the global *get_users* permission.

The administrator can get the specific *get_users* permission for the account that should obtain read access in two ways:

- Create the account oneself because administrators automatically have the specific *get_users* permission for accounts they created.
- With the help of a super administrator.

A super administrator can grant specific *get_users* permissions to an administrator as follows:

1. Log in to the web interface as a super administrator (see Chapters *7.2.1.5* (page 76) and *9.2.5* (page 191)).
2. Select *Administration* > *Users* in the menu bar.
3. Click on the name of the account who should obtain read access from the administrator.
4. Click 🔍.
5. Click on the register *Permissions*.
6. Create a new permission by clicking 🆕 in the section *Permissions*.
7. Select *read* in the drop-down list *Grant* (see Fig. 9.10).

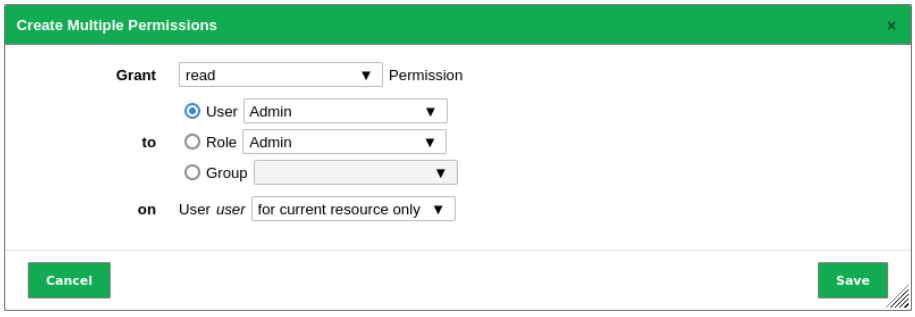
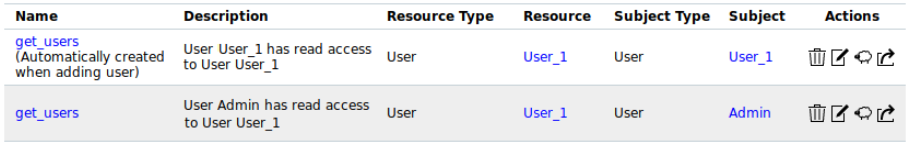


Fig. 9.10: Granting an administrator a specific *get_users* permission

8. Select the radio button *User*.
9. Select the administrator that should be able to grant read access in the drop-down list *User*.
10. Click *Save*.

    → The specific *get_users* permission is created and displayed in the list (see Fig. 9.11).

    The administrator is now able to grant read access to the respective user as described in Chapter *9.4.3.2* (page 202).



Name	Description	Resource Type	Resource	Subject Type	Subject	Actions
get_users (Automatically created when adding user)	User User_1 has read access to User User_1	User	User_1	User	User_1	
get_users	User Admin has read access to User User_1	User	User_1	User	Admin	

Fig. 9.11: Specific *get_users* permission for an administrator

Requirements for Regular Users

Regular users do not have the global *get_users* permission by default. It can be added as follows:

1. Log in to the web interface as an administrator.
2. Select *Administration* > *Roles* in the menu bar.
3. Create a new role by clicking .
4. Enter `GrantReadPriv` in the input box *Name*.
5. Click *Save*.

   → The role is created and displayed on the page *Roles*.
6. In the row of the newly created role, click .
7. In the drop-down list *Name* in the section *New Permission* select *get_users* (see Fig. 9.12).

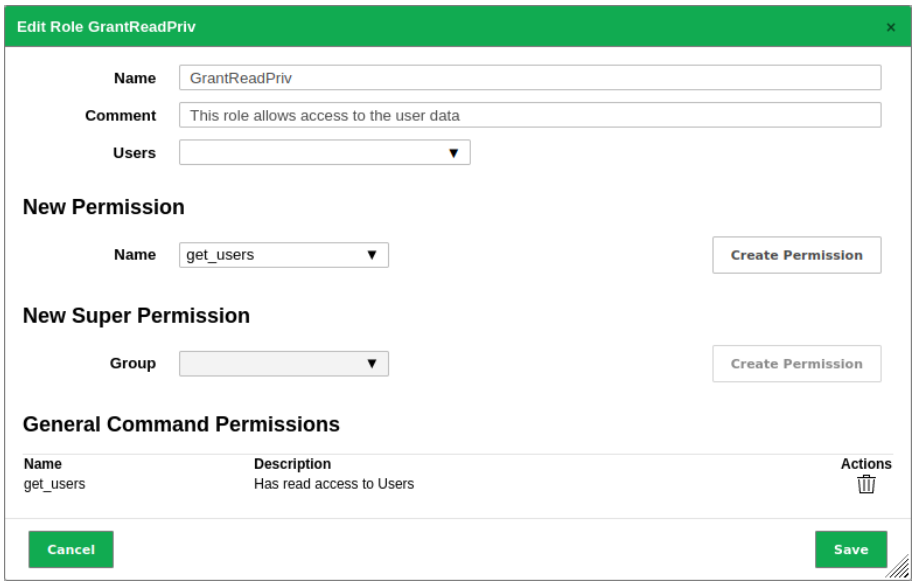


Fig. 9.12: Selecting permissions for a new role

8. Click *Create Permission*.

   → The permission is displayed in the section *General Command Permissions* (see Fig. 9.12).
9. Click *Save*.
10. Select *Administration* > *Users* in the menu bar.
11. In the row of the user which should be assigned the newly created role, click .
12. In the drop-down list *Roles* add the role *GrantReadPriv*.
13. Click *Save*.

A super administrator can grant specific *get_users* permissions to a user as follows:

1. Log in to the web interface as a super administrator (see Chapters *7.2.1.5* (page 76) and *9.2.5* (page 191)).
2. Select *Administration* > *Users* in the menu bar.
3. Click on the name of the account who should obtain read access from the user.
4. Click .
5. Click on the register *Permissions*.
6. In the section *Permissions* click .
7. Select *read* in the drop-down list *Grant* (see Fig. 9.13).

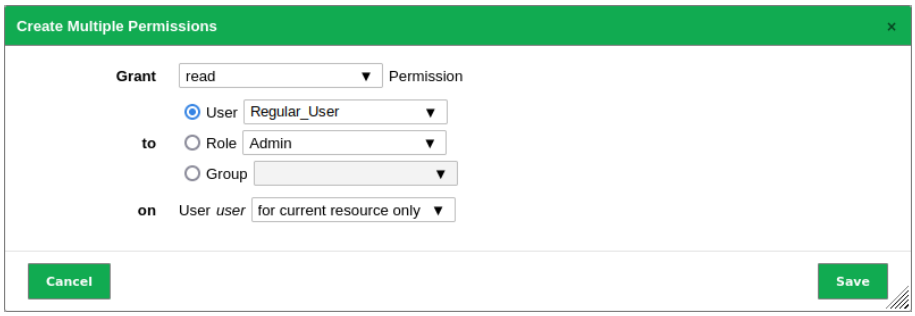


Fig. 9.13: Granting a user a specific *get_users* permission

8. Select the radio button *User*.
9. Select the user that should be able to grant read access in the drop-down list *User*.
10. Click *Save*.

    → The specific *get_users* permission is created and displayed in the list (see Fig. 9.14).

    The user is now able to grant read access to the respective user as described in Chapter *9.4.3.2* (page 202).

Fig. 9.14: Specific *get_users* permission for a user

9.4.3.2 Granting Read Access

When a user has the **global** and the **specific** *get_users* permission (see Chapter *9.4.3.1* (page 199)), the user can share resources as follows:

1. On the respective page click on the name of the resource which should be shared.
2. Open the details page by clicking .

   → The object ID can be found in the upper right corner (see Fig. 9.15).

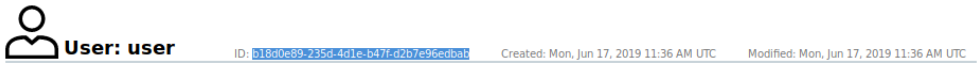


Fig. 9.15: ID of a resource

3. Note or copy the ID.
4. Select *Administration* > *Permissions* in the menu bar.
5. Create a new permission by clicking .
6. In the drop-down list *Name* select the permission for the object to be shared.
   - Filter: *get_filters*
   - Scan configuration: *get_configs*
   - Alert: *get_alerts*
   - Note: *get_notes*
   - Override: *get_overrides*
   - Tag: *get_tags*
   - Target: *get_targets*
   - Task with report: *get_tasks*
   - Schedule: *get_schedules*
7. Select the radio button *User* (see Fig. 9.16).
8. In the according drop-down list select the user the object should be shared with.
9. Enter or paste the previously determined resource ID in the input box *ID*.

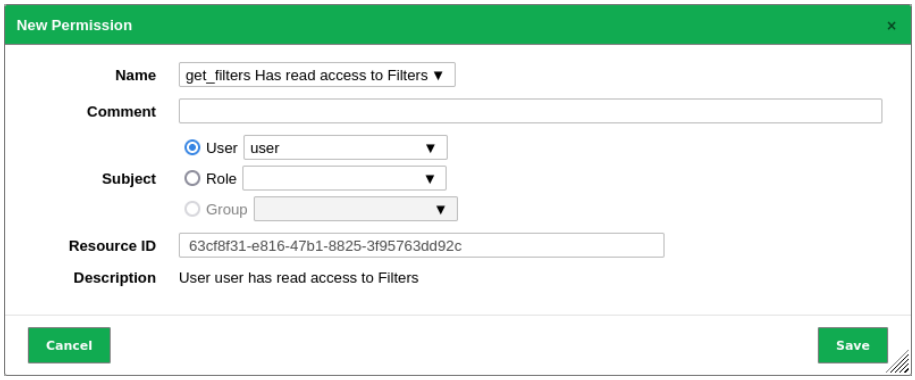


Fig. 9.16: Share objects with other users

10. Click *Save*.

    → The permission is created and displayed on the page *Permissions*.

Note: Additionally, resources can be shared with roles or groups.

For this, the global and specific permissions *get_groups* – granting read access to a group – or *get_roles* – granting read access to a role – are required and follow the same principle as described in Chapter *9.4.3.1* (page 199).

Exception: users with a default role already have the specific *get_roles* permissions for all default roles.

9.5 Using a Central User Management

Especially in larger environments with multiple users it is often difficult to achieve password synchronization. The effort to create new or reset passwords is often very high. To avoid this, the appliance supports the usage of a central password store using LDAPS or RADIUS.

The appliance will use the service only for authentication on a per user basis, i.e., users who should be able to authenticate by the service must be configured for authentication and to exist on the appliance as well.

Note: Prerequisite for using central authentication is the naming of the users with the same names as the objects in the LDAPS tree or the RADIUS server.

9.5.1 LDAPS

The appliance only supports encrypted connections via LDAP using StartTLS (port 389) or LDAPS using SSL/TLS (port 636). The LDAPS server must make its services available to SSL/TLS.

The following references are helpful for the exact configuration of all available LDAPS servers:

- Microsoft: https://social.technet.microsoft.com/wiki/contents/articles/2980.ldap-over-ssl-ldaps-certificate.aspx
- OpenLDAP: https://www.openldap.org/doc/admin24/tls.html

9.5.1.1 Storing the Server's Certificate on the Appliance

To verify the identity of the LDAPS server, the appliance must trust the server's certificate. For this, the certificate of the issuing certificate authority (CA) must be stored on the appliance.

To do so, the certificate of the CA must be exported as a Base64 encoded file. A Base64 encoded certificate often has the file extension `.pem`. The file itself starts with `------BEGIN CERTIFICATE-------`.

If the CA is an intermediate CA, the complete certificate chain needs to be imported. This is often true if an official CA is used because the Root CA is separated from the Issuing CA.

In these cases, the content of the file looks as follows:

```
-----BEGIN CERTIFICATE-----
......
Issuing CA
......
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
......
Root CA
......
-----END CERTIFICATE-----
```

The actual location where the certificate can be found may vary based on the environment.

- Univention Corporate Server (UCS)

  Here the CA certificate is retrieved from the file `/etc/univention/ssl/ucsCA/CAcert.pem`. This file already contains the certificate in the correct format and has to be uploaded when enabling LDAPS.

- Active Directory LDAPS

  If the Active Directory LDAP service does not yet use LDAPS, the following article may be helpful: https://social.technet.microsoft.com/wiki/contents/articles/2980.ldap-over-ssl-ldaps-certificate.aspx.

  The Active Directory LDAPS CA certificate can then be exported as follows:

  Note: The steps have to be executed from a desktop or server that has access to the CA console.

  1. Open the CA console from any domain-joined computer or server.
  2. Right click the name of the CA and select *Properties*.
  3. In the CA certificates dialog box, select the tab *General*.
  4. Select the certificate for the CA that should be accessed.
  5. Click *View Certificate*.
  6. In the dialog box *Certificate*, select the tab *Certification Authority*.
  7. Select the name of the root CA and click *View Certificate*.
  8. In the dialog box *Certificate*, select the tab *Details*.
  9. Click *Copy to File*.

     → The certificate export wizard is opened.
  10. Click *Next*.
  11. Select *Base-64 encoded X.509 (.CER)* on the page *Export File Format*.
  12. Click *Next*.
  13. Enter the path and the name for the certificate in the input box *File to Export*.
  14. Click *Next*.
  15. Click *Finish*.

      → The CER file is created in the specified location. A dialog box informs that the export was successful.
  16. Click *OK*.

  The content of the file must be uploaded when enabling LDAPS.

9.5.1.2 Connecting to the LDAPS Tree

For the connection to an LDAPS tree, the appliance uses a very simple interface and a simple bind operation with a hard-coded object path. The LDAPS authentication is done as follows:

1. Log in as an administrator.
2. Select *Administration* > *LDAP* in the menu bar.
3. Click .
4. Activate the checkbox *Enable* (see Fig. 9.17).

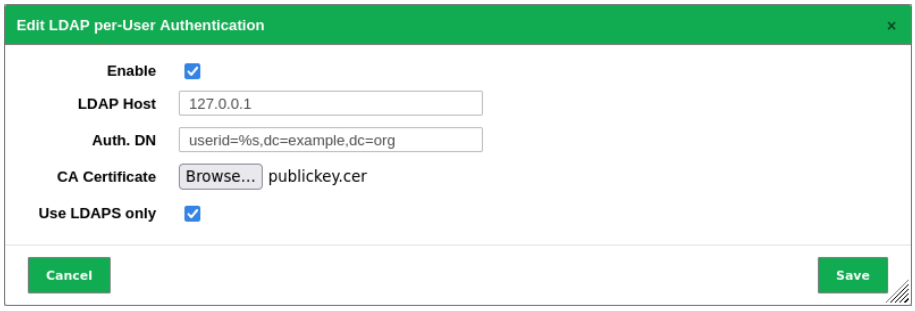


Fig. 9.17: Configuring an LDAPS authentication

5. Enter the LDAPS host in the input box *LDAP Host*.

Note: Only one system can be entered by IP address or by name.

The appliance accesses the LDAPS host using SSL/TLS. For verifying the host, the certificate of the host has to be uploaded to the appliance (see Chapter *9.5.1.1* (page 203)). Without SSL/TLS, the LDAPS authentication will not be accepted.

---

6. Enter the distinguished name (DN) of the objects in the input box *Auth. DN*.

Note: The wildcard `%s` replaces the user name.

Examples for the *Auth. DN* are:

- **`cn=%s,ou=people,dc=domain,dc=de`** This format works for any LDAPS server with the correct attributes. The attribute *cn* (common name) is used. Users in different sub trees or different recursive depths of an LDAPS tree are not supported. All users logging into the appliance must be in the same branch and in the same level of the LDAPS tree.
- **`uid=%s,ou=people,dc=domain,dc=de`** This format works for any LDAPS server with the correct attributes. The attribute *uid* (user ID) is used as a filter. It should be in the first place. The attributes *ou=people,dc=domain,dc=de* are used as base objects to perform a search and to retrieve the corresponding DN.
- **`%s@domain.de`** This format is typically used by Active Directory. The exact location of the user object is irrelevant.
- **`domain.de\%s`** This format is typically used by Active Directory. The exact location of the user object is irrelevant.

---

7. To verify the host, upload the certificate of the host by clicking *Browse...*.

8. Activate the checkbox *Use LDAPS only* if only connections via LDAPS should be allowed.

   Note: This option disables StartTLS and plain text connections to the LDAP server, allowing only connections via LDAPS. This is useful in cases where the LDAP port is blocked by a firewall.

9. Click *OK*.

   → When the LDAPS authentication is enabled (see Fig. 9.18), the option *LDAP Authentication Only* is available when creating or editing a user. By default, this option is disabled.

Fig. 9.18: Enabled LDAPS authentication

10. Create a new user or edit an existing user (see Chapter *9.1* (page 182)).
11. Activate the checkbox *LDAP Authentication Only* when the user should be allowed to authenticate using LDAPS (see Fig. 9.19).

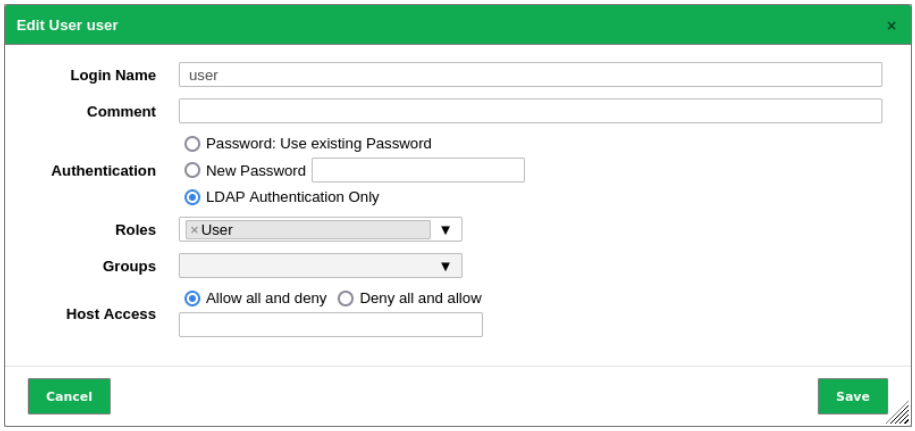


Fig. 9.19: Enabling authentication using LDAPS

Note: The user has to exist with the same name in LDAPS before the authentication with LDAPS can be used. The appliance does not add, modify or remove users in LDAPS and it does not automatically grant any user from LDAPS access to the appliance.

If the LDAPS authentication does not work, verify that the entry in *LDAP Host* matches the commonName of the certificate of the LDAPS server. If there are deviations, the appliance refuses using the LDAPS server.

9.5.2 RADIUS

The RADIUS authentication is done as follows:

1. Log in as an administrator.
2. Select *Administration* > *Radius* in the menu bar.
3. Click .
4. Activate the checkbox *Enable* (see Fig. 9.20).
5. Enter the host name or IP address of the RADIUS server in the input box *RADIUS Host*.
6. Enter the common preshared secret key in the input box *Secret Key*.

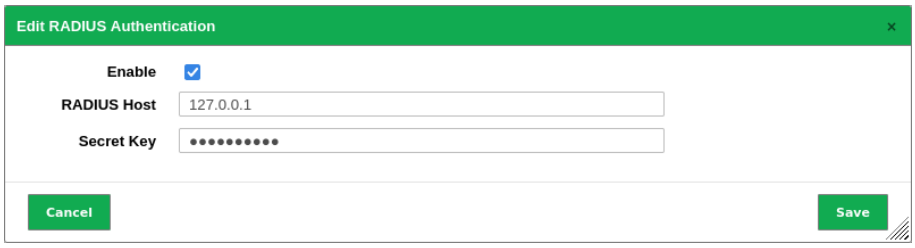


Fig. 9.20: Configuring a RADIUS authentication

7. Click *OK*.

   → When the RADIUS authentication is enabled, the option *RADIUS Authentication Only* is available when creating or editing a user. By default, this option is disabled.
8. Create a new user or edit an existing user (see Chapter *9.1* (page 182)).
9. Activate the checkbox *RADIUS Authentication Only* when the user should be allowed to authenticate using RADIUS (see Fig. 9.21).

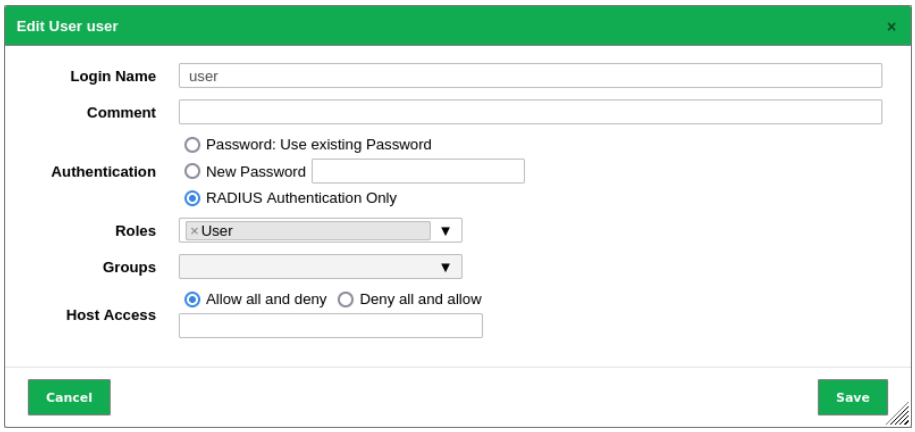


Fig. 9.21: Enabling authentication using RADIUS

CHAPTER 10

Scanning a System

Note: This chapter documents all possible menu options.

However, not all appliance models support all of these menu options. Check the tables in Chapter *3* (page 20) to see whether a specific feature is available for the used appliance model.

10.1 Using the Task Wizard for a First Scan

The task wizard can configure and start a basic scan with minimal user input.

10.1.1 Using the Task Wizard

A new task with the task wizard can be configured as follows:

1. Select *Scans > Tasks* in the menu bar.
2. Start the wizard by moving the mouse over and clicking *Task Wizard*.
3. Enter the IP address or host name of the target system in the input box (see Fig. 10.1).

   Note: If using a DNS name however, the appliance must be able to resolve the name.

4. Click *Start Scan*.

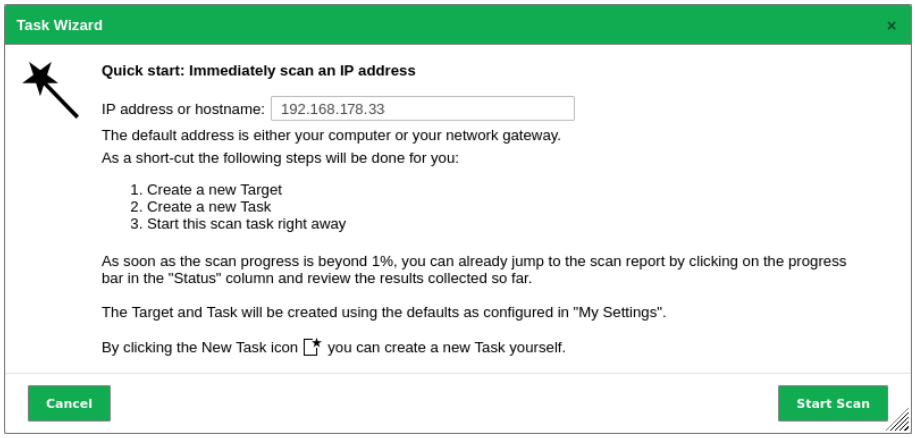


Fig. 10.1: Configuring the task wizard

→ The task wizard performs the following steps automatically:

1. Creating a new scan target on the appliance.
2. Creating a new scan task on the appliance.
3. Starting the scan task immediately.
4. Displaying the page *Tasks*.

After the task is started, the progress can be monitored (see Fig. 10.2).

Fig. 10.2: Page *Tasks* displaying the progress of the task

For the status of a task see Chapter *10.8* (page 254).

Tip: The report of a task can be displayed as soon as the task has been started by clicking the bar in the column *Status*. For reading, managing and downloading reports see Chapter *11* (page 283).

As soon as the status changes to *Done* the complete report is available. At any time the intermediate results can be reviewed (see Chapter *11.2.1* (page 288)).

Note: It can take a while for the scan to complete. The page is refreshing automatically if new data is available.

10.1.2 Using the Advanced Task Wizard

Next to the simple wizard, the appliance also provides an advanced wizard that allows for more configuration options.

A new task with the advanced task wizard can be configured as follows:

1. Select *Scans* > *Tasks* in the menu bar.
2. Start the wizard by moving the mouse over and clicking *Advanced Task Wizard*.
3. Define the task (see Fig. 10.3).

Tip: For the information to enter in the input boxes see Chapters *10.2.1* (page 212) and *10.2.2* (page 215).

If an e-mail address is entered in the input box *Email report to* an alert is created sending an e-mail as soon as the task is completed (see Chapter *10.12* (page 272)).

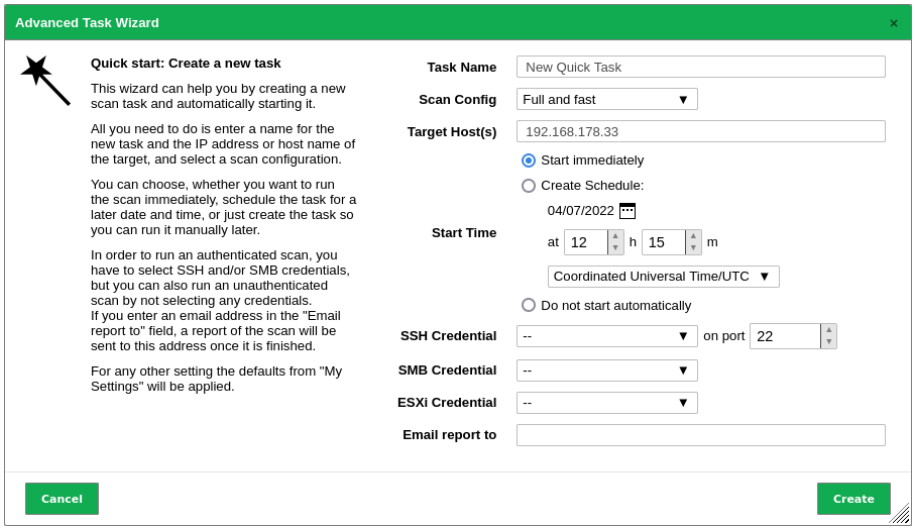


Fig. 10.3: Configuring the advanced task wizard

4. Click *Create*.

   → The advanced task wizard performs the following steps automatically:

   1. Starting the scan task immediately.
   2. Displaying the page *Tasks*.

For the status of a task see Chapter *10.8* (page 254).

Tip: The report of a task can be displayed as soon as the task has been started by clicking the bar in the column *Status*. For reading, managing and downloading reports see Chapter *11* (page 283).

As soon as the status changes to *Done* the complete report is available. At any time the intermediate results can be reviewed (see Chapter *11.2.1* (page 288)).

Note: It can take a while for the scan to complete. The page is refreshing automatically if new data is available.

10.1.3 Using the Wizard to Modify a Task

An additional wizard can modify an existing task:

1. Select *Scans* > *Tasks* in the menu bar.
2. Start the wizard by moving the mouse over and clicking *Modify Task Wizard*.
3. Select the task which should be modified in the drop-down list *Task* (see Fig. 10.4).

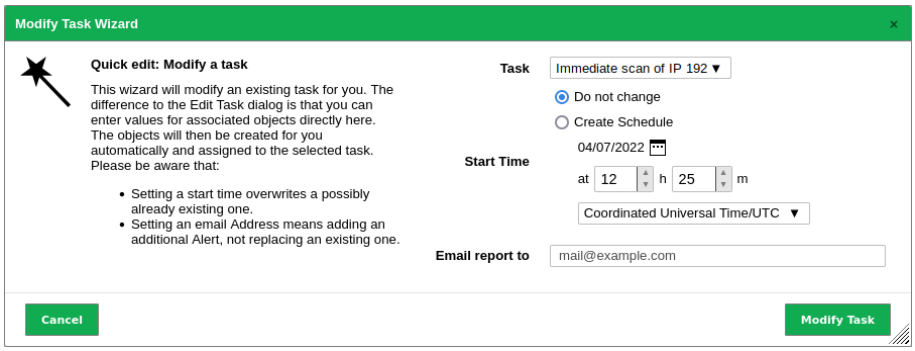


Fig. 10.4: Modifying a task using the wizard

4. Create a schedule for the task by selecting the radio button *Create Schedule* (see Chapter *10.10* (page 268)).

   The date of the first scan can be selected by clicking and the time can be set using the input boxes.
5. Enter the e-mail address to which the report should be sent in the input box *Email report to*.
6. Click *Modify Task*.

10.2 Configuring a Simple Scan Manually

Generally speaking, the appliance can use two different approaches to scan a target:

- Simple scan
- Authenticated scan using local security checks

The following steps have to be executed to configure a simple scan:

- Creating a target (see Chapter *10.2.1* (page 212))
- Creating a task (see Chapter *10.2.2* (page 215))
- Running the task (see Chapter *10.2.3* (page 217))

10.2.1 Creating a Target

The first step is to define a scan target as follows:

1. Select *Configuration* > *Targets* in the menu bar.
2. Create a new target by clicking .
3. Define the target (see Fig. 10.5).

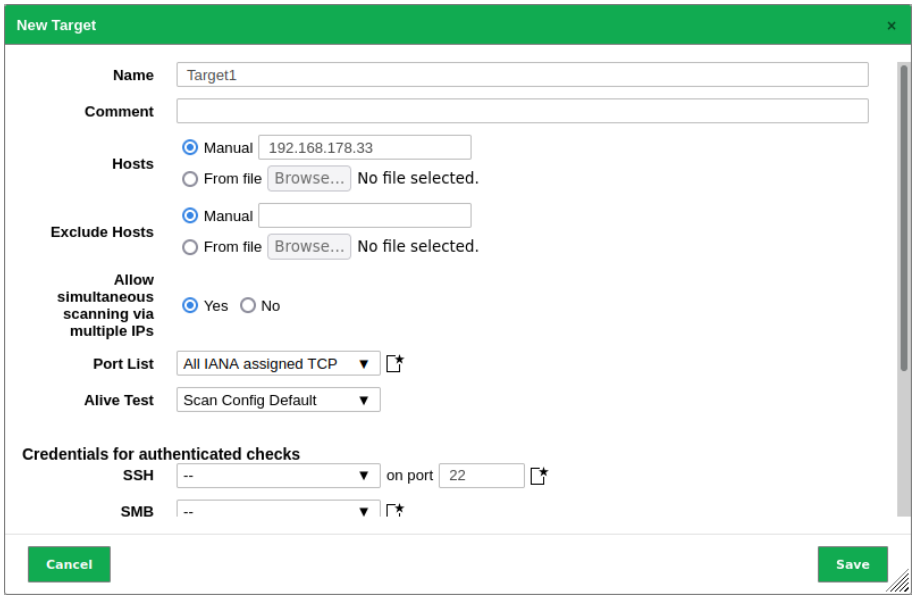


Fig. 10.5: Creating a new target

4. Click *Save*.

The following information can be entered:

Name The name can be chosen freely. A descriptive name should be chosen if possible. Possibilities are Mailserver, ClientNetwork, Webserverfarm, DMZ or describing the entered systems in more detail.

Comment The optional comment allows specifying background information. It simplifies understanding the configured targets later.

Hosts Manual entry of the hosts that should be scanned, separated by commas, or importing a list of hosts.

Note: The IP address or the host name is required. In both cases it is necessary that the appliance can connect to the system. If using the host name, the appliance must also be able to resolve the name.

The maximum configurable number of IP addresses is 4096 for most appliance models. For the Greenbone Enterprise 6500, the maximum configurable number of IP addresses is 16777216.

When entering manually the following options are available:

- Single IP address, e.g., 192.168.15.5
- Host name, e.g., mail.example.com
- IPv4 address range in long format, e.g., 192.168.15.5-192.168.15.27
- IPv4 address range in short format, e.g., 192.168.55.5-27

- IPv4 address range in CIDR notation, e.g., 192.168.15.0/24

Note: Because of the maximum configurable number of IP addresses (see above), the maximum subnet mask is /20 for IPv4 if no other hosts are part of the configuration. If the maximum number of IP addresses is higher, e.g., for the Greenbone Enterprise 6500, correspondingly larger subnet masks can be configured.

Traditionally, the first IP address (network address, e.g., 192.168.15.0) and last IP address (broadcast address, e.g., 192.168.15.255) of a subnet are not included in the number of usable IP addresses and thus are not considered in scans when this notation is used. If the IP addresses are actually usable and scannable, they must be explicitly added to the scan target, e.g., `192.168.15.0/24, 192.168.15.0, 192.168.15.255`.

- Single IPv6 address, e.g., fe80::222:64ff:fe76:4cea
- IPv6 address range in long format, e.g., ::12:fe5:fb50-::12:fe6:100
- IPv6 address range in short format, e.g., ::13:fe5:fb50-fb80
- IPv6 address range in CIDR notation, e.g., fe80::222:64ff:fe76:4cea/120

Note: Because of the maximum configurable number of IP addresses (see above), the maximum subnet mask is /116 for IPv6 if no other hosts are part of the configuration. If the maximum number of IP addresses is higher, e.g., for the Greenbone Enterprise 6500, correspondingly larger subnet masks can be configured.

Multiple options can be mixed. If importing from a file, the same syntax can be used. Entries can be separated with commas or by line breaks. If many systems have to be scanned, using a file with the hosts is simpler than entering all hosts manually. The file must use ASCII character encoding.

Alternatively the systems can be imported from the host asset database.

Note: Importing a host from the asset database is only possible if a target is created from the page *Hosts* (see Chapter *13.1.3* (page 344)).

Exclude Hosts Manual entry of the hosts that should be excluded from the list mentioned above, separated by commas, or importing a list of hosts.

The same specifications as for *Hosts* apply.

Allow simultaneous scanning via multiple IPs Some services, especially IoT devices, may crash when scanned via multiple connections coming from the same host at the same time. This can happen, for example, if the device is connected via IPv4 and IPv6.

Selecting the radio button *No* will avoid scanning via several addresses at the same time.

Port list Port list used for the scan (see Chapter *10.7* (page 252)).

Note: A port list can be created on the fly by clicking next to the drop-down list.

Alive Test This options specifies the method to check if a target is reachable. Options are:

- Scan Config Default (the alive test method *ICMP Ping* is used by default)
- ICMP Ping
- TCP-ACK Service Ping

- TCP-SYN Service Ping
- ICMP & TCP-ACK Service Ping
- ICMP & ARP Ping
- TCP-ACK Service & ARP Ping
- ICMP, TCP-ACK Service & ARP Ping
- Consider Alive

Sometimes there are problems with this test from time to time. In some environments routers and firewall systems respond to a TCP service ping with a TCP-RST even though the host is actually not alive (see Chapter *10.13* (page 281)).

Network components exist that support Proxy-ARP and respond to an ARP ping. Therefore this test often requires local customization to the environment.

SSH Credential Selection of a user that can log into the target system of a scan if it is a Linux or Unix system. This allows for an authenticated scan using local security checks (see Chapters *10.3.2* (page 219) and *10.3* (page 218)).

- **Elevate Privileges** It is also possible to store credentials for elevated privileges, e.g., root. For this, SSH credentials must be selected first. Then a new drop-down list is displayed for selecting the elevated credentials.

  Note: To see the new feature for elevated SSH credentials, the cache of the browser used for the web interface may need to be emptied. Clearing the browser cache can be done in the options of the used browser.

  Alternatively, the page cache can be emptied by pressing `Ctrl` and `F5`.

  Note: The feature is still experimental. Depending on the target system and its configuration, the feature may not be reliable.

  For more information about root rights for scans see Chapter *10.3.5* (page 235).

  The elevated user's rights must be configured on the target system beforehand. The appliance only executes the command `su - <username>` which has no control over the rights of use.

  If elevated SSH credentials are configured, the default SSH credentials are only used for logging in on the target system. The elevated credentials are used for the scan.

  The programs *stty* and *unset* must be available/accessible for the elevated-privileges user.

  The elevated-privileges user must be allowed to change the login prompt via an `export PS1=` prepended to the commands sent.

  If elevated SSH credentials are configured, they are always used even if the scan configuration does not contain relevant vulnerability tests.

  Default and elevated SSH credentials must not be the same.

  Note: Using elevated SSH credentials may create increased load on the appliance, as well as an increased number of SSH connections from the appliance to the target system. This may need to be taken into account for firewalls, intrusion detection and logging systems.

  In addition, the duration of scans using elevated SSH credentials can be much longer than scans without elevated credentials due to the system load mentioned above.

SMB Credential Selection of a user that can log into the target system of a scan if it is a Microsoft Windows system. This allows for an authenticated scan using local security checks (see Chapters *10.3.2* (page 219) and *10.3* (page 218)).

ESXi Credential Selection of a user that can log into the target system of a scan if it is a VMware ESXi system. This allows for an authenticated scan using local security checks (see Chapters *10.3.2* (page 219) and *10.3* (page 218)).

SNMP Credential Selection of a user that can log into the target system of a scan if it is an SNMP aware system. This allows for an authenticated scan using local security checks (see Chapters *10.3.2* (page 219) and *10.3* (page 218)).

Note: All credentials can be created on the fly by clicking next to the credential.

Reverse Lookup Only Only scan IP addresses that can be resolved into a DNS name.

Reverse Lookup Unify If multiple IP addresses resolve to the same DNS name the DNS name will only get scanned once.

Note: For reverse lookup unify, all target addresses are checked prior to the scan in order to reduce the number of actual scanned addresses. For large targets and for networks in which reverse lookup causes delays, this leads to a long phase where the task remains at 1 % progress.

This option is not recommended for large networks or networks in which reverse lookups cause delays.

10.2.2 Creating a Task

The second step is to create a task.

The appliance controls the execution of a scan using tasks. These tasks can be repeated regularly or run at specific times (see Chapter *10.10* (page 268)).

A task can be created as follows:

1. Select *Scans* > *Tasks* in the menu bar.
2. Create a new task by moving the mouse over and clicking *New Task*.
3. Define the task (see Fig. 10.6).
4. Click *Save*.

   → The task is created and displayed on the page *Tasks*.

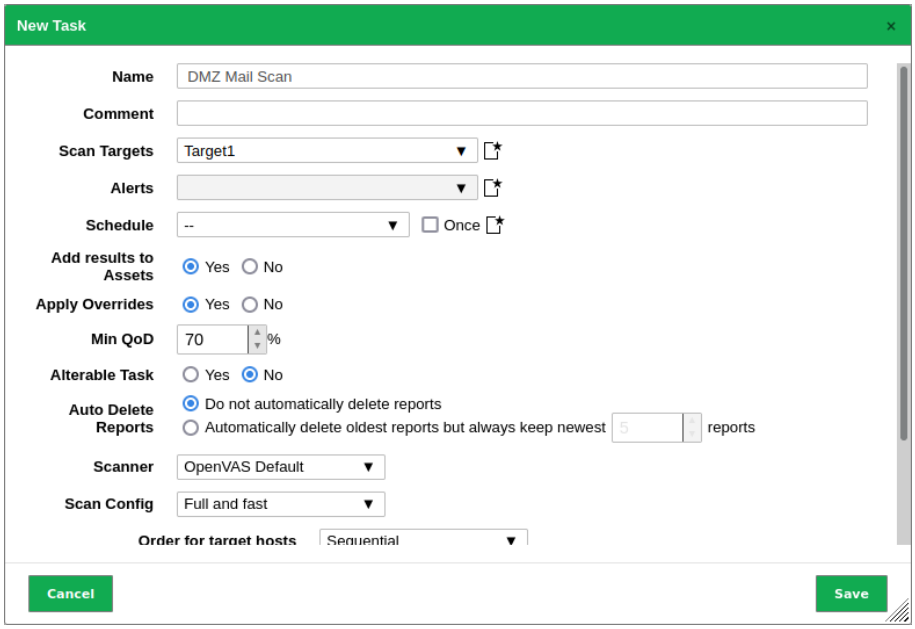


Fig. 10.6: Creating a new task

The following information can be entered:

Name The name can be chosen freely. A descriptive name should be chosen if possible. Possibilities are Mailserver, ClientNetwork, Webserverfarm, DMZ or describing the entered systems in more detail.

Comment The optional comment allows for the entry of background information. It simplifies understanding the configured task later.

Scan Targets Select a previously configured target from the drop-down list (see Chapter *10.2.1* (page 212)).

Alternatively, the target can be created on the fly by clicking next to the drop-down list.

Alerts Select a previously configured alert from the drop-down list (see Chapter *10.12* (page 272)). Status changes of a task can be communicated via e-mail, Syslog, HTTP or a connector.

Alternatively, an alert can be created on the fly by clicking next to drop-down list.

Schedule Select a previously configured schedule from the drop-down list (see Chapter *10.10* (page 268)). The task can be run once or repeatedly at a predetermined time, e.g., every Monday morning at 6:00 a.m.

Alternatively, a schedule can be created on the fly by clicking next to the drop-down list.

Add results to Assets Selecting this option will make the systems available to the appliance's asset management automatically (see Chapter *13* (page 341)). This selection can be changed at a later point as well.

Apply Overrides Overrides can be directly applied when adding the results to the asset database (see Chapter *11.8* (page 307)).

Min QoD Here the minimum quality of detection can be specified for the addition of the results to the asset database (see Chapter *11.2.6* (page 296)).

Alterable Task Allow for modification of the task's scan target(s), scanner and scan configuration, even if reports were already created. The consistency between reports can no longer be guaranteed if tasks are altered.

Auto Delete Reports This option may automatically delete old reports. The maximum number of reports to store can be configured. If the maximum is exceeded, the oldest report is automatically deleted. The

factory setting is *Do not automatically delete reports*.

Scanner By default, only the built-in OpenVAS and CVE scanners are supported (see Chapter *10.11* (page 271)). Sensors can be used as additional scanning engines but need to be configured first (see Chapter *16* (page 371)).

Note: The following options are only relevant for the OpenVAS scanner. The CVE scanner does not support any options.

Scan Config The appliance comes with several pre-configured scan configurations for the OpenVAS scanner (see Chapter *10.9* (page 258)). Only one scan configuration can be configured per task.

Order for target hosts Select in which order the specified target hosts are processed during vulnerability tests. Available options are:

- Sequential
- Random
- Reverse

In order to improve the scan progress estimation, the setting *Random* is recommended (see Chapter *17.2.3* (page 383)).

This setting does not affect the alive test during which active hosts in a target network are identified. The alive test is always random.

Maximum concurrently executed NVTs per host/Maximum concurrently scanned hosts Select the speed of the scan on one host. The default values are chosen sensibly. If more VTs run simultaneously on a system or more systems are scanned at the same time, the scan may have a negative impact on either the performance of the scanned systems, the network or the appliance itself. These values “maxhosts” and “maxchecks” may be tweaked.

Tag Select a previously configured tag from the drop-down list (see Chapter *8.4* (page 174)) to link it to the task.

10.2.3 Starting the Task

In the row of the newly created task, click ▷.

Note: For scheduled tasks 🕒 is displayed additionally. The task is starting at the time that was defined in the schedule (see Chapter *10.10* (page 268)).

→ The task is added to the waiting queue. Afterwards, the scanner begins with the scan.

Note: In some cases, the task may remain in the queue. For more information see Chapter *17.3* (page 384).

For the status of a task see Chapter *10.8* (page 254).

The report of a task can be displayed as soon as the task has been started by clicking the bar in the column *Status*. For reading, managing and downloading reports see Chapter *11* (page 283).

As soon as the status changes to *Done* the complete report is available. At any time the intermediate results can be reviewed (see Chapter *11.2.1* (page 288)).

Note: It can take a while for the scan to complete. The page is refreshing automatically if new data is available.

10.3 Configuring an Authenticated Scan Using Local Security Checks

An authenticated scan can provide more vulnerability details on the scanned system. During an authenticated scan the target is both scanned from the outside using the network and from the inside using a valid user login.

During an authenticated scan, the appliance logs into the target system in order to run local security checks (LSC). The scan requires the prior setup of user credentials. These credentials are used to authenticate to different services on the target system. In some circumstances the results could be limited by the permissions of the users used.

The VTs in the corresponding VT families (local security checks) will only be executed if the appliance was able to log into the target system. The local security check VTs in the resulting scan are minimally invasive.

The appliance only determines the risk level but does not introduce any changes on the target system. However, the login by the appliance is probably logged in the protocols of the target system.

The appliance can use different credentials based on the nature of the target. The most important ones are:

- **SMB** On Microsoft Windows systems, the appliance can check the patch level and locally installed software such as Adobe Acrobat Reader or the Java suite.
- **SSH** This access is used to check the patch level on Unix and Linux systems.
- **ESXi** This access is used for testing of VMware ESXi servers locally.
- **SNMP** Network components like routers and switches can be tested via SNMP.

The following table lists the required port – given the authenticating service uses the default port – and the allowed credential types (see Chapter *10.3.2* (page 219)) for each authentication method:

	Required port	Allowed credential types
SMB	• 445/tcp, 139/tcp	• *Username + Password*
SSH	• 22/tcp, configurable in the *New Target*/*Edit Target* dialog (see Chapter *10.2.1* (page 212))	• *Username + Password* • *Username + SSH Key*
ESXi	• See https://kb.vmware.com/s/article/2039095	• *Username + Password*
SNMP	• 161/udp	• *SNMP*

10.3.1 Advantages and Disadvantages of Authenticated Scans

The extent and success of the testing routines for authenticated scans depend heavily on the permissions of the used account.

On Linux systems an unprivileged user is sufficient and can access most interesting information while especially on Microsoft Windows systems unprivileged users are very restricted and administrative users provide more results. An unprivileged user does not have access to the Microsoft Windows registry and the Microsoft Windows system folder `\windows` which contains the information on updates and patch levels.

Local security checks are the most gentle method to scan for vulnerability details. While remote security checks try to be least invasive as well, they may have some impact.

Simply stated an authenticated scan is similar to a Whitebox approach. The appliance has access to prior information and can access the target from within. Especially the registry, software versions and patch levels are accessible.

A remote scan is similar to a Blackbox approach. The appliance uses the same techniques and protocols as a potential attacker to access the target from the outside. The only information available was collected by the appliance itself. During the test, the appliance may provoke malfunctions to extract any available information on the used software, e.g., the scanner may send a malformed request to a service to trigger a response containing further information on the deployed product.

During a remote scan using the scan configuration *Full and fast* all remote checks are safe. The used VTs may have some invasive components but none of the used VTs try to trigger a defect or malfunction in the target (see example below). This is ensured by the scan preference `safe_checks=yes` in the scan configuration (see Chapter *10.9.4* (page 263)). All VTs with very invasive components or which may trigger a denial of service (DoS) are automatically excluded from the test.

Example for an Invasive VT

An example for an invasive but safe VT is the Heartbleed VT. It is executed even with `safe_checks` enabled because the VT does not have any negative impact on the target.

The VT is still invasive because it tests the memory leakage of the target. If the target is vulnerable, actual memory of the target is leaked. The appliance does not evaluate the leaked information. The information is immediately discarded.

10.3.2 Using Credentials

Credentials for local security checks are required to allow VTs to log into target systems, e.g., for the purpose of locally checking the presence of all vendor security patches.

10.3.2.1 Creating a Credential

A new credential can be created as follows:

1. Select *Configuration > Credentials* in the menu bar.
2. Create a new credential by clicking ☆.
3. Define the credential (see Fig. 10.7).
4. Click *Save*.

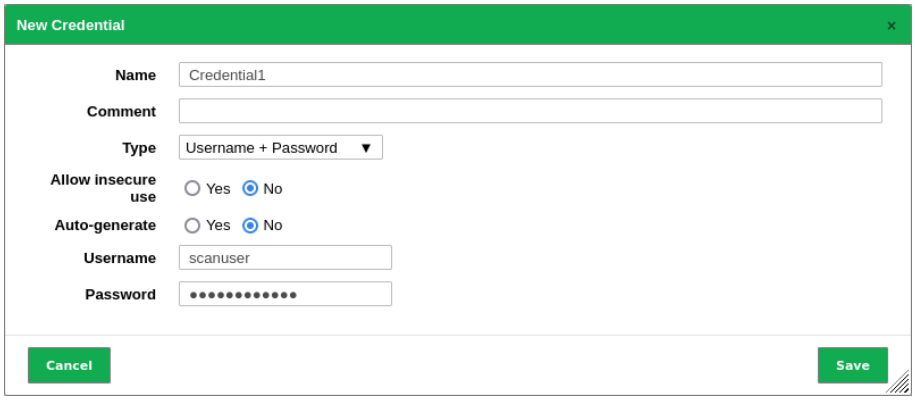


Fig. 10.7: Creating a new credential

The following details of the credential can be defined:

Name Definition of the name. The name can be chosen freely.

Comment An optional comment can contain additional information.

Type Definition of the credential type. The following types are possible:

- Username + Password
- Username + SSH Key
- SNMP
- S/MIME Certificate
- PGP Encryption Key
- Password only

Allow insecure use Select whether the appliance can use the credential for unencrypted or otherwise insecure authentication methods.

Depending on the selected type further options are shown:

Username + Password

- **Auto-generate** Select whether the appliance creates a random password.

  Note: If the radio button *Yes* is selected, it is not possible to define a password in the input box *Password*.

- **Username** Definition of the login name used by the appliance to authenticate on the scanned target system.

  Note: Only the following characters are allowed for the user name:

  – All English alphanumeric characters
  – - (dash)
  – _ (underscore)
  – \ (backslash)
  – . (full stop)
  – @ (at sign)

This also excludes the German umlauts, which must be replaced as follows:

- “ß” → “ss”
- “ä” → “a”
- “ö” → “o”
- “ü” → “u”

- **Password** Definition of the password used by the appliance to authenticate on the scanned target system.

Username + SSH Key

- **Auto-generate** Select whether the appliance creates a random password.

Note: If the radio button *Yes* is selected, it is not possible to define a password in the input box *Password*.

- **Username** Definition of the login name used by the appliance to authenticate on the scanned target system.

Note: Only the following characters are allowed for the user name:

- All English alphanumeric characters
- - (dash)
- _ (underscore)
- \ (backslash)
- . (full stop)
- @ (at sign)

This also excludes the German umlauts, which must be replaced as follows:

- “ß” → “ss”
- “ä” → “a”
- “ö” → “o”
- “ü” → “u”

- **Passphrase** Definition of the passphrase of the private SSH key.
- **Private Key** Upload of the private SSH key.
- **Certificate** Upload of the certificate file.
- **Private Key** Upload of the corresponding private key.

SNMP SNMPv3 requires a user name, an authentication password, and a privacy password, while all older SNMP versions (SNMPv1 and SNMPv2) only require an SNMP community.

Note: Due to the singular nature of the SNMP credential, it is currently not possible to configure either SNMPv1/v2 or SNMPv3 mode.

This means that the appliance will always try to log in with all SNMP protocol versions. It is possible to see both the result *SNMP Login Successful For Authenticated Checks* and the result *SNMP Login Failed For Authenticated Checks* for a scan, e.g., if the SNMPv3 login information in the credential is correct, but the SNMPv1/2 information is incorrect.

- **SNMP Community** Definition of the community for SNMPv1 or SNMPv2c.
- **Username** Definition of the user name for SNMPv3.

  Note: Only the following characters are allowed for the user name:

  – All English alphanumeric characters

  – - (dash)

  – _ (underscore)

  – \ (backslash)

  – . (full stop)

  – @ (at sign)

  This also excludes the German umlauts, which must be replaced as follows:

  – “ß” → “ss”

  – “ä” → “a”

  – “ö” → “o”

  – “ü” → “u”

- **Password** Definition of the password for SNMPv3.
- **Privacy Password** Definition of the password for the encryption for SNMPv3.
- **Auth Algorithm** Selection of the authentication algorithm (MD5 or SHA1).
- **Privacy Algorithm** Selection of the encryption algorithm (AES, DES or none).

S/MIME Certificate

- **S/MIME Certificate** Upload of the certificate file.

PGP Encryption Key

- **PGP Public Key** Upload of the key file.

Password only

- **Password** Definition of the password used by the appliance to authenticate on the scanned target system.

Note: The credential has to be linked to at least one target. This allows the scan engine to apply the credential.

10.3.2.2 Managing Credentials

List Page

All existing credentials can be displayed by selecting *Configuration > Credentials* in the menu bar.

For all credentials the following information is displayed:

Name Name of the credential.

Type Chosen credential type.

Allow insecure use Indication whether the appliance can use the credential for unencrypted or otherwise insecure authentication methods.

Login User name for the credential if a credential type that requires a user name is chosen.

For all credentials the following actions are available:

- Move the credential to the trashcan. Only credentials which are currently not used can be moved to the trashcan.
- Edit the credential.
- Clone the credential.
- Export the credential as an XML file.

Depending on the chosen credential type (see Chapter *10.3.2.1* (page 219)) more actions may be available:

- Download an EXE package for Microsoft Windows. This action is available if *Username + Password* was chosen.
- Download an RPM package for Red Hat Enterprise Linux and its derivates. This action is available if *Username + SSH Key* was chosen.
- Download a Debian package for Debian GNU/Linux and its derivates. This action is available if *Username + SSH Key* was chosen.
- Download a public key. This action is available if *Username + SSH Key* was chosen.

These installation packages simplify the installation and creation of accounts for authenticated scans. They create the user and the most important permissions for the authenticated scan and reset them during uninstalling.

Note: If the auto-generation of passwords is enabled (see Chapter *10.3.2.1* (page 219)), the packages have to be used, otherwise the usage is optional.

Note: By clicking or below the list of credentials more than one credential can be moved to the trashcan or exported at a time. The drop-down list is used to select which credentials are moved to the trashcan or exported.

Details Page

Click on the name of a credential to display the details of the credential. Click to open the details page of the credential.

The following registers are available:

Information General information about the credential.

User Tags Assigned tags (see Chapter *8.4* (page 174)).

Permissions Assigned permissions (see Chapter *9.4* (page 193)).

The following actions are available in the upper left corner:

- Open the corresponding chapter of the user manual.
- Show the list page of all credentials.
- Create a new credential (see Chapter *10.3.2.1* (page 219)).
- Clone the credential.
- Edit the credential.
- Move the credential to the trashcan. Only credentials which are currently not used can be moved to the trashcan.
- Export the credential as an XML file.

Depending on the chosen credential type (see Chapter *10.3.2.1* (page 219)) more actions may be available:

- Download an EXE package for Microsoft Windows. This action is available if *Username + Password* was chosen.
- Download an RPM package for Red Hat Enterprise Linux and its derivates. This action is available if *Username + SSH Key* was chosen.
- Download a Debian package for Debian GNU/Linux and its derivates. This action is available if *Username + SSH Key* was chosen.
- Download a public key. This action is available if *Username + SSH Key* was chosen.

10.3.3 Requirements on Target Systems with Microsoft Windows

10.3.3.1 General Notes on the Configuration

- The remote registry service must be started in order to access the registry.

  This is achieved by configuring the service to automatically start up. If an automatic start is not preferred, a manual startup can be configured. In that case, the service is started while the system is scanned by the appliance and afterwards it is disabled again. To ensure this behavior, the following information about LocalAccountTokenFilterPolicy must be considered.

- It is necessary that for all scanned systems the file and printer sharing is activated. If using Microsoft Windows XP, take care to disable the setting *Use Simple File Sharing*.

- For individual systems not attached to a domain the following registry key must be set:

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\
DWORD: LocalAccountTokenFilterPolicy = 1
```

- On systems with domain controller the user account in use must be a member of the group *Domain Administrators* to achieve the best possible results. Due to the permission concept it is not possible to discover all vulnerabilities using the *Local Administrator* or the administrators assigned by the domain. Alternatively follow the instructions in Chapter *10.3.3.2* (page 226).

  → Should a *Local Administrator* be selected – which it explicitly not recommended – it is mandatory to set the following registry key as well:

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\
DWORD: LocalAccountTokenFilterPolicy = 1
```

- Generated install package for credentials: The installer sets the remote registry service to auto start. If the installer is executed on a domain controller, the user account will be assigned to the group *BUILTIN/Administrators* (`SID S-1-5-32-544`).

- An exception rule for the appliance on the Microsoft Windows firewall must be created. Additionally, on XP systems the service *File and Printer Sharing* must be set to *enabled*.

- Generated install package for credentials: During the installation, the installer offers a dialog to enter the appliance's IP address. If the entry is confirmed, the firewall rule is configured. The service *File and Printer Sharing* will be enabled in the firewall rules.

- Powershell execution privileges on a target system may be required for the account utilized in an authenticated scan. Policy and vulnerability tests may occasionally execute Powershell commands to increase the accuracy of results, requiring privileges for the duration of a scan.

- For compliance audits targeting Windows operating systems, it is recommended to set the *Maximum concurrently executed NVTs per host/Maximum concurrently scanned hosts* to `1` in order to maximize the accuracy of the results (see Chapter *12.2.1.1* (page 317)).

- For a fully working Windows Management Instrumentation (WMI) access which is used for, e.g., file search or policy scans, the following settings are required:

  – Allow WMI access in the Windows Firewall settings[24] or a possible third-party firewall solution.

  – Verify that the user or the group of the scan user is allowed to access WMI remotely.

[24] https://learn.microsoft.com/en-us/windows/win32/wmisdk/connecting-to-wmi-remotely-starting-with-vista#windows-firewall-settings

10.3.3.2 Configuring a Domain Account for Authenticated Scans

For authenticated scans of Microsoft Windows target systems, it is highly recommended to use a domain account with a domain policy that grants local administrator privileges. This has several advantages:

- A domain policy only needs to be created once and can then be applied or revoked for different user accounts.
- Editing the Microsoft Windows registry locally is no longer required. User administration is thus centralized, which saves time in the long term and reduces possible configuration errors.
- From a vulnerability assessment perspective, only a domain account allows for the detection of domain-related scan results. These results will be missing if using a local user account.
- There are also several security advantages to using a domain account with the domain policy recommended by Greenbone: the corresponding user may not log in locally or via the remote desktop protocol (RDP), limiting possible attack vectors. Additionally, the user credentials are secured via Kerberos, while the password of a local user account is at much greater risk of being exposed through exploits.

In order to use a domain account for host based remote audits on a Microsoft Windows target, the following configuration must be made under Windows XP Professional, Windows Vista, Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows 7, Windows 8, Windows 8.1 or Windows 10. The system must also be part of the domain.

Creating a Security Group

1. Log into a domain controller and open *Active Directory Users and Computers*.
2. Select *Action* > *New* > *Group* in the menu bar.
3. Enter `Greenbone Local Scan` in the input box *Name*.
4. Select *Global* for *Group Scope* and *Security* for *Group Type*.
5. Add the account used for the local authenticated scans by the appliance under Microsoft Windows to the group.
6. Click *OK*.

Creating a Group Policy Object (GPO)

1. In the left panel open the console *Group Policy Management*.
2. Right click *Group Policy Objects* and select *New*.
3. Enter `Greenbone Local SecRights` in the input box *Name* (see Fig. 10.8).
4. Click *OK*.

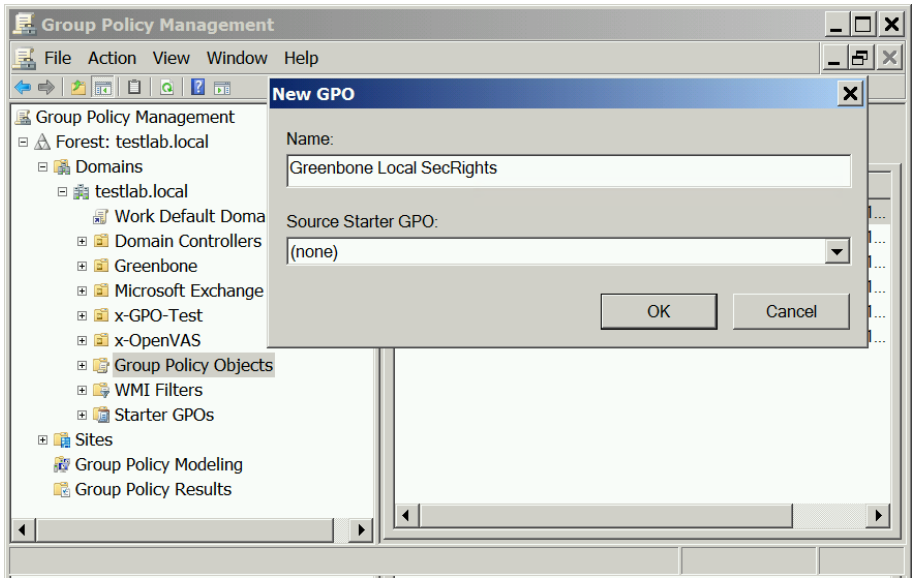


Fig. 10.8: Creating a new Microsoft Windows group policy object for Greenbone scans

Configuring the Policy

1. Click the policy *Greenbone Local SecRights* and select *Edit*.
2. Select *Computer Configuration* > *Policies* > *Windows Settings* > *Security Settings* in the left panel.
3. Click *Restricted Groups* and select *Add Group*.
4. Click *Browse...* and enter `Greenbone Local Scan` in the input box (see Fig. 10.9).

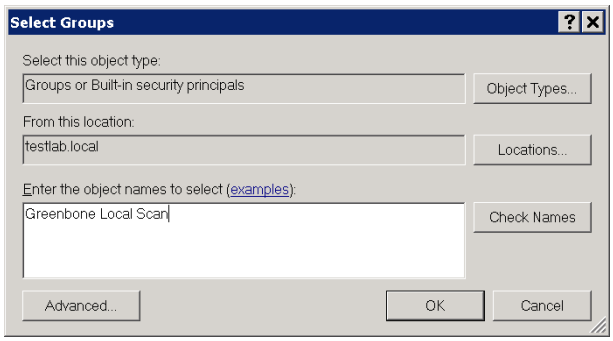


Fig. 10.9: Checking Microsoft Windows group names

5. Click *Check Names*.
6. Click *OK* twice to close the open windows.
7. At *This group is member of* click *Add*.
8. Enter `Administrators` in the input box *Group* (see Fig. 10.10) and click *OK* twice to close the open windows.

Note: On non-English systems enter the respective name of the local administrator group.

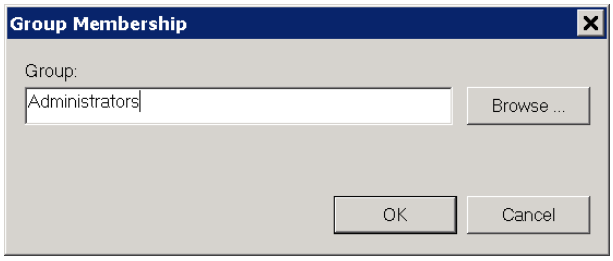


Fig. 10.10: Adding a group membership

Configuring the Policy to Deny the Group “Greenbone Local Scan” Logging into the System Locally

1. Click the policy *Greenbone Local SecRights* and select *Edit*.
2. Select *Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment* in the left panel.
3. In the right panel double click *Deny log on locally*.
4. Activate the checkbox *Define these policy settings* and click *Add User or Group*.
5. Click *Browse...* and enter `Greenbone Local Scan` in the input box (see Fig. 10.11).
6. Click *Check Names*.

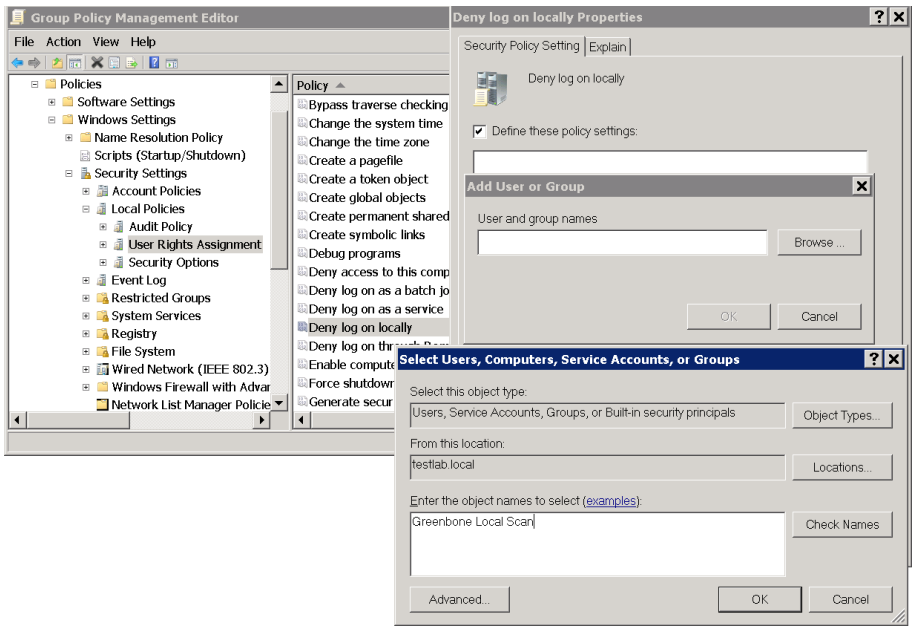


Fig. 10.11: Editing the policy

7. Click *OK* three times to close the open windows.

Configuring the Policy to Deny the Group “Greenbone Local Scan” Logging into the System via Remote Desktop

1. Click the policy *Greenbone Local SecRights* and select *Edit*.
2. Select *Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment* in the left panel.
3. In the right panel double click *Deny log on through Remote Desktop Services*.
4. Activate the checkbox *Define these policy settings* and click *Add User or Group*.
5. Click *Browse...* and enter `Greenbone Local Scan` in the input box (see Fig. 10.12).
6. Click *Check Names*.

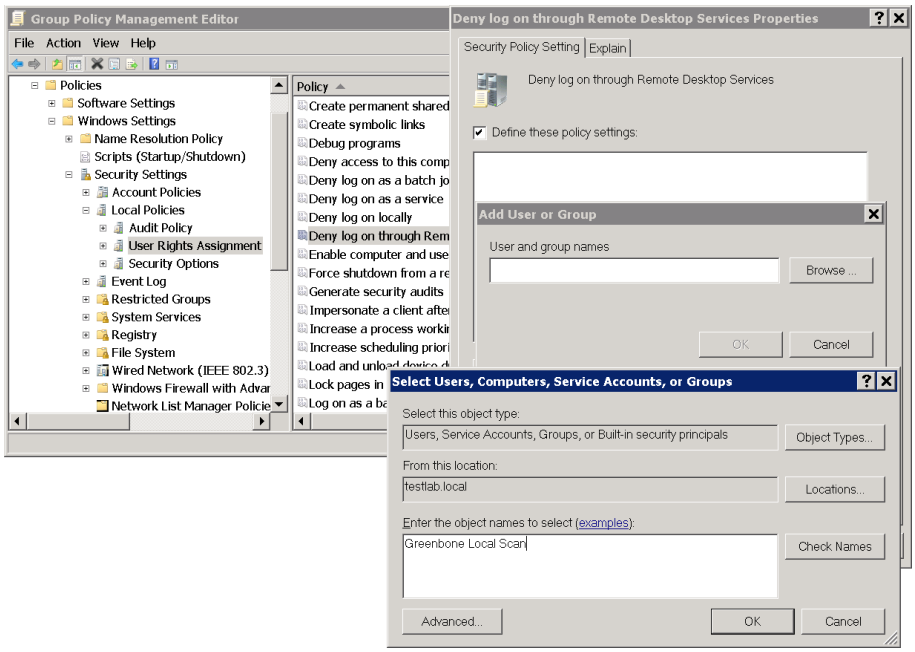


Fig. 10.12: Editing the policy

7. Click *OK* three times to close the open windows.

Configuring the Policy to Give Read Permissions Only to the Registry for the Group “Greenbone Local Scan”

Important: This setting still exists after the GPO has been removed (“tattooing GPO”).

This changes fundamental privileges which may not be simply reversed by removing the GPO.

Research whether the settings are compatible with the environment.

Note: The following steps are optional.

1. In the left panel right click *Registry* and select *Add Key*.
2. Select *USERS* and click *OK* (see Fig. 10.13).

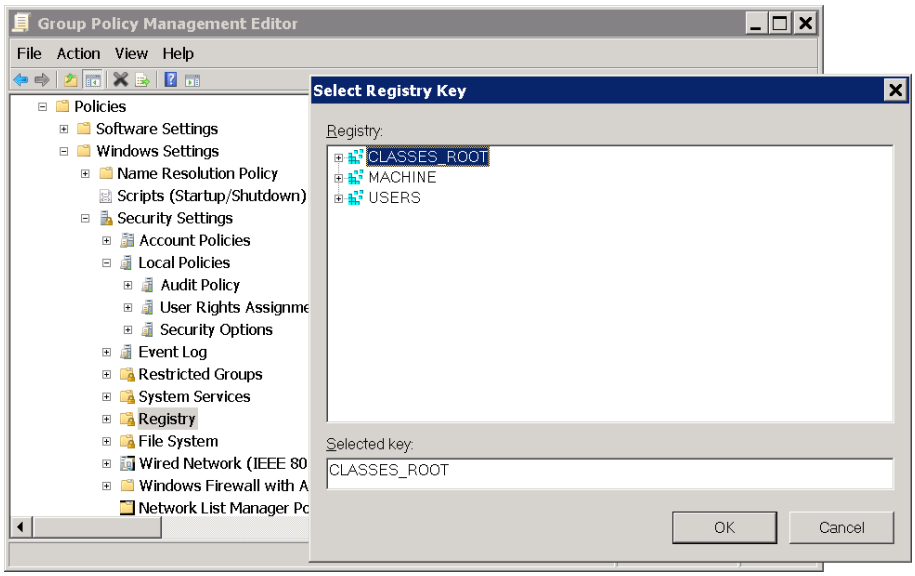


Fig. 10.13: Selecting the registry key

3. Click *Advanced* and *Add*.
4. Enter `Greenbone Local Scan` in the input box and click *OK* (see Fig. 10.14).
5. Select *This object and child objects* in the drop-down list *Apply to*.
6. Deactivate all checkboxes for *Allow* and activate the checkboxes *Set Value*, *Create Subkey*, *Create Link*, *Delete*, *Change Permissions* and *Take Ownership* for *Deny* (see Fig. 10.15).
7. Click *OK* twice and confirm the warning message by clicking *Yes*.
8. Click *OK*.

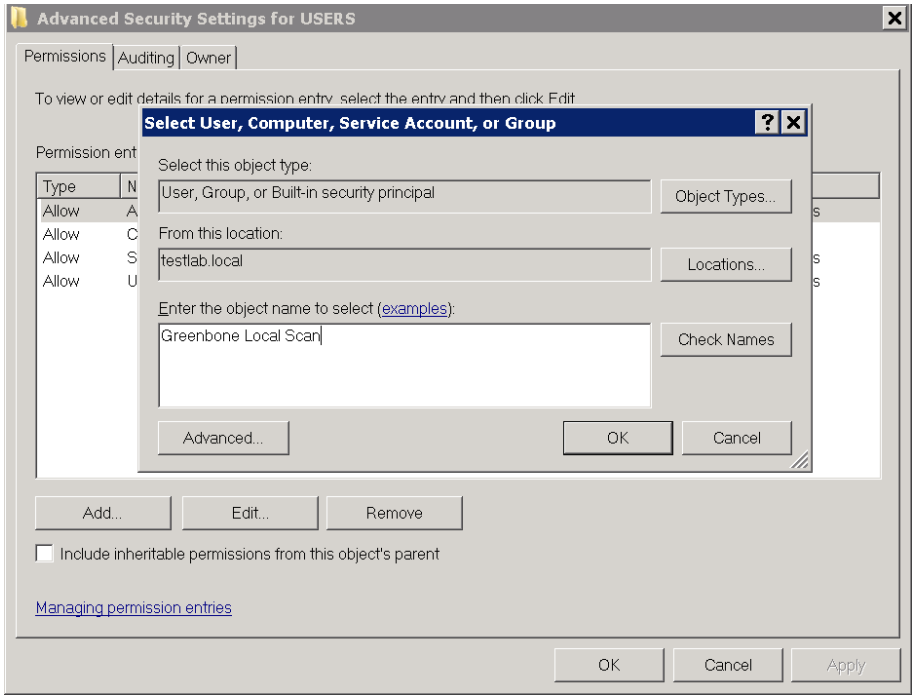


Fig. 10.14: Selecting the group *Greenbone Local Scan*

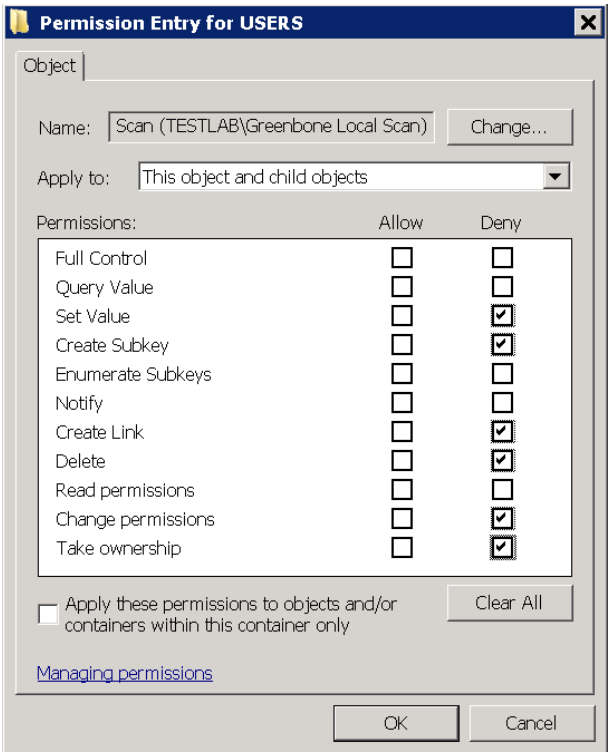


Fig. 10.15: Disallowing edition of the registry

9. Select the radio buttons *Configure this key then* and *Propagate inheritable permissions to all subkeys* and click *OK* (see Fig. 10.16).

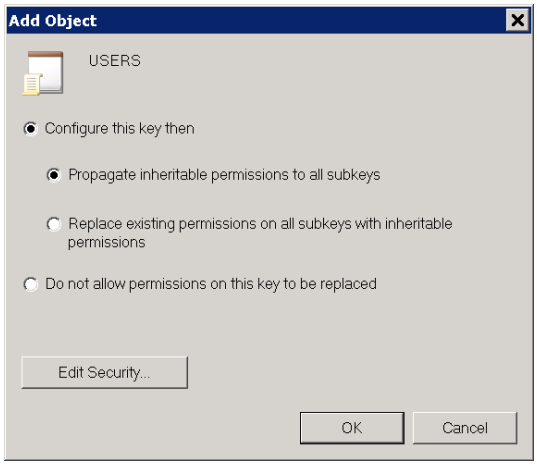


Fig. 10.16: Making the permissions recursive

10. Repeat the steps 2 to 9 for *MACHINE* and *CLASSES_ROOT*.

Linking the Group Policy Object

1. In the right panel right click the domain and select *Link an Existing GPO...*.
2. Select *Greenbone Local SecRights* in the section *Group Policy objects* and click *OK* (see Fig. 10.17).

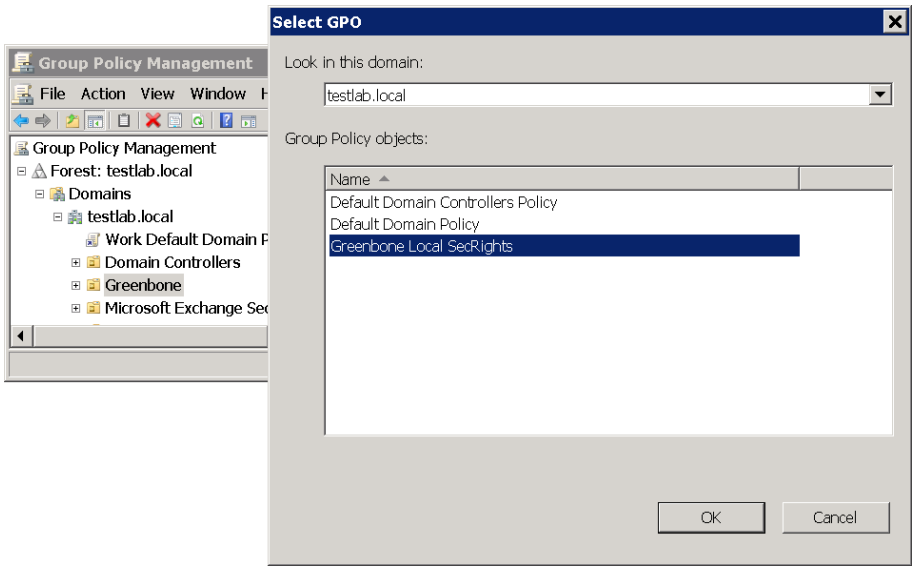


Fig. 10.17: Linking the policy

10.3.3.3 Restrictions

Based on the fact that write permissions to the registry and system drive have been removed, the following two tests will no longer work:

- ***Leave information on scanned Windows hosts* (OID 1.3.6.1.4.1.25623.1.0.96171)** This test, if desired, creates information about the start and end of a scan under HKLM\Software\VulScanInfo. Due to denying write access to HKLM this is no longer possible. If the test should be possible, the GPO must be adjusted respectively.
- ***Windows file Checksums* (OID 1.3.6.1.4.1.25623.1.0.96180)** This test, if desired, saves the tool ReHash under C:\Windows\system32 (for 32-bit systems) or C:\Windows\SysWOW64 (for 64-bit systems). Due to denying write access this is no longer possible. If the test should be possible, the tool must be saved separately or the GPO must be adjusted respectively.

  More information can be found in Chapter *12.4.3* (page 328).

10.3.3.4 Scanning Without Domain Administrator and Local Administrator Permissions

It is possible to build a GPO in which the user also does not have any local administrator permissions. But the effort to add respective read permissions to each registry branch and folder is huge. Unfortunately, inheriting of permissions is deactivated for many folders and branches. Additionally, these changes can be set by GPO but cannot be removed again (tattooing GPO). Specific permissions could be overwritten so that additional problems could occur as well.

Building a GPO in which the user does not have any local administrator permissions does not make sense from a technical and administrative point of view.

10.3.4 Requirements on Target Systems with ESXi

Note: If a vCenter Server Appliance (VCSA) is used to control ESXi hosts and users are created on the VCSA, they are only known on the VCSA and not on the ESXi hosts.

Scan users must be created on each ESXi host that will be scanned.

By default, local ESXi users are limited to read-only roles. Either an administrative account or a read-only role with permission to global settings has to be used.

A read-only role with permission to global settings can be set up as follows:

1. Open the web interface of the VMware ESXi instance and log in.
2. Select *Host > Manage* in the *Navigator* column on the left.
3. Select the register *Security & users*.
4. Select *Roles* in the left menu panel (see Fig. 10.18).
5. Click *Add role*.
6. Enter a name for the role in the input box *Role name*.
7. Activate the checkbox *System*.
8. Click *Global* and activate the checkbox *Settings* (see Fig. 10.19).
9. Click *Add*.
10. Right click *Host* and select *Permissions* in the *Navigator* column on the left.
11. Select the scan user account used by the appliance.

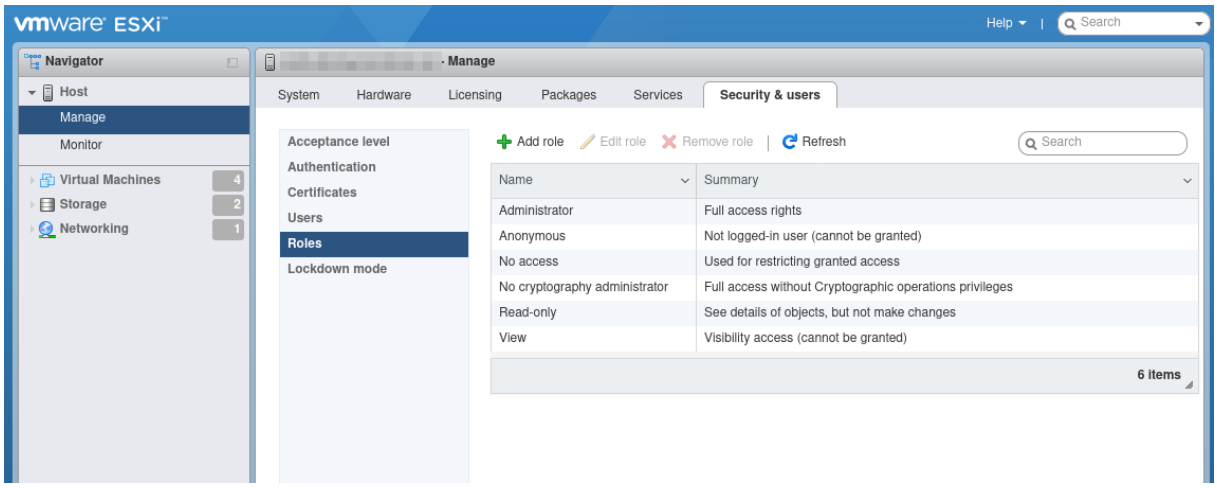


Fig. 10.18: Displaying the roles

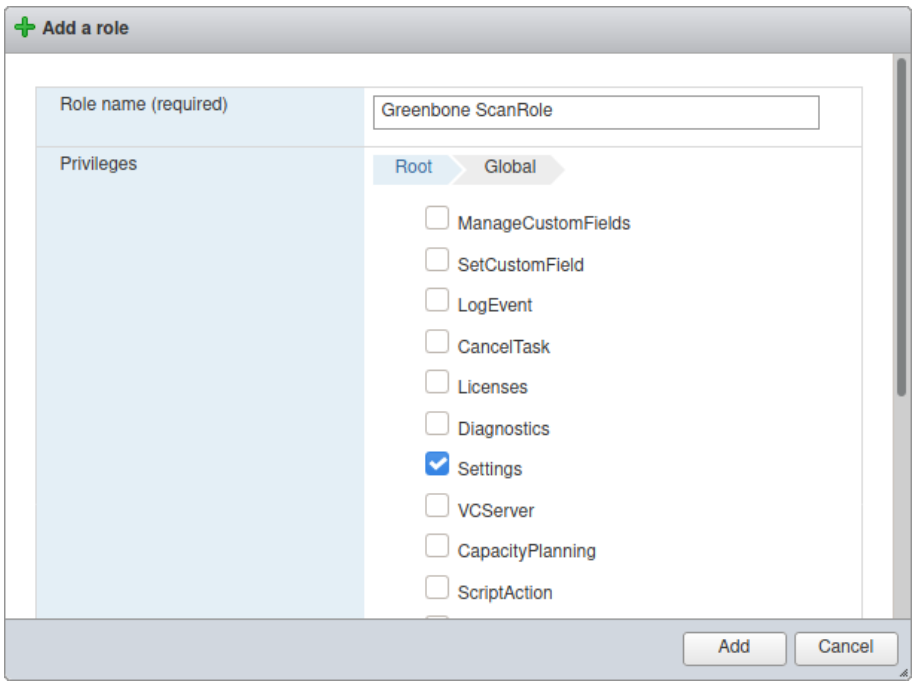


Fig. 10.19: Creating a role

12. Click *Assign role*.
13. Select the previously created role in the drop-down list (see Fig. 10.20).

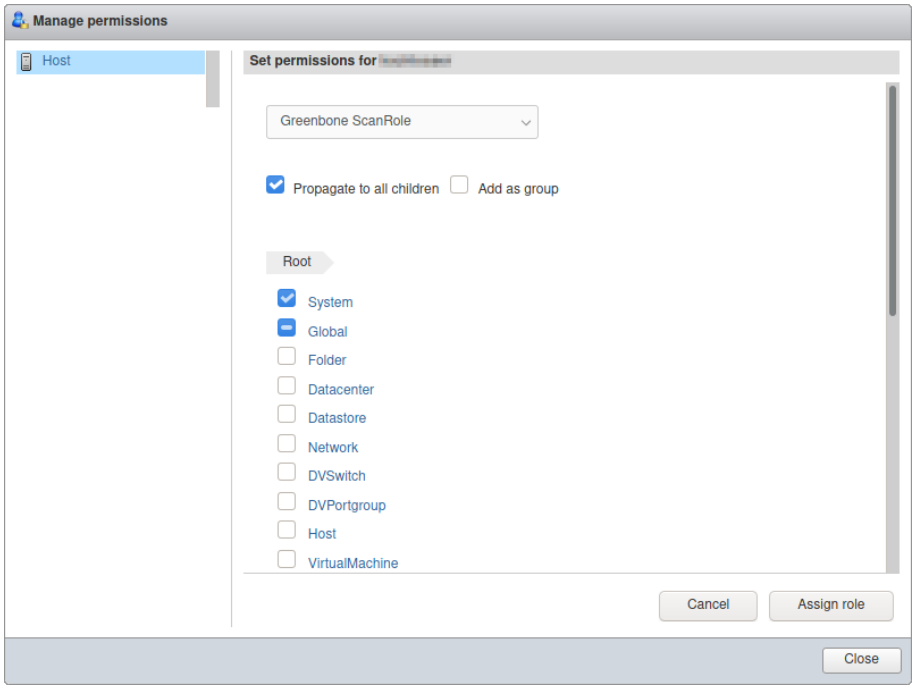


Fig. 10.20: Assigning the role to the scan user

14. Click *Assign role*.
15. Click *Close*.

10.3.5 Requirements on Target Systems with Linux/Unix

- For authenticated scans on Linux or Unix systems, regular user access is usually enough. The login is performed via SSH. The authentication is done either with passwords or a private SSH key stored on the appliance.
- A remote SSH server should have the following defaults configured in the file `sshd_config`:
  - `MaxSessions`: 10
  - `MaxAuthTries`: 6

  When using non-default and lower values, failed logins may occur.
- Generated installation package for credentials: the install package for Linux distributions based on Debian is a DEB file, the install package for Linux distributions based on Red Hat is an RPM file. Both install packages create a new user without any specific permissions. A public SSH key that is created on the appliance is stored in the user's home folder. For users of other Linux distributions or Unix derivatives, the public key is offered for download. Creating a user and saving the public key with the proper file permissions is the responsibility of the user.
- In both cases it must be made sure that public key authentication is not prohibited by the SSH daemon. The line `PubkeyAuthentication no` must not be present.
- Existing SSH key pairs may also be used. SSH key pairs can be generated using the command `ssh-keygen` on Linux or `puttygen.exe` if using PuTTY on Microsoft Windows. To use an existing SSH key pair for authentication, the private key must be supplied when the credential is created. The

private SSH key must be either in PEM or OpenSSH format. The key types Ed25519, ECDSA, RSA and DSA are supported.

- For scans that include policy testing, root permission or the membership in specific groups (often `wheel`) may be necessary. For security reasons, many configuration files are only readable by super users or members of specific groups.
- The more permissions a user has, the more results and settings can be detected on a system. In some cases root user access may be required.
- The following commands are executed with root user access during an authenticated scan.

Important:

- This list is not static. New or changed VTs may add new commands at any time.
- Depending on the found software, additional commands may be executed.
- The executed commands depend on the Linux distribution and the selected scan configuration.

  - bash
  - cat
  - date
  - dpkg
  - egrep
  - find
  - grep
  - host
  - id
  - ip
  - lastlog
  - locate
  - ls
  - md5sum
  - mlocate
  - netstat
  - perl
  - ps
  - rpm
  - sh
  - sha1sum
  - slocate
  - uname
  - uptime
  - whereis

  - which

- The installation of the package `locate` (alternatively `mlocate`) to provide the command `locate`/`mlocate` on the target system is recommended. The use of this command reduces calls to the command `find` used to search for files and thus, improves the search performance and lowers the resource usage on the target system.

  For the commands to work, the corresponding database permissions and regular database updates, e.g., via a cron job, may need to be configured.

10.3.6 Requirements on Target Systems with Cisco OS

The appliance can check network components like routers and switches for vulnerabilities as well. While the usual network services are discovered and checked via the network, some vulnerabilities can only be discovered by an authenticated scan. For the authenticated scan, the appliance can use either SNMP or SSH.

10.3.6.1 SNMP

The appliance can use the SNMP protocol to access the Cisco network component. The appliance supports SNMPv1, v2c and v3. SNMP uses the port 161/udp. The default port list does not include any UDP port. Therefore, this port is ignored during the vulnerability test using *Full and fast* and no SNMP check is enabled. To scan network components the port list should be modified to include at least the following ports:

- 22/tcp SSH
- 80/tcp 8080/tcp HTTP
- 443/tcp 8443/tcp HTTPS
- 2000/tcp SCCP
- 2443/tcp SCCPS
- 5060/tcp 5060/udp SIP
- 5061/tcp 5061/udp SIPS
- 67/udp DHCP Server
- 69/udp TFTP
- 123/udp NTP
- 161/udp SNMP
- 162/udp SNMP Traps
- 500/udp IKE
- 514/udp Syslog
- 546/udp DHCPv6
- 6161/udp 6162/udp Unified CM

The administrator can set up special port lists used only for such network components.

The appliance needs to access only very few objects from the SNMP tree. For a less privileged access an SNMP view should be used to constrain the visibility of the SNMP tree for the appliance. The following two examples explain how to set up the view using either a community string or an SNMPv3 user.

To use an SNMP community string the following commands are required on the target:

```
# configure terminal
```

Using an access list the usage of the community can be restricted. The appliance's IP address is 192.168.222.74 in this example:

```
(config) # access-list 99 permit 192.168.222.74
```

The view `gsm` should only allow accessing the system description:

```
(config) # snmp-server view gsm system included
(config) # snmp-server view gsm system.9 excluded
```

The last command links the community `gsm-community` with the view `gsm` and the access list 99:

```
(config) # snmp-server community gsm-community view gsm RO 99
```

If using an SNMPv3 user including encryption the following configuration lines are required on the target:

```
# configure terminal
(config) # access-list 99 permit 192.168.222.74
(config) # snmp-server view gsm system included
(config) # snmp-server view gsm system.9 excluded
```

SNMPv3 requires the setup of a group first. Here the group `gsmgroup` is linked to the view `gsm` and the access list 99:

```
(config) # snmp-server group gsmgroup v3 priv read gsm access 99
```

Now the user can be created supplying the password `gsm-password` and the encryption key `gsm-encrypt`. The authentication is done using MD5 while the encryption is handled by AES128:

```
(config) # snmp-server user gsm-user gsm-group v3 auth md5 gsm-password priv
aes 128 gsm-encrypt
```

To configure either the community or the SNMPv3 user on the appliance, the administrator selects *Configuration > Credentials* in the menu bar (see Chapter *10.3.2* (page 219)).

10.3.6.2 SSH

The authenticated scan can be performed via SSH as well. If using SSH, the usage of a special unprivileged user is recommended. The appliance currently requires only the command `show version` to retrieve the current version of the firmware of the device.

To set up a less privileged user who is only able to run this command, several approaches are possible. The following example uses the role-based access control feature.

Note: Before using the following example, make sure all side effects of the configuration are understood. If used without verification, the system may restrict further logins via SSH or console.

To use role-based access control AAA and views have to be enabled:

```
> enable
# configure terminal
(config)# aaa new-model
(config)# exit
> enable view
# configure terminal
```

The following commands create a restricted view including just the command `show version`. The supplied password `view-pw` is not critical:

```
(config)# parser view gsm-view
(config-view)# secret 0 view-pw
(config-view)# commands exec include show version
(config-view)# exit
```

Now the user `gsm-user` with the password `gsm-pw` is created and linked to the view `gsm-view`:

```
(config)# username gsm-user view gsm-view password 0 gsm-pw
(config)# aaa authorization console
(config)# aaa authorization exec default local
```

If SSH is not enabled yet the following commands take care of that. Use the appropriate host name and domain:

```
(config)# hostname switch
(config)# ip domain-name greenbone.net
(config)# crypto key generate rsa general-keys modulus 2048
```

Finally, enable SSH logins using the following commands:

```
(config)# line vty 0 4
(config-line)# transport input ssh
(config-line)# Crtl-Z
```

Note: For executing a full scan, e.g., with the scan configuration *Full and fast*, the setting *ssh server rate-limit* must be set to `240`. Before scanning, this value should be checked and adjusted if necessary.

The credentials of the user must be entered on the appliance. Select *Configuration* > *Credentials* in the menu bar and create the appropriate user (see Chapter *10.3.2* (page 219)).

Link the credentials to the target to be used as SSH credentials.

10.3.7 Requirements on Target Systems with Huawei VRP

The appliance can check network components like routers and switches for vulnerabilities as well. While the usual network services are discovered and checked via the network, some vulnerabilities can only be discovered by an authenticated scan. For the authenticated scan, the appliance can use either SNMP or SSH.

Note: The commands in this chapter serve as an example and should work on most Huawei routers.

Depending on the software version or hardware, some commands may differ (e.g., the order of the parameters or values), may not be necessary, or may not be available.

More information can be found in the related documentation for the respective device and software version.

10.3.7.1 SNMP

The appliance can use the SNMP protocol to access the Huawei network component. The appliance supports SNMPv1, v2c and v3. SNMP uses the port 161/udp. The default port list does not include any UDP port. Therefore, this port is ignored during the vulnerability test using *Full and fast* and no SNMP check is enabled. To scan network components, the port list should be modified to include at least the following ports:

- 22/tcp SSH
- 80/tcp 8080/tcp HTTP
- 443/tcp 8443/tcp HTTPS
- 2000/tcp SCCP
- 2443/tcp SCCPS
- 5060/tcp 5060/udp SIP
- 5061/tcp 5061/udp SIPS
- 67/udp DHCP Server
- 69/udp TFTP
- 123/udp NTP
- 161/udp SNMP
- 162/udp SNMP Traps
- 500/udp IKE
- 514/udp Syslog
- 546/udp DHCPv6

The administrator can set up special port lists used only for such network components.

The appliance needs to access only very few objects from the SNMP tree. For a less privileged access, an SNMP view should be used to constrain the visibility of the SNMP tree for the appliance. The following two examples explain how to set up the view using either a community string or an SNMPv3 user.

To use an SNMP community string the following commands are required on the target:

```
<HUAWEI>system-view
```

Using an access list the usage of the community can be restricted. The appliance's IP address is 192.168.222.74 in this example:

```
[~HUAWEI]acl 2000
[~HUAWEI-acl4-basic-2000]rule permit source 192.168.222.74 32
[*HUAWEI-acl4-basic-2000]commit
[~HUAWEI-acl4-basic-2000]quit
```

Allow Version 2c of SNMPv:

```
[~HUAWEI]snmp-agent sys-info version v3 v2c
[*HUAWEI]commit
```

The view `gsm` should only allow accessing the system description:

```
[~HUAWEI]snmp-agent mib-view included gsm system
[*HUAWEI]snmp-agent mib-view excluded gsm system.9
[*HUAWEI]commit
```

The last command links the community `gsm-community` with the view `gsm` and the access list 2000:

```
[~HUAWEI]snmp-agent community read gsm-community mib-view gsm acl 2000
[*HUAWEI]commit
```

If using an SNMPv3 user including encryption, the following configuration lines are required on the target:

```
<HUAWEI>system-view
[~HUAWEI]acl 2000
[~HUAWEI-acl4-basic-2000]rule permit source 192.168.222.74 32
[*HUAWEI-acl4-basic-2000]quit
[*HUAWEI]snmp-agent sys-info version v3
[*HUAWEI]snmp-agent mib-view included gsm system
[*HUAWEI]snmp-agent mib-view excluded gsm system.9
[*HUAWEI]commit
```

SNMPv3 requires the setup of a group first. Here the group `gsmgroup` is linked to the view `gsm` and the access list 2000:

```
[~HUAWEI]snmp-agent group v3 gsmgroup privacy read-view gsm acl 2000
[*HUAWEI]commit
```

Now the user can be created supplying the password `gsm-password` and the encryption key `gsm-encrypt`. The authentication is done using MD5 while the encryption is handled by AES128. This is done in three steps:

Configure the password `gsm-password`:

```
[~HUAWEI]snmp-agent usm-user v3 gsm-user authentication-mode md5
Please configure the authentication password (8-255)
[*HUAWEI]commit
```

Configure encryption key `gsm-encrypt`:

```
[~HUAWEI]snmp-agent usm-user v3 gsm-user privacy-mode aes128
Please configure the privacy password (8-255)
[*HUAWEI]commit
```

Add the user to the group:

```
[*HUAWEI]snmp-agent usm-user v3 gsm-user group gsmgroup
[*HUAWEI]commit
```

To configure either the community or the SNMPv3 user on the appliance, the administrator selects *Configuration > Credentials* in the menu bar (see Chapter *10.3.2* (page 219)).

10.3.7.2 SSH

The authenticated scan can be performed via SSH as well. If using SSH, the usage of a special unprivileged user is recommended. The appliance currently requires only the commands `display device`, `display version` and `display patch-information` to retrieve the device's current firmware version.

Note: If a compliance scan is performed, the following additional commands may be used:

- `display arp speed-limit`
- `display arp-miss speed-limit source-ip`
- `display current-configuration`
- `display current-configuration configuration bgp`
- `display current-configuration configuration pim`
- `display current-configuration configuration user-interface`
- `display current-configuration configuration vpn-instance`
- `display current-configuration interface`
- `display current-configuration | include multicast`
- `display current-configuration | include ntp`
- `display current-configuration | include snmp`
- `display current-configuration | include ssh`
- `display ftp-server`
- `display isis peer`
- `display mpls ldp session verbose`
- `display mpls rsvp-te interface`
- `display ospf peer brief`
- `display ospfv3 peer`
- `display snmp-agent sys-info version`
- `display ssh server status`
- `display telnet server`
- `display telnet server status`
- `display vrrp`

To set up a less privileged user who is only able to run this command, several approaches are possible. The following example uses the role-based access control feature.

Note: Before using the following example, make sure all side effects of the configuration are understood. If used without verification, the system may restrict further logins via SSH or console.

The following commands create a restricted view including just the commands `display device`, `display version` and `display patch-information`. The supplied password `Hello-secret123` is not critical.

```
<HUAWEI> system-view
[~HUAWEI]aaa
[~HUAWEI-aaa]local-user gsm-user password cipher Hello-secret123
[*HUAWEI-aaa]local-user gsm-user level 0
[*HUAWEI-aaa]local-user gsm-user service-type ssh
[*HUAWEI-aaa]commit
[~HUAWEI-aaa]quit
[~HUAWEI]ssh user gsm-user authentication-type password
[*HUAWEI]ssh user gsm-user service-type stelnet
[*HUAWEI]commit
```

The following commands add just the commands `display version`, `display patch-information` and `display device` to “level 0”, so that `gsm-user` is restricted:

```
[~HUAWEI] command-privilege level 0 view global display device
[*HUAWEI] command-privilege level 0 view global display version
[*HUAWEI] command-privilege level 0 view global display patch-information
[*HUAWEI]commit
```

If SSH is not enabled yet the following commands take care of that:

```
[~HUAWEI] rsa local-key-pair create
[*HUAWEI]commit
```

Enable SSH logins using the following commands:

```
[~HUAWEI] user-interface vty 0 4
[*HUAWEI-ui-vty0-4] authentication-mode aaa
[*HUAWEI-ui-vty0-4] protocol inbound ssh
[*HUAWEI-ui-vty0-4] quit
[*HUAWEI]commit
```

Enable the STelnet server:

```
[~HUAWEI] stelnet server enable
[*HUAWEI] ssh authentication-type default password
[*HUAWEI]commit
```

Using an access list, the usage of the SSH login can be restricted. The appliance’s IP address is 192.168.222.74 in this example.

Note: This may restrict any SSH logins from other IP addresses and render the device inaccessible via network.

```
[~HUAWEI]acl 2000
[*HUAWEI-acl4-basic-2000] rule permit source 192.168.222.74 32
[*HUAWEI-acl4-basic-2000] quit
[*HUAWEI] HUAWEI acl 2000
[*HUAWEI] commit
```

Depending on the security settings the password for `gsm-view` has to be changed on the first login. This should be checked by logging in manually once via SSH.

The credentials of the user need to be entered on the appliance. Select *Configuration > Credentials* in the menu bar and create the appropriate user (see Chapter *10.3.2* (page 219)).

Link the credentials to the target to be used as SSH credentials.

10.3.8 Requirements on Target Systems with EulerOS

- For authenticated scans on EulerOS, regular user access is usually enough. The login is performed via SSH. The authentication is done either with passwords or a private SSH key stored on the appliance.
- Generated installation package for credentials: the install package for EulerOS is an RPM file. The install package creates a new user without any specific permissions. A public SSH key that is created on the appliance is stored in the user's home folder.
- In both cases it needs to be made sure that public key authentication is not prohibited by the SSH daemon. The line `PubkeyAuthentication no` must not be present.
- Existing SSH key pairs may also be used. SSH key pairs can be generated using the command `ssh-keygen` on EulerOS or `puttygen.exe` if using PuTTY on Microsoft Windows. To use an existing SSH key pair for authentication, the private key must be supplied when the credential is created. The private SSH key must be either in PEM or OpenSSH format. The key types Ed25519, ECDSA, RSA and DSA are supported.
- For scans that include policy testing, root permission or the membership in specific groups (often `wheel`) may be necessary. For security reasons, many configuration files are only readable by super users or members of specific groups.
- The more permissions a user has, the more results and settings can be detected on a system. In some cases root user access may be required.
- The following commands are executed with root user access during an authenticated scan.

Important:

- This list is not static. New or changed VTs may add new commands at any time.
- Depending on the found software, additional commands may be executed.

  - bash
  - cat
  - date
  - dpkg
  - egrep
  - find
  - grep
  - host
  - id
  - ip
  - lastlog
  - locate
  - ls
  - md5sum
  - mlocate
  - netstat
  - perl

  - ps
  - rpm
  - sh
  - sha1sum
  - slocate
  - uname
  - uptime
  - whereis
  - which

- The installation of the package `locate` (alternatively `mlocate`) to provide the command `locate`/`mlocate` on the target system is recommended. The use of this command reduces calls to the command `find` used to search for files and thus, improves the search performance and lowers the resource usage on the target system.

  For the commands to work, the corresponding database permissions and regular database updates, e.g., via a cron job, may need to be configured.

10.3.9 Requirements on Target Systems with GaussDB

Note: It has to be ensured that the scan is performed by a user that has GaussDB executing permissions.

10.3.9.1 Requirements for System User *root*

Note: Generally, scanning with the user *root* is not recommended.

A root user has the following requirements for scanning a target system with GaussDB:

- On the appliance:
  - Credentials for the target host(s), either as a password or as an SSH key
- On the target system:
  - Root user is able to execute `zsql`/`zengine` (e.g., `LD_LIBRARY_PATH` is set properly and not on default)
  - `PermitRootLogin yes` in `sshd_config` or `PermitRootLogin prohibit-password` in `sshd_config` for SSH key based credentials

10.3.9.2 Requirements for Database Administrator Accounts (e.g., *gaussdba*)

A database administrator has the following requirements for scanning a target system with GaussDB:

- On the appliance:
  - Credentials for the target host(s), either as a password or as an SSH key
- On the target system:
  - User *gaussdba* is the database installation user

10.3.9.3 Requirements for a Regular User Accounts

A regular user has the following requirements for scanning a target system with GaussDB:

- On the appliance:
  - Credentials for the target host(s), either as a password or as an SSH key
- On the target system:
  - User is able to execute `zsql`/`zengine` (e.g., `LD_LIBRARY_PATH` is set properly and not on default)

10.3.9.4 Requirements for a Regular Database User Accounts (e.g., *gauss*)

A regular database user has the following requirements for scanning a target system with GaussDB:

- On the appliance:
  - Credentials with the user name `gauss` and a password configured in each used scan configuration
- On the target system:
  - Public facing database server port

10.4 Configuring a CVE Scan

Not every vulnerability justifies a new scan of the network or of individual systems. If the appliance has already obtained information about vulnerabilities by previous scans, it can make a prognosis of which security risks could currently exist.

Using the CVE scanner allows for a quick prediction of possible security risks without the need of another vulnerability scan. This is especially interesting for environments in which most vulnerabilities have been removed or remediated by using the appliance. If new security risks are predicted, an actual vulnerability scan can be run to verify the prognosis.

The CVE scanner checks the CPEs of the target hosts present in the latest report for the same IP address for assigned CVEs present in the current SecInfo (see Chapter *14* (page 348)). Only reports of tasks that have the *Add results to Assets* setting enabled will be included. It is not relevant whether the setting is enabled before or after the scan.

Note: The CVE scanner might show false positives for the following reasons:

- The scanner does not check whether the vulnerability actually exists.
- The scanner has no capabilities to detect “backported” security fixes, e.g., on Unix-like systems, because it depends on the National Vulnerability Database (NVD)[25], which does not maintain this fixed status and because there is no exposure of the fixed status in the version of the product.

---

[25] https://nvd.nist.gov/

Note: There are some prerequisites for successfully running a CVE scan:

- In order to be detected, a CVE must have a CPE assigned in the National Vulnerability Database (NVD)[26].
  - As long as *Undergoing analysis* is shown on the related NVD web page[27], no results are expected for a CVE when running a CVE scan.
  - Additionally, a *correct* CPE must be assigned to the CVE in the NVD. In case of doubt, the CPE-CVE assignment should be checked manually on the related NVD web page(s).
- The asset database requires current data for the CVE scanner. For detecting the products, a full scan, e.g., with the scan configuration *Full and fast*, must be performed before running the CVE scan.
  - Whether a product was detected can be checked in the *Applications* register of the full scan's report.
  - For the full scan, the task option *Add results to Assets* must be activated, so that the results are added to the asset database and are available to the CVE scanner.
  - Running a full scan with authentication may increase the results found by the CVE scan.
  - A full scan of the systems should be run regularly.

A CVE scan can be run as follows:

1. Run a full scan (see Chapter *10.2* (page 211)).

   Note: A full scan configuration has to be chosen, e.g., *Full and fast*.

   Additionally, the radio button *Yes* has to be selected for *Add results to Assets*.

2. Select *Scans* > *Tasks* in the menu bar.
3. Create a new task by moving the mouse over and clicking *New Task*.
4. Define the task (see Chapter *10.2.2* (page 215)).
5. Select *CVE* in the drop-down list *Scanner*.
6. Click *Save*.
7. In the row of the task, click ▷.

   → The scan is running. For the status of a task see Chapter *10.8* (page 254).

   Tip: The report of a task can be displayed as soon as the task has been started by clicking the bar in the column *Status*. For reading, managing and downloading reports see Chapter *11* (page 283).

   As soon as the status changes to *Done* the complete report is available. At any time the intermediate results can be reviewed (see Chapter *11.2.1* (page 288)).

   Note: It can take a while for the scan to complete. The page is refreshing automatically if new data is available.

8. When the scan is completed select *Scans* > *Reports* in the menu bar.
9. Click on the date of the report to show the results.

   → The report shows each found CVE as a vulnerability (see Fig. 10.21).

[26] https://nvd.nist.gov/
[27] https://nvd.nist.gov/vuln/full-listing

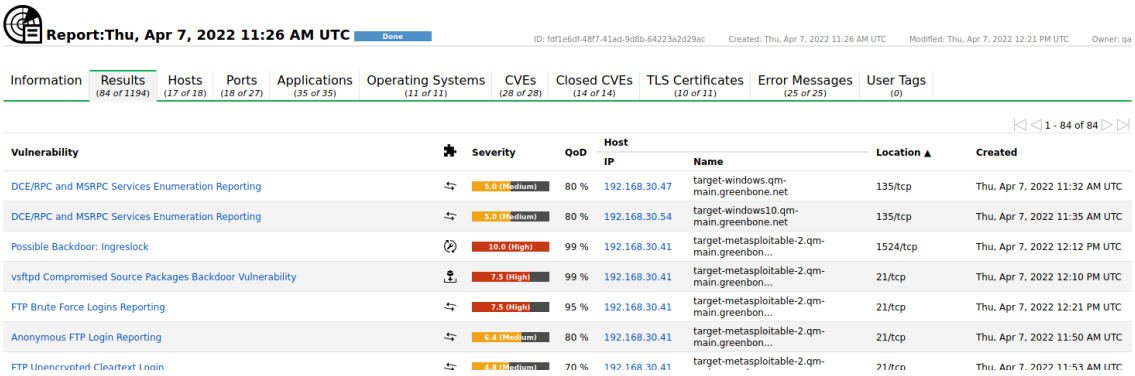


Fig. 10.21: Results of a CVE scan

10. Click on a vulnerability and click 🔍.

    → The details page of the vulnerability is opened.

    The VT to which the result is assigned is displayed in the section *Detection Method* (see Fig. 10.22). By clicking on the VT, the details page of the corresponding VT is opened.

Tip: For available actions on this page see Chapter *11.2.1* (page 288).

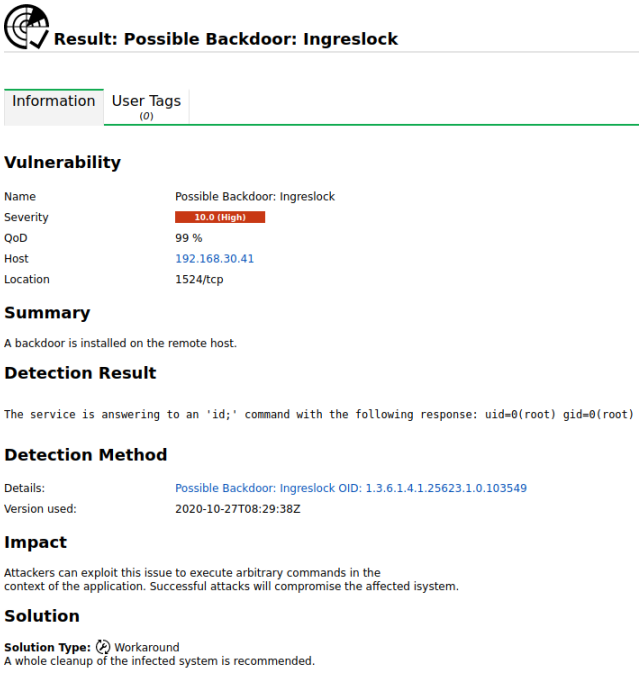


Fig. 10.22: Details of a detected CVE

10.5 Using Container Tasks

10.5.1 Creating a Container Task

A container task can be used to import and provide reports created on other appliances.

A container task can be created as follows:

1. Select *Scans* > *Tasks* in the menu bar.
2. Create a new container task by moving the mouse over and clicking *New Container Task*.
3. Enter the name of the container task in the input box *Name* (see Fig. 10.23).

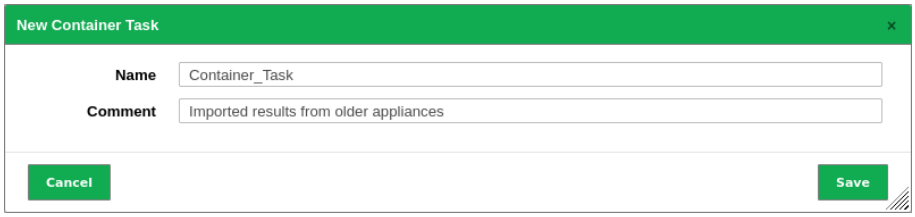


Fig. 10.23: Creating a container task

4. Click *Save*.
5. To add a report to the container task click in the row of the container task.
6. Click *Browse...* and select the XML file of a report (see Fig. 10.24).

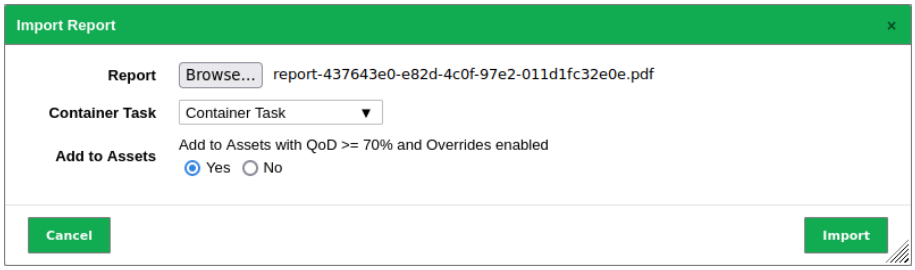


Fig. 10.24: Adding a report to a container task

7. Select the radio button *Yes* to add the report to the assets (see Chapter *13* (page 341)).
8. Click *Import*.

10.5.2 Managing Container Tasks

List Page

All existing container tasks can be displayed by selecting *Scans* > *Tasks* in the menu bar.

Note: Container tasks can be identified by Container in the column *Status*.

For all container tasks the following actions are available:

- Import reports to the container task.
- Move the container task to the trashcan.
- Edit the container task.
- Clone the container task.
- Export the container task as an XML file.

Note: By clicking or below the list of tasks more than one task can be moved to the trashcan or exported at a time. The drop-down list is used to select which tasks are moved to the trashcan or exported.

Details Page

Click on the name of a container task to display the details of the container task. Click to open the details page of the container task.

The following registers are available:

Information General information about the container task.

User Tags Assigned tags (see Chapter *8.4* (page 174)).

Permissions Assigned permissions (see Chapter *9.4* (page 193)).

The following actions are available in the upper left corner:

- Open the corresponding chapter of the user manual.
- Show the list page of all container tasks.
- Create a new task (see Chapter *10.2.2* (page 215)) or container task (see Chapter *10.5* (page 249)).
- Clone the container task.
- Edit the container task.
- Move the container task to the trashcan.
- Export the container task as an XML file.
- Import reports to the container task.
- Show the last report for the container task or show all reports for the container task.
- Show the results for the container task.
- Show the notes for the container task.
- Show the overrides for the container task.

10.6 Managing Targets

List Page

All existing targets can be displayed by selecting *Configuration > Targets* in the menu bar.

For all targets the following information is displayed:

Name Name of the target.

Hosts Hosts that are scanned if the target is used for a scan (see Chapter *10.2.2* (page 215)).

IPs Number of scanned hosts.

Port List Port list used if the target is used for a scan (see Chapter *10.2.2* (page 215)).

Credentials Credentials configured for the target.

For all targets the following actions are available:

- Move the target to the trashcan. Only targets which are currently not used can be moved to the trashcan.
- Edit the target.
- Clone the target.
- Export the target as an XML file.

Note: By clicking or below the list of targets more than one target can be moved to the trashcan or exported at a time. The drop-down list is used to select which targets are moved to the trashcan or exported.

Details Page

Click on the name of a target to display the details of the target. Click to open the details page of the target.

The following registers are available:

Information General information about the target.

User Tags Assigned tags (see Chapter *8.4* (page 174)).

Permissions Assigned permissions (see Chapter *9.4* (page 193)).

The following actions are available in the upper left corner:

- Open the corresponding chapter of the user manual.
- Show the list page of all targets.
- Create a new target (see Chapter *10.2.1* (page 212)).
- Clone the target.
- Edit the target.
- Move the target to the trashcan. Only targets which are currently not used can be moved to the trashcan.
- Export the target as an XML file.

10.7 Creating and Managing Port Lists

If applications run on unusual ports and they should be monitored and tested with the appliance, the default port lists should be adapted. If necessary, an individual port list including the desired port can be created.

All default port lists by Greenbone are data objects that are distributed via the feed. They are downloaded and updated with each feed update.

If no default port lists are available, a feed update may be necessary, or the Feed Import Owner may need to be set (see Chapter *7.2.1.10.1* (page 81)).

Default port lists cannot be edited. Additionally, they can only be deleted temporarily by the Feed Import Owner or by a super administrator. During the next feed update, they will be downloaded again.

Note: To permanently delete a default port list, the Feed Import Owner has to delete it. Afterwards the Feed Import Owner has to be changed to *(Unset)* (see Chapter *7.2.1.10.1* (page 81)).

In addition to the default port lists, custom port lists can be created (see Chapter *10.7.1* (page 252)) or imported (see Chapter *10.7.2* (page 253)).

10.7.1 Creating a Port List

A new port list can be created as follows:

1. Select *Configuration* > *Port Lists* in the menu bar.
2. Create a new port list by clicking ☆.
3. Define the port list (see Fig. 10.25).

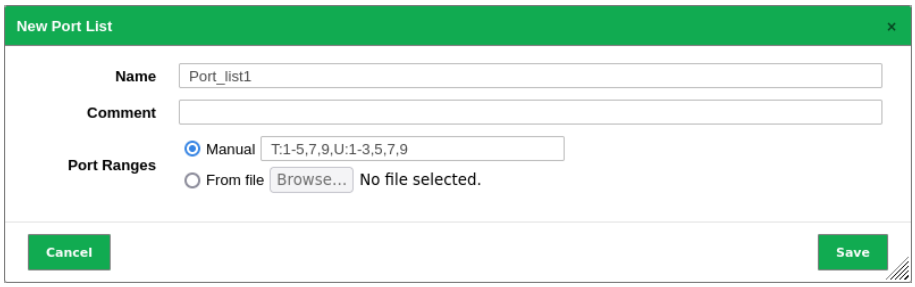


Fig. 10.25: Creating a new port list

4. Click *Save*.

The following details of the port list can be defined:

Name Definition of the name. The name can be chosen freely.

Comment An optional comment can contain additional information.

Port Ranges Manual entry of the port ranges or importing of a list of the port ranges. If entering manually, the port ranges are separated by commas. If importing from a file, the entries can be separated with commas or line breaks. The file must use ASCII character encoding.

Each value in the list can be a single port (e.g., `7`) or a port range (e.g., `9-11`). These options can be mixed (e.g., `5, 7, 9-11, 13`).

An entry in the list can be preceded by a protocol specifier (`T:` for TCP, `U:` for UDP), e.g., `T:1-3, U:7, 9-11` (TCP ports 1, 2 and 3, UDP ports 7, 9, 10 and 11). If no specifier is given, TCP is assumed.

10.7.2 Importing a Port List

A port list can be imported as follows:

1. Select *Configuration > Port Lists* in the menu bar.
2. Click .
3. Click *Browse...* and select the XML file of the port list.
4. Click *Import*.

   → The imported port list is displayed on the page *Port Lists*.

10.7.3 Managing Port Lists

List Page

All existing port lists can be displayed by selecting *Configuration > Port Lists* in the menu bar.

For all port lists the following information is displayed:

Name Name of the port list.

Port Counts – Total Total number of ports in the port list.

Port Counts – TCP Number of TCP ports in the port list.

Port Counts – UDP Number of UDP ports in the port list.

For all port lists the following actions are available:

- Move the port list to the trashcan. Only port lists which are currently not used can be moved to the trashcan. As long as the port list is not deleted from the trashcan, it is not downloaded anew during the next feed update.
- Edit the port list. Only self-created port lists which are currently not used can be edited.
- Clone the port list.
- Export the port list as an XML file.

Note: By clicking or below the list of port lists more than one port list can be moved to the trashcan or exported at a time. The drop-down list is used to select which port lists are moved to the trashcan or exported.

Details Page

Click on the name of a port list to display the details of the port list. Click to open the details page of the port list.

The following registers are available:

Information General information about the port list.

Port Ranges All port ranges included in this port list. The first and the last port of a range as well as the protocol specifier are displayed.

User Tags Assigned tags (see Chapter *8.4* (page 174)).

Permissions Assigned permissions (see Chapter *9.4* (page 193)).

The following actions are available in the upper left corner:

- Open the corresponding chapter of the user manual.
- Show the list page of all port lists.
- Create a new port list (see Chapter *10.7.1* (page 252)).
- Clone the port list.
- Edit the port list. Only self-created port lists which are currently not used can be edited.
- Move the port list to the trashcan. Only port lists which are currently not used can be moved to the trashcan. As long as the port list is not deleted from the trashcan, it is not downloaded anew during the next feed update.
- Export the port list as an XML file.

10.8 Managing Tasks

List Page

All existing tasks can be displayed by selecting *Scans* > *Tasks* in the menu bar.

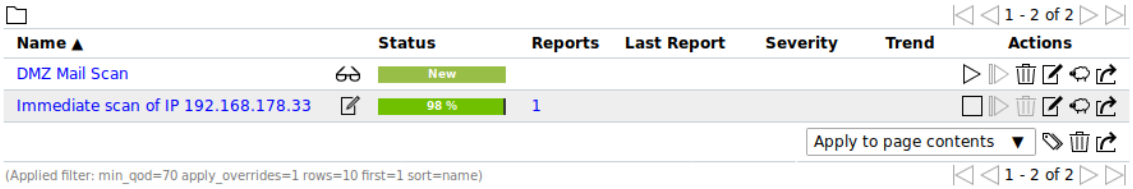


Fig. 10.26: Page *Tasks* displaying all tasks

For all tasks the following information is displayed:

Name Name of the task. The following icons may be displayed:

The task is marked as alterable. The task's scan target(s), scanner and scan configuration can be edited, even if reports were already created.

The task is configured to run on a remote scanner (see Chapter *16* (page 371)).

The task is visible to one or more other user(s).

The task is owned by another user.

Status Current status of the task. The following status bars are possible:

New There are no runs/reports for the task.

Requested The task was just started. The appliance is preparing the scan. Tasks with this status cannot be stopped, resumed, or deleted.

Queued The task was added to the waiting queue. In some cases, it may remain in the queue. For more information see Chapter *17.3* (page 384).

21 % The task is currently running. The percent value is based on the number of VTs executed on the selected hosts. For this reason the value does not necessarily correlate with the time spent.

Processing The scan or the container task upload is complete and the appliance is processing data. Tasks with this status cannot be stopped, resumed, or deleted.

Done The task has been completed successfully.

Stop Requested The task was requested to stop recently. However, the scan engine has not yet reacted to this request yet. Tasks with this status cannot be stopped, resumed, or deleted.

Stopped at 84 % The task was stopped. The latest report is possibly not yet complete. Other reasons for this status could be the reboot of the appliance or a power outage. After restarting the scanner, the task will be resumed automatically.

Resume Requested The task was just resumed. The appliance is preparing the scan. Tasks with this status cannot be stopped, resumed, or deleted.

When resuming a scan, all unfinished hosts are scanned completely anew. The data of hosts that were already fully scanned is kept.

Delete Requested The task was deleted. The actual deletion process can take some time as reports need to be deleted as well. Tasks with this status cannot be stopped, resumed, or deleted.

Interrupted at 42 % An error has occurred and the task was interrupted. The latest report is possibly not complete yet or is missing completely.

Container The task is a container task.

Uploading The report is currently being uploaded into the container task.

Reports Number of reports for the task. By clicking on the number of reports the page *Reports* is opened. A filter is applied to show only the reports for the selected task.

Last Report Date and time of the latest report. By clicking it the details page of the latest report is opened.

Severity Highest severity found by a scan of the task.

Trend Change of vulnerabilities between the newest and the second newest report (see Chapter *11.5* (page 300)).

For all tasks the following actions are available:

- Start the task. Only currently not running tasks can be started.
- Stop the currently running task. All discovered results will be written to the database.
- Show details of the assigned schedule (only available for scheduled tasks, see Chapter *10.10* (page 268)).
- Resume the stopped task. All unfinished hosts are scanned completely anew. The data of hosts that were already fully scanned is kept.
- Move the task to the trashcan.
- Edit the task.
- Clone the task.
- Export the task as an XML file.

Note: By clicking or below the list of tasks more than one task can be moved to the trashcan or exported at a time. The drop-down list is used to select which tasks are moved to the trashcan or exported.

Details Page

Click on the name of a task to display the details of the task. Click to open the details page of the task.

The following registers are available:

Information General information about the task.

User Tags Assigned tags (see Chapter *8.4* (page 174)).

Permissions Assigned permissions (see Chapter *9.4* (page 193)).

The following actions are available in the upper left corner:

- Open the corresponding chapter of the user manual.
- Show the list page of all tasks.
- Create a new task (see Chapter *10.2.2* (page 215)) or container task (see Chapter *10.5* (page 249)).
- Clone the task.
- Edit the task.
- Move the task to the trashcan.
- Export the task as an XML file.
- Start the task. Only currently not running tasks can be started.
- Stop the currently running task. All discovered results will be written to the database.
- Resume the stopped task. All unfinished hosts are scanned completely anew. The data of hosts that were already fully scanned is kept.
- Show the last report for the task or show all reports for the task.
- Show the results for the task.
- Show the notes for the task.
- Show the overrides for the task.

10.8.1 Granting Permissions for a Task

On the details page of a task permissions for the task can be managed as follows:

Note: By default, regular users cannot create permissions for other users as they do not have access to the user database. To be able to create permissions for other users, a user must have the global and the specific *get_users* permission (see Chapter *9.4.3* (page 199)).

1. Select *Scans* > *Tasks* in the menu bar.
2. Click on the name of a task to display the details of the task. Click to open the details page of the task.
3. Click on the register *Permissions*.
4. In the section *Permissions* click .
5. Select the permission type in the drop-down list *Grant*.
6. Select the radio button *User*, *Group* or *Role* and select the user/role/group in the respective drop-down list (see Fig. 10.27).

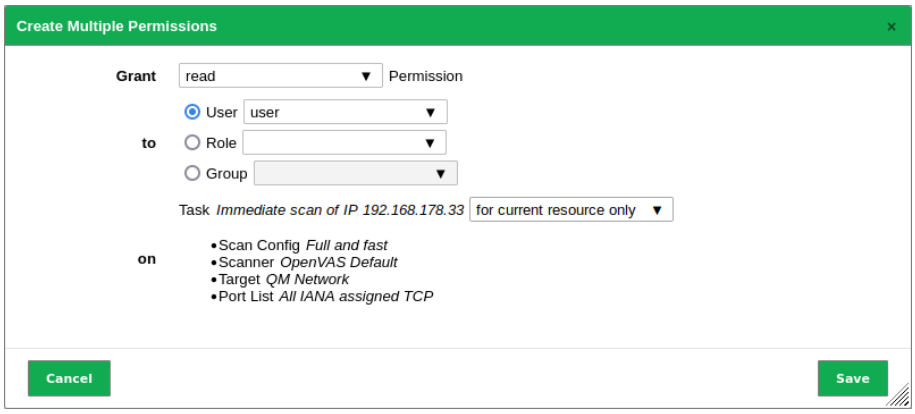


Fig. 10.27: Creating a new permission

7. Click *Save*.

   → The permission is displayed on the details page of the task (see Fig. 10.28).

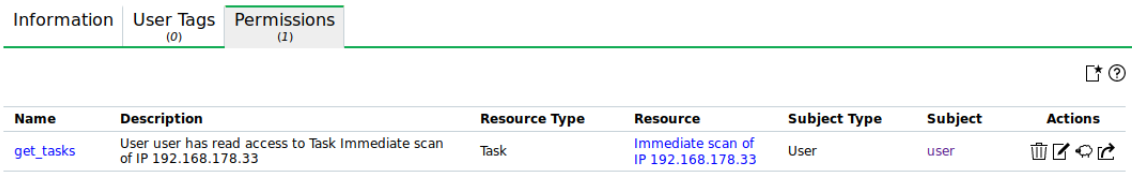


Fig. 10.28: Permission displayed on the details page of a task

After logging in the user can see the task and can access the respective reports.

10.9 Configuring and Managing Scan Configurations

The appliance comes with various predefined scan configurations. They can be customized and new scan configurations can be created.

10.9.1 Default Scan Configurations

All default scan configurations by Greenbone are data objects that are distributed via the feed. They are downloaded and updated with each feed update.

If no default scan configurations are available, a feed update may be necessary, or the Feed Import Owner may need to be set (see Chapter *7.2.1.10.1* (page 81)).

Default scan configurations cannot be edited. Additionally, they can only be deleted temporarily by the Feed Import Owner or by a super administrator. During the next feed update, they will be downloaded again.

Note: To permanently delete a default scan configuration, the Feed Import Owner has to delete it. Afterwards the Feed Import Owner has to be changed to *(Unset)* (see Chapter *7.2.1.10.1* (page 81)).

Note: In addition to the default scan configurations, custom scan configurations can be created (see Chapter *10.9.2* (page 259)) or imported (see Chapter *10.9.3* (page 263)).

By default, the following scan configurations are available:

Empty This scan configuration is an empty template containing no VTs. It can be cloned and used for a completely individual created scan configuration.

The VT families are static, i.e., new VTs of the chosen VT families are not added and used automatically.

Base This scan configuration only uses VTs which collect information about the target system. No vulnerabilities are being detected. It can be cloned and used for a completely individual created scan configuration.

The used port scanner is *Ping Host* which detects whether a host is alive. Additionally, information about the operating system is collected.

The VT families are static, i.e., new VTs of the chosen VT families are not added and used automatically.

Discovery This scan configuration only uses VTs that provide information about the target system. No vulnerabilities are being detected.

Amongst others, the collected information contains information about open ports, used hardware, firewalls, used services, installed software and certificates. The system is inventoried completely.

The VT families are dynamic, i.e., new VTs of the chosen VT families are added and used automatically.

Host Discovery This scan configuration is used to detect target systems. No vulnerabilities are being detected.

The used port scanner is *Ping Host* which detects whether a host is alive.

The VT families are static, i.e., new VTs of the chosen VT families are not added and used automatically.

System Discovery This scan configuration is used to detect target systems including installed operating systems and used hardware. No vulnerabilities are being detected.

The used port scanner is *Ping Host* which detects whether a host is alive.

The VT families are static, i.e., new VTs of the chosen VT families are not added and used automatically.

Full and fast For many environments this is the best option to start with.

This scan configuration is based on the information gathered in the previous port scan and uses almost all VTs. Only VTs that will not damage the target system are used. VTs are optimized in the best possible way to keep the potential false negative rate especially low. The other “Full” configurations only provide more value in rare cases but with much higher effort.

The VT families are dynamic, i.e., new VTs of the chosen VT families are added and used automatically.

Full and fast ultimate This scan configuration expands the scan configuration *Full and fast* with VTs that could disrupt services or systems or even cause shutdowns.

The VT families are dynamic, i.e., new VTs of the chosen VT families are added and used automatically.

This scan configuration may not always be absolutely reliable depending on environmental conditions, which may be reflected in an increased false-positive rate. Narrowing down the suspected false-positive edge cases may require manual analysis and setting overrides (see Chapter *11.8* (page 307)).

Full and very deep This scan configuration is based on the scan configuration *Full and fast* but the results of the port scan or the application/service detection do not have an impact on the selection of the VTs. Therefore, VTs that wait for a timeout or test for vulnerabilities of an application/service which were not detected previously are used. A scan with this scan configuration is very slow.

The VT families are dynamic, i.e., new VTs of the chosen VT families are added and used automatically.

Full and very deep ultimate This scan configuration expands the scan configuration *Full and very deep* with dangerous VTs that could cause possible service or system disruptions. A scan with this scan configuration is very slow.

The VT families are dynamic, i.e., new VTs of the chosen VT families are added and used automatically.

This scan configuration may not always be absolutely reliable depending on environmental conditions, which may be reflected in an increased false-positive rate. Narrowing down the suspected false-positive edge cases may require manual analysis and setting overrides (see Chapter *11.8* (page 307)).

10.9.2 Creating a Scan Configuration

Note: Any custom scan configuration with the scanner preference *safe_checks* set to *no* (see Chapter *10.9.4.1* (page 263)) may not always be absolutely reliable depending on environmental conditions, which may be reflected in an increased false-positive rate. Narrowing down the suspected false-positive edge cases may require manual analysis and setting overrides (see Chapter *11.8* (page 307)).

A new scan configuration can be created as follows:

1. Select *Configuration* > *Scan Configs* in the menu bar.
2. Create a new scan configuration by clicking .

   Note: Alternatively, a scan configuration can be imported (see Chapter *10.9.3* (page 263)).

3. Enter the name of the scan configuration in the input box *Name* (see Fig. 10.29).
4. Select the radio button of the base that should be used.

   It can be chosen between *Base with a minimum set of NVTs*, *Empty, static and fast*, *Full and fast* and a previously created scan configuration.

5. Click *Save*.

   → The scan configuration is created and displayed on the page *Scan Configs*.

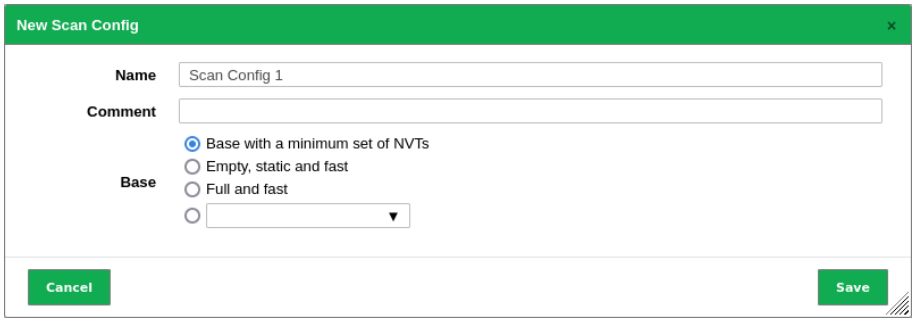


Fig. 10.29: Creating a new scan configuration

6. In the row of the scan configuration, click ✎.
7. In the section *Edit Network Vulnerability Test Families* select the radio button ↗ if newly introduced VT families should be included and activated automatically (see Fig. 10.30).

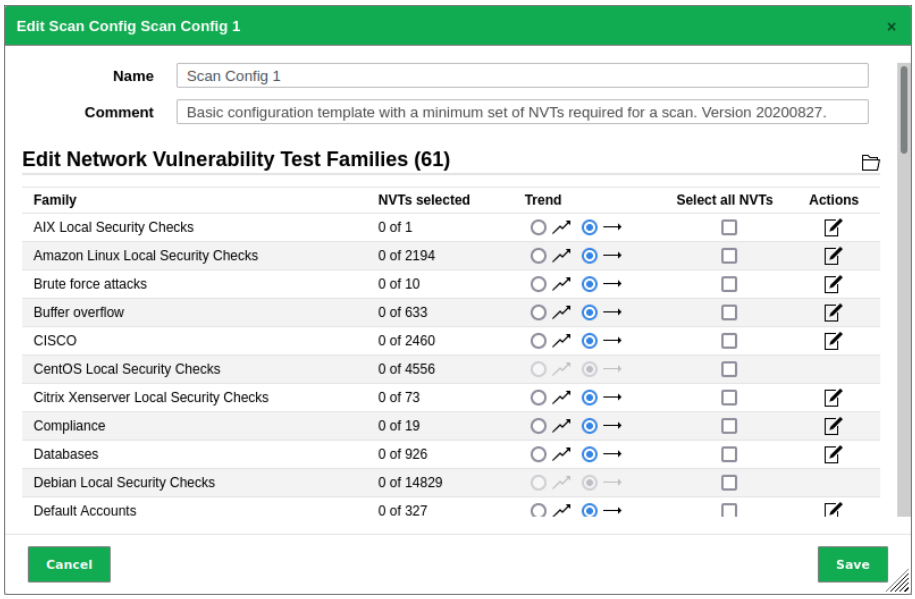


Fig. 10.30: Editing the new scan configuration

8. In the section *Edit Network Vulnerability Test Families* activate the checkboxes in the column *Select all NVTs* if all VTs of a family should be activated.

9. Click for a VT family to edit it (see Fig. 10.31).

Note: The following VT families cannot be edited:

- AIX Local Security Checks
- AlmaLinux Local Security Checks
- Amazon Linux Local Security Checks
- CentOS Local Security Checks
- Debian Local Security Checks
- Fedora Local Security Checks
- FreeBSD Local Security Checks
- Gentoo Local Security Checks
- HP-UX Local Security Checks
- Huawei EulerOS Local Security Checks
- Mageia Linux Local Security Checks
- Mandrake Local Security Checks
- Oracle Linux Local Security Checks
- Red Hat Local Security Checks
- Rocky Linux Local Security Checks
- Slackware Local Security Checks
- Solaris Local Security Checks
- SuSE Local Security Checks
- Ubuntu Local Security Checks

For more information see Chapter *6.5.1* (page 63).

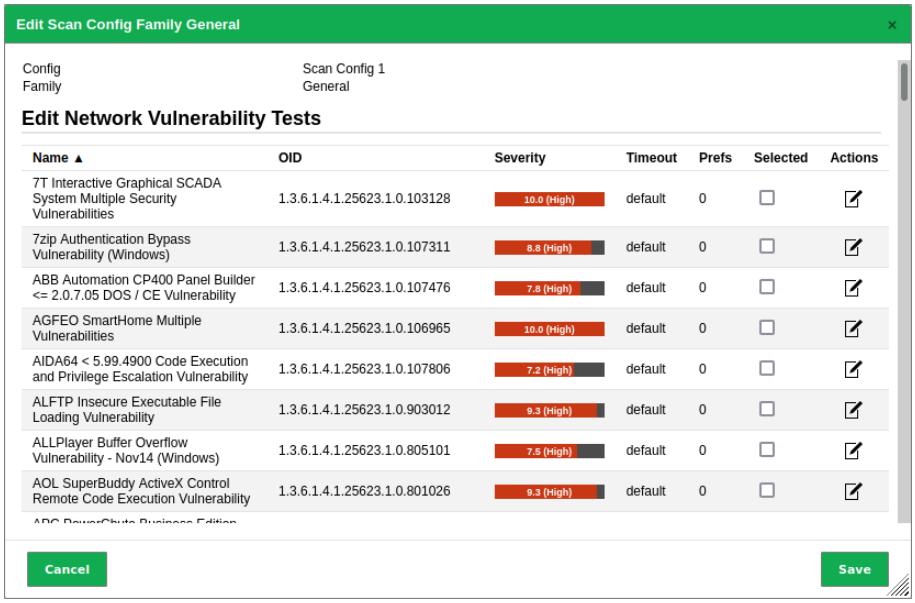


Fig. 10.31: Editing a family of VTs

10. In the column *Selected* activate the checkboxes of the VTs that should be activated.

Note: For the Notus Scanner (see Chapter *6.5.1* (page 63)) to work, the VT *Determine OS and list of installed packages via SSH login* (OID: 1.3.6.1.4.1.25623.1.0.50282) must be activated.

11. Click for a VT to edit it (see Fig. 10.32).

Note: If editing the VT includes uploading a text file, the file should use UTF-8 text encoding.

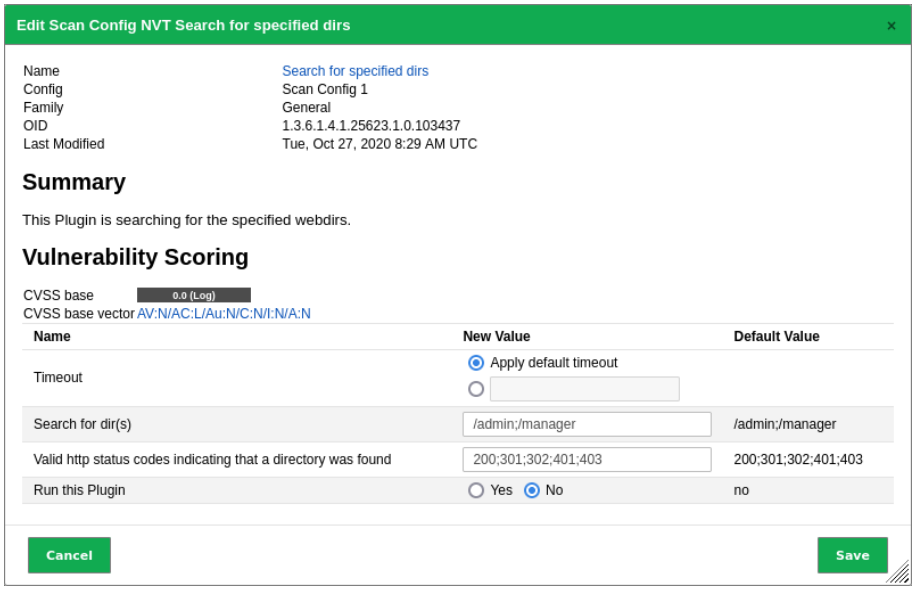


Fig. 10.32: Editing a VT

12. Click *Save* to save the VT.
13. Click *Save* to save the family of VTs.
14. Optional: edit scanner preferences (see Chapter *10.9.4* (page 263)).
15. Optional: edit VT preferences (see Chapter *10.9.5* (page 265)).
16. Click *Save* to save the scan configuration.

10.9.3 Importing a Scan Configuration

Note: Only scan configurations created with the currently used GOS version should be imported. Importing scan configurations from other GOS versions may cause an error message or unexpected behavior.

Any custom scan configuration with the scanner preference *safe_checks* set to *no* (see Chapter *10.9.4.1* (page 263)) may not always be absolutely reliable depending on environmental conditions, which may be reflected in an increased false-positive rate. Narrowing down the suspected false-positive edge cases may require manual analysis and setting overrides (see Chapter *11.8* (page 307)).

A scan configuration can be imported as follows:

1. Select *Configuration > Scan Configs* in the menu bar.
2. Click .
3. Click *Browse...* and select the XML file of the scan configuration.
4. Click *Import*.

   Note: If the name of the imported scan configuration already exists, a numeric suffix is added to the name.

   → The imported scan configuration is displayed on the page *Scan Configs*.
5. Execute steps 6 to 16 of Chapter *10.9.2* (page 259) to edit the scan configuration.

10.9.4 Editing the Scanner Preferences

Scanner preferences can be edited as follows:

1. Select *Configuration > Scan Configs* in the menu bar.
2. In the row of the scan configuration, click .
3. In the section *Edit Scanner Preferences* click to edit the scanner preferences (see Fig. 10.33).
4. After editing the scanner preferences click *Save* to save the scan configuration.

10.9.4.1 Description of Scanner Preferences

Note: Documenting all scanner preferences is out of scope of this document. Only the most important preferences of the scanner are covered.

Undocumented preferences may also be deprecated despite still being visible. These preferences will be ignored by the scanner and should not be considered.

- *alive_test_ports*: TCP ports used by the Boreas alive scanner for the alive test. This setting only affects the alive test methods *TCP-ACK Service Ping* and *TCP-SYN Service Ping*. Only valid ports (port range 0–65535) may be configured. If an invalid value is configured, the Boreas alive scanner uses the default ports.
- *auto_enable_dependencies*: this defines whether VTs that are required by other VTs are activated automatically.
- *cgi_path*: path used by the VTs to access CGI scripts.

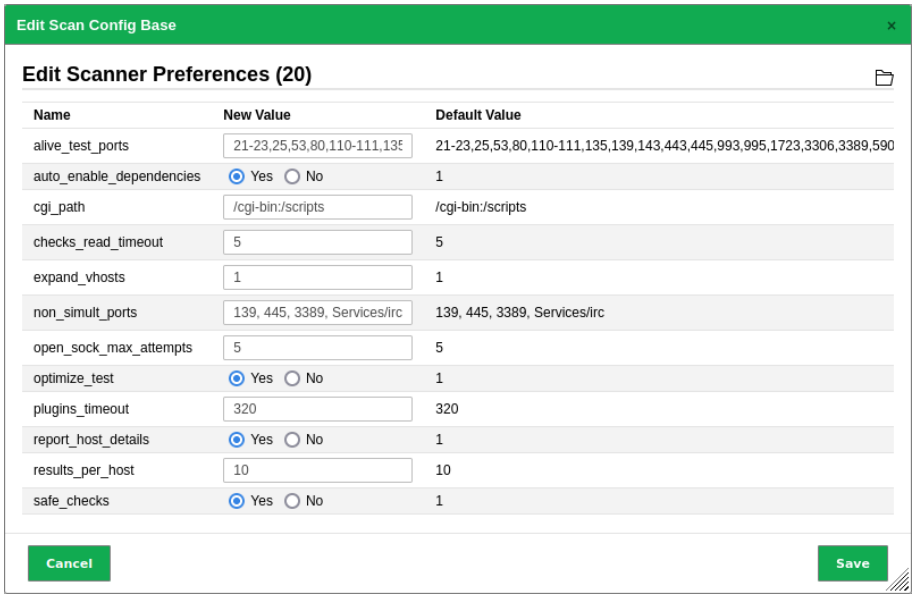


Fig. 10.33: Editing the scanner preferences

- *checks_read_timeout*: timeout for the network sockets during a scan.
- *test_alive_wait_timeout*: timeout for the Boreas alive scanner to wait for replies after the last packet was sent. Values between 1 and 20 are allowed.
- *test_empty_vhost*: the scanner also scans the target by using empty vhost values in addition to the target's associated vhost values.
- *max_sysload*: maximum load on the appliance. Once this load is reached, no further VTs are started until the load drops below this value again.
- *min_free_mem*: minimum available memory (in MB) which should be kept free on the appliance. Once this limit is reached, no further VTs are started until sufficient memory is available again.
- *non_simult_ports*: these ports are not being tested simultaneously by VTs.
- *optimize_test*: VTs will only be started if specific prerequisites are met (e.g., open ports or detected application).
- *plugins_timeout*: maximum run time of a VT.
- *safe_checks*: some VTs can cause damage on the host system. This setting disables those respective VTs.
- *scanner_plugins_timeout*: maximum run time (in seconds) for all VTs of the VT family *Port scanners*. If a VT runs longer, it is terminated.
- *expand_vhosts*: the target's host list of vhosts is expanded with values gathered from sources such as reverse lookup queries and VT checks for SSL/TLS certificates.
- *time_between_request*: wait time (in milliseconds) between two actions such as opening a TCP socket, sending a request through the open tcp socket and closing the TCP socket.
- *timeout_retry*: number of retries if a socket connection attempt times out.
- *unscanned_closed*: this defines whether TCP ports that were not scanned should be treated like closed ports.
- *unscanned_closed_udp*: this defines whether UDP ports that were not scanned should be treated as closed ports.

10.9.5 Editing the VT Preferences

1. Select *Configuration > Scan Configs* in the menu bar.
2. In the row of the scan configuration, click ✎.
3. In the section *Network Vulnerability Test Preferences* click 🗀 to edit the VT preferences.
4. In the row of the VT preference, click ✎.
5. Edit the VT preference.
6. Click *Save* to save the VT preference.
7. Click *Save* to save the scan configuration.

10.9.5.1 Description of VT Preferences

Note: Documenting all VT preferences is out of scope of this document. Only the VT preferences of the Nmap and Ping Host port scanners are covered for now.

Preferences of the VT *Ping Host*

Note: Most of the *Ping Host* parameters are no longer supported in GOS 22.04, because they are incompatible with the new Boreas alive scanner. Parameters that are not documented here are not supported and may not be functional.

The VT *Ping Host* in the VT family *Port scanners* contains the following configuration parameter:

- *Report about reachable Hosts*: this defines whether a host discovered by this VT should be listed.

Preferences of the VT *Nmap (NASL wrapper)*

The following options of the VT *Nmap (NASL wrapper)* in the VT family *Port scanners* will be directly translated into options for the execution of the Nmap command. Additional information can be found in the documentation for Nmap[28].

- *Do not randomize the order in which ports are scanned*: Nmap will scan the ports in ascending order.
- *Do not scan targets not in the file*: see *File containing grepable results*.
- *Fragment IP packets*: Nmap fragments the packets for the attack. This allows bypassing simple packet filters.
- *Identify the remote OS*: Nmap tries to identify the operating system.
- *RPC port scan*: Nmap tests the system for Sun RPC ports.
- *Run dangerous ports even if safe checks are set*: UDP and RPC scans can cause problems and usually are disabled with the setting *safe_checks*. With this setting, they can be enabled anyway.
- *Service scan*: Nmap tries to identify services.
- *Use hidden option to identify the remote OS*: Nmap tries to identify more aggressively.
- *Data length*: Nmap adds random data of specified length to the packet.

[28] https://nmap.org/docs.html

- *Host Timeout*: host timeout.
- *Initial RTT timeout*: initial round trip timeout. Nmap can adjust this timeout dependent on the results.
- *Max RTT timeout*: maximum RTT.
- *Min RTT timeout*: minimum RTT.
- *Max Retries*: maximum number of retries.
- *Maximum wait between probes*: this regulates the speed of the scan.
- *Minimum wait between probes*: this regulates the speed of the scan.
- *Ports scanned in parallel (max)*: this defines how many ports should at most be scanned simultaneously.
- *Ports scanned in parallel (min)*: this defines how many ports should at least be scanned simultaneously.
- *Source port*: source port. This is of interest when scanning through a firewall if connections are in general allowed from a specific port.
- *File containing grepable results*: allows for the specification of a file containing line entries in the form of `Host: IP address`. If the option *Do not scan targets not in the file* is set at the same time only systems contained in the file will be scanned.
- *TCP scanning technique*: actual scan technique.
- *Timing policy*: instead of changing the timing values individually the timing policy can be modified.

The timing policy uses the following values:

	Paranoid	Sneaky	Polite	Normal	Aggressive	Insane
initial_rtt_timeout	5 min	15 s	1 s	1 s	500 ms	250 ms
min_rtt_timeout	100 ms	100 ms	100 ms	100 ms	100 ms	50 ms
max_rtt_timeout	10 s	10 s	10 s	10 s	1250 ms	300 ms
max_parallelism	serial	serial	serial	parallel	parallel	parallel
scan_delay	5 min	15 s	400 ms	0 s	0 s	0 s
max_scan_delay	1 s	1 s	1 s	1 s	10 ms	5 ms

10.9.6 Managing Scan Configurations

List Page

All existing scan configurations can be displayed by selecting *Configuration > Scan Configs* in the menu bar (see Fig. 10.34).

For all scan configurations the following information is displayed:

Name Name of the scan configuration.

Type Type of the scan configuration.

Family – Total Number of activated VT families for the scan configuration.

Family – Trend Trend of VT families

↗ New VT families are included and activated automatically after a feed update. This ensures that new VTs are available immediately and without any interaction by the administrator.

→ New VT families are not included automatically after a feed update.

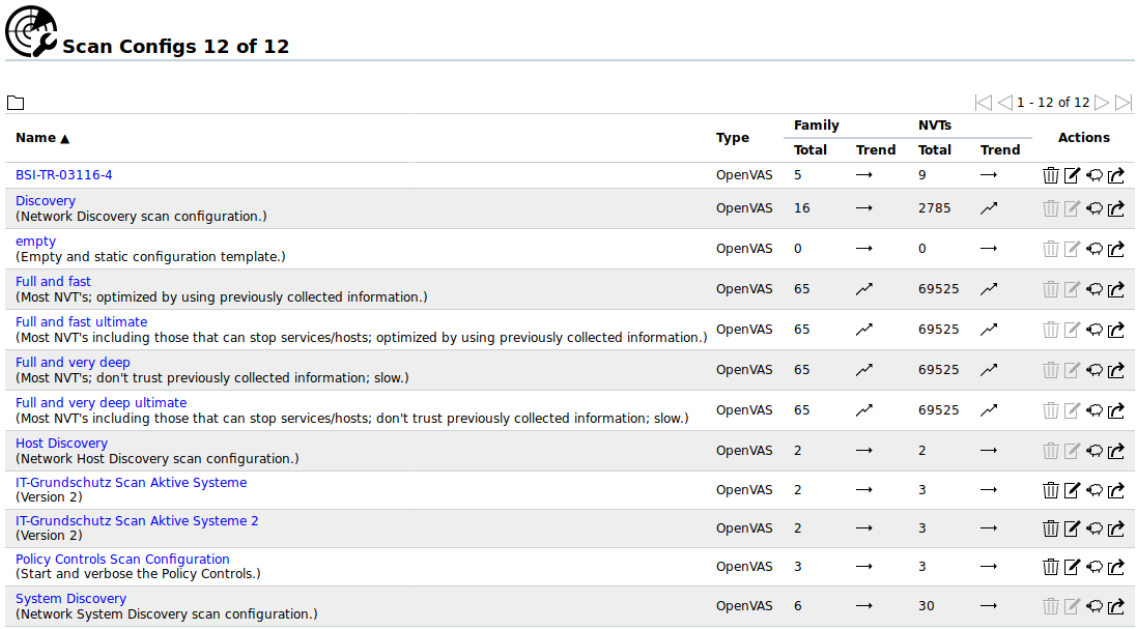
NVTs – Total Number of activated VTs for the scan configuration.

NVTs – Trend Trend of VTs.

↗ New VTs of the activated VT families are included and activated automatically after a feed update. This ensures that new VTs are available immediately and without any interaction by the administrator.

→ New VTs are not included automatically after a feed update.

Note: Greenbone publishes new VTs regularly. New families of VTs can be introduced through the Greenbone Enterprise Feed as well.



Scan Configs 12 of 12

1 - 12 of 12

Name ▲	Type	Family		NVTs		Actions
		Total	Trend	Total	Trend	
BSI-TR-03116-4	OpenVAS	5	→	9	→	
Discovery (Network Discovery scan configuration.)	OpenVAS	16	→	2785	↗	
empty (Empty and static configuration template.)	OpenVAS	0	→	0	→	
Full and fast (Most NVT's; optimized by using previously collected information.)	OpenVAS	65	↗	69525	↗	
Full and fast ultimate (Most NVT's including those that can stop services/hosts; optimized by using previously collected information.)	OpenVAS	65	↗	69525	↗	
Full and very deep (Most NVT's; don't trust previously collected information; slow.)	OpenVAS	65	↗	69525	↗	
Full and very deep ultimate (Most NVT's including those that can stop services/hosts; don't trust previously collected information; slow.)	OpenVAS	65	↗	69525	↗	
Host Discovery (Network Host Discovery scan configuration.)	OpenVAS	2	→	2	→	
IT-Grundschutz Scan Aktive Systeme (Version 2)	OpenVAS	2	→	3	→	
IT-Grundschutz Scan Aktive Systeme 2 (Version 2)	OpenVAS	2	→	3	→	
Policy Controls Scan Configuration (Start and verbose the Policy Controls.)	OpenVAS	3	→	3	→	
System Discovery (Network System Discovery scan configuration.)	OpenVAS	6	→	30	→	

Fig. 10.34: Page *Scan Configs* displaying all available scan configurations

For all scan configurations the following actions are available:

- Move the scan configuration to the trashcan. Only scan configurations which are currently not used can be moved to the trashcan. As long as the scan configuration is not deleted from the trashcan, it is not downloaded anew during the next feed update.
- Edit the scan configuration. Only self-created scan configurations which are currently not used can be edited.
- Clone the scan configuration.
- Export the scan configuration as an XML file.

Note: By clicking or below the list of scan configurations more than one scan configuration can be moved to the trashcan or exported at a time. The drop-down list is used to select which scan configurations are moved to the trashcan or exported.

Details Page

Click on the name of a scan configuration to display the details of the scan configuration. Click to open the details page of the scan configuration.

The following registers are available:

Scanner Preferences All scanner preferences for the scan configuration with current and default values (see Chapter *10.9.4.1* (page 263)).

NVT Families All VT families for the scan configuration with the number of activated VTs and the trend.

NVT Preferences All VT preferences for the scan configuration (see Chapter *10.9.5.1* (page 265)).

User Tags Assigned tags (see Chapter *8.4* (page 174)).

Permissions Assigned permissions (see Chapter *9.4* (page 193)).

The following actions are available in the upper left corner:

- Open the corresponding chapter of the user manual.
- Show the list page of all scan configurations.
- Create a new scan configuration (see Chapter *10.9.2* (page 259)).
- Clone the scan configuration.
- Edit the scan configuration. Only self-created scan configurations which are currently not used can be edited.
- Move the scan configuration to the trashcan. Only scan configurations which are currently not used can be moved to the trashcan. As long as the scan configuration is not deleted from the trashcan, it is not downloaded anew during the next feed update.
- Export the scan configuration as an XML file.
- Import a scan configuration (see Chapter *10.9.3* (page 263)).

10.10 Performing a Scheduled Scan

For continuous vulnerability management the manual execution of task is tedious. The appliance supports the scheduling of tasks for their automation and refers to schedules as automatic scans at a specific time. They can be run once or repeatedly.

The appliance does not provide any schedules by default.

10.10.1 Creating a Schedule

A new schedule can be created as follows:

1. Select *Configuration* > *Schedules* in the menu bar.
2. Create a new schedule by clicking .
3. Define the schedule (see Fig. 10.35).
4. Click *Save*.

   → The schedule is created and can be selected when creating a new task (see Chapter *10.2.2* (page 215)).

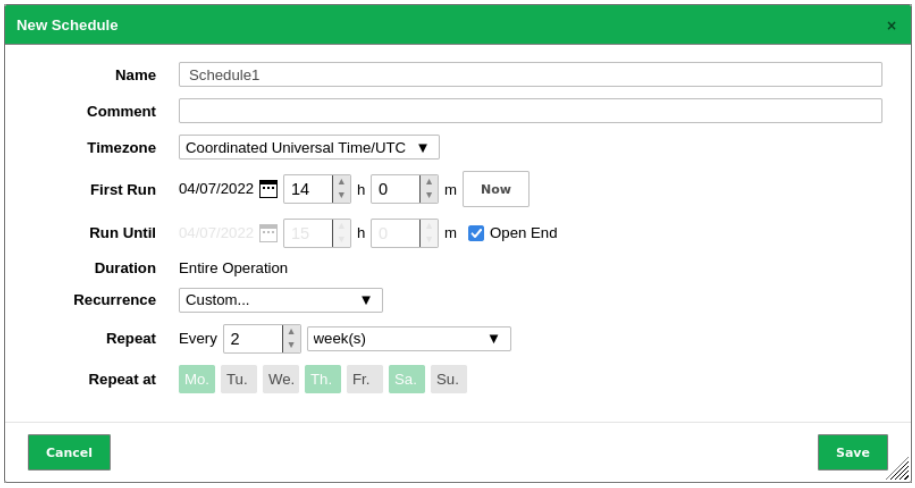


Fig. 10.35: Creating a new schedule

The following details of the schedule can be defined:

Name Definition of the name. The name can be chosen freely.

Comment An optional comment can contain additional information.

Timezone Definition of the timezone the time refers to. UTC±00:00 is default.

> **Note:** Since the appliance runs in the UTC±00:00 timezone internally, the chosen time zone is very important. For Eastern Standard Time (EST) *America/New York* has to be selected.

First Run Definition of the date and time for the first scan to start.

By clicking the date can be chosen. By clicking *Now* the current date and time are set for the first run.

Run Until Definition of the date and time for the first scan to end. Tasks with a specified end time cannot be started manually.

By clicking the date can be chosen. Activate the checkbox *Open End* to leave the end time open.

Duration Definition of the maximum duration a task can take for its execution. The duration depends on the given start and end time. If an end time is defined and the assigned time is expired, the task is aborted and will be suspended until the next scheduled time slot becomes available. This way it can be ensured that the scan will always run with a specific (maintenance) time window.

Recurrence Definition of the repetition rate of the task. It can be selected between *Once*, *Hourly*, *Daily*, *Weekly*, *Monthly*, *Yearly*, *Workweeks (Monday till Friday)* or *Custom*. If the option *Custom* is selected, the repetition rate and the days on which the task should be run can be chosen.

10.10.2 Managing Schedules

List Page

All existing schedules can be displayed by selecting *Configuration > Schedules* in the menu bar.

For all schedules the following information is displayed:

Name Name of the schedule.

First Run Start time of the first run of the task.

Next Run Next run of the task according to the current date and time.

Recurrence Repetition rate of the task.

Duration Maximum duration a task can take for its execution. The duration depends on the given start and end time. If an end time is defined and the assigned time is expired, the task is aborted and will be suspended until the next scheduled time slot becomes available. This way it can be ensured that the scan will always run with a specific (maintenance) time window.

For all schedules the following actions are available:

- Move the schedule to the trashcan. Only schedules which are currently not used can be moved to the trashcan.
- Edit the schedule.
- Clone the schedule.
- Export the schedule as an XML file.

Note: By clicking or below the list of schedules more than one schedule can be moved to the trashcan or exported at a time. The drop-down list is used to select which schedules are moved to the trashcan or exported.

Details Page

Click on the name of a schedule to display the details of the schedule. Click to open the details page of the schedule.

The following registers are available:

Information General information about the schedule.

User Tags Assigned tags (see Chapter *8.4* (page 174)).

Permissions Assigned permissions (see Chapter *9.4* (page 193)).

The following actions are available in the upper left corner:

- Open the corresponding chapter of the user manual.
- Show the list page of all schedules.
- Create a new schedule (see Chapter *10.10.1* (page 268)).
- Clone the schedule.
- Edit the schedule.
- Move the schedule to the trashcan. Only schedules which are currently not used can be moved to the trashcan.
- Export the schedule as an XML file.

10.11 Creating and Managing Scanners

The appliance comes with two predefined scanners. They can be managed and new scanners can be created.

The following scanners are already available:

- OpenVAS Default
- CVE: the CVE scanner allows forecasting possible security risks based on current information about known vulnerabilities from the SecInfo management (see Chapter *14* (page 348)) without the need of a new scan (see Chapter *10.4* (page 246)).

Note: The desired scanner for a task is selected when creating the task (see Chapter *10.2.2* (page 215)).

10.11.1 Creating a Scanner

Note: The creation of a new scanner is only used for creating a new remote scanner (see Chapter *16.4* (page 377)).

10.11.2 Managing Scanners

List Page

All existing scanners can be displayed by selecting *Configuration > Scanners* in the menu bar (see Fig. 10.36).

For all scanners the following actions are available:

- Move the scanner to the trashcan. Only self-created scanners can be moved to the trashcan.
- Edit the scanner. Only self-created scanners can be edited.
- Clone the scanner. Only self-created scanners can be cloned.
- Export the scanner as an XML file.
- Verify that the scanner is online and that the manager can connect to it using the provided certificates and credentials.
- Download the certificate or CA certificate. The certificate or CA certificate can only be downloaded for self-created scanners.

Note: By clicking or below the list of scanners more than one scanner can be moved to the trashcan or exported at a time. The drop-down list is used to select which scanners are moved to the trashcan or exported.

Details Page

Click on the name of a scanner to display the details of the scanner. Click to open the details page of the scanner.

The following registers are available:

Information General information about the scanner.

User Tags Assigned tags (see Chapter *8.4* (page 174)).

Permissions Assigned permissions (see Chapter *9.4* (page 193)).

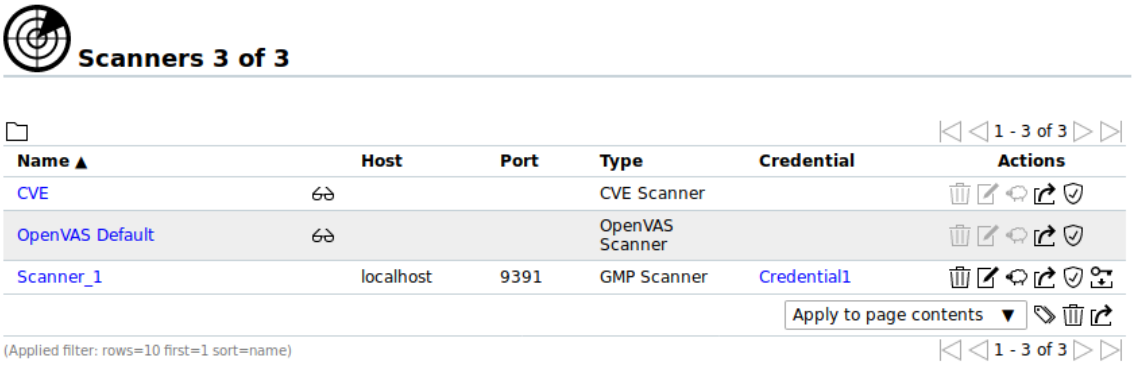


Fig. 10.36: Page *Scanners* displaying all existing scanners

The following actions are available in the upper left corner:

- Open the corresponding chapter of the user manual.
- Show the list page of all scanners.
- Create a new scanner (see Chapter *10.11.1* (page 271)).
- Clone the scanner. Only self-created scanners can be cloned.
- Edit the scanner. Only self-created scanners can be edited.
- Move the scanner to the trashcan. Only self-created scanners can be moved to the trashcan.
- Export the scanner as an XML file.
- Verify that the scanner is online and that the manager can connect to it using the provided certificates.

10.12 Using Alerts

Alerts are anchored within the system. If a configured event (e.g., a task is finished) happens, a specified condition is checked (e.g., vulnerability with a high severity category detected). If the conditions is met, an action is performed, e.g., an e-mail is sent to a defined address.

10.12.1 Creating an Alert

A new alert can be created as follows:

1. Select *Configuration* > *Alerts*.
2. Create a new alert by clicking .
3. Define the alert (see Fig. 10.37).
4. Click *Save*.

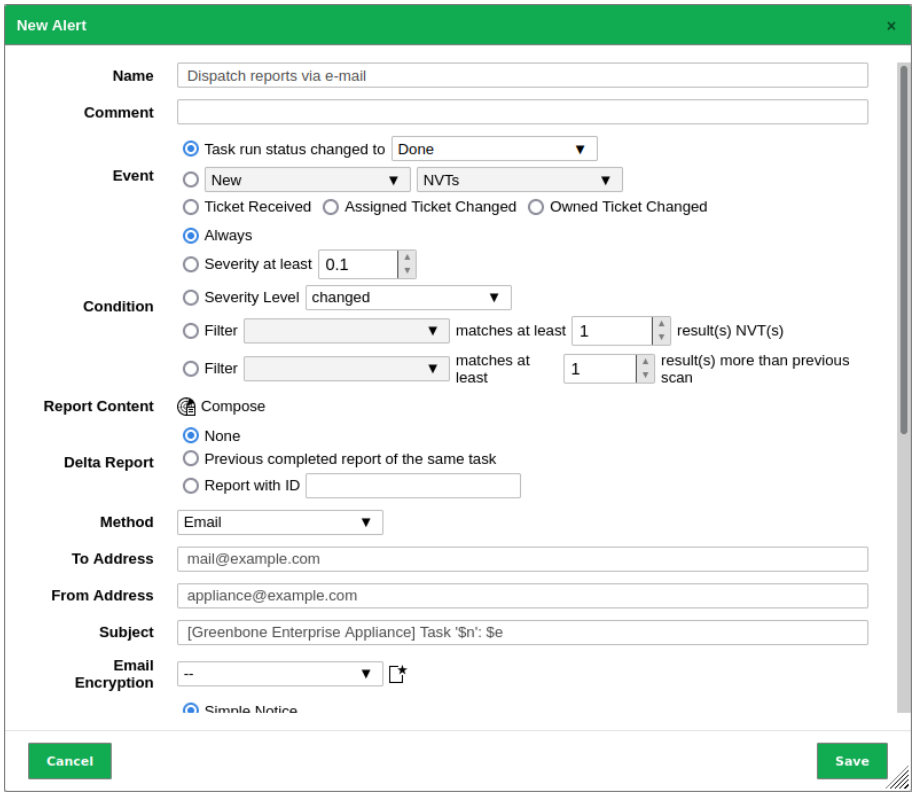


Fig. 10.37: Creating a new alert

The following details of the alert can be defined:

Name Definition of the name. The name can be chosen freely.

Comment An optional comment can contain additional information.

Event Definition of the event for which the alert message is sent. Alerts can be sent if the status of a task changes, if SecInfo (VTs, CVEs, CPEs, CERT-Bund Advisories, DFN-CERT Advisories) is added or updated or if a ticket is assigned or edited (see Chapter *11.6* (page 301)).

Condition Definition of the additional conditions that have to be met.

Note: The options differ for task, for SecInfo and for ticket related alerts.

The alert message can occur:

- Always
- If a specific severity level is reached.
- If the severity level changes, increases or decreases.
- If a Powerfilter matches at least the specified number of results more than in the previous scan.

Report Content (only for task related alerts) The report content can be limited with an additional filter. By clicking the scan report content composer is opened and a Powerfilter can be chosen (see Chapter *11.2.2* (page 292)). The filter must be created previously (see Chapter *8.3* (page 167)). For *Include*, activate the checkbox *Notes* to include attached notes, and the checkbox *Overrides* to label enabled overrides and include their text field content. For *Pagination*, activate the checkbox *Ignore* to have the filter settings for the results displayed per page on the web interface not apply to the results in the sent report.

Details URL (only for SecInfo related alerts) Definition of the URL from which the SecInfo is obtained.

Delta Report (only for task related alerts) Optionally, a delta report can be created, either in comparison to a previous report or to a report with a certain ID.

Method Selection of the method for the alert. Only one method per alert can be chosen. If different alerts for the same event should be triggered, multiple alerts must be created and linked to the same event.

Note: Some methods cannot be used for SecInfo or ticket related alerts.

The following methods are possible:

Email The report is sent to a given e-mail address.

To use this method the used mailhub must be configured using the GOS administration menu (see Chapter *7.2.11* (page 129)).

The settings *To Address*, *From Address* and *Content* have to be configured for the e-mail alert to work. The e-mail subject and encryption is optional.

- **To Address** E-mail address to which the e-mail is sent.
- **From Address** E-mail address that is stated as the e-mail's sender.
- **Subject** For the subject the following placeholders can be used:
  - $d: the date of the last SecInfo check or blank for task/ticket alerts.
  - $e: the event description.
  - $n: the task name or blank for SecInfo/ticket alerts.
  - $N: the alert name.
  - $q: the type of SecInfo event (*New*, *Updated*) or blank for task/ticket alerts.
  - $s: the SecInfo type (e.g., *NVT* or *CERT-Bund Advisory*) or blank for task/ticket alerts.
  - $S: see *$s*, but pluralized (e.g., *NVTs*, *CERT-Bund Advisories*) or blank for task/ticket alerts.
  - $T: the total number of objects in the list for SecInfo alerts or 0 for task/ticket alerts.
  - $u: the owner of the alert or the name of the currently logged in user if the alert was triggered manually.
  - $U: the UUID of the alert.
  - $$: the dollar sign ($).
- **Email Encryption** The e-mail can be encrypted using a configurable S/MIME or PGP key. The key can be selected in the drop-down list *Email Encryption* or created by clicking . The certificate file must fulfill the following conditions:
  - PEM encoded (a binary DER file cannot be used)
  - Using the X.509 format
  - Issued for the recipient e-mail address (*To Address*) and valid (not expired)
  - If the certificate originally came in a bundled format that included the private key as well, only the unencrypted certificate must be uploaded.

  In case of S/MIME credentials, the certificate file additionally must fulfill the following condition:
  - Combines all certificates of the chain (root certificate and all intermediate certificates)
- **Content** The content of the e-mail can be a simple notice, an included or an attached report.

  - **Include Report** The report can be included directly in the e-mail. Any report format that uses a content type starting with *text/* can be chosen because e-mails do not support binary content directly.
  - **Attach Report** The report can be attached to the e-mail. Any report format can be chosen. The report will be attached to the generated e-mail in its correct MIME type.

  The content of the e-mail message can be edited for both, the included and the attached report. For the message the following placeholders can be used:

  - $c: the condition description.
  - $d: the date of the last SecInfo check or blank for task/ticket alerts.
  - $e: the event description.
  - $F: the name of filter.
  - $f: the filter term.
  - $H: the host summary.
  - $i: the report text or list of SecInfo objects (only if including the report/list).
  - $n: the task name or blank for SecInfo/ticket alerts.
  - $N: the alert name.
  - $q: the type of SecInfo event (*New*, *Updated*) or blank for task/ticket alerts.
  - $r: the name of the report format.
  - $s: the SecInfo type (e.g., *NVT* or *CERT-Bund Advisory*) or blank for task/ticket alerts.
  - $S: see *$s*, but pluralized (e.g., *NVTs*, *CERT-Bund Advisories*) or blank for task/ticket alerts.
  - $t: the note if the report was truncated.
  - $T: the total number of objects in the list for SecInfo alerts or 0 for task/ticket alerts.
  - $u: the owner of the alert or the name of the currently logged in user if the alert was triggered manually.
  - $U: the UUID of the alert.
  - $z: the timezone.
  - $$: the dollar sign ($).

HTTP Get The URL is issued as HTTP Get. For example, an SMS text message can be sent via HTTP Get gateway or a bug report can be created in an issue tracker. For the URL the following placeholders can be used:

  - $n: the task name or blank for SecInfo/ticket alerts.
  - $e: the event description.
  - $c: the condition description.
  - $$: the dollar sign ($).

  Example: `https://example.com/$n` → `https://example.com/Scan_task_1`

SCP The report is copied to the given destination via Secure Copy Protocol (SCP) using the given login credentials for authentication.

  All settings (*Credential*, *Host*, *Known Hosts*, *Path* and *Report*) have to be configured for the SCP alert to work.

  - **Credential** A user name and password or user name and SSH key credential that contains valid login information for the destination system.

- **Host** The host name or IP address of the destination system. Only one destination system per SCP alert is supported.
- **Port** The port used to connect to the destination system. By default, port 22 is used. Only values corresponding to the list of standardized ports[29] (between 1 and 65535) are supported. If an unsupported value is saved, either the default value `22` is used instead, or the entered value is truncated, e.g., `70000` becomes `7000`.
- **Known Hosts** The SSH public key of the destination system in the format "host protocol public_key", e.g., `localhost ssh-rsa AAAAB3NzaC1y...P3pCquVb`. The "host" part must match the host name or IP address respectively.
- **Path** The full path of the destination directory and file, e.g., `/home/user/Downloads/report.xml`. Shortening the path, e.g., by using `~` is not supported. For the file name the following placeholders can be used:
  - $$: the dollar sign ($).
  - $n: the task name.
- **Report** Format of the copied report.

Send to host The report is sent to an arbitrary host-port combination via TCP. The IP address or the host name is allowed.

The format of the report can be chosen from the installed report formats.

SMB The report is copied to the given destination via Server Message Block (SMB) protocol using the given login credentials for authentication.

The settings *Credential*, *Share path* and *File path* have to be configured for the SMB alert to work. The selection of a report format is optional.

- **Credential** A user name and password credential that contains valid login information for the destination system.
- **Share path** The share path contains the part of the UNC path containing the host and the share name, e.g., `\\host\share`. The share path has to be created on the destination system before the alert can be used.
- **File path** Location of the report in the share folder that is defined by the share path.

Note: If the file path contains subdirectories which do not exist, the necessary subdirectories are created.

The file extension is appended corresponding to the format selected in the drop-down list *Report Format*.

The default report export file name (see Chapter *8.7* (page 178)) is appended to the file path if the file path ends with `\`.

Note: If a task uses the tag `smb-alert:file_path` with a value, then the value is used as the file path instead of the one that has been configured with the alert (see Chapter *8.4* (page 174)). Example: `smb-alert:file_path=alert_1` assigns the file path `alert_1`.

For the file path the following placeholders can be used:

- %C: the creation date in the format YYYYMMDD. Changed to the current date if a creation date is not available.

[29] https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.txt

  - %c: the creation time in the format HHMMSS. Changed to the current time if a creation time is not available.
  - %D: the current date in the format YYYYMMDD.
  - %F: the name of the used report format (XML for lists and types other than reports).
  - %M: the modification date in the format YYYYMMDD. Changed to the creation date or to the current date if a modification date is not available.
  - %m: the modification time in the format HHMMSS. Changed to the creation time or to the current time if a modification time is not available.
  - %N: the name for the object or the associated task for reports. Lists and types without a name will use the type (see %T).
  - %T: the object type, e.g., “task”, “port_list”. Pluralized for list pages.
  - %t: the current time in the format HHMMSS.
  - %U: the unique ID of the object or “list” for lists of multiple objects.
  - %u: the name of the currently logged in user.
  - %%: the percent sign (%).
- **Report Format** Format of the copied report. If no report format is defined, XML is used by default.
- **Max Protocol** SMB version in case the SMB server only supports a specific version. The following options can be selected:
  - Default
  - SMB3
  - SMB2
  - NT1 (for SMBv1)

  If no SMB version or *Default* is selected, the latest supported version is used.

SNMP An SNMP trap is sent to the given agent. The provided community string is used to authenticate the SNMP trap. The agent is the targeted SNMP trap receiver. For the message the following placeholders can be used:

- $$: the dollar sign ($).
- $d: the date of the last SecInfo check or blank for task/ticket alerts.
- $e: the event description.
- $n: the task name or blank for SecInfo/ticket alerts.
- $q: the type of SecInfo event (*New*, *Updated*) or blank for task/ticket alerts.
- $s: the SecInfo type (e.g., *NVT* or *CERT-Bund Advisory*) or blank for task/ticket alerts.
- $S: see *$s*, but pluralized (e.g., *NVTs*, *CERT-Bund Advisories*) or blank for task/ticket alerts.
- $T: the total number of objects in the list for SecInfo alerts or 0 for task/ticket alerts.

Sourcefire Connector The data can be sent to a Cisco Firepower Management Center (formerly known as Sourcefire Defense Center) automatically. For more information see Chapter *18.3* (page 394).

Start Task The alert can start an additional task. The task is selected in the drop-down list.

System Logger The alert is sent to a Syslog daemon. The Syslog server is defined using the GOS administration menu (see Chapter *7.2.12* (page 133)).

Note: The time zone of the appliance (UTC±00:00) is used for the time stamps of the logs unless adjusted on the syslog server.

verinice.PRO Connector The data can be sent to a verinice.PRO installation automatically. For more information see Chapter *18.1* (page 386).

TippingPoint SMS An HTTPS API is used to upload a report in CSV format to the TippingPoint Security Management System (SMS).

- **Hostname** / **IP** Host name or IP address of the TippingPoint SMS. The CSV report is then sent to `https://<address>/vulnscanner/import` where `<address>` is the entered host name/IP address.
- **Credentials** A user name and password credential that contains valid login information for the TippingPoint SMS.
- **SSL** / **TLS Certificate** A CA certificate used to verify that the host the alert connects to is the TippingPoint SMS. The certificate file must fulfill the following conditions:
  - PEM encoded (a binary DER file cannot be used)
  - Using the X.509 format
- **Use workaround for default certificate** By default, the certificate uses *Tippingpoint* as the common name (CN) which does not match the host name/IP address of the TippingPoint SMS in most cases. If enabled, the workaround temporarily changes the CN and resolves it to the actual host name/IP address within the internal connector script.

Alemba vFire A new ticket in the service management application vFire is created. The report can be attached in one or more formats. For more information see Chapter *18.4* (page 397).

10.12.2 Assigning an Existing Alert to a Task

If an alert should be used afterwards, the alert has to be defined for a specific task as follows:

Note: Already defined and used tasks can be edited as well as it does not have any effect on already created reports.

1. Select *Scans* > *Tasks* in the menu bar.
2. In the row of the task, click ☑.
3. Select the alert in the drop-down list *Alerts* (see Fig. 10.38).

   Note: A new alert can be created by clicking ☆.

4. Click *Save*.

   → Afterwards the task using the alert appears on the details page of the alert (see Fig. 10.39).

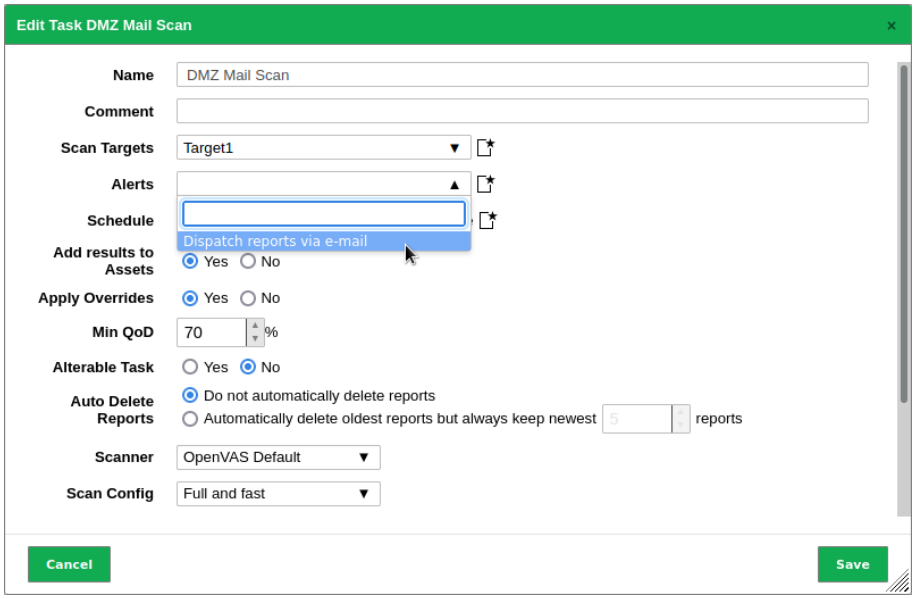


Fig. 10.38: Configuring a task with an alert

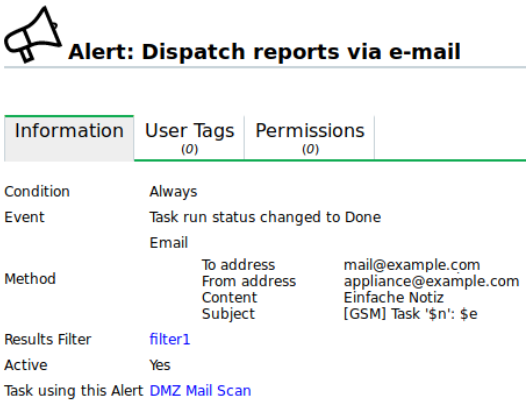


Fig. 10.39: Task using a specific alert

10.12.3 Managing Alerts

List Page

All existing alerts can be displayed by selecting *Configuration > Alerts* in the menu bar.

For all alerts the following information is displayed:

Name Name of the alert.

Event Event for that the alert is triggered.

Condition Condition that has to be fulfilled to trigger the alert.

Method Chosen alert method with additional information, e.g., to which IP address or e-mail address the alert message is sent.

Filter (only for task related alerts) Filter that is applied to the report content.

Active Indication whether the alert is enabled or disabled.

For all alerts the following actions are available:

- Move the alert to the trashcan. Only alerts which are currently not used can be moved to the trashcan.
- Edit the alert.
- Clone the alert.
- Export the alert as an XML file.
- Test the alert.

Note: By clicking or below the list of alerts more than one alert can be moved to the trashcan or exported at a time. The drop-down list is used to select which alerts are moved to the trashcan or exported.

Details Page

Click on the name of an alert to display the details of the alert. Click to open the details page of the alert.

The following registers are available:

Information General information about the alert.

User Tags Assigned tags (see Chapter *8.4* (page 174)).

Permissions Assigned permissions (see Chapter *9.4* (page 193)).

The following actions are available in the upper left corner:

- Open the corresponding chapter of the user manual.
- Show the list page of all alerts.
- Create a new alert (see Chapter *10.12.1* (page 272)).
- Clone the alert.
- Edit the alert.
- Move the alert to the trashcan. Only alerts which are currently not used can be moved to the trashcan.
- Export the alert as an XML file.

10.13 Obstacles While Scanning

There are several typical problems which might occur during a scan using the default values of the appliance. While the default values of the appliance are valid for most environments and customers, depending on the actual environment and the configuration of the scanned hosts they might require some tweaking.

10.13.1 Hosts not Found

During a typical scan (either *Discovery* or *Full and fast*), the appliance will by default first use the ping command to check the availability of the configured targets. If the target does not reply to the ping request it is presumed to be dead and will not be scanned by the port scanner or any VT.

In most LAN environments this does not pose any problems because all devices will respond to a ping request. But sometimes (local) firewalls or other configuration might suppress the ping response. If this happens the target will not be scanned and will not be included in the results and the scan report.

To remediate this problem, both the target configuration and the scan configuration support the setting of the alive test (see *Alive Test* (page 213)).

If the target does not respond to a ping request, a TCP ping may be tested. If the target is located within the same broadcast domain, an ARP ping may be tried as well.

10.13.2 Long Scan Periods

Once the target is discovered to be alive using the ping command, the appliance uses a port scanner to scan the target. By default, a TCP port list containing around 5000 ports is used. If the target is protected by a (local) firewall dropping most of these packets the port scan will need to wait for the timeout of each individual port. If the hosts are protected by (local) firewalls the port lists or the firewalls may be tuned. If the firewall does not drop the request but rejects the request the port scanner does not have to wait for the timeout. This is especially true if UDP ports are included in the scan.

10.13.3 VT not Used

This happens especially very often if UDP based VTs like VTs using the SNMP protocol are used. If the default configuration *Full and fast* is used, the SNMP VTs are included. But if the target is configured using the default port list, the VTs are not executed. This happens because the default port list does not include any UDP ports. Therefore, the port 161/udp (SNMP) is not discovered and excluded from further scans. Both the discovery scans and the recommended scan configuration *Full and fast* optimize the scan based on the discovered services. If the UDP port is not discovered, no SNMP VTs are executed.

Do not enable all ports per default in the port lists. This will prolong the scans considerably. Best practice is the tuning of the port lists to the ports which are used in the environment and are supported by the firewalls.

10.13.4 Scanning vhosts

The scanner is able to find all relationships of host names and IP addresses without needing additional user input.

In environments with virtual hosts (vhosts)[30], the scan reports will have less results because duplicates are avoided.

Two scanner preferences handle vhost scanning (see Chapter *10.9.4* (page 263)):

test_empty_vhost If this preference is enabled, the scanner also tests the target by using empty vhost values in addition to the target's associated vhost values.

expand_vhosts If this preference is enabled, the target's host list of vhosts is expanded with values gathered from sources such as reverse lookup queries and VT checks for SSL/TLS certificates.

[30] https://httpd.apache.org/docs/current/vhosts/

CHAPTER 11

Reports and Vulnerability Management

Note: This chapter documents all possible menu options.

However, not all appliance models support all of these menu options. Check the tables in Chapter *3* (page 20) to see whether a specific feature is available for the used appliance model.

The results of a scan are summarized in a report. Reports can be displayed on the web interface and downloaded in different formats.

The appliance saves all reports of all scans in a local database. Not only is the last report of a scan saved but all reports of all scans ever run. This allows access to information from the past. The reports contain the discovered vulnerabilities and information of a scan.

Once a scan has been started, the report of the results found so far can be viewed. When a scan is completed, the status changes to *Done* and no more results will be added.

11.1 Configuring and Managing Report Formats

Report formats are defined as the formats a report is created from, based on the scan results. Many report formats reduce the available data in order to display it in a meaningful way.

The report formats can be used to export report information into other document formats, so they can be processed by other third-party applications (connectors).

The name of the exported report is configurable in the user settings (see Chapter *8.7* (page 178)).

The native appliance XML format contains all data and can be used to import exported reports on another appliance. To do so, create a container task (see Chapter *10.5* (page 249)).

11.1.1 Default Report Formats

All default report formats by Greenbone are data objects that are distributed via the feed. They are downloaded and updated with each feed update.

Note: Report formats may be deprecated. They are marked with *(Deprecated)* on the web interface, and are no longer documented in the following list.

Deprecated report formats can no longer be used. If a report is exported in such a format, the downloaded file may be empty or otherwise not suitable for use.

If no default report formats are available, a feed update may be necessary, or the Feed Import Owner may need to be set (see Chapter *7.2.1.10.1* (page 81)).

Default report formats cannot be edited. Furthermore, they can only be deleted temporarily by the Feed Import Owner or by a super administrator. During the next feed update, they will be downloaded again.

Note: To permanently delete a default report format, the Feed Import Owner has to delete it. Afterwards the Feed Import Owner has to be changed to *(Unset)* (see Chapter *7.2.1.10.1* (page 81)).

By default, the following report formats are available:

Anonymous XML This is the anonymous version of the XML format. IP addresses are replaced by random IP addresses.

ARF: Asset Reporting Format v1.0.0 This format creates a report that represents the NIST Asset Reporting Format.

CPE – Common Platform Enumeration CSV Table This report selects all CPE tables and creates a single comma-separated file.

CSV Hosts This report creates a comma-separated file containing the systems discovered.

CSV Results This report creates a comma-separated file with the results of a scan.

GCR PDF – Greenbone Compliance Report This is the complete Greenbone Compliance Report for compliance audits (see Chapter *12.2* (page 317)) with all vulnerabilities in graphical format as a PDF file. The language of the report is English.

GSR HTML – Greenbone Security Report This is the complete Greenbone Security Report with all vulnerabilities and results. It can be opened with a web browser in which JavaScript must be enabled. It contains dynamically sortable lists as known from the web interface. The language of the report is English.

GSR PDF – Greenbone Security Report This is the complete Greenbone Security Report with all vulnerabilities in graphical format as a PDF file. The topology graph is not included if more than 100 hosts are covered in the report. The language of the report is English.

GXCR PDF – Greenbone Executive Compliance Report This is the shortened Greenbone Compliance Report for compliance audits (see Chapter *12.2* (page 317)) with all vulnerabilities in graphical format as a PDF file for management. The language of the report is English.

GXR PDF – Greenbone Executive Report This is the shortened Greenbone Security Report with all vulnerabilities in graphical format as a PDF file for management. The topology graph is not included if more than 100 hosts are covered in the report. The language of the report is English.

LaTeX This report is offered as LaTeX source text. The language of the report is English.

NBE This is the old OpenVAS/Nessus report format. It does not have support for notes, overrides and some additional information.

PDF This is a complete report in PDF. Like the HTML format it is neutral. The language of the report is English.

TLS Map This is the report format for TLS Map scans (see Chapter *12.6* (page 339)).

Topology SVG This presents the results in an SVG picture.

TXT This creates a text file. This format is especially useful when being sent by e-mail. The language of the report is English.

Verinice ISM Creates an import file for the ISMS tool *verinice* (see Chapter *18.1* (page 386)).

Verinice ISM all results Creates an import file for the ISMS tool *verinice* (see Chapter *18.1* (page 386)).

Verinice ITG (obsolete) Creates an import file for the ISMS tool *verinice* (see Chapter *18.1* (page 386)).

Vulnerability Report HTML (recommended) This is the new complete Greenbone Security Report with all vulnerabilities and results. It can be opened with a web browser or HTML viewer. The language of the report is English.

Vulnerability Report PDF (recommended) This is the new complete Greenbone Security Report with all vulnerabilities in graphical format as a PDF file. The language of the report is English.

Reports with this report format are limited to the first 500 results per host. Subsequent results per host will be left out and a warning will be shown on the title page of the report.

XML The report is exported in the native XML format. Contrary to the other formats this format contains all results and does not format them at all.

11.1.2 Managing Report Formats

List Page

All existing report formats can be displayed by selecting *Configuration > Report Formats* in the menu bar.

For all report formats the following information is displayed:

Name Name of the report format.

Extension The file name of the downloaded report consists of the UUID (unique internal ID of the report) and this extension. Among others, the extension supports the browser to start a compatible application in case the specified content type is not recognized.

Content Type The content type specifies the format in use and is transmitted when being downloaded. By this, a compatible application can be launched by the browser.

Additionally, the content type is important internally: it is used to offer suitable plug-ins within its context. For example, when sending a report via e-mail all plug-ins of the type `text/\*` are offered as they can be embedded in an e-mail in a humanly readable way.

Trust Some report formats only convert data, while others perform more complex operations and also execute programs. To prevent abuse, each report format plug-in has to be digitally signed by Greenbone. The digital signatures are distributed via the Greenbone Enterprise Feed. If a signature is authentic and the publisher is trusted, it is ensured that the report format exists in the exact format as certified by the publisher. The trust check is automatic and the result can be seen in the column *Trust (Last Verified)*.

Active The report formats are only available in the respective selection menus if they are activated. Newly imported report formats are always deactivated at first. A report format can only be activated if it is trusted.

For all report formats the following actions are available:

- Move the report format to the trashcan. As long as the report format is not deleted from the trashcan, it is not downloaded anew during the next feed update.
- Edit the report format. Only self-created report formats can be edited.

Note: By clicking below the list of report formats more than one report format can be moved to the trashcan at a time. The drop-down list is used to select which report formats are moved to the trashcan.

Details Page

Click on the name of a report format to display the details of the report format. Click to open the details page of the report format.

The following actions are available in the upper left corner:

- Open the corresponding chapter of the user manual.
- Show the list page of all report formats.
- Add a new report format (see Chapter *11.1.3* (page 287)).
- Edit the report format. Only self-created report formats can be edited.
- Move the report format to the trashcan. As long as the report format is not deleted from the trashcan, it is not downloaded anew during the next feed update.

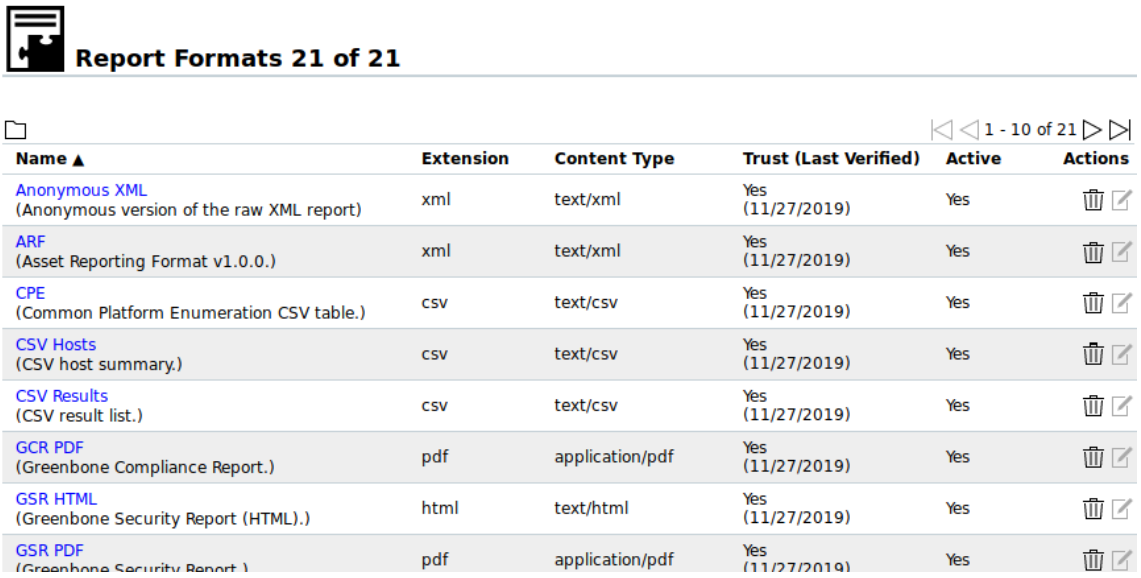


Fig. 11.1: Page *Report Formats* displaying all available report formats

11.1.3 Adding a Report Format

Note: To prevent abuse, all additionally imported report formats have to be reviewed and digitally signed by Greenbone. Report formats that are not signed by Greenbone are not supported in GOS, and cannot be used.

For more information see Chapter *11.1.2* (page 285) – *Trust*.

A new report format can be imported as follows:

1. Provide or obtain a report format plug-in that has been reviewed and accepted by Greenbone.
2. Select *Configuration* > *Report Formats* in the menu bar.
3. Click .
4. Click *Browse...* and select the report format plug-in (see Fig. 11.2).

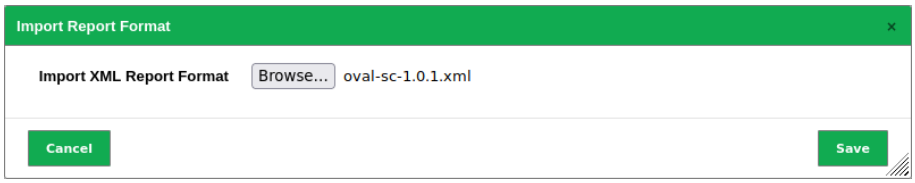


Fig. 11.2: Importing a report format plug-in

5. Click *Save*.

   → The imported report format is displayed on the page *Report Formats*.
6. In the row of the report format, click .
7. For *Active* select the radio button *Yes* (see Fig. 11.3).
8. Click *Save*.

Fig. 11.3: Activating a new report format

11.2 Using and Managing Reports

All existing reports for all scans can be displayed by selecting *Scans* > *Reports* in the menu bar.

The total number of reports of a specific task is displayed on the page *Tasks* in the column *Reports*.

The reports for a specific task can be displayed as follows:

1. Select *Scans* > *Tasks* in the menu bar.
2. For the desired task click on the total number of reports in the column *Reports* to display all reports.

   → The page *Reports* is opened. A filter is applied to show only the reports for the selected task.

Tip: By clicking on the date in the column *Last Report* the details page of the latest report is opened (see Chapter *11.2.1* (page 288)).

Reports	Last Report
1	Mon, Jun 17, 2019 1:13 PM UTC
3	Mon, Jun 17, 2019 1:14 PM UTC

Fig. 11.4: Number of reports saved in total and date of the last report

For every report the following information is displayed:

Date Date and time of report creation.

Status Status of the corresponding task.

Task Corresponding task.

Severity Highest severity found by the scan.

High/Medium/Low/Log/False Pos. Number of found vulnerabilities for each severity.

For all reports the following actions are available:

- Δ Create a delta report (see Chapter *11.2.5* (page 294)).
- ✕ Delete the report.

Note: By clicking ✕ below the list of reports more than one report can be deleted at a time. The drop-down list is used to select which reports are deleted.

11.2.1 Reading a Report

Click on the date of a report to display the details of the report.

The following registers are available:

Information General information about the corresponding scan.

Results List of all results in this report (see Chapter *11.2.1.1* (page 289)).

Hosts Scanned hosts with host names and IP addresses. The detected operating systems, the number of found vulnerabilities for each severity and the highest severity found by the scan are displayed.

Ports Scanned ports with port name, number of hosts and highest severity found by the scan.

Applications Scanned applications with CPE of the application, number of hosts, number of occurrences of results that detected this CPE and highest severity found by the scan.

Operating Systems Scanned operating systems with system name, host name, number of scanned hosts and highest severity found by the scan.

CVEs CVEs found with the scan.

Closed CVEs CVEs of originally detected vulnerabilities which were already confirmed as solved during the scan.

TLS Certificates TLS certificates found with the scan.

Error Messages Error messages that occurred during the scan.

User Tags Assigned tags (see Chapter *8.4* (page 174)).

The report content can be sorted by a chosen column by clicking on the column title. The content can be sorted ascending or descending:

- ▲ in the column title shows that the objects are sorted ascending.
- ▼ in the column title shows that the objects are sorted descending.

The following actions are available in the upper left corner:

- Open the corresponding chapter of the user manual.
- Show the list page of all report formats.
- Add the report contents that have at least a QoD of 70 % and enabled overrides to the assets.
- Remove the report contents from the assets.
- Show the corresponding task.
- Open the page *Results*. A filter is applied to show only the results for this report.
- Open the page *Vulnerabilities*. A filter is applied to show only the vulnerabilities for this report.
- Open the page *TLS Certificates*. A filter is applied to show only the TLS certificates for this report.
- Open the page *Performance*. The system performance for the scan's duration is displayed.
- Download a filtered report (see Chapter *11.2.2* (page 292)).
- ▷ Trigger an alert to send a report (see Chapter *11.2.4* (page 293)).

11.2.1.1 Results of a Report

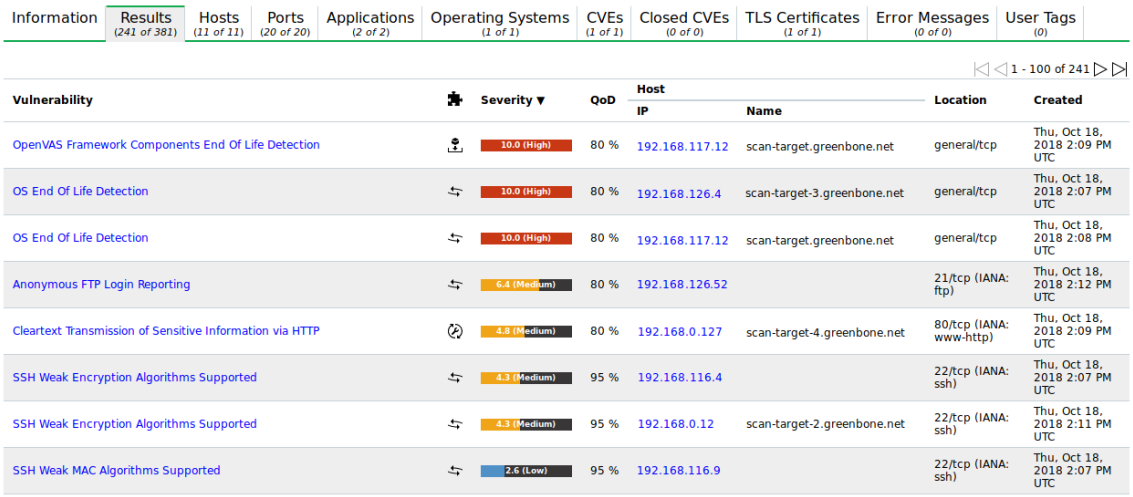
The register *Results* contains a list of all vulnerabilities detected by the appliance (see Fig. 11.5).

Note: By default, overrides are not applied. They can be applied by filtering the report (see Chapter *11.2.1.3* (page 291)).

For every result the following information is displayed:

Vulnerability Name of the found vulnerability. By clicking on the name of a vulnerability details of the vulnerability are shown (see Fig. 11.6). The details page of the vulnerability is opened by clicking .

Vulnerabilities with an attached note are marked with . Vulnerabilities with an attached ticket are marked with .



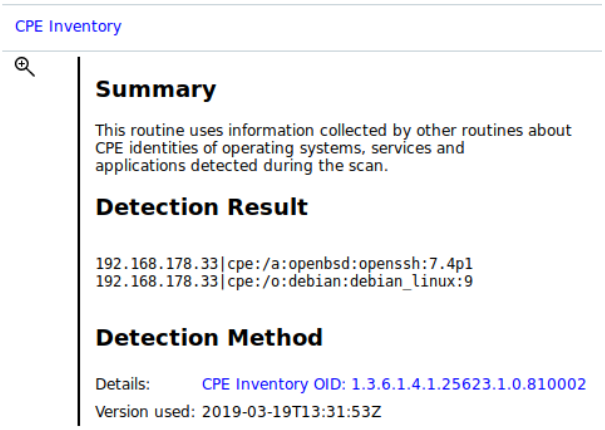
Information | Results (241 of 381) | Hosts (11 of 11) | Ports (20 of 20) | Applications (2 of 2) | Operating Systems (1 of 1) | CVEs (1 of 1) | Closed CVEs (0 of 0) | TLS Certificates (1 of 1) | Error Messages (0 of 0) | User Tags (0)

1 - 100 of 241

Vulnerability	Severity ▼	QoD	Host IP	Host Name	Location	Created
OpenVAS Framework Components End Of Life Detection	10.0 (High)	80 %	192.168.117.12	scan-target.greenbone.net	general/tcp	Thu, Oct 18, 2018 2:09 PM UTC
OS End Of Life Detection	10.0 (High)	80 %	192.168.126.4	scan-target-3.greenbone.net	general/tcp	Thu, Oct 18, 2018 2:07 PM UTC
OS End Of Life Detection	10.0 (High)	80 %	192.168.117.12	scan-target.greenbone.net	general/tcp	Thu, Oct 18, 2018 2:08 PM UTC
Anonymous FTP Login Reporting	6.4 (Medium)	80 %	192.168.126.52		21/tcp (IANA: ftp)	Thu, Oct 18, 2018 2:12 PM UTC
Cleartext Transmission of Sensitive Information via HTTP	4.8 (Medium)	80 %	192.168.0.127	scan-target-4.greenbone.net	80/tcp (IANA: www-http)	Thu, Oct 18, 2018 2:09 PM UTC
SSH Weak Encryption Algorithms Supported	4.3 (Medium)	95 %	192.168.116.4		22/tcp (IANA: ssh)	Thu, Oct 18, 2018 2:07 PM UTC
SSH Weak Encryption Algorithms Supported	4.3 (Medium)	95 %	192.168.0.12	scan-target-2.greenbone.net	22/tcp (IANA: ssh)	Thu, Oct 18, 2018 2:11 PM UTC
SSH Weak MAC Algorithms Supported	2.6 (Low)	95 %	192.168.116.9		22/tcp (IANA: ssh)	Thu, Oct 18, 2018 2:07 PM UTC

Fig. 11.5: Register *Results* showing a list of discovered vulnerabilities

Note: If the column of the vulnerability still appears empty the respective VT has not been updated yet.



CPE Inventory

Summary

This routine uses information collected by other routines about CPE identities of operating systems, services and applications detected during the scan.

Detection Result

192.168.178.33|cpe:/a:openbsd:openssh:7.4p1
192.168.178.33|cpe:/o:debian:debian_linux:9

Detection Method

Details: CPE Inventory OID: 1.3.6.1.4.1.25623.1.0.810002
Version used: 2019-03-19T13:31:53Z

Fig. 11.6: Detailed information about the vulnerability

Solution type Solution for the found vulnerability. The following the solutions are possible:

- A vendor patch is available.
- A workaround is available.
- A mitigation by configuration is available.
- No fix is and will be available.
- No solution exists.

Severity The severity of the vulnerability (CVSS, see Chapter *14.2.3* (page 354)) is displayed as a bar to support the analysis of the results.

QoD The quality of detection (QoD) is a value between 0 % and 100 % describing the reliability of the executed vulnerability detection or product detection.

By default, only results that were detected by VTs with a QoD of 70 % or higher are displayed. The filter can be adjusted to show results with a lower QoD (see Chapter *8.3.1* (page 167)).

For more information about the QoD see Chapter *11.2.6* (page 296).

Host Host for which the result was found. The IP address and the name of the host are displayed separately.

Location Port number and protocol type used to find the vulnerability on the host.

Created Date and time of the report creation.

11.2.1.2 Interpreting a Report

To interpret the results note the following information:

- **False Positives** False Pos. A false positive is a finding that describes a problem that does not really exist. Vulnerability scanners often find evidence that point at a vulnerability but a final judgment cannot be made. There are two options available:
  - Reporting of a potentially non-existent vulnerability (false positive).
  - Ignoring reporting of a potentially existing vulnerability (false negative).

  Since a user can identify, manage and as such deal with false positives compared to false negatives, the appliance's vulnerability scanner reports all potentially existing vulnerabilities. If the user knows that false positives exist an override can be configured (see Chapter *11.8* (page 307)).
- **Multiple findings can have the same cause.** If an especially old software package is installed, often multiple vulnerabilities exist. Each of these vulnerabilities is tested by an individual VT and causes an alert. The installation of a current package will remove a lot of vulnerabilities at once.
- **High** High **and Medium** Medium Findings of the severity levels *High* and *Medium* are most important and should be addressed with priority. Before addressing medium level findings, high level findings should get addressed. Only in exceptional cases this approach should be deviated from, e.g., if it is known that the high level findings need to be less considered because the service cannot be reached through the firewall.
- **Low** Low **and Log** Log Findings of the severity levels *Low* and *Log* are mostly interesting for detail understanding. These findings are filtered out by default but can hold very interesting information. Considering them will increase the security of the network and the systems. Often a deeper knowledge of the application is required for their understanding. Typical for a result with the severity *Log* is that a service uses a banner with its name and version number. This could be useful for an attacker when this version has a known vulnerability.

11.2.1.3 Filtering a Report

Since a report often contains a lot of findings, the complete report as well as only filtered results can be displayed and downloaded.

The report can be filtered as follows:

1. Click ✎ in the filter bar.
2. Enter a keyword which should be searched for in the input box *Filter* (see Fig. 11.7).
3. For *Apply Overrides* select the radio button *Yes* to enable overrides (see Chapter *11.8* (page 307)).

   For *Apply Overrides* select the radio button *No* to disable overrides.
4. Activate the checkbox *Only show hosts that have results* if only the hosts with results should be included.
5. For *QoD* select the desired QoD (see Chapter *11.2.6* (page 296)).
6. For *Severity (Class)* activate the checkboxes of the desired severity classes.
7. For *Solution Type* select the radio buttons of the desired solution types.

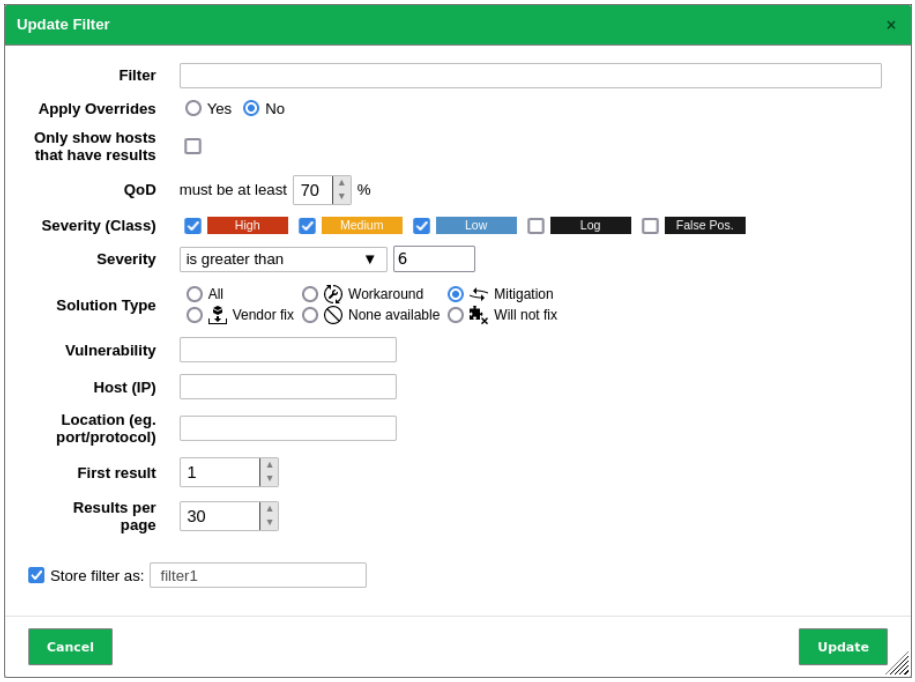


Fig. 11.7: Adjusting the filter for the report

8. Enter the (part of a) vulnerability's name, host or location in the according input box.
9. Click *Update*.

11.2.2 Exporting a Report

For supported export formats see Chapter *11.1* (page 283).

A report can be exported as follows:

1. Select *Scans* > *Reports* in the menu bar.
2. Click on the date of a report to open the details page of the report.
3. Click .

   → The scan report content composer is opened (see Fig. 11.8).

Note: The applied filter is displayed in the input box *Filter* and cannot be changed. For changing the filter see Chapter *11.2.1.3* (page 291).

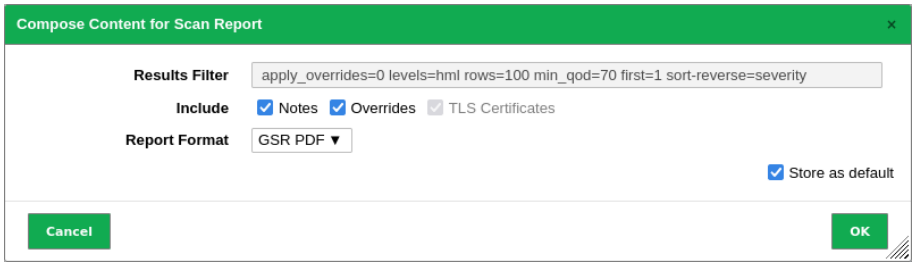


Fig. 11.8: Composing the content of a report export

4. Activate the checkbox *Notes* to include attached notes, and the checkbox *Overrides* to label enabled overrides and include their text field content.

   Note: Overrides are only considered if they are enabled when filtering the report (see Chapter *11.2.1.3* (page 291)).

5. Select the report format in the drop-down list *Report Format*.
6. Activate the checkbox *Store as default* to save the settings for future exports.
7. Click *OK*.
8. Save the report by clicking *Save File*.

11.2.3 Importing a Report

Reports can be imported to the appliance as follows:

1. Select *Scans* > *Reports* in the menu bar.
2. Click .
3. Click *Browse...* and select the XML file of a report (see Fig. 11.9).

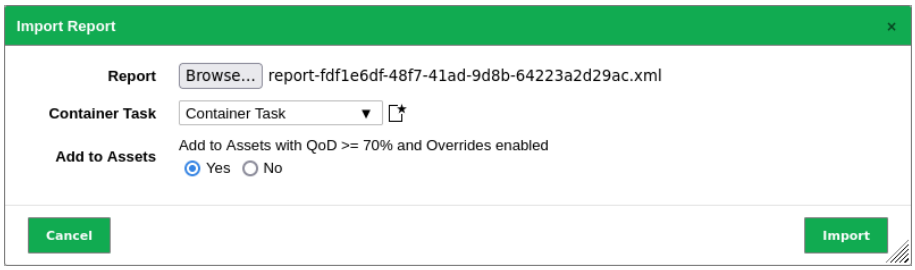


Fig. 11.9: Importing a report

4. Select the container task to which the report should be added in the drop-down list *Container Task*.

   Tip: By clicking a new container task can be created (see Chapter *10.5* (page 249)).

5. Select the radio button *Yes* to add the report to the assets.
6. Click *Import*.

11.2.4 Triggering an Alert for a Report

Often an alert includes the sending of a report. The report sent by an alert is subject to a filter defined in the alert content composer (see Chapter *10.12* (page 272)). Triggering an alert for a report adds a second filter originating from the scan report content composer (see Chapter *11.2.2* (page 292)).

The alert can be triggered manually as follows:

1. Select *Scans* > *Reports* in the menu bar.
2. Click on the date of a report to show the results.

3. Filter the report so that only the results that should be sent are displayed by using the Powerfilter (see Chapter *11.2.1.3* (page 291)) or selecting a register.

   Note: The filter that is configured in the alert content composer (see Chapter *10.12* (page 272)) is applied additionally.

   To mimic the behavior of this filter, adjust the filter of the report in a way that no results are filtered out.

4. Click ▷.

   → The scan report content composer is opened (see Fig. 11.8).

   Note: The applied filter for displaying the results is entered in the input box *Filter* and cannot be changed. For changing the filter see Chapter *11.2.1.3* (page 291).

5. Activate the checkbox *Notes* to include attached notes, and the checkbox *Overrides* to label enabled overrides and include their text field content.

   Note: Overrides are only considered if they are enabled when filtering the report (see Chapter *11.2.1.3* (page 291)).

6. Select the alert in the drop-down list *Alert*.

   Tip: A new alert can be created by clicking ☆. For the information to enter in the input boxes see Chapter *10.12* (page 272).

7. Activate the checkbox *Store as default* to save the settings for future sendings of the report.
8. Click *OK*.

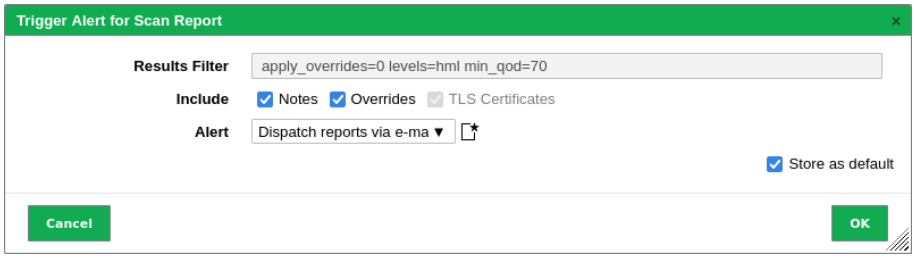


Fig. 11.10: Triggering an alert manually

11.2.5 Creating a Delta Report

If more than one report of a single task is available (see Chapter *11.2* (page 288)), a delta report can be created as follows:

1. Select *Scans* > *Tasks* in the menu bar.
2. Click on the total number of reports in the column *Reports*.

   → The page *Reports* is opened. A filter is applied to show only the reports for the selected task.

3. Select the newer report by clicking Δ in the column *Actions* of the respective report (see Fig. 11.11).

   → The icon Δ is grayed out for the selected report.

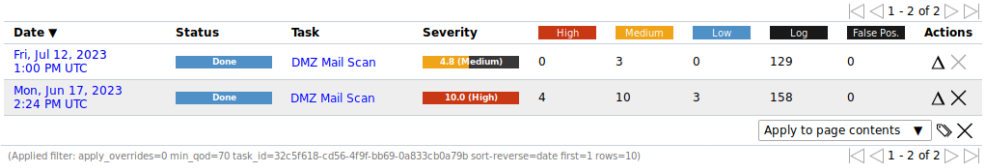


Fig. 11.11: Selecting the first report

4. Select the older report by clicking in the column *Actions* of the respective report (see Fig. 11.12).

   → The delta report with the delta results is displayed (see Fig. 11.13) and can be exported.

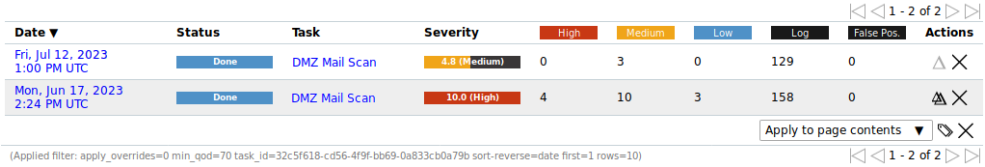


Fig. 11.12: Selecting the second report

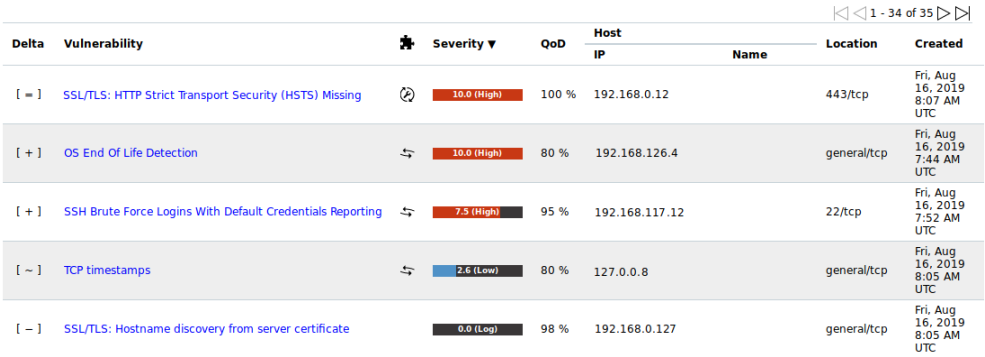


Fig. 11.13: Delta report with delta results

The type of the delta result is displayed in the column *Delta*. There are four types of delta results:

- **Gone *[–]*** The result exists in the second (older) report but not in the first (newer) report.
- **New *[+]*** The result exists in the first (newer) report but not in the second (older) report.
- **Same *[=]*** The result exists in both reports and is equal.
- **Changed *[~]*** The result exists in both reports but is different.

The term `delta_states=` can be entered into the filter bar to show only a specific type of delta results (see Chapter *8.3* (page 167)).

- `delta_states=g` shows all results of the type *Gone*.
- `delta_states=n` shows all results of the type *New*.
- `delta_states=s` shows all results of the type *Same*.
- `delta_states=c` shows all results of the type *Changed*.

Tip: Multiple types can be displayed at the same time, e.g., `delta_states=gs` shows all results of the type *Gone* and *Same*.

11.2.6 Quality of Detection Concept

The quality of detection (QoD) is a value between 0 % and 100 % describing the reliability of the executed vulnerability detection or product detection.

While the QoD range allows to express the quality quite fine-grained, most tests use a standard methodology. Therefore, QoD types are associate with a QoD value. The current list of types may be extended over time.

Note:

- The QoD of a “Detection” result is higher than that of an actual “Vulnerability” result as it reflects the quality of the product detection itself – which is reliable – and not the quality of the related vulnerability tests which may be unreliable for various reasons (see table).
- The lowest QoD that could apply is always used, for example in case of multiple detection methods (remote or local/authenticated).

QoD	QoD Type	Description
100 %	exploit	The detection happened via an exploit and is therefore fully verified.
99 %	remote_vul	Remote active checks (code execution, traversal attack, SQL injection etc.) in which the response clearly shows the presence of the vulnerability.
98 %	remote_app	Remote active checks (code execution, traversal attack, SQL injection etc.) in which the response clearly shows the presence of the vulnerable application.
97 %	package	Authenticated package-based checks for, e.g., Linux(oid) systems.
97 %	registry	Authenticated registry based checks for Microsoft Windows systems.
95 %	remote_active	Remote active checks (code execution, traversal attack, SQL injection etc.) in which the response shows the likely presence of the vulnerable application or of the vulnerability. “Likely” means that only rare circumstances are possible in which the detection would be wrong.
80 %	remote_banner	Remote banner checks of applications that offer patch level in version. Many proprietary products do so.
80 %	executable_version	Authenticated executable version checks for Linux(oid) or Microsoft Windows systems where applications offer patch level in version.
75 %		If results without any QoD information are processed (e.g., when migrating data from a legacy system to a currently supported system), they are assigned this value.
70 %	remote_analysis	Remote checks that perform some analysis, but may not always be completely reliable depending on environmental conditions. Narrowing down suspected false-positive or false-negative edge cases may require analysis by the user (see Chapter *11.8* (page 307)).

QoD	QoD Type	Description
50 %	remote_probe	Remote checks in which intermediate systems such as firewalls may pretend correct detection so that it is actually not clear whether the application itself answered. For example, this can happen for non-TLS connections.
30 %	remote_banner_unreliable	Remote banner checks of applications that do not offer patch level in version identification. For example, this is the case for many open-source products due to backport patches.
30 %	executable_version_unreliable	Authenticated executable version checks for Linux(oid) systems where applications do not offer patch level in version identification.
30 %	package_unreliable	Authenticated package-based checks which are not always fully reliable for, e.g., Linux(oid) systems.
1 %	general_note	General note on potential vulnerability without finding any present application.

By default, only results that were detected by VTs with a QoD of 70 % or higher are displayed. Results detected by a test with a lower QoD are prone to false positives. The filter can be adjusted to show results with a lower QoD (see Chapter *8.3.1* (page 167)).

Note: When changing the default filter to show results detected by a test with a low QoD, it is one's own responsibility to determine if it is a false positive.

11.3 Displaying all Existing Results

List Page

While the reports only contain the results of one single scan, all results are saved in the internal database and can be viewed by selecting *Scans* > *Results* in the menu bar.

Powerfilters can be used to display only interesting results (see Chapter *8.3* (page 167)).

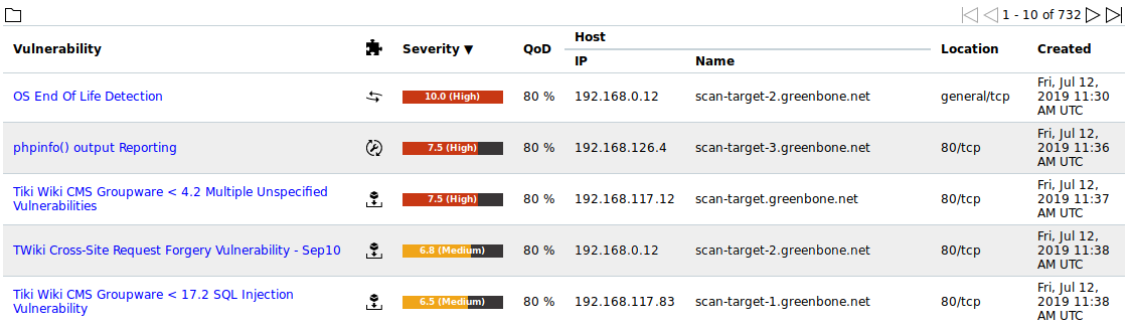


Fig. 11.14: Page *Results* showing all results of all scans

For all results the following information is displayed:

Vulnerability Name of the found vulnerability.

Vulnerabilities with an attached note are marked with . Vulnerabilities with an attached ticket are marked with .

Note: If the column of the vulnerability still appears empty the respective VT has not been updated yet.

Note: Even though the results contain a lot of information, external references are always listed in the details.

These refer to webpages on which the vulnerability was already discussed.

Additional background information is available such as who discovered the vulnerability, what effects it could have and how it can be remediated.

Solution type To simplify the elimination of vulnerabilities every result offers a solution for problems. The column *Solution type* displays the existence of a solution. The following the solutions are possible:

- A vendor patch is available.
- A workaround is available.
- A mitigation by configuration is available.
- No fix is and will be available.
- No solution exists.

Severity Severity of the vulnerability. The severity of the vulnerability (CVSS, see Chapter *14.2.3* (page 354)) is displayed as a bar to support the analysis of the results.

QoD The quality of detection (QoD) is a value between 0 % and 100 % describing the reliability of the executed vulnerability detection or product detection.

By default, only results that were detected by VTs with a QoD of 70 % or higher are displayed. The filter can be adjusted to show results with a lower QoD (see Chapter *8.3.1* (page 167)).

For more information about the QoD see Chapter *11.2.6* (page 296).

Host Host for which the result was found. The IP address and the name of the host are displayed separately.

Location Port number and protocol type used to find the result on the host.

Created Date and time of the report creation.

Note: By clicking below the list of results more than one result can be exported at a time. The drop-down list is used to select which results exported.

Details Page

Click on the name of a result to display the details of the result. Click to open the details page of the result.

The following registers are available:

Information General information about the result.

User Tags Assigned tags (see Chapter *8.4* (page 174)).

The following actions are available in the upper left corner:

- Open the corresponding chapter of the user manual.

- Show the list page of all results.
- Export the result as an XML file.
- Create a new note for the result (see Chapter *11.7.1* (page 305)).
- Create a new override for the result (see Chapter *11.8.1* (page 307)).
- Create a new ticket for the result (see Chapter *11.6.1* (page 301)).
- Show the corresponding task.
- Show the corresponding report.

11.4 Displaying all Existing Vulnerabilities

List Page

While the reports only contain the vulnerabilities of one single scan, all vulnerabilities are saved in the internal database and can be viewed by selecting *Scans* > *Vulnerabilities* in the menu bar.

Powerfilters can be used to display only interesting vulnerabilities (see Chapter *8.3* (page 167)).

1 - 10 of 60

Name	Oldest Result	Newest Result	Severity ▼	QoD	Results	Hosts
SMB NativeLanMan	Fri, Jul 12, 2019 11:38 AM UTC	Fri, Jul 12, 2019 11:38 AM UTC	10.0 (High)	80 %	1	1
OS End Of Life Detection	Fri, Jul 12, 2019 11:30 AM UTC	Fri, Jul 12, 2019 11:30 AM UTC	10.0 (High)	80 %	1	1
Tiki Wiki CMS Groupware < 4.2 Multiple Unspecified Vulnerabilities	Fri, Jul 12, 2019 11:37 AM UTC	Fri, Jul 12, 2019 11:37 AM UTC	7.5 (High)	80 %	1	1
phpinfo() output Reporting	Fri, Jul 12, 2019 11:36 AM UTC	Fri, Jul 12, 2019 11:36 AM UTC	7.5 (High)	80 %	1	1
TWiki Cross-Site Request Forgery Vulnerability - Sep10	Fri, Jul 12, 2019 11:38 AM UTC	Fri, Jul 12, 2019 11:38 AM UTC	6.8 (Medium)	80 %	1	1
Tiki Wiki CMS Groupware < 17.2 SQL Injection Vulnerability	Fri, Jul 12, 2019 11:38 AM UTC	Fri, Jul 12, 2019 11:38 AM UTC	6.5 (Medium)	80 %	1	1
TWiki Cross-Site Request Forgery Vulnerability	Fri, Jul 12, 2019 11:38 AM UTC	Fri, Jul 12, 2019 11:38 AM UTC	6.0 (Medium)	80 %	1	1
Tiki Wiki CMS Groupware 'fixedURLData' Local File Inclusion Vulnerability	Fri, Jul 12, 2019 11:38 AM UTC	Fri, Jul 12, 2019 11:38 AM UTC	5.0 (Medium)	80 %	1	1
Tiki Wiki CMS Groupware Input Sanitation Weakness Vulnerability	Fri, Jul 12, 2019 11:37 AM UTC	Fri, Jul 12, 2019 11:37 AM UTC	5.0 (Medium)	80 %	1	1
Cleartext Transmission of Sensitive Information via HTTP	Fri, Jul 12, 2019 11:19 AM UTC	Fri, Jul 12, 2019 1:04 PM UTC	4.8 (Medium)	80 %	6	3

Fig. 11.15: Page *Vulnerabilities* showing all vulnerabilities of all scans

For all vulnerabilities the following information is displayed:

Name Title of the vulnerability.

Oldest Result Date and time of the oldest result that was found for the vulnerability.

Newest Result Date and time of the newest result that was found for the vulnerability.

Severity Severity of the vulnerability. To support the administrator with the analysis of the results, the severity of a vulnerability (CVSS, see also Chapter *14.2.3* (page 354)) is displayed as a bar.

QoD The quality of detection (QoD) is a value between 0 % and 100 % describing the reliability of the executed vulnerability detection or product detection.

By default, only results that were detected by VTs with a QoD of 70 % or higher are displayed. The filter can be adjusted to show results with a lower QoD (see Chapter *8.3.1* (page 167)).

For more information about the QoD see Chapter *11.2.6* (page 296).

Results Number of results found for this vulnerability. By clicking on the number of results the page *Results* is opened. A filter is applied to show only the results for the selected vulnerability.

Note: By clicking below the list of results more than one result can be exported at a time. The drop-down list is used to select which results exported.

Details Page

Click on the name of a vulnerability to open the details page of the vulnerability.

The following actions are available in the upper left corner:

- Open the corresponding chapter of the user manual.
- Show the list page of all vulnerabilities.
- Export the vulnerability as an XML file.
- Create a new note for the vulnerability (see Chapter *11.7.1* (page 305)).
- Create a new override for the vulnerability (see Chapter *11.8.1* (page 307)).
- Show the corresponding results.
- Show the corresponding vulnerability.

11.5 Trend of Vulnerabilities

If a task has been run multiple times the trend of discovered vulnerabilities is displayed on the page *Tasks* (see Fig. 11.16).

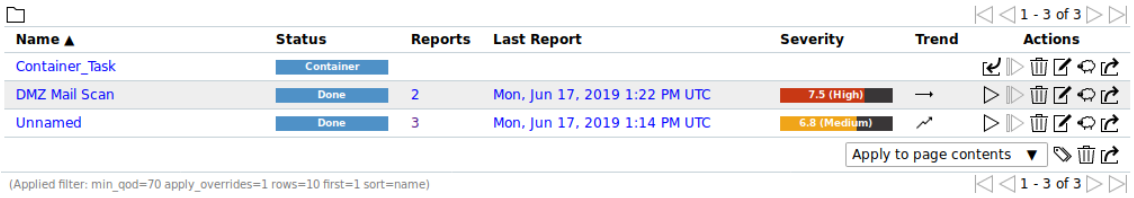


Fig. 11.16: Task with trend

To get there select *Scans* > *Tasks* in the menu bar.

The trend describes the change of vulnerabilities between the newest and the second newest report. It is displayed in the column *Trend*.

The following trends are possible:

- In the newest report the highest severity is higher than the highest severity in the second newest report.
- The highest severity is the same for both reports. However, the newest report contains more security issues of this severity than the second newest report.
- The highest severity and the amount of security issues are the same for both reports.
- The highest severity is the same for both reports. However, the newest report contains less security issues of this severity than the second newest report.
- In the newest report the highest severity is lower than the highest severity in the second newest report.

11.6 Using Tickets

Users can task other users or themselves to resolve findings of a scan.

Note: When creating a ticket for another user, that user gets read and write access to the ticket. Additionally, the user automatically gets read access to the respective task and to its reports and results.

If the assignment of a ticket is withdrawn from a user, the read access to the task and the reports remains. The permissions for a task can be checked and revoked on a task's details page (see Chapter *10.8* (page 254)). If multiple tickets are created for results of the same report and assigned to the same user, the same permission will appear multiple times.

If the assignee of a ticket is changed, the new assignee does not automatically get read access to the task. Instead, the ticket owner must edit the permissions via the task's details page (see Chapter *10.8* (page 254)) and grant read access to the new assignee.

11.6.1 Creating a Ticket

A ticket can be created as follows:

1. Select *Scans* > *Reports* in the menu bar and click on the date of a report to show the results.
2. Click on an item in the column *Vulnerability* and to open the details page of the result.

   or

1. Select *Scans* > *Results* in the menu bar.
2. Click on an item in the column *Vulnerability* and to open the details page of the result.
3. Create a new ticket by clicking .
4. Select the user to whom the ticket should be assigned in the drop-down list *Assign to User* (see Fig. 11.17).
5. Enter a note for the ticket in the input box *Note*.

Fig. 11.17: Creating a new ticket

6. Click *Save*.

   → The number of tickets for a result are displayed in the upper left corner of the details page of the result (see Fig. 11.18). By clicking the corresponding tickets are displayed.

Fig. 11.18: Number of assigned tickets

11.6.2 Changing the Status of a Ticket

A ticket can have the following status:

- Open: the vulnerability has not been fixed yet.
- Fixed: the vulnerability has been fixed.
- Fixed verified: the task has been run again and the vulnerability was not found anymore. This status is set automatically.
- Closed: the fix of the vulnerability was verified or the ticket is not required anymore.

The status of a ticket can be changed as follows:

1. Select *Resilience* > *Remediation Tickets* in the menu bar.
2. In the row of the ticket, click .
3. Select the new status in the drop-down list *Status* (see Fig. 11.19).
4. Select the user to whom the ticket with the new status should be assigned in the drop-down list *Assigned User*.
5. Enter a note for the new status in the respective input box.

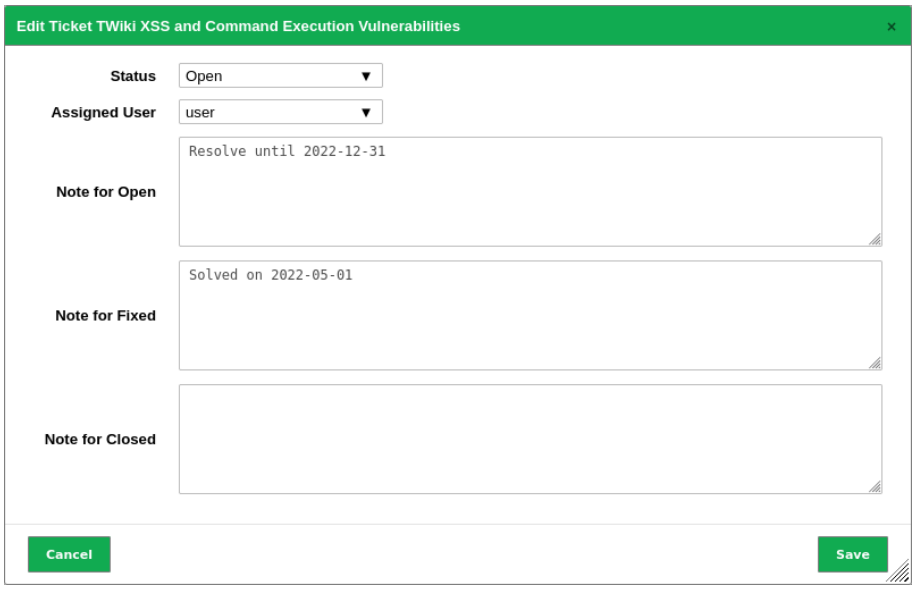


Fig. 11.19: Changing the status of a ticket

6. Click *Save*.

11.6.3 Setting an Alert for a Ticket

Alerts for tickets can be set for the following events:

- A new ticket is received.
- The status of an assigned ticket changed.
- The status of an own ticket changed.

An alert for tickets is set up as follows:

1. Select *Configuration > Alerts* in the menu bar.
2. Create a new alert by clicking .
3. Define the alert (see Fig. 11.20).
4. Click *Save*.

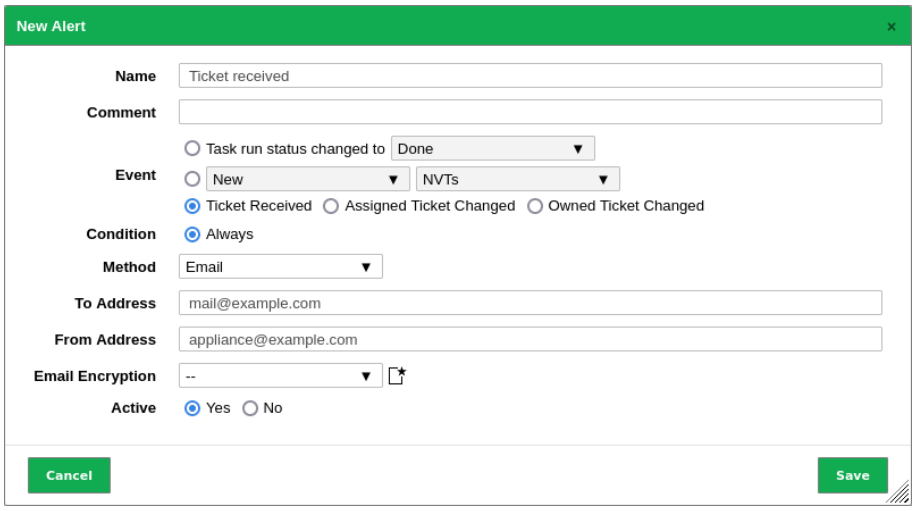


Fig. 11.20: Setting an alert for a ticket

The following details of the alert can be defined:

Name Definition of the name. The name can be chosen freely.

Comment An optional comment can contain additional information.

Event Select *Ticket Received* if an alert should be sent when a new ticket is assigned to oneself.

Select *Assigned Ticket Changed* if an alert should be sent when the status of a ticket assigned to oneself changes.

Select *Owned Ticket Changed* if an alert should be sent when the status of ticket assigned to another user changes.

Method Selection of the method for the alert. Only one method per alert can be chosen.

If different alerts for the same event should be triggered, multiple alerts must be created and linked to the same task.

The following methods are possible:

Email An e-mail is sent to the given address.

The transmission of the e-mail can by encrypted using a configurable S/MIME or GPG key. The encryption can be selected in the drop-down list *Email Encryption* or created by clicking .

Start Task The alert can start an additional task. The task is selected in the drop-down list *Start Task*.

System Logger The alert is sent to a Syslog daemon.

The Syslog server is defined using the console (see Chapter *7.2.12* (page 133)).

11.6.4 Managing Tickets

List Page

All existing tickets can be displayed by selecting *Resilience* > *Remediation Tickets* in the menu bar.

For all tickets the following information is displayed:

Vulnerability Vulnerability for which the ticket is created.

Severity Severity of the vulnerability for which the ticket is created.

Host Host on which the vulnerability was found.

Solution Type Solution type of the vulnerability for which the ticket is created.

Assigned User User to which the ticket is assigned.

Modification Time Date and time of the last modification of the ticket.

Status Status of the ticket.

For all tickets the following actions are available:

- Move the ticket to the trashcan. Only the owner may move a ticket to the trashcan.
- Edit the ticket.
- Clone the ticket.

Note: By clicking or below the list of tickets more than one ticket can be moved to the trashcan or exported at a time. The drop-down list is used to select which tickets are moved to the trashcan or exported.

Details Page

Click on the name of a ticket to display the details of the ticket. Click to open the details page of the ticket.

The following registers are available:

Information General information about the ticket.

User Tags Assigned tags (see Chapter *8.4* (page 174)).

The following actions are available in the upper left corner:

- Open the corresponding chapter of the user manual.
- Show the list page of all tickets.
- Clone the ticket.
- Edit the ticket.
- Move the ticket to the trashcan. Only the owner may move a ticket to the trashcan.
- Export the ticket as an XML file.

11.7 Using Notes

Notes allow adding comments to a VT and are displayed in the reports as well. A note can be added to a specific result, task, severity, port or host and as such will only appear in specific reports. A note can be generalized as well so that it will be displayed in all reports.

11.7.1 Creating a Note

11.7.1.1 Creating a Note Through a Scan Result

Notes can be created in different ways. The simplest way is through the respective scan result in a report:

1. Select *Scans* > *Reports* in the menu bar.
2. Click on the date of the report to show the results.
3. Select the register *Results*.
4. Click on a result in the column *Vulnerability*.
5. Click to to open the details page of the result.
6. Click in the upper left corner of the page.
7. Define the note (see Fig. 11.21).

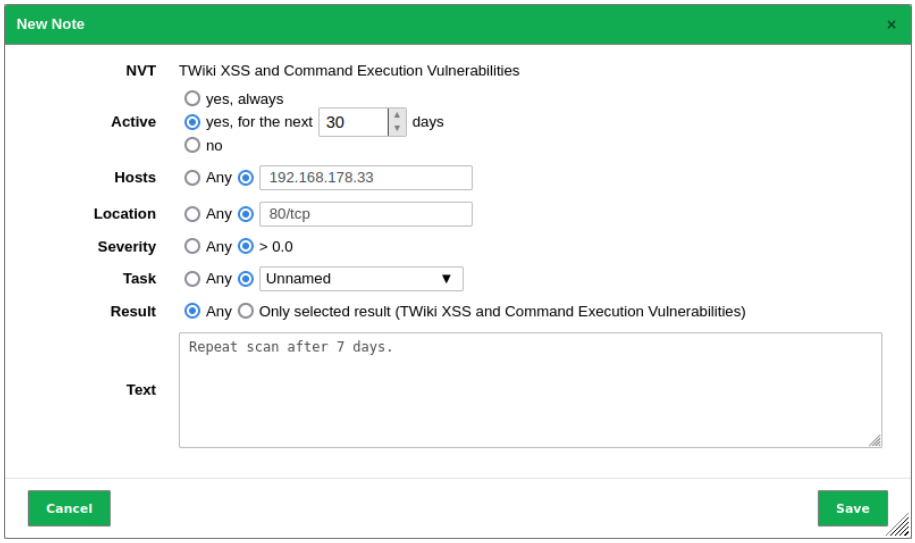


Fig. 11.21: Creating a new note

8. Click *Save*.

   → The note is displayed on the details page of the result (see Fig. 11.22).

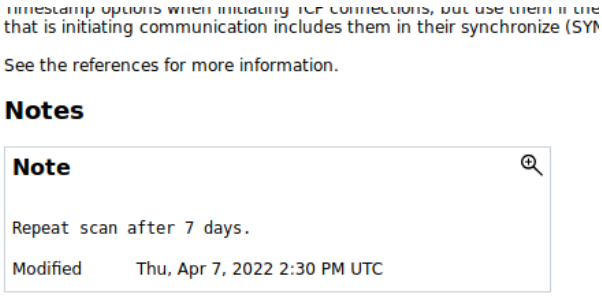


Fig. 11.22: Report containing a note

11.7.1.2 Creating a Note on the Page *Notes*

Notes can be created on the page *Notes* as well:

1. Select *Scans* > *Notes* in the menu bar.
2. Create a new note by clicking .
3. Enter the ID of the VT in the input box *NVT OID*.
4. Define the note.

Tip: It is possible to enter ranges of IP addresses and CIDR blocks in the input box *Hosts*. In that way, notes for entire subnets can be created without having to specify every host in a comma-separated list.

Notes can be generalized by selecting the radio button *Any* for hosts, locations, severities, tasks or results.

---

5. Click *Save*.

11.7.2 Managing Notes

List Page

All existing notes can be displayed by selecting *Scans* > *Notes* in the menu bar (see Fig. 11.23).

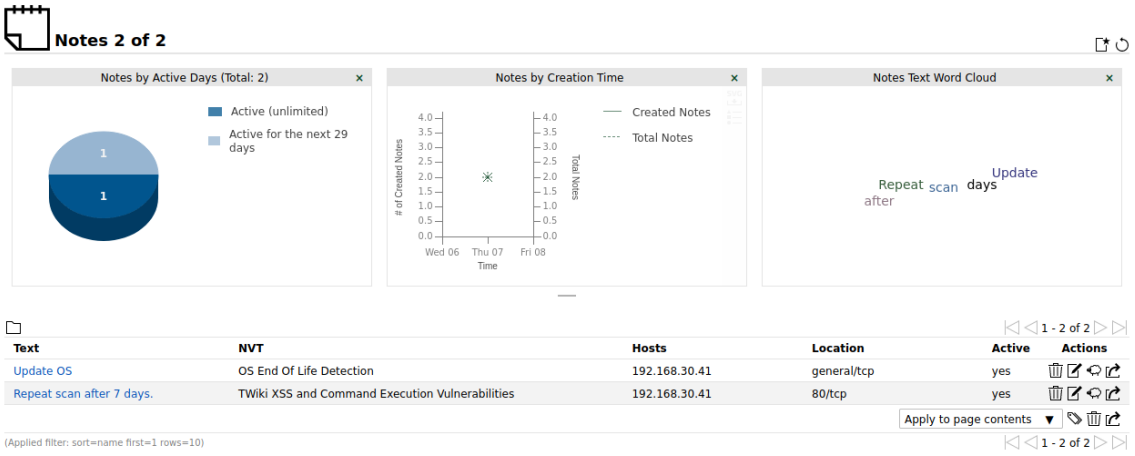


Fig. 11.23: Managing notes

For all notes the following actions are available:

- Move the note to the trashcan.
- Edit the note.
- Clone the note.
- Export the note as an XML file.

Note: By clicking or below the list of notes more than one note can be moved to the trashcan or exported at a time. The drop-down list is used to select which notes are moved to the trashcan or exported.

Details Page

Click on the name of a note to display the details of the note. Click to open the details page of the note.

The following registers are available:

Information General information about the note.

User Tags Assigned tags (see Chapter *8.4* (page 174)).

Permissions Assigned permissions (see Chapter *9.4* (page 193)).

The following actions are available in the upper left corner:

- Open the corresponding chapter of the user manual.
- Show the list page of all notes.
- Create a new note (see Chapter *11.7.1* (page 305)).
- Clone the note.
- Edit the note.
- Move the note to the trashcan.
- Export the note as an XML file.

11.8 Using Overrides and False Positives

The severity of a result can be modified. This is called override.

Overrides are especially useful to manage results that are detected as a false positive and that have been given a critical severity but should be given a different severity in the future.

The same applies to results that only have been given the severity *Log* but should be assigned a higher severity locally. This can be managed with an override as well.

Overrides are also used to manage acceptable risks.

11.8.1 Creating an Override

11.8.1.1 Creating an Override Through a Scan Result

Overrides can be created in different ways. The simplest way is through the respective scan result in a report:

1. Select *Scans* > *Reports* in the menu bar.
2. Click on the date of the report to show the results.

3. Select the register *Results*.
4. Click on a result in the column *Vulnerability*.
5. Click to to open the details page of the result.
6. Click in the upper left corner of the page.
7. Define the override. Select the new severity in the drop-down list *New Severity* (see Fig. 11.24).

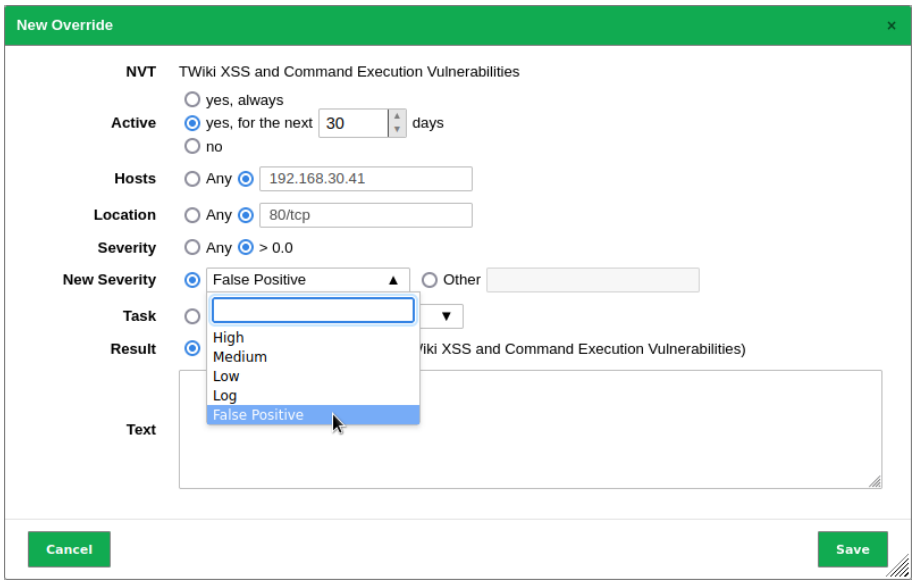


Fig. 11.24: Creating a new override

8. Click *Save*.

The following information can be entered:

Note: If an override is created through a scan result, some settings are already filled in.

NVT VT for which the override is applied.

Active Selection whether the override should be activated. An activation for an arbitrary number of days is possible as well.

Hosts Host or range of hosts for which the result must be found for the override to apply.

Tip: It is possible to enter ranges of IP addresses and CIDR blocks. In that way, overrides for entire subnets can be created without having to specify every host in a comma-separated list.

Host ranges are specified with a minus, e.g. `198.168.1.1-198.168.1.25`. A range bigger than 4096 is not supported.

Note: Conflicting overrides, e.g. an override for a host range and another override for a host inside that range, are not permitted.

Location Port for which the result must be found for the override to apply. Only a specific port or the setting *Any* are supported per override. A specific port must be supplied as a number followed by `/tcp` or `/udp`.

Severity Range of severity of the VT for which the overrides should be applied.

New Severity Severity the VT should have after the override is applied.

Task Selection of tasks for which the override should be applied.

Result Selection of results for which the override should be applied.

Note: The radio button *Any* has to be selected if the override should be applied to reports in the future.

Text A text describes the override in more detail.

Note: If several overrides apply to the same VT in the same report the most recent override is used and applied.

11.8.1.2 Creating an Override on the Page *Overrides*

Overrides can be created on the page *Overrides* as well:

1. Select *Scans* > *Overrides* in the menu bar.
2. Create a new override by clicking .
3. Enter the ID of the VT in the input box *NVT OID*.
4. Define the override.

Note: For the information to enter in the input boxes see Chapter *11.8.1.1* (page 307).

5. Select the new severity in the drop-down list *New Severity*.
6. Click *Save*.

11.8.2 Managing Overrides

List Page

All existing overrides can be displayed by selecting *Scans* > *Overrides* in the menu bar.

For all overrides the following actions are available:

- Move the override to the trashcan.
- Edit the override.
- Clone the override.
- Export the override as an XML file.

Note: By clicking or below the list of overrides more than one override can be moved to the trashcan or exported at a time. The drop-down list is used to select which overrides are moved to the trashcan or exported.

Details Page

Click on the name of an override to display the details of the override. Click to open the details page of the override.

The following registers are available:

Information General information about the override.

User Tags Assigned tags (see Chapter *8.4* (page 174)).

Permissions Assigned permissions (see Chapter *9.4* (page 193)).

The following actions are available in the upper left corner:

- Open the corresponding chapter of the user manual.
- Show the list page of all overrides.
- Create a new override (see Chapter *11.8.1* (page 307)).
- Clone the override.
- Edit the override.
- Move the override to the trashcan.
- Export the override as an XML file.

11.8.3 Disabling and Enabling Overrides

If overrides change the display of the results, the overrides can be enabled or disabled.

This is done by setting the filter as follows:

1. Click in the filter bar.
2. For *Apply Overrides* select the radio button *Yes* to enable overrides.

   For *Apply Overrides* select the radio button *No* to disable overrides.
3. Click *Update*.

Tip: Overrides can be labelled in exported reports (see Chapter *11.2.2* (page 292)).

CHAPTER 12

Performing Compliance Scans and Special Scans

In information technology, compliance is the most important approach for organizations to protect and secure their information and assets.

Information security organizations and associations such as the Information Systems Audit and Control Association (ISACA) or the Center for Internet Security (CIS) publish IT security standards, frameworks and guidelines. Those require organizations to implement appropriate security measures to protect themselves and their information assets from attacks.

Vulnerability assessment systems such as the Greenbone Enterprise Appliance can assist in evaluating the IT security arrangements by performing audits based on policies.

The Chapters *12.4* (page 322), *12.5* (page 335) and *12.6* (page 339) show some examples for policy audits.

Note: Since the goal of most audits is to verify local security configurations on the target systems, it is generally and in case of doubt recommended to perform authenticated audits (see Chapter *10.3.2* (page 219)). Exceptions exist for audits that only check externally available services, e.g., SSL/TLS.

12.1 Configuring and Managing Policies

Policies are scan configurations with the flag *policy*.

All default policies by Greenbone are data objects that are distributed via the feed. They are downloaded and updated with each feed update.

If no default policies are available, a feed update may be necessary, or the Feed Import Owner may need to be set (see Chapter *7.2.1.10.1* (page 81)).

Default policies cannot be edited. Furthermore, they can only be deleted temporarily by the Feed Import Owner or by a super administrator. During the next feed update, they will be downloaded again.

Note: To permanently delete a default policy, the Feed Import Owner has to delete it. Afterwards the Feed Import Owner has to be changed to *(Unset)* (see Chapter *7.2.1.10.1* (page 81)).

In addition to the default policies, custom policies can be created (see Chapter *12.1.1* (page 312)) or imported (see Chapter *12.1.2* (page 315)).

12.1.1 Creating a Policy

A new policy can be created as follows:

1. Select *Resilience* > *Compliance Policies* in the menu bar.
2. Create a new policy by clicking .

   Note: Alternatively, a policy can be imported (see Chapter *12.1.2* (page 315)).

   ---

3. Enter the name of the policy in the input box *Name* (see Fig. 12.1).

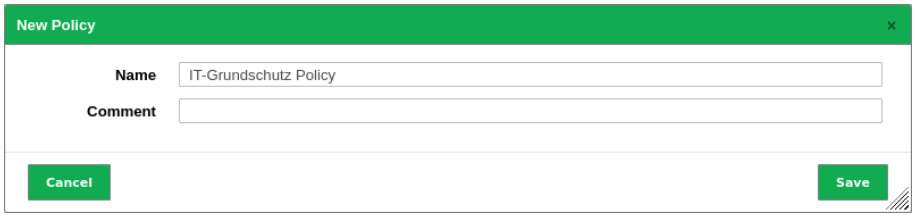


Fig. 12.1: Creating a new policy

4. Click *Save*.

   → The policy is created and displayed on the page *Policies*.

5. In the row of the policy, click .
6. In the sections *Edit Network Vulnerability Test Families* select the radio button if newly introduced VT families should be included and activated automatically (see Fig. 12.2).
7. In the section *Edit Network Vulnerability Test Families* activate the checkboxes in the column *Select all NVTs* if all VTs of a family should be activated.

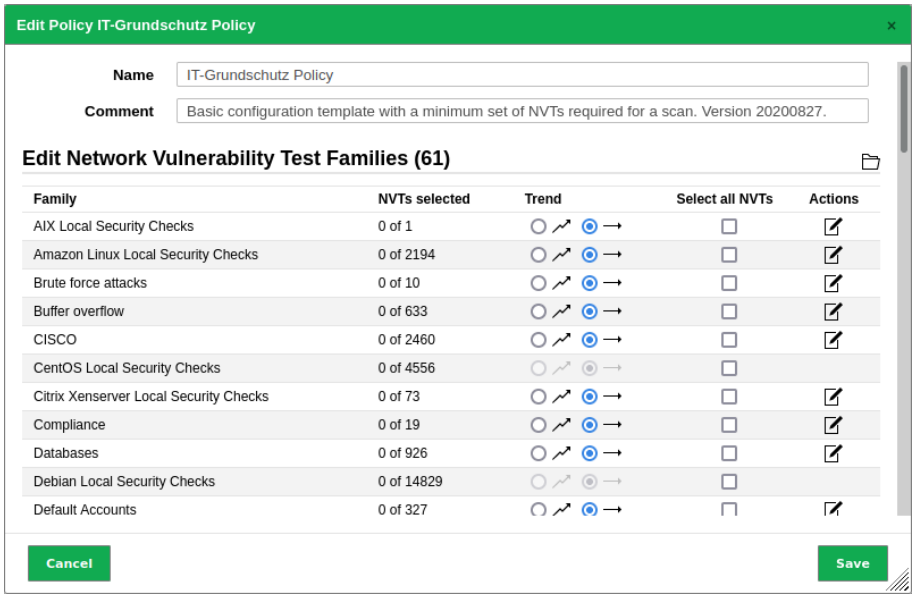


Fig. 12.2: Editing the new policy

8. Click for a VT family to edit it (see Fig. 12.3).

Note: The following VT families cannot be edited:

- CentOS Local Security Checks
- Debian Local Security Checks
- Fedora Local Security Checks
- Huawei EulerOS Local Security Checks
- Oracle Linux Local Security Checks
- Red Hat Local Security Checks
- SuSE Local Security Checks
- Ubuntu Local Security Checks

9. In the column *Selected* activate the checkboxes of the VTs that should be activated.
10. Click for a VT to edit it (see Fig. 12.4).

Note: If system-specific VTs of the VT family *Policy* are used (e.g., beginning with “Linux”, “Microsoft Windows”, “Microsoft Office”), the radio button *Yes* has to be selected for *Verbose Policy Controls* in the VT *Compliance Tests* (VT family *Compliance*).

Note: If editing the VT includes uploading a text file, the file should use UTF-8 text encoding.

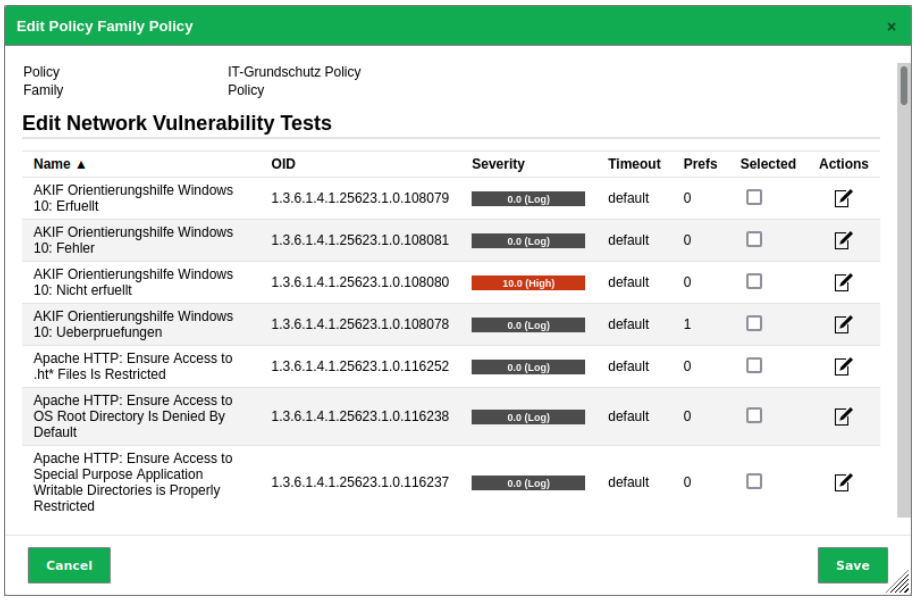


Fig. 12.3: Editing a family of VTs

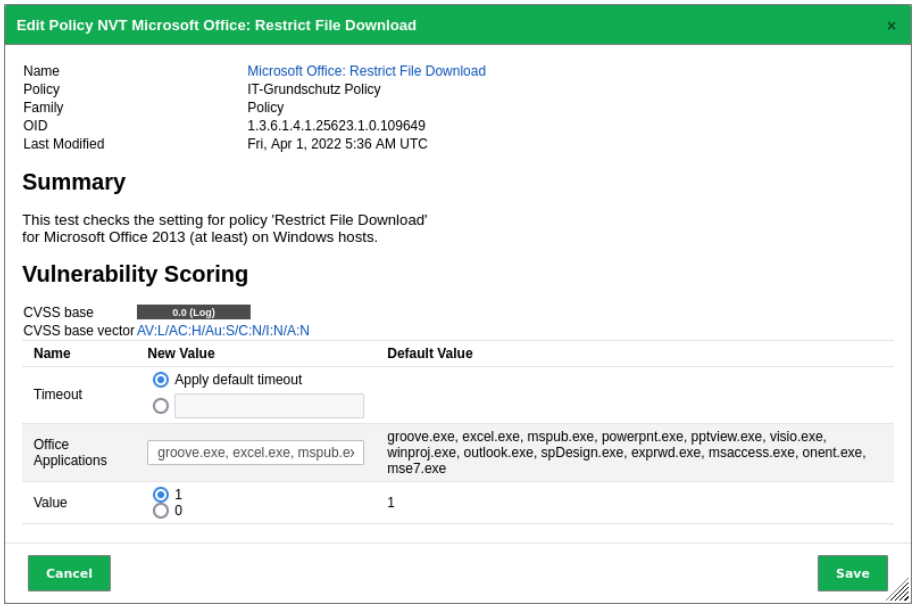


Fig. 12.4: Editing a VT

11. Click *Save* to save the VT.
12. Click *Save* to save the family of VTs.
13. Optional: edit scanner preferences (see Chapter *10.9.4* (page 263)).
14. Optional: edit VT preferences (see Chapter *10.9.5* (page 265)).
15. Click *Save* to save the policy.

12.1.2 Importing a Policy

A policy can be imported as follows:

1. Select *Resilience* > *Compliance Policies* in the menu bar.
2. Click .
3. Click *Browse...* and select the XML file of the policy (see Fig. 12.5).

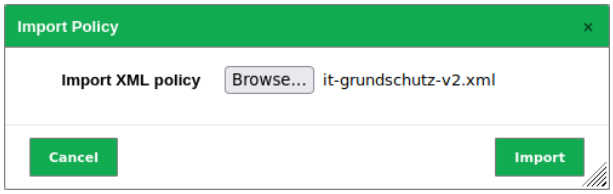


Fig. 12.5: Importing a policy

4. Click *Import*.

Note: If the name of the imported policy already exists, a numeric suffix is added to the name.

→ The imported policy is displayed on the page *Policies*.

5. Execute steps 5 to 15 of Chapter *12.1.1* (page 312) to edit the policy.

12.1.3 Managing Policies

List Page

All existing policies can be displayed by selecting *Resilience* > *Compliance Policies* in the menu bar (see Fig. 12.6).

For all policies the following information is displayed:

Name Name of the policy.

For all policies the following actions are available:

- Move the policy to the trashcan. Only policies which are currently not used can be moved to the trashcan. As long as the policy is not deleted from the trashcan, it is not downloaded anew during the next feed update.
- Edit the policy. Only self-created policies which are currently not used can be edited.
- Clone the policy.
- Create a new audit for the policy (see Chapter *12.2.1.2* (page 318)).
- Export the policy as an XML file.

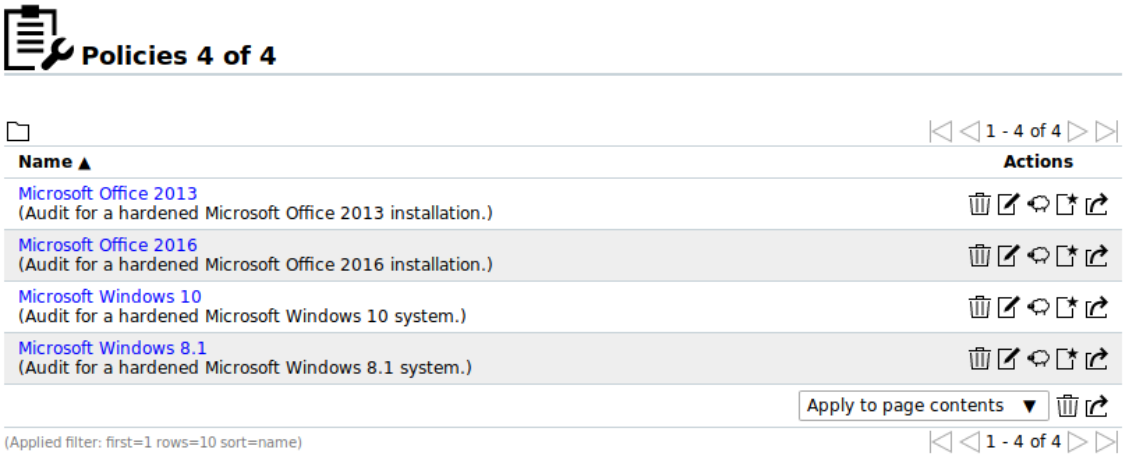


Fig. 12.6: Page *Policies* displaying all available policies

Note: By clicking or below the list of policies more than one policy can be moved to the trashcan or exported at a time. The drop-down list is used to select which policies are moved to the trashcan or exported.

Details Page

Click on the name of a policy to display the details of the policy. Click to open the details page of policy.

The following registers are available:

Information General information about the policy.

Scanner Preferences All scanner preferences for the policy with current and default values.

NVT Families All VT families for the policy with the number of activated VTs and the trend.

NVT Preferences All VT preferences for the policy.

Permissions Assigned permissions (see Chapter *9.4* (page 193)).

The following actions are available in the upper left corner:

- Open the corresponding chapter of the user manual.
- Show the list page of all policies.
- Create a new policy (see Chapter *12.1.1* (page 312)).
- Clone the policy.
- Edit the policy. Only self-created policies which are currently not used can be edited.
- Move the policy to the trashcan. Only policies which are currently not used can be moved to the trashcan. As long as the policy is not deleted from the trashcan, it is not downloaded anew during the next feed update.
- Export the policy as an XML file.
- Import a policy (see Chapter *12.1.2* (page 315)).

12.2 Configuring and Managing Audits

Audits are scan tasks with the flag *audit*.

12.2.1 Creating an Audit

12.2.1.1 Creating an Audit on the Page *Audits*

An audit can be created on the page *Audits* as follows:

1. Select *Resilience > Compliance Audits* in the menu bar.
2. Create an audit by clicking .
3. Define the audit (see Fig. 12.7).
4. Click *Save*.

   → The audit is created and displayed on the page *Audits*.

The following information can be entered:

Name The name can be chosen freely. A descriptive name should be chosen if possible.

Comment The optional comment allows for the entry of background information. It simplifies understanding the configured audit later.

Scan Targets Select a previously configured target from the drop-down list (see Chapter *10.2.1* (page 212)).

Additionally, the target can be created on the fly by clicking next to the drop-down list.

Alerts Select a previously configured alert from the drop-down list (see Chapter *10.12* (page 272)). Status changes of an audit can be communicated via e-mail, Syslog, HTTP or a connector.

Additionally, an alert can be created on the fly by clicking next to drop-down list.

Schedule Select a previously configured schedule from the drop-down list (see Chapter *10.10* (page 268)). The audit can be run once or repeatedly at a predetermined time, e.g., every Monday morning at 6:00 am.

Additionally, a schedule can be created on the fly by clicking next to the drop-down list.

Add results to Assets Selecting this option will make the systems available to the appliance's asset management automatically (see Chapter *13* (page 341)). This selection can be changed at a later point as well.

Alterable Audit Allow for modification of the audits's scan target(s) and scanner, even if reports were already created. The consistency between reports can no longer be guaranteed if audits are altered.

Auto Delete Reports This option may automatically delete old reports. The maximum number of reports to store can be configured. If the maximum is exceeded, the oldest report is automatically deleted. The factory setting is *Do not automatically delete reports*.

Policy The appliance comes with several pre-configured policies. Only one policy can be configured per audit.

Order for target hosts Select in which order the specified target hosts are processed during vulnerability tests. Available options are:

- Sequential
- Random
- Reverse

In order to improve the scan progress estimation, the setting *Random* is recommended (see Chapter *17.2.3* (page 383)).

This setting does not affect the alive test during which active hosts in a target network are identified. The alive test is always random.

Maximum concurrently executed NVTs per host/Maximum concurrently scanned hosts Select the speed of the scan on one host. The default values are chosen sensibly. If more VTs run simultaneously on a system or more systems are scanned at the same time, the scan may have a negative impact on either the performance of the scanned systems, the network or the appliance itself. These values “maxhosts” and “maxchecks” may be tweaked.

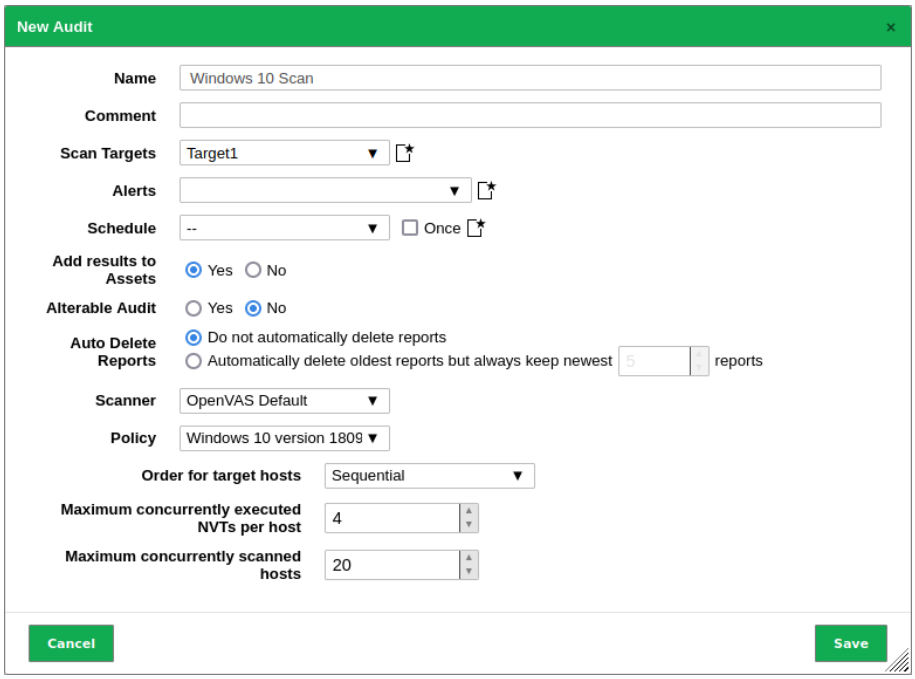


Fig. 12.7: Creating a new audit

12.2.1.2 Creating an Audit Through a Policy

An audit can directly be created for a policy as follows:

1. Select *Resilience* > *Compliance Policies* in the menu bar.
2. In the row of the desired policy, click .

   → The policy is already selected in the drop-down list *Policy*.
3. Define the audit.

   Tip: For the information to enter in the input boxes see Chapter *12.2.1.1* (page 317).
4. Click *Save*.

   → The audit is created and displayed on the page *Audits*.

12.2.2 Starting an Audit

In the row of the newly created audit, click ▷.

Note: For scheduled audits 🕒 is displayed. The audit is starting at the time that was defined in the schedule (see Chapter *10.10* (page 268)).

→ The audit is added to the waiting queue. Afterwards, the scanner begins with the scan.

Note: In some cases, the audit may remain in the queue. For more information see Chapter *17.3* (page 384).

For the status of an audit see Chapter *12.2.3* (page 319).

The report of an audit can be displayed as soon as the audit has been started by clicking the bar in the column *Status*. For reading, managing and downloading reports see Chapter *11* (page 283).

As soon as the status changes to *Done* the complete report is available. At any the time the intermediate results can be reviewed (see Chapter *11.2.1* (page 288)).

Note: It can take a while for the scan to complete. The page is refreshing automatically if new data is available.

12.2.3 Managing Audits

List Page

All existing audits can be displayed by selecting *Resilience* > *Compliance Audits* in the menu bar (see Fig. 12.8).

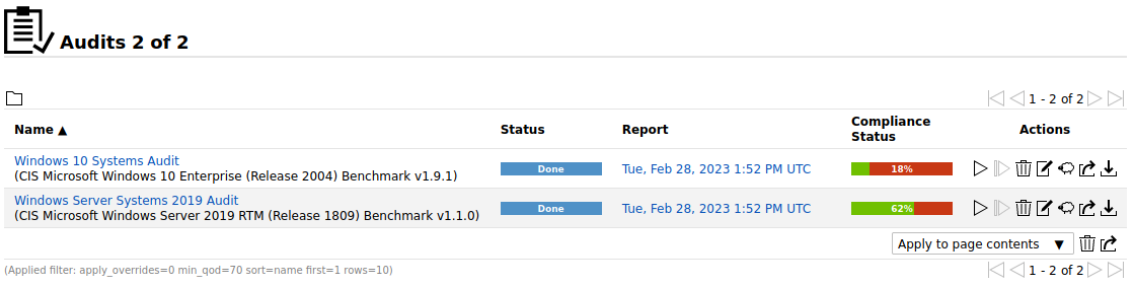


Fig. 12.8: Page *Audits* displaying all available audits

For all audits the following information is displayed:

Name Name of the audit. The following icons may be displayed:

- ✎ The audit is marked as alterable. The audit's scan target(s) and scanner can be edited, even if reports were already created.
- 🌡 The audit is configured to run on a remote scanner (see Chapter *16* (page 371)).
- 👁 The audit is visible to one or more other user(s).
- 👓 The audit is owned by another user.

Status Current status of the audit. The following status bars are possible:

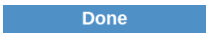
- New There are no runs/reports for the audit.

The audit was just started. The appliance is preparing the scan. Audits with this status cannot be stopped, resumed, or deleted.

The audit was added to the waiting queue. In some cases, it may remain in the queue. For more information see Chapter *17.3* (page 384).

The audit is currently running. The percent value is based on the number of VTs executed on the selected hosts. For this reason the value does not necessarily correlate with the time spent.

The scan is complete and the appliance is processing data. Audits with this status cannot be stopped, resumed, or deleted.



The audit has been completed successfully.

The audit was requested to stop recently. However, the scan engine has not yet reacted to this request yet. Audits with this status cannot be stopped, resumed, or deleted.

The audit was stopped. The latest report is possibly not yet complete. Other reasons for this status could be the reboot of the appliance or a power outage. After restarting the scanner, the audit will be resumed automatically.

The audit was just resumed. The appliance is preparing the scan. Audits with this status cannot be stopped, resumed, or deleted.

When resuming a scan, all unfinished hosts are scanned completely anew. The data of hosts that were already fully scanned is kept.

The audit was deleted. The actual deletion process can take some time as reports need to be deleted as well. Audits with this status cannot be stopped, resumed, or deleted.

An error has occurred and the audit was interrupted. The latest report is possibly not complete yet or is missing completely.

Report Date and time of the latest report. By clicking it the details page of the latest report is opened.

Compliance Status Relation of requirements identified as compliant to requirements identified as non-compliant (percentage).

For all audits the following actions are available:

- Start the audit. Only currently not running audits can be started.
- Stop the currently running audit. All discovered results will be written to the database.
- Show details of the assigned schedule (only available for scheduled audits, see Chapter *10.10* (page 268)).
- Resume the stopped audit. All unfinished hosts are scanned completely anew. The data of hosts that were already fully scanned is kept.
- Move the audit to the trashcan.
- Edit the audit.
- Clone the audit.
- Export the audit as an XML file.
- Download the report of the audit as a GCR file (Greenbone Compliance Report as PDF format).

Note: By clicking or below the list of audits more than one audit can be moved to the trashcan or exported at a time. The drop-down list is used to select which audits are moved to the trashcan or exported.

Details Page

Click on the name of an audit to display the details of the audit. Click to open the details page of the audit.

The following registers are available:

Information General information about the audit.

Permissions Assigned permissions (see Chapter *9.4* (page 193)).

The following actions are available in the upper left corner:

- Open the corresponding chapter of the user manual.
- Show the list page of all audits.
- Create a new audit (see Chapter *12.2.1.1* (page 317)).
- Clone the audit.
- Edit the audit.
- Move the audit to the trashcan.
- Export the audit as an XML file.
- Start the audit. Only currently not running audits can be started.
- Stop the currently running audit. All discovered results will be written to the database.
- Resume the stopped audit. All unfinished hosts are scanned completely anew. The data of hosts that were already fully scanned is kept.
- Show the last report for the audit or show all reports for the audit.
- Show the results for the audit.

12.3 Using and Managing Policy Reports

Reports for audits are similar to reports of all other tasks.

Once a scan has been started, the report of the results found so far can be viewed. When a scan is completed, the status changes to *Done* and no more results will be added.

12.3.1 Using a Policy Report

A policy report can be used in the same way as any other report. Chapter *11.2* (page 288) contains information about reading, interpreting, filtering, exporting, importing and comparing reports.

For further information about results and vulnerabilities see Chapters *11.3* (page 297) and *11.4* (page 299).

12.3.2 Exporting a Policy Report

Note: A policy reports must always be downloaded in the report format *Greenbone Compliance Report PDF (GCR PDF)*. Downloading it in any other report format will result in an empty report.

Additionally, the report can be downloaded from the page *Audits* as follows:

1. Select *Resilience* > *Compliance Audits* in the menu bar.

2. In the row of the desired audit, click .
3. Download the PDF file.

12.4 Generic Policy Scans

When performing policy scans, there are groups of four VTs in the VT family *Policy* that can be configured accordingly.

At least the base VT and one additional VT are required to run a policy scan.

The four VT types are:

Base This VT performs the actual scan of the policy.

Errors This VT summarizes any items in which some errors occurred when running the base VT.

Matches This VT summarizes any items which match the checks performed by the base VT.

Violations This VT summarizes any items which did not match the checks performed by the base VT.

Note: The base VT must always be selected for a policy check since it performs the actual tests. The other three VTs may be selected according to the needs. For example, if matching patterns are of no concern then only a VT of the type *Violations* should be selected additionally.

12.4.1 Checking File Content

File content checks belong to policy audits which do not explicitly test for vulnerabilities but rather test the compliance of file contents (e.g., configuration files) regarding a given policy.

The appliance provides a policy module to check if a file content is compliant with a given policy.

In general, this is an authenticated scan, i.e., the scan engine will have to log into the target system to perform the check (see Chapter *10.3* (page 218)).

The file content check can only be performed on systems supporting the command `grep`. Normally this means Linux or Linux-like systems.

Four different VTs in the VT family *Policy* provide the file content check:

- *File Content*: this VT performs the actual file content check.
- *File Content: Errors*: this VT shows the files in which errors occurred (e.g., the file is not found on the target system).
- *File Content: Matches*: this VT shows the patterns and files which passed the file content check (the predefined pattern matches in the file).
- *File Content: Violations*: this VT shows the patterns and files which did not pass the file content check (the predefined pattern does not match in the file).

12.4.1.1 Checking File Content Patterns

1. Create a reference file with the patterns to check. Following is an example:

```
filename|pattern|presence/absence
/tmp/filecontent_test|^paramter1=true.*$|presence
/tmp/filecontent_test|^paramter2=true.*$|presence
/tmp/filecontent_test|^paramter3=true.*$|absence
/tmp/filecontent_test_notthere|^paramter3=true.*$|absence
```

Note: This file must contain the row `filename|pattern|presence/absence`.

The subsequent rows each contain a test entry.

Each row contains three fields which are separated by `|`.

The first field contains the path and file name, the second field contains the pattern to check (as a regular expression) and the third field indicates if a pattern has to be present or absent.

2. Select *Resilience* > *Compliance Policies* in the menu bar.
3. In the row of the desired policy, click .

   → The cloned policy is displayed on the page *Policies*.
4. In the row of the cloned policy, click .
5. In the section *Edit Network Vulnerability Test Families* click for the VT family *Policy*.

   → All VTs that allow special configuration are listed (see Fig. 12.9).

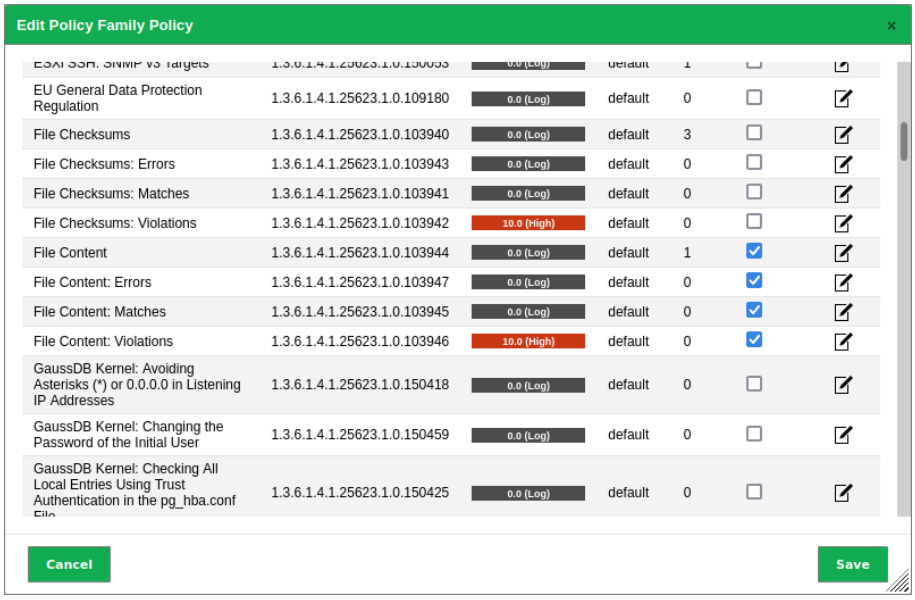


Fig. 12.9: Editing the family of VTs

6. Click for *File Content*.

7. Activate the checkbox *Upload file* (see Fig. 12.10).

Tip: If a reference file was already uploaded, the checkbox *Replace existing file* is displayed instead. The possibility to change the reference file is only available if the policy is currently not used.

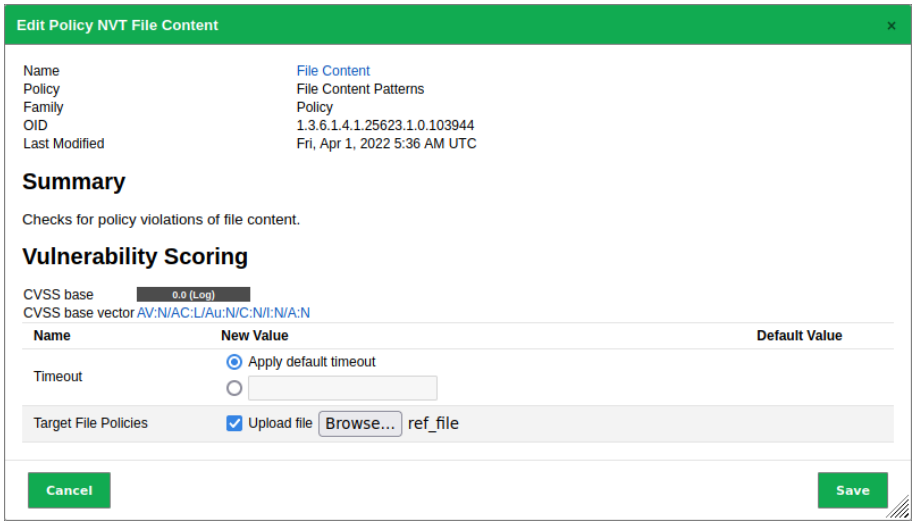


Fig. 12.10: Uploading the reference file

8. Click *Browse...* and select the previously created reference file.
9. Click *Save* to save the VT.
10. Click *Save* to save the family of VTs.
11. Click *Save* to save the policy.

12.4.1.2 Changing the Severity

The VTs of the type *Violations* have a default severity of 10.

This default severity can be changed using overrides (see Chapter *11.8* (page 307)).

By sectioning into three different VTs, it is possible to create distinct overrides for the severity according to the needs.

In the following example the severities of *File Content: Violations* and *File Content: Errors* have been changed which will be shown in the reports accordingly (see Fig. 12.11).

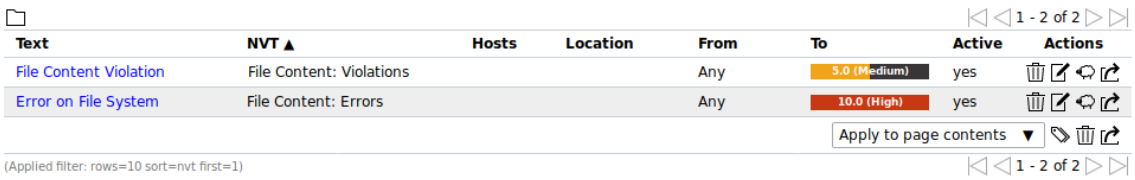


Fig. 12.11: Overrides changing the severity

12.4.2 Checking Registry Content

The registry[31] is a database in Microsoft Windows containing important information about system hardware, installed programs, settings and user accounts on the computer. Microsoft Windows continually refers to the information in the registry.

Due to the nature of the Microsoft Windows registry every program/application installed under Microsoft Windows will register itself in the Microsoft Windows registry. Even malware and other malicious code usually leave traces within the registry.

The registry can be utilized to search for specific applications or malware related information such as version levels and numbers. Also, missing or changed registry settings could point to a potential security policy violation on an endpoint.

The appliance provides a policy module to verify registry entries on target systems. This module checks for the presence or absence of registry settings as well as registry violations.

Since the registry is unique to Microsoft Windows systems, this check can only be run on these systems.

To access the registry on the target system an authenticated scan has to be run.

Four different VTs in the VT family *Policy* provide the registry content check:

- *Windows Registry Check*: this VT performs the actual registry content check on the files.
- *Windows Registry Check: Errors*: this VT shows the files in which errors occurred (e.g., registry content not found on the target system).
- *Windows Registry Check: OK*: this VT shows the registry settings which passed the registry check (right registry content).
- *Windows Registry Check: Violations*: this VT shows the registry content which did not pass the registry check (wrong registry content).

[31] https://learn.microsoft.com/en-us/windows/win32/sysinfo/registry

12.4.2.1 Checking Registry Content Patterns

1. Create a reference file with the reference registry content. Following is an example:

```
Present|Hive|Key|Value|ValueType|ValueContent
TRUE|HKLM|SOFTWARE\Macromedia\FlashPlayer\SafeVersions|8.0|REG_DWORD|33
TRUE|HKLM|SOFTWARE\Microsoft\Internet Explorer
TRUE|HKLM|SOFTWARE\Microsoft\Internet Explorer|Version|REG_SZ|9.11.10240.16384
TRUE|HKLM|SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\
 System|LocalAccountTokenFilterPolicy|REG_DWORD|1
FALSE|HKLM|SOFTWARE\Virus
TRUE|HKLM|SOFTWARE\ShouldNotBeHere
TRUE|HKLM|SOFTWARE\Macromedia\FlashPlayer\SafeVersions|8.0|REG_DWORD|*
```

Note: This file must contain the row `Present|Hive|Key|Value|ValueType|ValueContent`.

The subsequent rows each contain a test entry.

Each row contains six fields which are separated by `|`.

The first field sets whether a registry entry should be present or not, the second the hive the registry entry is located in, the third the key, the fourth the value, the fifth the value type and the sixth the value content. If a star `*` is used in the last column any value is valid and accepted for existence or non-existence.

2. Select *Resilience > Compliance Policies* in the menu bar.
3. In the row of the policy *Microsoft Windows Registry Check*, click .

   → The cloned policy is displayed on the page *Policies*.
4. In the row of the cloned policy, click .
5. In the section *Edit Network Vulnerability Test Families* click for the VT family *Policy*.

   → All VTs that allow special configuration are listed (see Fig. 12.12).

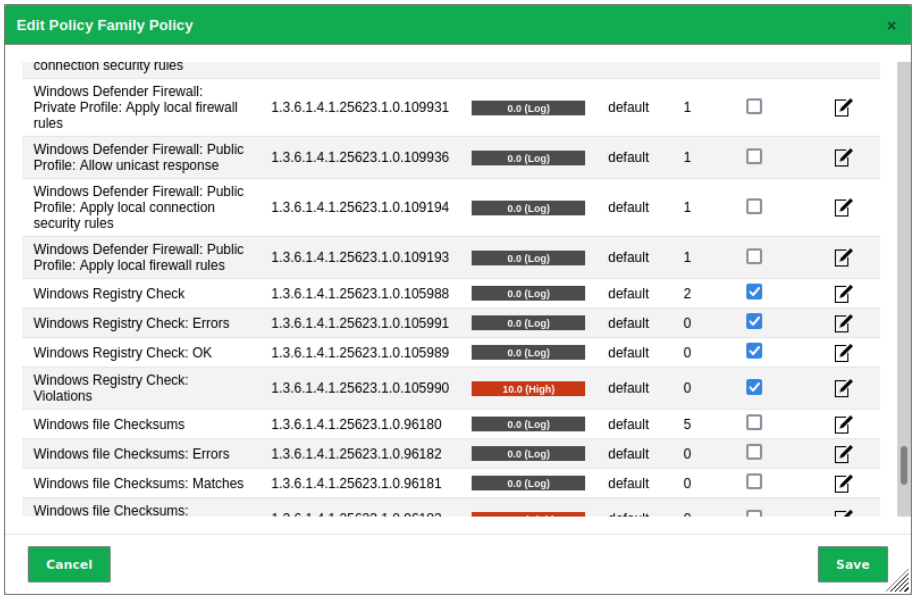


Fig. 12.12: Editing the family of VTs

6. Click for *Windows Registry Check*.

7. Activate the checkbox *Upload file* (see Fig. 12.13).

Tip: If a reference file was already uploaded, the checkbox *Replace existing file* is displayed instead. The possibility to change the reference file is only available if the policy is currently not used.

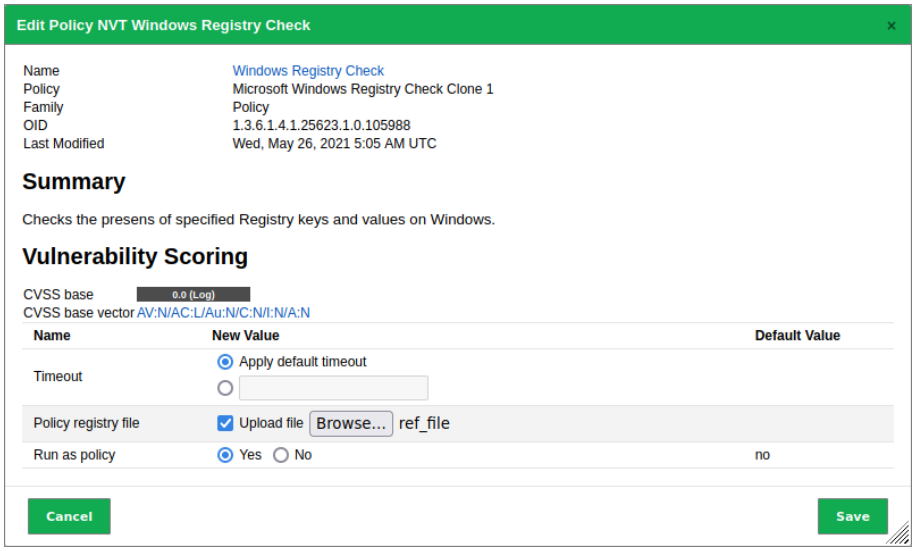


Fig. 12.13: Uploading the reference file

8. Click *Browse...* and select the previously created reference file.
9. Click *Save* to save the VT.
10. Click *Save* to save the family of VTs.
11. Click *Save* to save the policy.

12.4.2.2 Changing the Severity

The VTs of the type *Violations* have a default severity of 10.

This default severity can be changed using overrides (see Chapter *11.8* (page 307)).

By sectioning into three different VTs, it is possible to create distinct overrides for the severity according to the needs.

In the following example the severities of *Windows Registry Check: Violations* and *Windows Registry Check: Errors* have been changed which will be shown in the reports accordingly (see Fig. 12.14).

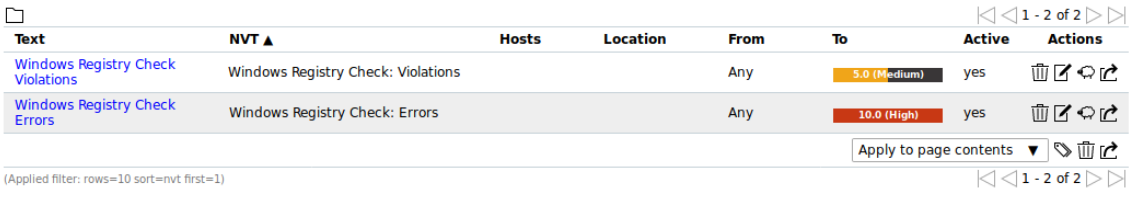


Fig. 12.14: Overrides changing the severity

12.4.3 Checking File Checksums

File checksum checks belong to policy audits which do not explicitly test for vulnerabilities but rather for file integrity.

The appliance provides a policy module to verify file integrity on target systems. This module checks the file content by MD5 or SHA1 checksums.

In general, this is an authenticated check, i.e., the scan engine will have to log into the target system to perform the check.

The file checksum check can only be performed on systems supporting checksums. Normally this means Linux or Linux-like systems. However, the appliance provides a module for checksum checks for Microsoft Windows systems as well (see Chapter *12.4.3.3* (page 330)).

Four different VTs in the VT family *Policy* provide the file checksum check:

- *File Checksums*: this VT performs the actual checksum check on the files.
- *File Checksums: Errors*: this VT shows the files in which errors occurred (e.g., file not found on the target system).
- *File Checksums: Matches*: this VT shows the files which passed the checksum check (checksum matches).
- *File Checksums: Violations*: this VT shows the files which did not pass the checksum check (wrong checksum).

12.4.3.1 Checking File Checksum Patterns

1. Create a reference file with the reference checksums. Following is an example:

```
Checksum|File|Checksumtype
6597ecf8208cf64b2b0eaa52d8169c07|/bin/login|md5
ed3ed98cb2efa9256817948cd27e5a4d9be2bdb8|/bin/bash|sha1
7c59061203b2b67f2b5c51e0d0d01c0d|/bin/pwd|md5
```

Note: This file must contain the row `Checksum|File|Checksumtype`.

The subsequent rows each contain a test entry.

Each row contains three fields which are separated by `|`.

The first field contains the checksum in hex, the second field the path and file name and the third field the checksum type. Currently MD5 and SHA1 checksums are supported.

Important: Checksums and checksum types must be lowercase.

2. Select *Resilience > Compliance Policies* in the menu bar.
3. In the row of the desired policy, click .

   → The cloned policy is displayed on the page *Policies*.
4. In the row of the cloned policy, click .
5. In the section *Edit Network Vulnerability Test Families* click for the VT family *Policy*.

   → All VTs that allow special configuration are listed (see Fig. 12.15).
6. Click for *File Checksums*.

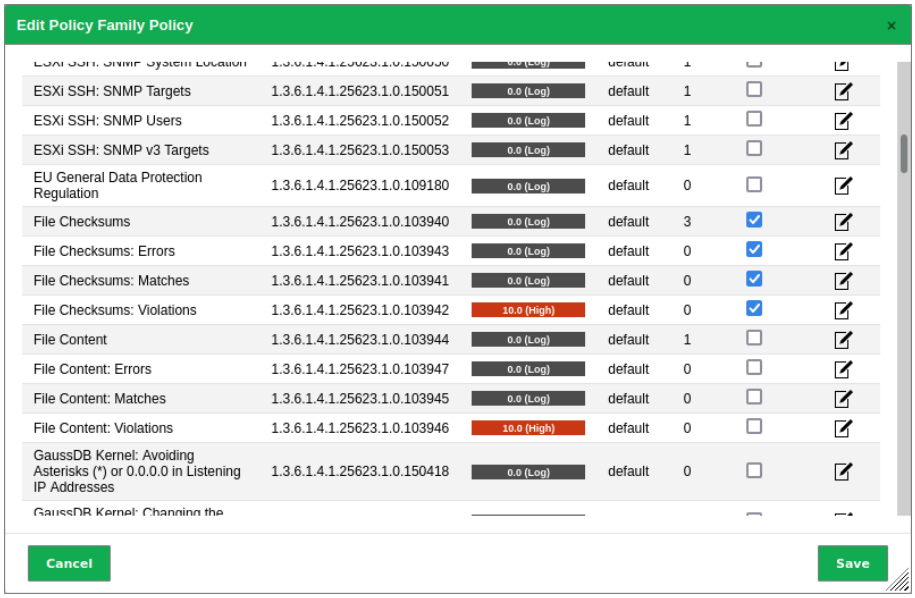


Fig. 12.15: Editing the family of VTs

7. Activate the checkbox *Upload file* (see Fig. 12.16).

Tip: If a reference file was already uploaded, the checkbox *Replace existing file* is displayed instead. The possibility to change the reference file is only available if the policy is currently not used.

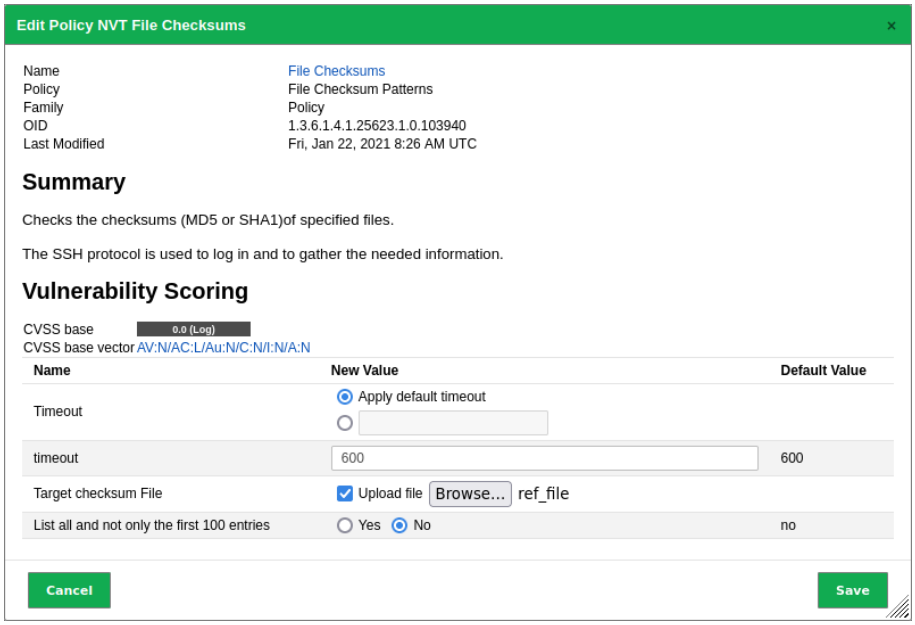


Fig. 12.16: Uploading the reference file

8. Click *Browse...* and select the previously created reference file.

9. Click *Save* to save the VT.
10. Click *Save* to save the family of VTs.
11. Click *Save* to save the policy.

12.4.3.2 Changing the Severity

The VTs of the type *Violations* have a default severity of 10.

This default severity can be changed using overrides (see Chapter *11.8* (page 307)).

By sectioning into three different VTs, it is possible to create distinct overrides for the severity according to the needs.

In the following example the severities of *File Checksum: Violations* and *File Checksum: Errors* have been changed which will be shown in the reports accordingly (see Fig. 12.17).

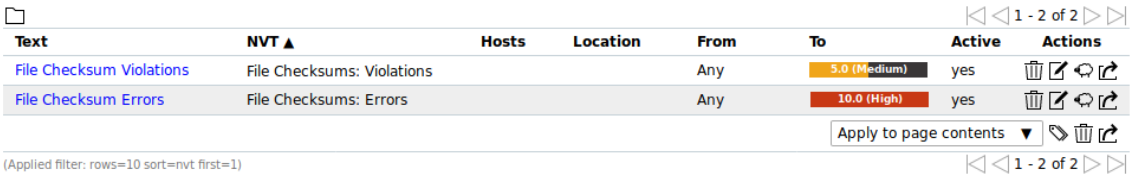


Fig. 12.17: Overrides changing the severity

12.4.3.3 Checking File Checksum Patterns for Microsoft Windows

The appliance provides a similar module for Microsoft Windows systems for file checksum checks.

Since Microsoft Windows does not provide an internal program for creating checksums it has to be installed one either manually or automatically by the VT. The appliance uses ReHash[32] for creating checksums on Microsoft Windows systems.

Note: There are two operating modes for these checks:

- Using a tool that was installed on the target system manually.
- The tool ReHash will automatically be installed and deinstalled as well if requested on the target system during the checking routine.

As for Linux systems the VTs for checksum checks are located in the VT family *Policy*.

1. Create a reference file with the patterns to check. Following is an example:

```
Checksum|File|Checksumtype
6597ecf8208cf64b2b0eaa52d8169c07|/bin/login|md5
ed3ed98cb2efa9256817948cd27e5a4d9be2bdb8|/bin/bash|sha1
7c59061203b2b67f2b5c51e0d0d01c0d|/bin/pwd|md5
```

2. In the row of the respective policy, click ✎.
3. In the section *Edit Network Vulnerability Test Families* click ✎ for the VT family *Policy*.

   → All VTs that allow special configuration are listed (see Fig. 12.18).
4. Click ✎ for *Windows file Checksums*.

[32] https://rehash.sourceforge.net/

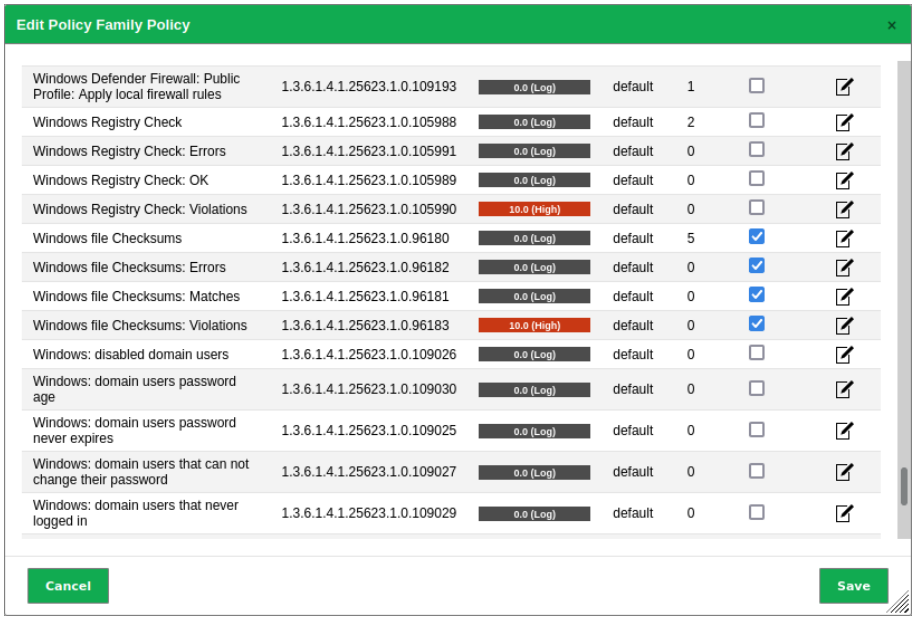


Fig. 12.18: Editing the family of VTs

5. For *Delete hash test Programm after the test* select the radio button *Yes* if the checksum program ReHash should be deleted after the check (see Fig. 12.19).

   Tip: The program can be left on the target system, e.g., to speed up recurring tests and therefore does not have to be transferred each time.

6. For *Install hash test Programm on the Target* select the radio button *Yes* if the checksum program ReHash should be installed on the target system automatically.

   Note: If it is not installed automatically, it has to be installed manually under `C:\Windows\system32` (on 32-bit systems) or `C:\Windows\SysWOW64` (on 64-bit systems) and has to be executable for the authenticated user.

7. Activate the checkbox *Upload file*.

   Tip: If a reference file was already uploaded, the checkbox *Replace existing file* is displayed instead. The possibility to change the reference file is only available if the policy is currently not used.

8. Click *Browse...* and select the previously created reference file.
9. Click *Save* to save the VT.
10. Click *Save* to save the family of VTs.
11. Click *Save* to save the policy.

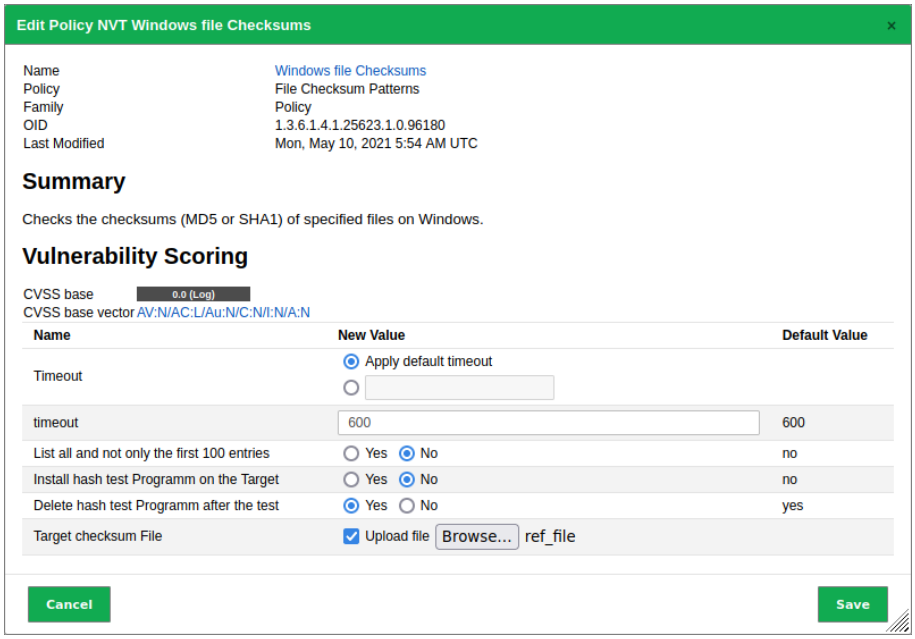


Fig. 12.19: Uploading the reference file

12.4.4 Performing CPE-Based Checks

For detailed information about Common Platform Enumeration (CPE) see Chapter *14.2.2* (page 353).

12.4.4.1 Simple CPE-Based Checks for Security Policies

With any executed scan, CPEs for the identified products are stored. This happens independently of whether the product actually reveals a security problem or not. On this basis it is possible to describe simple security policies and the checks for compliance with these.

With the Greenbone Enterprise Appliance, it is possible to describe policies to check for the presence as well as for the absence of a product. These cases can be associated with a severity to appear in the scan report.

The examples demonstrate how to check the compliance of a policy regarding specific products in an IT infrastructure and how the reporting with the corresponding severity can be done.

The information about whether a certain product is present on the target system is gathered by a single Vulnerability Test (VT) or even independently by a number of special VTs. This means that for a certain product an optimized policy that only concentrates on this product and does not do any other scan activity can be specified.

12.4.4.2 Detecting the Presence of Problematic Products

This example demonstrates how the presence of a certain product in an IT infrastructure is classified as a severe problem and reported as such.

1. Select *Resilience* > *Compliance Policies* in the menu bar.
2. Create a new policy by clicking .
3. Define the name of the policy.
4. Click *Save*.

   → The policy is created and displayed on the page *Policies*.

5. In the row of the policy, click .
6. In the row of the VT family *Policy*, click .
7. In the row of the VT *CPE Policy Check*, click .
8. Either a single CPE or multiple CPEs can be searched for at the same time.

   Enter a single CPE in the input box *Single CPE*, e.g., `cpe:/a:microsoft:ie:6` (see Fig. 12.20).

   or

   Activate the checkbox *Upload file*, click *Browse...* and select a file containing a list of CPEs.

   Note: The file must be a text file in which the CPEs are separated by commas or line breaks.

9. The problematic product should **not** be present, i.e., the condition must be set to *missing*. However, if the product is discovered, this is evaluated as critical.

   Select the radio button *missing*.

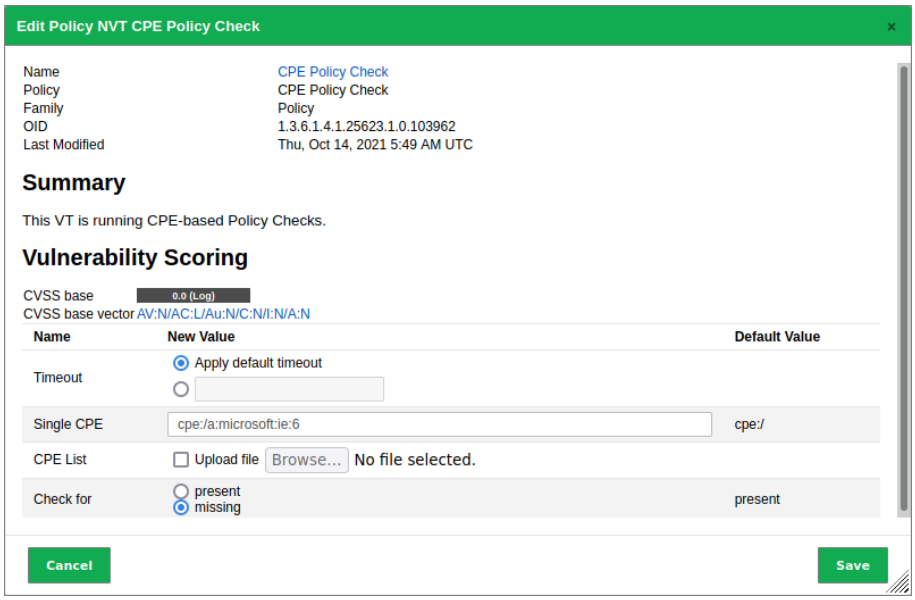


Fig. 12.20: Editing *CPE Policy Check*

10. Click *Save* to save the VT.
11. Activate the checkbox *Selected* for the following VTs: *CPE Policy Check*, *CPE-based Policy Check Error*, *CPE-based Policy Check OK* and *CPE-based Policy Check Violations*.
12. Click *Save* to save the family of VTs.
13. Activate the checkbox *Selected* for the VT family *Product Detection* (see Fig. 12.21).
14. Click *Save* to save the policy.

Note: In case the mere availability of a product should be considered, it is required to configure remote access using credentials to apply local security checks (see Chapter *10.3.2* (page 219)). If just running network services should be searched, it normally does not help but rather increases the number of false positives.

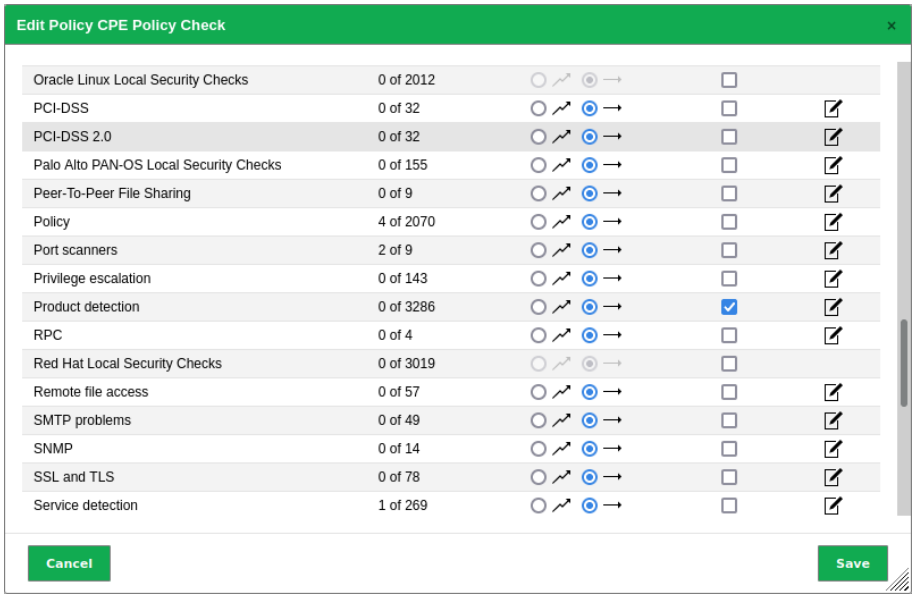


Fig. 12.21: Activated VT families

15. Create a new target (see Chapter *10.2.1* (page 212)), create a new audit (see Chapter *12.2.1.1* (page 317)) and run the audit (see Chapter *12.2.2* (page 319)).

    When creating the audit, use the previously created policy.

16. When the scan is completed select *Scans* > *Reports* in the menu bar.

Tip: To show only the results of the CPE-based policy checks, a suitable filter can be applied.

17. Enter `cpe` in the input box *Filter*.

    → The reports for CPE-based policy checks are displayed.

18. Click on the date of a report.

    → The report for CPE-based policy checks is displayed.

    The report can be used as described in Chapter *11.2.1* (page 288).

Note: The VTs of the type *Violations* have a default severity of 10.

This default severity can be changed using overrides (see Chapter *11.8* (page 307)).

If the problematic product is found on one of the target systems, it is reported as a problem.

12.5 Checking Standard Policies

12.5.1 IT-Grundschutz

The German Federal Office for Information Security (BSI)[33] publishes the IT-Grundschutz Compendium[34], which replaced the IT-Grundschutz Catalogs in 2017 and provides useful information for detecting weaknesses and combating attacks on IT environments.

Greenbone provides a policy for testing the compliance with the following modules of the IT-Grundschutz Compendium:

- SYS.1.2.2 Windows Server 2012
- SYS.1.3 Server on Linux and Unix
- SYS.2.2.2 Clients on Windows 8.1
- SYS.2.2.3 Clients on Windows 10
- SYS.2.3 Clients on Linux and Unix

An IT-Grundschutz scan can be carried out as follows:

1. Create a new target (see Chapter *10.2.1* (page 212)), create a new audit (see Chapter *12.2.1.1* (page 317)) and run the audit (see Chapter *12.2.2* (page 319)).

   When creating the audit, use the policy *IT-Grundschutz Kompendium*.

2. When the scan is completed select *Scans* > *Reports* in the menu bar.
3. Click on the date of the report.

   → The report for the IT-Grundschutz scan is displayed.

   The report can be used as described in Chapter *11.2.1* (page 288). The report contains detailed information about compliant, not compliant and incomplete requirements.

4. To export the report click .
5. For *Include* activate the checkbox *Notes* to include attached notes and the checkbox *Overrides* to label enabled overrides and include their text field (see Chapter *11.2.2* (page 292)).
6. Select *GCR PDF* in the drop-down list *Report Format*.
7. Click *OK* and download the PDF file.

[33] https://www.bsi.bund.de/EN/Home/home_node.html
[34] https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html

12.5.2 BSI TR-03116: Kryptographische Vorgaben für Projekte der Bundesregierung

The German Federal Office for Information Security (BSI) published a technical guideline TR-03116: Kryptographische Vorgaben für Projekte der Bundesregierung[35]. Part 4 of this guideline describes the security requirements for services of the federal government using the cryptographic protocols SSL/TLS, S/MIME and OpenPGP.

The requirements are based on forecasts for the security of the algorithms and key lengths for the next years.

Greenbone provides a policy for testing the compliance of services with the technical guideline “TR-03116”.

The policy tests if the scanned hosts and services use SSL/TLS. If this is the case, the compliance with the guideline is tested.

The policy states three main requirements:

TLS version TLS versions lower than 1.2 are not allowed.

Supported ciphers If TLS 1.2 is enabled, one of the following ciphers has to be supported:

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

If TLS 1.3 is enabled, cipher TLS_AES_128_GCM_SHA256 has to be supported.

Allowed cipher suites If TLS 1.2 is enabled, only the following cipher suites are allowed:

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA

If TLS 1.3 is enabled, only the following cipher suites are allowed:

[35] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03116/TR-03116_node.html

- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384
- TLS_AES_128_CCM_SHA256

A BSI TR-03116 scan can be carried out as follows:

1. Create a new target (see Chapter *10.2.1* (page 212)), create a new audit (see Chapter *12.2.1.1* (page 317)) and run the audit (see Chapter *12.2.2* (page 319)).

   When creating the audit, use the policy *BSI TR-03116: Part 4*.

2. When the scan is completed select *Scans* > *Reports* in the menu bar.
3. Click on the date of the report.

   → The report for the BSI TR-03116 scan is displayed.

   The report can be used as described in Chapter *11.2.1* (page 288). The report contains detailed information about compliant, not compliant and incomplete requirements.

4. To export the report click .
5. For *Include* activate the checkbox *Notes* to include attached notes and the checkbox *Overrides* to label enabled overrides and include their text field (see Chapter *11.2.2* (page 292)).
6. Select *GCR PDF* in the drop-down list *Report Format*.
7. Click *OK* and download the PDF file.

12.5.3 BSI TR-02102: Kryptographische Verfahren: Empfehlungen und Schlüssellängen

The German Federal Office for Information Security (BSI) published a technical guideline TR-02102: Kryptographische Verfahren: Empfehlungen und Schlüssellängen[36]. Part 4 of this guideline describes the recommendations for the use of the Secure Shell (SSH) cryptographic protocol.

Greenbone provides a policy for testing the compliance of services with the technical guideline “TR-02102”.

The following SSH settings in the file `/etc/ssh/sshd_config` are tested in the policy:

- Protocol (OID: 1.3.6.1.4.1.25623.1.0.150066): SSH version 2 has to be used.
- KexAlgorithms (OID: 1.3.6.1.4.1.25623.1.0.150077): the following algorithms are allowed for key exchange during SSH connection establishment: diffie-hellman-group-exchange-sha256, diffie-hellman-group14-sha256, diffie-hellman-group15-sha512, diffie-hellman-group16-sha512, rsa2048-sha256, ecdh-sha2-*
- ReKeyLimit (OID: 1.3.6.1.4.1.25623.1.0.150560): the key material of a connection must be renewed after 1 hour or 1 GiB of transferred data.
- Ciphers (OID: 1.3.6.1.4.1.25623.1.0.150225): the following encryption methods are allowed: AEAD_AES_128_GCM, AEAD_AES_256_GCM, aes256-cbc, aes192-cbc, aes128-cbc, aes128-ctr, aes192-ctr, aes256-ctr
- MACs (OID: 1.3.6.1.4.1.25623.1.0.109795): the following MACs are allowed: hmac-sha1, hmac-sha2-256, hmac-sha2-512
- HostKeyAlgorithms (OID: 1.3.6.1.4.1.25623.1.0.150559): the following methods for server authentication are allowed: pgp-sign-rsa, pgp-sign-dss, ecdsa-sha2-*, x509v3-rsa2048-sha256, x509v3-ecdsa-sha2-*

[36] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr-02102.html?nn=451438

- AuthenticationMethods (OID: 1.3.6.1.4.1.25623.1.0.150561): the public key authentication (*publickey*) has to be used.
- PubkeyAuthentication (OID: 1.3.6.1.4.1.25623.1.0.150222): the public key authentication (*publickey*) has to be allowed.

A BSI TR-02102 scan can be carried out as follows:

1. Create a new target (see Chapter *10.2.1* (page 212)), create a new audit (see Chapter *12.2.1.1* (page 317)) and run the audit (see Chapter *12.2.2* (page 319)).

   When creating the audit, use the policy *BSI TR-02102-4*.

2. When the scan is completed select *Scans* > *Reports* in the menu bar.
3. Click on the date of the report.

   → The report for the BSI TR-02102 scan is displayed.

   The report can be used as described in Chapter *11.2.1* (page 288). The report contains detailed information about compliant, not compliant and incomplete requirements.

4. To export the report click .
5. For *Include* activate the checkbox *Notes* to include attached notes and the checkbox *Overrides* to label enabled overrides and include their text field (see Chapter *11.2.2* (page 292)).
6. Select *GCR PDF* in the drop-down list *Report Format*.
7. Click *OK* and download the PDF file.

12.6 Running a TLS Map Scan

The TLS (Transport Layer Security) protocol ensures the confidentiality, authenticity and integrity of communication in insecure networks. It establishes confidential communication between sender and receiver, e.g., web server and web browser.

With the Greenbone Enterprise Appliance, it is possible to identify systems that offer services using SSL/TLS protocols. Additionally, the appliance detects the protocol versions and offers encryption algorithms. Further details about the service can be achieved in case it can be properly identified.

12.6.1 Checking for TLS and Exporting the Scan Results

For an overview on TLS usage in the network or on single systems, Greenbone recommends using the scan configuration *TLS-Map*. This scan configuration identifies the used protocol versions and the offered encryption algorithms. Additionally, it tries to identify in-depth details of the service.

1. Select *Configuration* > *Port Lists* in the menu bar to have a look at the pre-configured port lists.

   Note: By clicking own port lists can be created (see Chapter *10.7.1* (page 252)).

2. Choose a suitable list of ports that should be scanned.

   Note: Pay attention that all ports of interest are covered by the list.

   The more extensive the list, the longer the scan will take but this may also detect services at unusual ports.

   The TLS protocol is mainly based on TCP. A port list with UDP ports will slow down the scan without benefits. If any TCP ports should be covered *All TCP* should be selected.

3. Create a new target (see Chapter *10.2.1* (page 212)), create a new task (see Chapter *10.2.2* (page 215)) and run the task (see Chapter *10.2.3* (page 217)).

   When creating the task, use the scan configuration *TLS-Map*.

4. When the scan is completed select *Scans* > *Reports* in the menu bar.

5. Click on the date of the report.

   → The report for the TLS-Map scan is displayed.

   The report can be used as described in Chapter *11.2.1* (page 288).

6. To export the report click .

7. For *Include* activate the checkbox *Notes* to include attached notes and the checkbox *Overrides* to label enabled overrides and include their text field (see Chapter *11.2.2* (page 292)).

8. Select *TLS Map* in the drop-down list *Report Format*.

9. Click *OK* and download the CSV file.

   → The report can be used in spreadsheet applications.

The file contains one line per port and systems where an SSL/TLS protocol is offered:

```
IP,Host,Port,TLS-Version,Ciphers,Application-CPE
192.168.12.34,www.local,443,TLSv1.0;SSLv3,SSL3_RSA_RC4_128_SHA;TLS1_RSA_RC4_128_SHA,
  cpe:/a:apache:http_server:2.2.22;cpe:/a:php:php:5.4.4
```

(continues on next page)

(continued from previous page)

```
192.168.56.78,www2.local,443,TLSv1.0;SSLv3,SSL3_RSA_RC4_128_SHA;TLS1_RSA_RC4_128_SHA,
  cpe:/a:apache:http_server:2.2.22
```

Separated by commas, each line contains the following information:

- **IP** The IP address of the system where the service was detected.
- **Host** The DNS name of the system in case it is available.
- **Port** The port where the service was detected.
- **TLS-Version** The protocol version offered by the service. In case more than one is offered, the versions are separated with semicolons.
- **Ciphers** The encryption algorithms offered by the service. In case more than one is offered, the algorithms are separated with semicolons.
- **Application-CPE** The detected application in CPE format. In case more than one is identified, the applications are separated with semicolons.

CHAPTER 13

Managing Assets

The assets include hosts, operating systems, and TLS certificates. They are collected during vulnerability scans.

When creating a new task, it is possible to specify whether the host details collected during a scan should be stored in the asset database (see Chapter *10.2.2* (page 215)). The details are stored if the default task settings are used.

13.1 Creating and Managing Hosts

During a scan, information about each scanned host is collected. The hosts are identified by their IP addresses.

For each identified host it is checked whether it already exists in the hosts assets. If not, a new host asset is created.

Both when scanning a newly created host and when scanning an existing host, several host details (host names, IP and MAC addresses, operating systems, SSH keys and X.509 certificates) are added to the host asset as identifiers.

If vhost[37] scanning is enabled – which it is by default – (see Chapter *10.13.4* (page 282)), each vhost will be added as its own asset entry. Thus, due to the nature of vhosts, IP address identifiers may appear multiple times. Such assets must then be distinguished by their other host identifiers.

13.1.1 Creating a Host

Hosts can also be manually added to the asset management to create targets from them (see Chapter *13.1.3* (page 344)).

Except for the IP address, no other details about the host can be defined but further details will be added when scanning the manually added host.

A host can be created as follows:

1. Select *Assets* > *Hosts* in the menu bar.

[37] https://httpd.apache.org/docs/current/vhosts/

2. Create a new host by clicking in the upper left corner of the page.
3. Enter the IP address of the host in the input box *Name* (see Fig. 13.1).

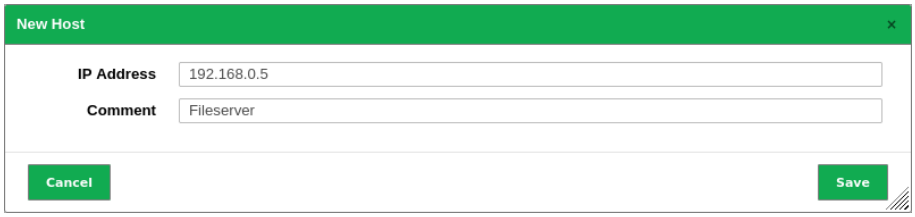


Fig. 13.1: Creating a new host

4. Click *Save*.

This feature is also available via GMP (see Chapter *15* (page 361)). The import of hosts from a configuration management database can be achieved using this option.

13.1.2 Managing Hosts

List Page

All existing hosts can be displayed by selecting *Assets* > *Hosts* in the menu bar (see Fig. 13.2).

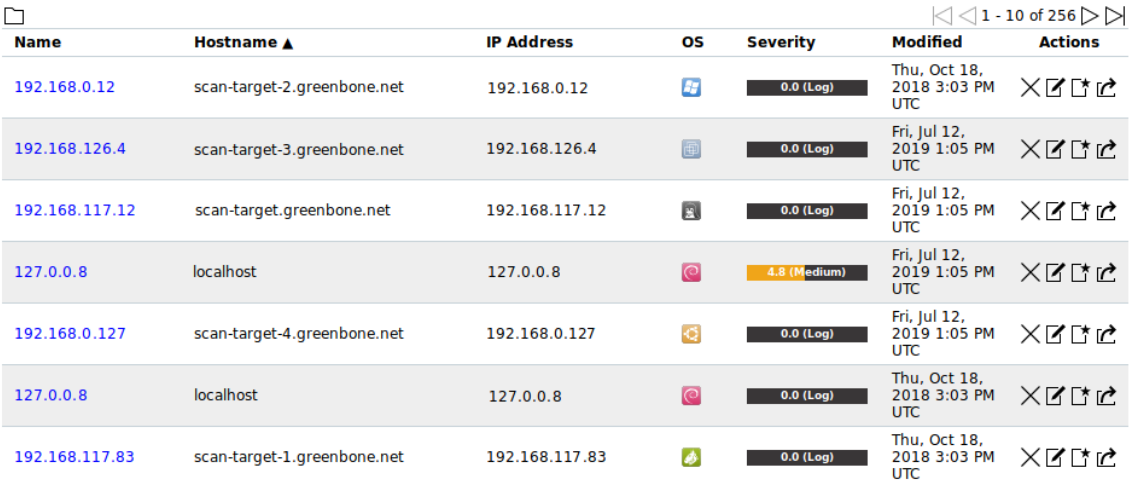


Fig. 13.2: Page *Hosts* displaying all scanned hosts

For all hosts the following actions are available:

- Delete the host.
- Edit the host.
- Create a new target from the host (see Chapter *13.1.3* (page 344)).
- Export the host as an XML file.

Note: By clicking , or below the list of hosts more than one host can be deleted, exported or used to create a new target at a time. The drop-down list is used to select which hosts are deleted, exported or used to create a new target.

Details Page

Click on the name of a host to display the details of the host. Click to open the details page of the host.

The following registers are available:

Information General information about the host.

Any identifying information collected for the host during scans, e.g., host names, IP and MAC addresses, operating systems, SSH keys and X.509 certificates, is displayed in the section *All Identifiers* (see Fig. 13.3).

Note: If identifiers have duplicates, only the latest identifiers are shown. In this case, the section is named *Latest Identifiers* and all identifiers can be displayed by clicking *Show all Identifiers* below the table.

For all host identifiers the following action is available:

- Delete the identifier.

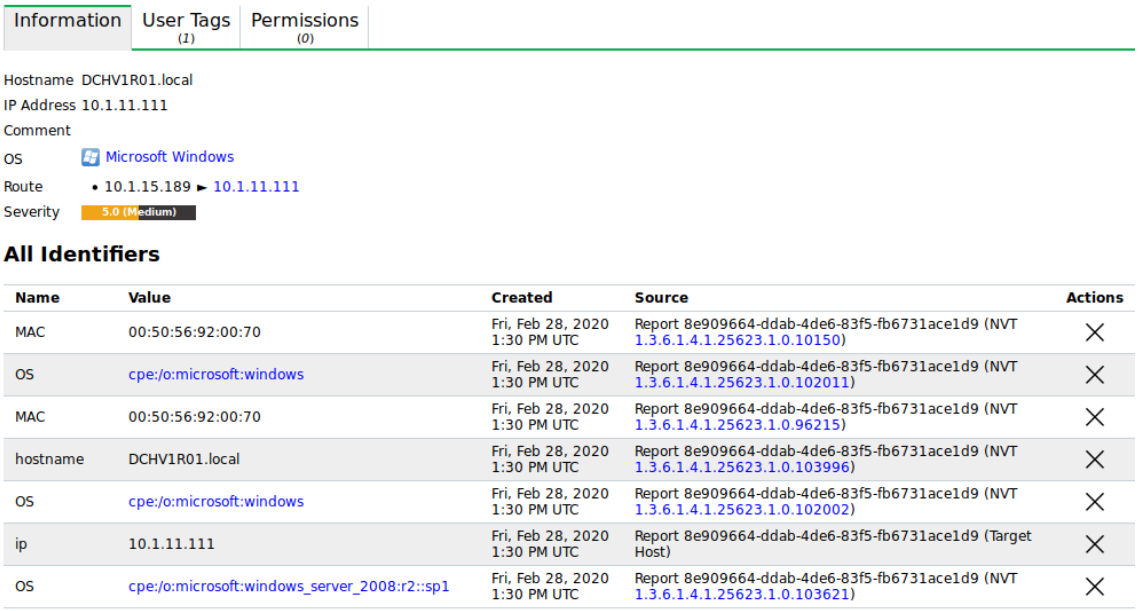


Fig. 13.3: All identifiers

User Tags Assigned tags (see Chapter *8.4* (page 174)).

Permissions Assigned permissions (see Chapter *9.4* (page 193)).

The following actions are available in the upper left corner:

- Open the corresponding chapter of the user manual.
- Show the list page of all hosts.
- Create a new host (see Chapter *13.1.1* (page 341)).
- Edit the host.
- Delete the host.
- Export the host as an XML file.
- Show the corresponding results.

13.1.3 Creating a Target from Hosts

A target with a set of hosts can be created as follows:

1. Filter the hosts so that only the hosts that should be used for the target (e.g., only Microsoft Windows hosts) are displayed (see Chapter *8.3* (page 167)).
2. Create a new target by clicking below the list of hosts (see Fig. 13.4).

   → The window for creating a target is opened. The input box *Hosts* is prefilled with the set of displayed hosts.

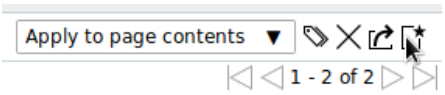


Fig. 13.4: Creating a target with the displayed hosts

3. Define the target and click *Save*.

Tip: For the information to enter in the input boxes see Chapter *10.2.1* (page 212).

Note: If additional suitable hosts show up in further scans they will **not** be added to the target.

13.2 Managing Operating Systems

The operating systems view within the asset management provides a different view on the stored data. While the hosts view is centered on the individual hosts, this view focuses on the operating systems detected during all vulnerability scans.

Note: For a reliable operating system identification, VT(s) specific to the operating system(s) in question must be available in the Greenbone Enterprise Feed. If no specific VTs are available, the appliance still tries to identify the operating system(s), but the identification happens with a lower quality of detection and is prone to false-positive detections.

List Page

All operating systems can be displayed by selecting *Assets* > *Operating Systems* in the menu bar (see Fig. 13.5).

For all operating systems the following information is displayed:

Name CPE (see Chapter *14.2.2* (page 353)) of the operating system.

Title Plain name of the operating system.

Severity – Latest Severity detected for the operating system during the last scan that found this operating system on a host. Only hosts where the respective operating system was determined to be the best match are taken into account.

Severity – Highest Highest severity detected for the operating system during all scans that found this operating system on a host. Only hosts where the respective operating system was determined to be the best match are taken into account.

Severity – Average Average severity detected for the operating system during all scans that found this operating system on a host. Only hosts where the respective operating system was determined to be the best match are taken into account.

Hosts – All All hosts where the operating system was detected. By clicking on the number of hosts, the page *Hosts* is opened. A filter is applied to show only the hosts for which the selected operating system was detected.

Hosts – Best OS Hosts where the operating system was detected as the best match. By clicking on the number of hosts, the page *Hosts* is opened. A filter is applied to show only the hosts for which the selected operating system was detected as the best match.

Modified Date and time of last modification.

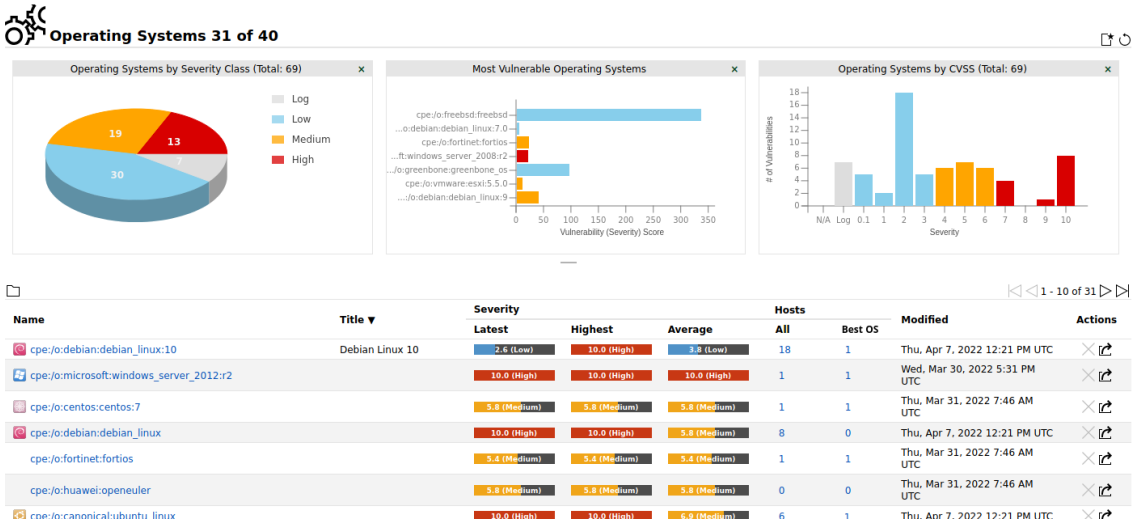


Fig. 13.5: Page *Operating Systems* displaying all scanned operating systems

For all operating systems the following actions are available:

- Delete the operating system. Only operating systems which are currently not used can be deleted.
- Export the operating system as an XML file.

Note: By clicking or below the list of operating systems more than one operating system can be deleted or exported at a time. The drop-down list is used to select which operating systems are deleted or exported.

Details Page

Click on the name of an operating system to open the details page of the operating system.

The following registers are available:

Information General information about the operating system.

User Tags Assigned tags (see Chapter *8.4* (page 174)).

Permissions Assigned permissions (see Chapter *9.4* (page 193)).

The following actions are available in the upper left corner:

- Open the corresponding chapter of the user manual.
- Show the list page of all operating systems.
- Delete the operating system. Only operating systems which are currently not used can be deleted.

- Export the operating system as an XML file.
- (left) Show the hosts for which the operating system was detected.
- (right) Show the hosts for which the operating system is the best match.

13.3 Managing TLS Certificates

This view focuses on the TLS certificates collected during all vulnerability scans and provides a quick overview of whether they are valid or expired.

Note: Only basic certificate information (host, port, activation and expiry dates, fingerprints) is included.

There is no support for Online Certificate Status Protocol (OCSP) or Certificate Revocation List (CRL) functionalities.

List Page

All existing TLS certificates can be displayed by selecting *Assets > TLS Certificates* in the menu bar (see Fig. 13.6).

For all TLS certificates the following actions are available:

- Delete the TLS certificate.
- Download the TLS certificate.
- Export the TLS certificate as an XML file.

Note: By clicking or below the list of TLS certificates more than one TLS certificate can be deleted or exported at a time. The drop-down list is used to select which TLS certificates are deleted or exported.

Details Page

Click on the name of a TLS certificate to display the details of the TLS certificate. Click to open the details page of the TLS certificate.

The following registers are available:

Information General information about the TLS certificate.

User Tags Assigned tags (see Chapter *8.4* (page 174)).

Permissions Assigned permissions (see Chapter *9.4* (page 193)).

The following actions are available in the upper left corner:

- Open the corresponding chapter of the user manual.
- Show the list page of all TLS certificates.
- Delete the TLS certificate.
- Download the TLS certificate.
- Export the TLS certificate as an XML file.

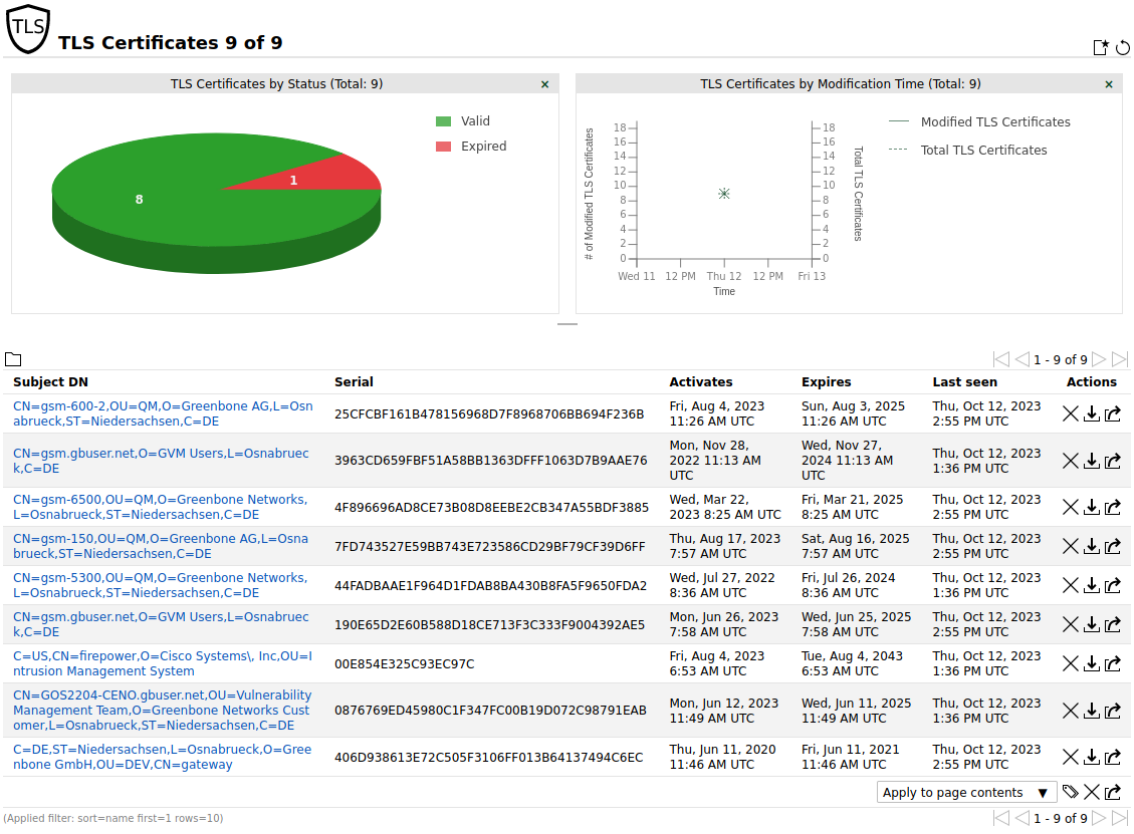


Fig. 13.6: Page *TLS Certificates* displaying all collected TLS certificates

CHAPTER 14

Managing SecInfo

The SecInfo management provides centralized access to a wide range of information technology (IT) security information including the following categories:

Vulnerability Tests (VT) VTs test the target system for potential vulnerabilities.

Common Vulnerabilities and Exposures (CVE) CVEs are vulnerabilities published by vendors and security researchers.

Common Platform Enumeration (CPE) CPE offers standardized names for products used in the IT.

CERT-Bund Advisories CERT-Bund Advisories are published by the CERT-Bund[38], the Computer Emergency Response Team of the German Federal Office for Information Security (BSI)[39] (German: Bundesamt für Sicherheit in der Informationstechnik, abbreviated as BSI). The main task of the CERT-Bund is the operation of a warning and information service publishing information regarding new vulnerabilities and security risks as well as threats for IT systems.

DFN-CERT Advisories DFN-CERT advisories are published by the DFN-CERT[40], the Computer Emergency Response Team of the German National Research and Education Network[41] (German: Deutsches Forschungsnetz, abbreviated as DFN).

CVEs and CPEs are published and made accessible by the National Institute of Standards and Technology (NIST)[42] as part of the National Vulnerability Database (NVD)[43] (see Chapter *14.2* (page 350)).

Note: Greenbone is also offering all SecInfo data online, accessible via the SecInfo portal[44]. The SecInfo portal provides all SecInfo described in the following chapters and the CVSS calculator.

Access to the SecInfo Portal is provided by activating a guest access (see Chapter *9.1.3* (page 186)).

[38] https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/CERT-Bund/cert-bund_node.html
[39] https://www.bsi.bund.de/EN/Home/home_node.html
[40] https://www.dfn-cert.de/en.html
[41] https://www.dfn.de/en/
[42] https://www.nist.gov
[43] https://nvd.nist.gov/
[44] https://secinfo.greenbone.net

14.1 Vulnerability Tests (VT)

VTs are test routines used by the appliance. They are part of the Greenbone Enterprise Feed which is updated regularly. VTs include information about development date, affected systems, impact of vulnerabilities and remediation.

List Page

All existing VTs can be displayed by selecting *SecInfo > NVTs* in the menu bar.

For all VTs the following information is displayed:

Name Name of the VT.

Family Family of VTs to which the VT belongs.

Created Date and time of creation.

Modified Date and time of last modification.

CVE CVE that is checked for using the VT.

Solution Type Solution for the vulnerability. The following solutions are possible:

- A vendor patch is available.
- A workaround is available.
- A mitigation by configuration is available.
- No fix is and will be available.
- No solution exists.

Severity The severity of the vulnerability (CVSS, see Chapter *14.2.3* (page 354)) is displayed as a bar to support the analysis of the results.

QoD QoD is short for Quality of Detection and represents how reliable the detection of a vulnerability is.

With the introduction of the QoD, the parameter *Paranoid* in the scan configuration (see Chapter *10.9* (page 258)) is removed without replacement. In the past a scan configuration without this parameter only used VTs with a QoD of at least 70%. Now all VTs are used and executed in a scan configuration.

Note: By clicking below the list of VTs more than one VT can be exported at a time. The drop-down list is used to select which VTs are exported.

Details Page

Click on the name of a VT to display the details of the VT. Click to open the details page of the VT.

The following actions are available in the upper left corner:

- Open the corresponding chapter of the user manual.
- Show the list page of all VTs.
- Export the VT as an XML file.
- Create a new note for the VT (see Chapter *11.7.1* (page 305)).
- Create a new override for the VT (see Chapter *11.8.1* (page 307)).
- Show the corresponding results.
- Show the corresponding vulnerability.

14.2 Security Content Automation Protocol (SCAP)

The National Institute of Standards and Technology (NIST)[45] provides the National Vulnerability Database (NVD)[46]. The NVD is a data repository for the vulnerability management of the US government. The goal is the standardized provision of the data for automated processing. By that, vulnerability management is supported and the implementation of compliance guidelines is verified.

The NVD provides different databases including the following:

- Checklists
- Vulnerabilities
- Misconfigurations
- Products
- Threat metrics

The NVD utilizes the Security Content Automation Protocol[47] (SCAP). SCAP is a combination of different interoperable standards. Many standards were developed or derived from public discussion.

The public participation of the community in the development is an important aspect for accepting and spreading SCAP standards. SCAP is currently specified in version 1.3 and includes the following components:

- **Languages**
  - XCCDF: Extensible Configuration Checklist Description Format
  - OVAL: Open Vulnerability and Assessment Language
  - OCIL: Open Checklist Interactive Language
  - Asset Identification
  - ARF: Asset Reporting Format
- **Collections**
  - CCE: Common Configuration Enumeration
  - CPE: Common Platform Enumeration
  - CVE: Common Vulnerabilities and Exposure
- **Metrics**
  - CVSS: Common Vulnerability Scoring System
  - CCSS: Common Configuration Scoring System
- **Integrity**
  - TMSAD: Trust Model for Security Automation Data

OVAL, CCE, CPE and CVE are trademarks of NIST.

The Greenbone Enterprise Appliance uses CVE, CPE and CVSS. By utilizing these standards, the interoperability with other systems is guaranteed. The standards also allow comparing the results.

Vulnerability assessment systems such as the Greenbone Enterprise Appliance can be validated by NIST respectively. The appliance has been validated with respect to SCAP version 1.0[48].

[45] https://www.nist.gov
[46] https://nvd.nist.gov/
[47] https://csrc.nist.gov/projects/security-content-automation-protocol/
[48] https://csrc.nist.gov/Projects/Security-Content-Automation-Protocol/SCAP-Releases

14.2.1 CVE

In order to avoid multiple naming of the same vulnerability by different organizations and to ensure a uniform naming convention, MITRE[49] founded the Common Vulnerabilities and Exposure (CVE) project[50]. Every vulnerability is assigned a unique identifier consisting of the release year and a simple number. This identifier serves as a central reference.

However, MITRE's CVE database is not a vulnerability database. Instead, it links the vulnerability database and other systems with each other and enables the comparison of security tools and services. The CVE database does not contain detailed technical information or information about the risk, impact or remediation of the vulnerability, but only the identification number with the status, a short description and references to reports and recommendations.

The National Vulnerability Database (NVD)[51] refers to the CVE database and complements the content with information regarding the elimination, severity, potential impact and affected products of the vulnerability. Greenbone refers to the CVE database of the NVD, and the appliance combines the CVE information, VTs and CERT-Bund/DFN-CERT advisories.

List Page

All existing CVEs can be displayed by selecting *SecInfo > CVEs* in the menu bar.

Note: The availability of a CVE on the appliance depends on its availability in the NVD. As soon as it has been published there, it takes 1–2 working days for it to appear in the SecInfo.

Columns like *Severity* may display *N/A* for one of the following reasons:

- The CVE was published but no vulnerability analysis/severity assessment was carried out by the NVD yet. This can take a few days up to a few weeks.

  Such CVEs can be identified when browsing the related entry[52]. As long as *Undergoing Analysis* is displayed there, *N/A* is shown in the columns for the CVE.

- There is always a delay of 1–2 working days between the vulnerability analysis/severity assessment and the time the updated information is displayed in the SecInfo management.

The column *CVSS Base Vector* shows the CVSS vector used for calculating the severity of a CVE. This vector includes the CVSS version defined for the CVE.

By clicking on the vector, the page *CVSSv2/CVSSv3 Base Score Calculator* is opened. The fields of the corresponding calculator are already filled in, depending on which CVSS version is used to calculate the severity of the CVE (see Chapter *14.2.3* (page 354)).

Note: By clicking ⇪ below the list of CVEs more than one CVE can be exported at a time. The drop-down list is used to select which CVEs are exported.

---

[49] https://www.mitre.org/
[50] https://cve.mitre.org/
[51] https://nvd.nist.gov/
[52] https://nvd.nist.gov/vuln/full-listing

Details Page

Click on the name of a CVE to display the details of the CVE. Click to open the details page of the CVE (see Fig. 14.1).

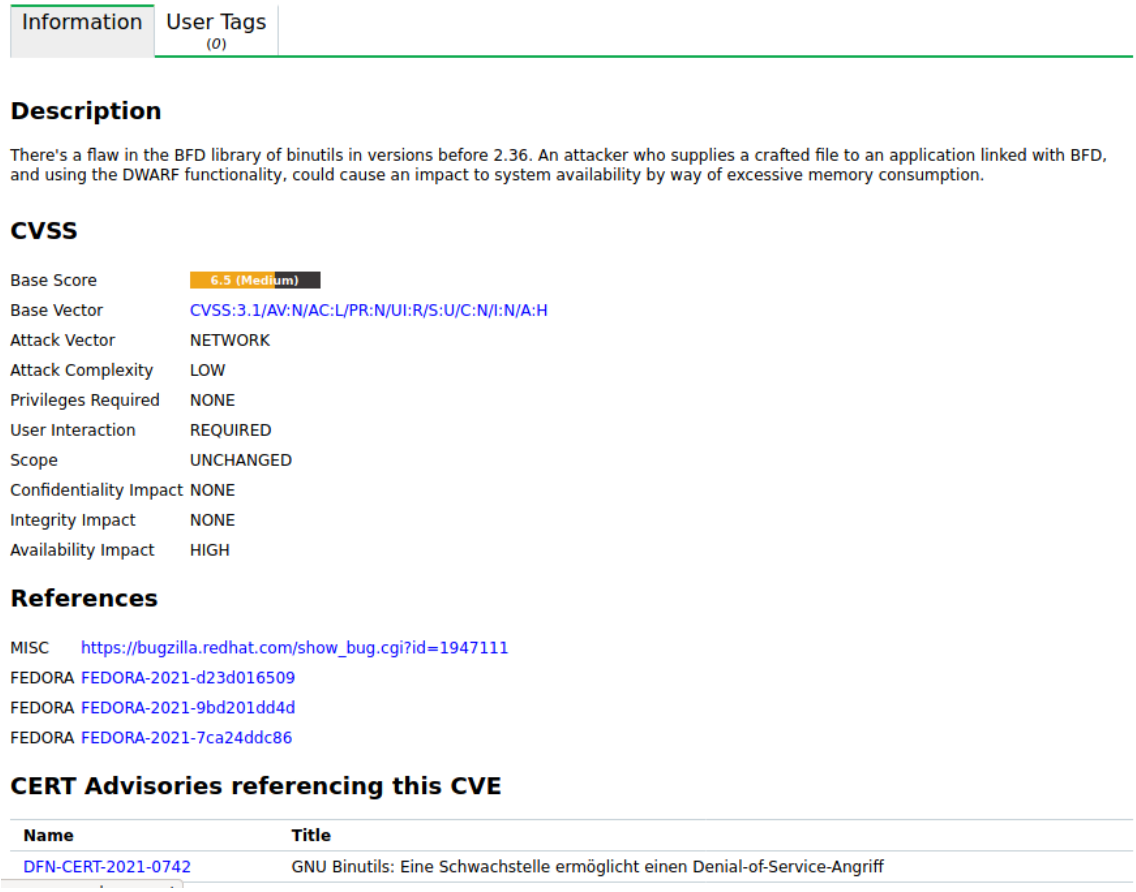


Fig. 14.1: Details page of a CVE

The following registers are available:

Information General information about the CVE.

User Tags Assigned tags (see Chapter *8.4* (page 174)).

The following actions are available in the upper left corner:

- Open the corresponding chapter of the user manual.
- Show the list page of all CVEs.
- Export the CVE as an XML file.

14.2.2 CPE

The Common Platform Enumeration (CPE)[53] is modelled after CVE. It is a structured naming scheme for applications, operating systems and hardware devices.

The CPE was initiated by MITRE[54] and is maintained by NIST as a part of the National Vulnerability Database (NVD)[55]. CPE is based on the generic syntax of the Uniform Resource Identifier (URI).

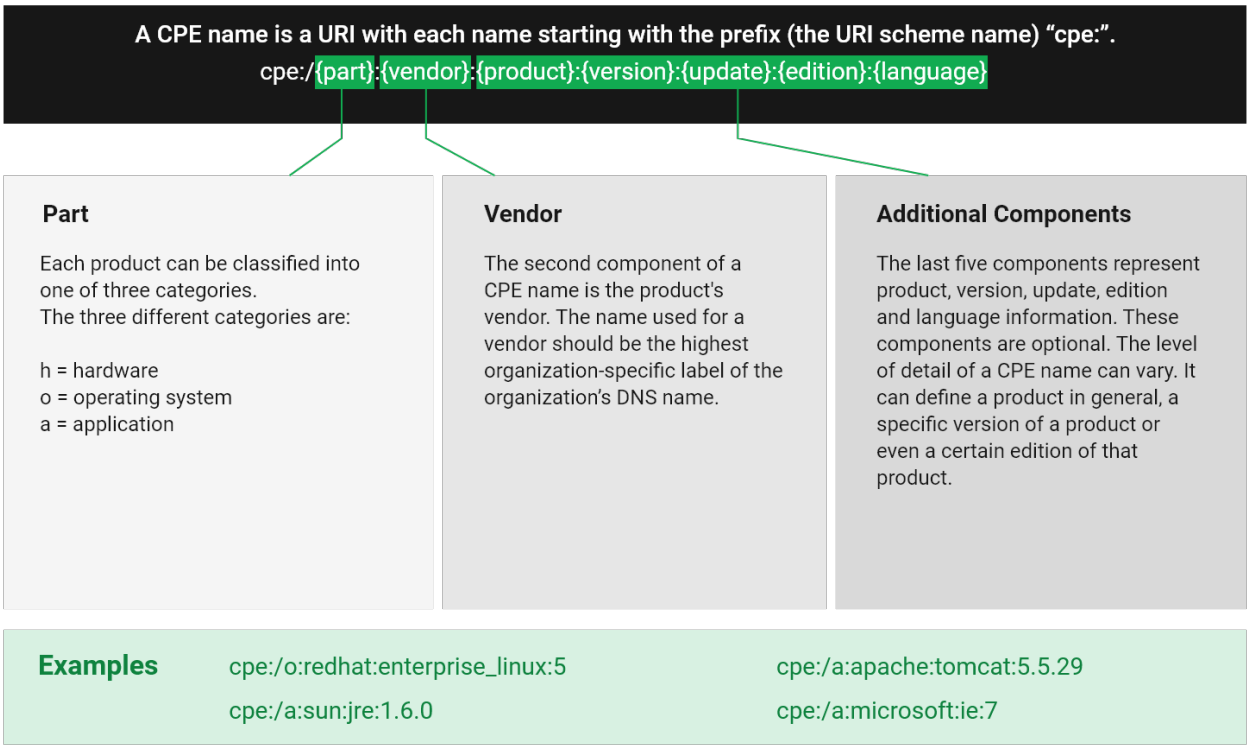


Fig. 14.2: Name structure of a CPE name

The combination of CPE and CVE standards enables the conclusion of existing vulnerabilities when discovering a platform or product.

CPE is composed of the following components:

- **Naming** The name specification describes the logical structure of well-formed names (WFNs), their binding to URIs and formatted character strings as well as their conversion.
- **Name Matching** The name matching specification describes the methods to compare WFNs with each other. This allows for the testing whether some or all WFNs refer to the same product.
- **Dictionary** The dictionary is a repository of CPE names and metadata. Every name defines a single class of an IT product. The dictionary specification describes the processes for using the dictionary, e.g., searching for a specific name or for entries belonging to a more general class.
- **Applicability Language** The applicability language specification describes the creation of complex logical expressions with the help of WFNs. These applicability statements can be used for tagging checklists, guidelines or other documents and, by that, for describing for which products the documents are relevant.

[53] https://csrc.nist.gov/projects/security-content-automation-protocol/specifications/cpe
[54] https://www.mitre.org/
[55] https://nvd.nist.gov/

List Page

All existing CPEs can be displayed by selecting *SecInfo > CPEs* in the menu bar.

Note: The availability of a CPE on the appliance depends on its availability in the NVD. As soon as it has been published there, it takes 1–2 working days for it to appear in the SecInfo.

Note: By clicking below the list of CPEs more than one CPE can be exported at a time. The drop-down list is used to select which CPEs are exported.

Details Page

Click on the name of a CPE to display the details of the CPE. Click to open the details page of the CPE.

The following registers are available:

Information General information about the CPE.

User Tags Assigned tags (see Chapter *8.4* (page 174)).

The following actions are available in the upper left corner:

- Open the corresponding chapter of the user manual.
- Show the list page of all CPEs.
- Export the CPE as an XML file.

14.2.3 CVSS

To support the interpretation of a vulnerability, the Common Vulnerability Scoring System (CVSS) was invented. The CVSS is an industry standard for describing the severity of security risks in computer systems.

Security risks are rated and compared using different criteria. This allows for the creation of a priority list of countermeasures.

The CVSS is developed by the CVSS Special Interest Group (CVSS-SIG)[56] of the Forum of Incident Response and Security Teams (FIRST)[57]. The current CVSS score version is 4.0.

GOS 22.04 supports CVSS v3.0/v3.1. The extent of the CVSS v3.0/v3.1 support depends on the Greenbone Enterprise Feed. However, VTs and CVEs may contain CVSS v2 and/or CVSS v3.0/v3.1 data.

- If a VT/CVE contains both CVSS v2 data and CVSS v3.0/v3.1 data, the CVSS v3.0/v3.1 data is always used and shown.
- The *CVSS Base Vector* shown in the details preview and on the details page of a VT can be v2, v3.0 or v3.1.
- The *CVSS Base Vector* shown in the table on the page *CVEs* can be v2, v3.0 or v3.1. Clicking on the CVSS base vector opens the page *CVSSv2/CVSSv3 Base Score Calculator*. The input boxes of the corresponding calculator are already pre-filled.

The CVSS score supports base score metrics, temporal score metrics, and environmental score metrics.

Base score metrics Base score metrics test the exploitability of a vulnerability and their impact on the target system. Access, complexity and requirement of authentication are rated. Additionally, they rate whether the confidentiality, integrity or availability is threatened.

[56] https://www.first.org/cvss/
[57] https://www.first.org/

Temporal score metrics Temporal score metrics test whether a completed example code exists, the vendor already supplied a patch and confirmed the vulnerability. The score will be changing drastically in the course of time.

Environmental score metrics Environmental score metrics describe the effect of a vulnerability within an organization. They take damage, target distribution, confidentiality, integrity and availability into account. This assessment strongly depends on the environment in which the vulnerable product is used.

Since the base score metrics are merely meaningful in general and can be determined permanently, the appliance provides them as part of the SecInfo data.

The CVSS calculator can be opened by selecting *Help > CVSS Calculator* in the menu bar (see Fig. 14.3). Both the calculator for CVSS version 2.0 and the calculator for CVSS version 3.0/3.1 are displayed.

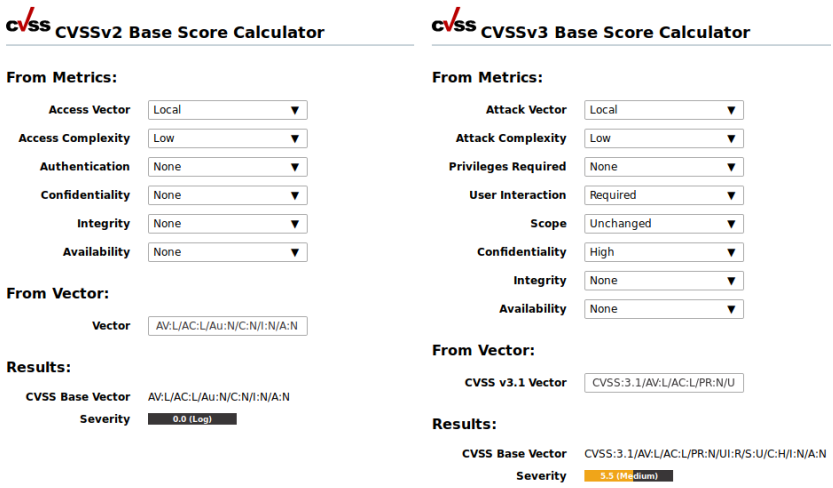


Fig. 14.3: CVSS calculator for calculating severity scores

14.2.3.1 CVSS Version 2.0

The following formula is used by the CVSS calculator for version 2.0:

```
BaseScore = roundTo1Decimal( ( ( 0.6 * Impact ) +
            ( 0.4 * Exploitability ) - 1.5 ) * f( Impact ) )
```

“Impact” is calculated as follows:

```
Impact = 10.41 * (1 - (1 - ConfImpact) *
         (1 - IntegImpact) * (1 - AvailImpact))
```

“Exploitability” is calculated as follows:

```
Exploitability = 20 * AccessVector * AccessComplexity * Authentication
```

Note: The function `f( Impact )` is 0, if the impact is 0.

In all other cases the value is 1.176.

The other values are constants:

- **Access Vector**
  - Requires local access: 0.395
  - Adjacent network accessible: 0.646
  - Network accessible: 1.0
- **Access Complexity**
  - High: 0.35
  - Medium: 0.61
  - Low: 0.71
- **Authentication**
  - Requires multiple instances of authentication: 0.45
  - Requires single instance of authentication: 0.56
  - Requires no authentication: 0.704
- **ConfImpact**
  - None: 0.0
  - Partial: 0.275
  - Complete: 0.660
- **IntegImpact**
  - None: 0.0
  - Partial: 0.275
  - Complete: 0.660
- **AvailImpact**
  - None: 0.0
  - Partial: 0.275
  - Complete: 0.660

14.2.3.2 CVSS Version 3.0/3.1

The following formula is used by the CVSS calculator for version 3.0/3.1:

```
* If Impact <= 0, BaseScore = 0

* If Scope is "Unchanged":
   BaseScore = Roundup (Minimum ((Impact + Exploitability), 10))

* If Scope is "Changed":
   BaseScore = Roundup (Minimum (1.08 * (Impact + Exploitability), 10))
```

“ISS” (Impact Sub-Score) is calculated as follows:

```
ISS = 1 - ((1 - Confidentiality) * (1 - Integrity) * (1 - Availability))
```

“Impact” is calculated as follows:

```
* If Scope is "Unchanged":
   Impact = 6.42 * ISS

* If Scope is "Changed":
   Impact = 7.52 * (ISS - 0.029) - 3.25 * (ISS - 0.02)^15
```

“Exploitability” is calculated as follows:

```
Exploitability = 8.22 * Attack Vector * Attack Complexity
                 * Privileges Required * User Interaction
```

The other values are constants:

- **Attack Vector**
  - Network: 0.85
  - Adjacent: 0.62
  - Local: 0.55
  - Physical: 0.2
- **Attack Complexity**
  - Low: 0.77
  - High: 0.44
- **Privileges Required**
  - None: 0.85
  - Low: 0.62 (or 0.68 if Scope is “Changed”)
  - High: 0.27 (or 0.5 if Scope is “Changed”)
- **User Interaction**
  - None: 0.85
  - Required: 0.62
- **Confidentiality**
  - None: 0.0
  - Low: 0.22
  - High: 0.56
- **Integrity**
  - None: 0.0
  - Low: 0.22
  - High: 0.56
- **Availability**
  - None: 0.0
  - Low: 0.22
  - High: 0.56

14.3 CERT-Bund Advisories

The CERT-Bund[58], the Computer Emergency Response Team of the German Federal Office for Information Security (BSI), is the central point of contact for preventive and reactive measures regarding security related computer incidents.

With the intention of avoiding harm and limiting potential damage, the work of CERT-Bund includes the following:

- Creating and publishing recommendations for preventive measures
- Pointing out vulnerabilities in hardware and software products
- Proposing measures to address known vulnerabilities
- Supporting public agencies efforts to respond to IT security incidents
- Recommending various mitigation measures
- Working closely with the National IT Situation Centre[59] and the National IT Crisis Response Centre[60]

The services of CERT-Bund are primarily available to federal authorities and include the following:

- 24 hour on call duty in cooperation with the IT Situation Centre
- Analyzing incoming incident reports
- Creating recommendations derived from incidents
- Supporting federal authorities during IT security incidents
- Operating a warning and information service
- Active alerting of the federal administration in case of imminent danger

The CERT-Bund offers a warning and information service (German: Warn- und Informationsdienst, abbreviated as “WID”). Currently this service offers two different types of information:

Advisories This information service is only available to federal agencies as a closed list. The advisories describe current information about security critical incidents in computer systems and detailed measures to remediate security risks.

Short Information Short information features the short description of current information regarding security risks and vulnerabilities. This information is not always verified and could be incomplete or even inaccurate.

The Greenbone Enterprise Feed contains the CERT-Bund Short Information. Both the information in the old format[61] [German only] (up to June 2022) and the information in the new format[62] [German only] (from June 2022) are included.

- There are very minor differences in the advisory metadata between both formats. The formats can be used interchangeably for all use cases.
- Information of the old format follow the scheme `CB-KYY/ID`, e.g., `CB-K22/0704`.
- Information of the new format follow the scheme `WID-SEC-YYYY-ID`, e.g., `WID-SEC-2022-0311`.

[58] https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/CERT-Bund/cert-bund_node.html

[59] https://www.bsi.bund.de/EN/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Service-fuer-KRITIS-Betreiber/IT-Lagezentrum/it-lagezentrum_node.html

[60] https://www.bsi.bund.de/EN/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Service-fuer-KRITIS-Betreiber/IT-Krisenreaktionszentrum/it-krisenreaktionszentrum_node.html

[61] https://www.bsi.bund.de/DE/Service-Navi/Abonnements/Warnmeldungen/warnmeldungen_node.html

[62] https://wid.cert-bund.de/portal/wid/kurzinformationen

List Page

All existing CERT-Bund advisories can be displayed by selecting *SecInfo > CERT-Bund Advisories* in the menu bar.

Note: By clicking below the list of CERT-Bund advisories more than one CERT-Bund advisory can be exported at a time. The drop-down list is used to select which CERT-Bund advisories are exported.

Details Page

Click on the name of a CERT-Bund advisory to display the details of the CERT-Bund advisory. Click to open the details page of the CERT-Bund advisory.

The following registers are available:

Information General information about the CERT-Bund advisory.

User Tags Assigned tags (see Chapter *8.4* (page 174)).

The following actions are available in the upper left corner:

- Open the corresponding chapter of the user manual.
- Show the list page of all CERT-Bund advisories.
- Export the CERT-Bund advisory as an XML file.

14.4 DFN-CERT Advisories

While the individual VTs, CVEs and CPEs are created primarily to be processed by computer systems, the DFN-CERT[63] publishes new advisories regularly.

The DFN-CERT is responsible for hundreds of universities and research institutions that are associated with the German Research and Education Network[64] (German: Deutsches Forschungsnetz, abbreviated as DFN). Additionally, it provides key security services to government and industry.

An advisory describes especially critical security risks that require fast reacting. The DFN-CERT advisory service includes the categorization, distribution and rating of advisories issued by different software vendors and distributors. Advisories are obtained by the Greenbone Enterprise Appliance and stored in the database for reference.

List Page

All existing DFN-CERT advisories can be displayed by selecting *SecInfo > DFN-CERT Advisories* in the menu bar.

Note: By clicking below the list of DFN-CERT advisories more than one DFN-CERT advisory can be exported at a time. The drop-down list is used to select which DFN-CERT advisories are exported.

Details Page

Click on the name of a DFN-CERT advisory to display the details of the DFN-CERT advisory. Click to open the details page of the DFN-CERT advisory.

The following registers are available:

Information General information about the DFN-CERT advisory.

[63] https://www.dfn-cert.de/en.html
[64] https://www.dfn.de/en/

User Tags Assigned tags (see Chapter *8.4* (page 174)).

The following actions are available in the upper left corner:

- Open the corresponding chapter of the user manual.
- Show the list page of all DFN-CERT advisories.
- Export the DFN-CERT advisory as an XML file.

CHAPTER 15

Using the Greenbone Management Protocol

The vulnerability management functionality of the Greenbone Enterprise Appliance is also available via the Greenbone Management Protocol (GMP).

Greenbone provides the Greenbone Vulnerability Management Tools (gvm-tools) to access the functionality made available by GMP (see Chapter *15.3* (page 362)). This user manual covers gvm-tools up to version 2.0.0 beta.

The newest version of GMP is documented at https://docs.greenbone.net/API/GMP/gmp-22.4.html.

15.1 Changes to GMP

GMP is regularly updated to apply changes in the functionality provided by the underlying service and to provide a consistent and comprehensive interface.

Updates result in a new version of GMP. Each new version includes a list of added, modified and removed protocol elements, e.g., commands or attributes. The most recent version of the list is available at https://docs.greenbone.net/API/GMP/gmp-22.4.html#changes.

Depending on the changes, the old version may be available for some time. During this transitional phase, the new and the old version are available at the same time.

This list helps to prepare for upcoming changes as soon as possible. It does not represent the complete list of upcoming changes.

15.2 Activating GMP

Before GMP can be used, it must be activated on the appliance.

While the web interface uses GMP locally on the appliance, GMP is not remotely accessible via the network by default.

The remote GMP service can be activated using the GOS administration menu (see Chapter *7.2.4.2* (page 107)).

In general, the access to GMP is authenticated and encrypted with SSL/TLS. The same users as for the web interface are used. The users are subject to the same restrictions and have the same permissions.

15.3 Using gvm-tools

The Greenbone Vulnerability Management Tools (gvm-tools) are a collection of tools that provide access to the functionalities of the Greenbone Management Protocol (GMP). GMP scripts executed with `gvm-script` use the API provided by the library python-gvm[65].

Note: python-gvm is automatically installed when installing gvm-tools.

gvm-tools are available as a command line interface (CLI) and as a Python shell for Microsoft Windows and any operating system that supports Python, including Linux.

Note: Both gvm-tools and python-gvm use a different version scheme than GOS, so the versions of gvm-tools, python-gvm and GOS are not necessarily the same.

It is recommended to use the latest versions of gvm-tools and python-gvm.

gvm-tools can be downloaded at the project's official GitHub repository[66]. Python 3.5 or later is required. To install gvm-tools, follow the instructions provided at https://gvm-tools.readthedocs.io/en/latest/install.html.

In addition, gvm-tools are available as statically linked EXE files for all currently supported versions of Microsoft Windows[67].

The EXE versions of gvm-tools do not require Python and may be downloaded directly from Greenbone at:

- CLI: gvm-cli.exe[68]
- Python shell: gvm-pyshell.exe[69]

Important: External links to the Greenbone download website are case-sensitive.

Note that upper cases, lower cases and special characters have to be entered exactly as they are written in the footnotes.

Note: gvm-tools are licensed under the GNU General Public License v3.0 and may be adapted and built for other uses cases, based on the source code.

15.3.1 Accessing with `gvm-cli.exe`

GMP is XML based. Every command and every response is a GMP object.

The command line tool `gvm-cli.exe` supplied by Greenbone offers direct sending and receiving of XML commands and responses.

[65] https://python-gvm.readthedocs.io/en/latest/
[66] https://github.com/greenbone/gvm-tools
[67] https://learn.microsoft.com/en-us/lifecycle/faq/windows
[68] https://download.greenbone.net/tools/gvm-cli.exe
[69] https://download.greenbone.net/tools/gvm-pyshell.exe

`gvm-cli.exe` supports the following connections:

- SSH
- TLS
- Unix Domain Socket

`gvm-cli.exe` supports several command line switches which can be displayed using:

```
$ gvm-cli -h
usage: gvm-cli [-h] [-c [CONFIG]]
               [--log [{DEBUG,INFO,WARNING,ERROR,CRITICAL}]]
               [--timeout TIMEOUT] [--gmp-username GMP_USERNAME]
               [--gmp-password GMP_PASSWORD] [-V] [--protocol {GMP,OSP}]
               CONNECTION_TYPE ...

optional arguments:
  -h, --help            show this help message and exit
  -c [CONFIG], --config [CONFIG]
                        Configuration file path (default: ~/.config/gvm-
                        tools.conf)
  --log [{DEBUG,INFO,WARNING,ERROR,CRITICAL}]
                        Activate logging (default level: None)
  --timeout TIMEOUT     Response timeout in seconds, or -1 to wait
                        indefinitely (default: 60)
  --gmp-username GMP_USERNAME
                        Username for GMP service (default: '')
  --gmp-password GMP_PASSWORD
                        Password for GMP service (default: '')
  -V, --version         Show version information and exit
  --protocol {GMP,OSP}  Service protocol to use (default: GMP)

connections:
  valid connection types

  CONNECTION_TYPE       Connection type to use
    ssh                 Use SSH to connect to service
    tls                 Use TLS secured connection to connect to service
    socket              Use UNIX Domain socket to connect to service
```

While `gvm-cli.exe` supports more command line switches the additional options are only displayed when the connection type is specified:

```
$ gvm-cli ssh -h
usage: gvm-cli ssh [-h] --hostname HOSTNAME [--port PORT]
                   [--ssh-username SSH_USERNAME]
                   [--ssh-password SSH_PASSWORD] [-X XML] [-r] [--pretty]
                   [--duration]
                   [infile]

positional arguments:
  infile                File to read XML commands from.

optional arguments:
  -h, --help            show this help message and exit
  --hostname HOSTNAME   Hostname or IP address
  --port PORT           SSH port (default: 22)
  --ssh-username SSH_USERNAME
                        SSH username (default: 'gmp')
  --ssh-password SSH_PASSWORD
```

(continues on next page)

(continued from previous page)

```
                        SSH password (default: 'gmp')
  -X XML, --xml XML     XML request to send
  -r, --raw             Return raw XML
  --pretty              Pretty format the returned xml
  --duration            Measure command execution time
```

All current appliances use SSH to encrypt GMP. The use of TLS is deprecated, not officially supported and may be removed in a future version.

The gvm-tools are mostly helpful for batch mode (`batch processing`, `scripting`).

With `gvm-cli.exe` GMP can be used in a simple way:

```
gvm-cli --xml "<get_version/>"
gvm-cli --xml "<get_tasks/>"
gvm-cli < file
```

15.3.1.1 Configuring the Client

For using command `gvm-cli` logging into the appliance is required.

The needed information is supplied either using command line switches or a configuration file (~/.config/gvm-tools.conf).

To provide the GMP user with command line switches use:

- `--gmp-username`
- `--gmp-password`

Alternatively a configuration file ~/.config/gvm-tools.conf containing the information can be created:

```
[Auth]
gmp_username=webadmin
gmp_password=kennwort
```

This configuration file is not read by default. The command line switch `--config` or `-c` has to be added to read the configuration file.

15.3.1.2 Starting a Scan Using the Command `gvm-cli`

A typical example for using GMP is the automatic scan of a new system.

In the example it is assumed that an Intrusion Detection System (IDS) is used that monitors the systems in the Demilitarized Zone (DMZ) and immediately discovers new systems and unusual TCP ports that are not used already. If such an event is discovered, the IDS should automatically initiate a scan of the new system with the help of a script.

For this, the command `gvm-cli` can be used although the command `gvm-pyshell` or using self written python scripts may be more suitable (see Chapter *15.3.2.1* (page 366)). The processing of the XML output is better supported by python than by using the shell.

Starting point is the IP address of the new suspected system. A target must be created on the appliance for this IP address.

The command `create_target` is described at:

https://docs.greenbone.net/API/GMP/gmp-22.4.html#command_create_target.

1. If the IP address is saved in the variable `IPADDRESS`, create the respective target as follows:

```
$ gvm-cli --gmp-username webadmin --gmp-password kennwort ssh \
--hostname 192.168.222.115 \
--xml "<create_target><name>Suspect Host</name>\
<hosts>$IPADDRESS</hosts></create_target>"

<create_target_response status="201" status_text="OK, resource
created" id="4574473f-a5d0-494c-be6f-3205be487793"/>
```

2. Create the task as follows:

```
$ gvm-cli --gmp-username webadmin --gmp-password kennwort ssh \
--hostname 192.168.222.115 \
--xml "<create_task><name>Scan Suspect Host</name> \
<target id=\"4574473f-a5d0-494c-be6f-3205be487793\"></target> \
<config id=\"daba56c8-73ec-11df-a475-002264764cea\"></config></create_task>"


<create_task_response status="201" status_text="OK, resource
created" id="ce225181-c836-4ec1-b83f-a6fcba70e17d"/>
```

→ The output is the ID of the task. It is required to start and monitor the task.

The other IDs used by the command can be retrieved using the following commands which display the available targets and scan configs:

```
$ gvm-cli --gmp-username webadmin --gmp-password kennwort ssh \
--hostname 192.168.222.115 --xml "<get_targets/>"

$ gvm-cli --gmp-username webadmin --gmp-password kennwort ssh \
--hostname 192.168.222.115 --xml "<get_configs/>"
```

Note: The output of the commands above is XML.

3. Start the task as follows:

```
$ gvm-cli --gmp-username webadmin --gmp-password kennwort ssh \
--hostname 192.168.222.115 \
--xml '<start_task task_id="ce225181-c836-4ec1-b83f-a6fcba70e17d"/>'
```

→ The connection will be closed by the appliance. The task is running.

4. Display the status of the task as follows:

```
$ gvm-cli --gmp-username webadmin --gmp-password kennwort ssh \
--hostname 192.168.222.115 \
--xml '<get_tasks task_id="ce225181-c836-4ec1-b83f-a6fcba70e17d"/>'

<get_tasks_response status="200" status_text="OK"><apply_overrides>
...<status>Running</status><progress>98<host_progress>
<host>192.168.255.254</host>98</host_progress></progress>.../>
```

→ As soon as the scan is completed, the report can be downloaded.

For this the ID that was output when the task was created is required and a meaningful report format has to be entered.

5. Display the IDs for the report formats as follows:

```
$ $ gvm-cli --gmp-username webadmin --gmp-password kennwort ssh \
--hostname 192.168.222.115 --xml '<get_report_formats/>'
```

6. Load the report as follows:

```
$ gvm-cli --gmp-username webadmin --gmp-password kennwort ssh \
--hostname 192.168.222.115 \
--xml '<get_reports report_id="23a335d6-65bd-4be2-a83e-be330289eef7" \
format_id="35ba7077-dc85-42ef-87c9-b0eda7e903b6"/>'
```

Tip: To fully and automatically process the data, the task can be combined with an alert that forwards the report based on a given condition.

15.3.2 Accessing with `gvm-pyshell.exe`

The command line tool `gvm-pyshell.exe` supplied by Greenbone offers the direct sending and receiving of XML commands and XML responses using python commands. The commands take care of the generation and parsing of the XML data.

The tool supports the following connections:

- TLS
- SSH
- Socket

While the current appliances use SSH to protect GMP, older appliances used TLS and Port 9390 to transport GMP. The gvm-tools can be used with both the older and the current GOS.

The gvm-tools are mostly helpful for batch mode (`batch processing`, `scripting`).

The authentication configuration of the command `gvm-pyshell` can be stored in a file in the home directory of the user. The syntax is explained in Chapter *15.3.1.1* (page 364).

The Python implementation follows the GMP API (https://docs.greenbone.net/API/GMP/gmp-22.4.html). Optional arguments in the API are identified by a `?`. The following example explains the usage of the Python functions:

```
gmp.create_task("Name","Config","Scanner","Target",comment="comment")
```

Tip: While mandatory arguments can be supplied in the correct order and are identified automatically they can also be specified using their identifier:

```
gmp.create_task(name="Name",config_id="Config",scanner_id="Scanner",
target_id="Target",comment="comment")
```

15.3.2.1 Starting a Scan Using the Command `gvm-pyshell`

A typical example for using GMP is the automatic scan of a new system.

In the example it is assumed that an Intrusion Detection System (IDS) is used that monitors the systems in the Demilitarized Zone (DMZ) and immediately discovers new systems and unusual TCP ports that are not used

already. If such an event is discovered, the IDS should automatically initiate a scan of the new system with the help of a script.

For this, the command `gvm-pyshell` is very suitable. The processing of the XML output is better supported by python than by using the shell.

Starting point is the IP address of the new suspected system. A target must be created on the appliance for this IP address.

The command `create_target` is described at:

https://docs.greenbone.net/API/GMP/gmp-22.4.html#command_create_target.

1. The following lines illustrate the commands required when using gvm-pyshell:

```
$ gvm-pyshell \
--gmp-username webadmin --gmp-password kennwort \
ssh --hostname 192.168.222.115
GVM Interactive Console 2.0.0 API 1.1.0. Type "help" to get information about
  functionality.
>>> res=gmp.create_target("Suspect Host", make_unique=True, \
  hosts=['192.168.255.254'])
>>> target_id = res.xpath('@id')[0]
```

The variable `target_id` contains the ID of the created target. This ID can be used to create the corresponding task.

Note: The task creation requires the following input:

- target_id
- config_id
- scanner_id
- task_name
- task_comment

---

2. All existing scan configurations can be displayed as follows:

```
>>> res = gmp.get_configs()
>>> for i, conf in enumerate(res.xpath('config')):
...     id = conf.xpath('@id')[0]
...     name = conf.xpath('name/text()')[0]
...     print('\n({0}) {1}: ({2})'.format(i, name, id))
```

3. All existing scanners can be displayed using the same technique. If only the built-in scanners are used the following IDs are hard coded:
   - OpenVAS scanner: 08b69003-5fc2-4037-a479-93b440211c73
   - CVE scanner: 6acd0832-df90-11e4-b9d5-28d24461215b

4. Create the task as follows:

```
>>> res=gmp.create_task(name="Scan Suspect Host",
... config_id="daba56c8-73ec-11df-a475-002264764cea",
... scanner_id="08b69003-5fc2-4037-a479-93b440211c73",
... target_id=target_id)
>>> task_id = res.xpath('@id')[0]
```

5. Start the task as follows:

```
>>> gmp.start_task(task_id)
```

→ The current connection is closed immediately. Further commands are not required.

All commands can be put in a Python script which may be invoked by the Python shell:

```
len_args = len(args.script) - 1
if len_args is not 2:
    message = """
    This script creates a new task with specific host and vt!
    It needs two parameters after the script name.
    First one is name of the target and the second one is the
    chosen host. The task is called target-task

    Example:
        $ gvm-pyshell ssh newtask target host
    """
    print(message)
    quit()

target = args.script[1]
host = args.script[2]
task = target + " Task"

# Full and Fast
myconfig_id = "daba56c8-73ec-11df-a475-002264764cea"

# OpenVAS Scanner
myscanner_id = "08b69003-5fc2-4037-a479-93b440211c73"

res=gmp.create_target(target, True, hosts=host)
mytarget_id = res.xpath('@id')[0]

res=gmp.create_task(name=task,
                    config_id=myconfig_id,
                        scanner_id=myscanner_id,
                            target_id=mytarget_id)
mytask_id = res.xpath('@id')[0]

gmp.start_task(mytask_id)
```

15.3.3 Example Scripts

The gvm-tools come with a collection of example scripts which can be used by the command `gvm-script`.

Currently the following scripts are available for gvm-tools version 2.0.0 (https://github.com/greenbone/gvm-tools/tree/main/scripts):

- application-detection.gmp.py: this script displays all hosts with the searched application.
- cfg-gen-for-certs.gmp.py: this script creates a new scan configuration with VTs based on a given CERT-Bund advisory.
- clean-sensor.gmp.py: this script removes all resources from a sensor except active tasks.
- create-dummy-data.gmp.py: this script generates dummy data.
- DeleteOverridesByFilter.gmp.py: this script deletes overrides using a filter.
- monthly-report2.gmp.py: this script displays all vulnerabilities based on the reports of a given months. Made for GOS 4.x.
- monthly-report.gmp.py: this script will display all vulnerabilities based on the reports of a given months. Made for GOS 3.1.
- nvt-scan.gmp.py: this script creates a new task with a specific host and VT using a hardcoded base configuration.
- startNVTScan.gmp.py: this script creates a new task with a specific host and VT interactively.
- SyncAssets.gmp.py: this script uploads assets to the asset database.
- SyncReports.gmp.py: this script pulls reports and uploads them to a second appliance using container tasks.

Tip: These scripts can serve as a starting point for the development of custom scripts.

15.4 Status Codes

GMP uses status codes similar to HTTP status codes. The following codes are used:

2xx: The command was sent, understood and accepted successfully.

200: OK

201: Resource created

202: Request submitted

4xx: A user error occurred.

400: Syntax error This includes different syntax errors. Often elements or attributes in the GMP command are missing. The status text shows additional information.

Currently this status code is also used for missing or wrong authentication.

401: Authenticate First This is the error code that is used for missing or wrong authentication. Currently the value 400 is still used.

403: Access to resource forbidden This is the error code that is used for not having enough permissions. Often *400: Permission denied* is displayed instead as well.

404: Resource missing The resource could not be found. The resource ID was empty or wrong.

409: Resource busy This error code happens, for example, if the feed synchronization is started while it is already in progress.

5xx: A server error occurred.

500: Internal Error This can be caused by entries that exceed an internal buffer size.

503: Scanner loading NVTs The scanner is currently busy loading the VTs from its cache. The request should be made again at a later time.

503: Service temporarily down Possibly the scanner daemon is not running. Often the problem are expired certificates.

503: Service unavailable The GMP command is blocked on the appliance.

CHAPTER 16

Using a Master-Sensor Setup

Note: This chapter documents all possible menu options.

However, not all appliance models support all of these menu options. Check the tables in Chapter *3* (page 20) to see whether a specific feature is available for the used appliance model.

Due to security reasons it is often not possible to scan specific network segments directly. For example, direct access to the internet may be prohibited. To overcome this issue, the Greenbone Enterprise Appliance supports the setup of a distributed scan system: two or more appliances in different network segments can be connected securely in order to run vulnerability tests for those network segments that are otherwise not accessible.

In this case, one appliance controls one or more other appliances remotely. A controlling appliance is referred to as a “master” and a controlled appliance is referred to as a “sensor”.

Master

- All appliance models from Greenbone Enterprise 400/DECA can be used as a master (see Chapter *3* (page 20)).

Sensor

- All appliance models except for Greenbone Enterprise ONE can be used as a sensor.
- The appliance models Greenbone Enterprise 35 and 25V can only be used as a sensor and are always controlled by a master.
- All sensors can be managed directly by the master including automatic or manual feed updates as well as upgrades of the Greenbone Operating System (GOS).
- A sensor does not require any network connectivity other than to the master and the scan targets.
- A sensor does not require any further administrative steps after the initial setup.
- If a sensor should perform scans remotely, it has to be configured as a remote scanner.
  - The user can configure a scan for the remote scanner individually using the web interface of the master depending on requirements and permissions.

  - The remote scanner runs the scan and relays the results to the master where all vulnerability information is managed.
  - The connection to a remote scanner is established by using the Open Scanner Protocol (OSP) via SSH.

The connection between master and sensor is established using the Secure Shell (SSH) protocol via port 22/TCP.

To distinguish between the sensor and remote scanner terminology:

- **Sensors** This feature requires the setup of the master-sensor link using the GOS administration menu of both the master and the sensor. This feature then supports the remote feed synchronization and the upgrade management of the sensor.
- **Remote Scanners** This feature requires the setup of the remote scanner using the web interface on the master. This feature then supports the execution of scans via the sensor.

16.1 Configuring a Master-Sensor Setup

A master can be linked to a sensor as follows:

1. Open the GOS administration menu of both the master and the sensor (see Chapter *7.1.2.2* (page 68)).
2. In the GOS administration menu of the master, select *Setup* and press `Enter`.
3. Select *Master* and press `Enter`.
4. Select *Master Identifier* and press `Enter`.
5. Select *Download* and press `Enter` (see Fig. 16.1).

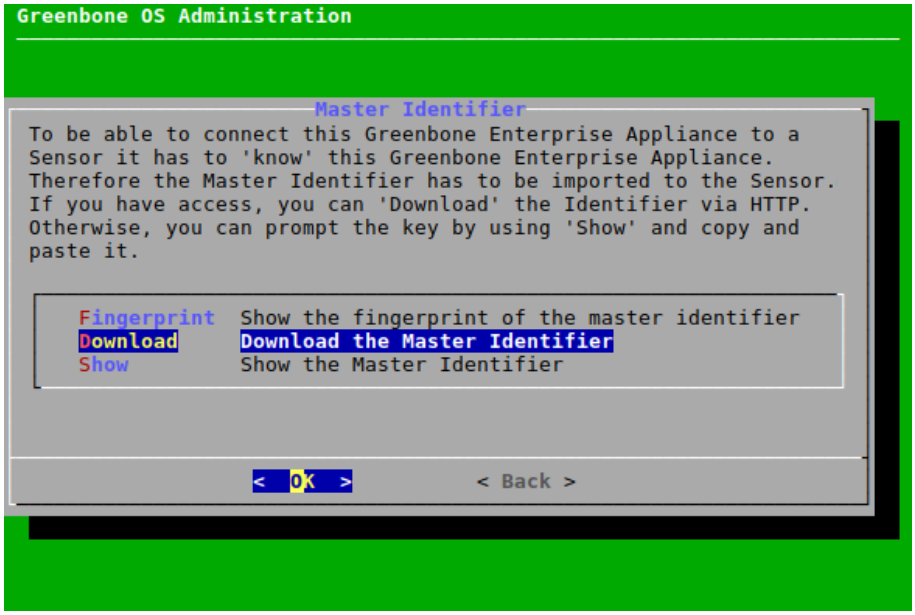


Fig. 16.1: Configuring the master

6. Open the web browser and enter the displayed URL.
7. Download the PUB file.

   → When the key is downloaded, the GOS administration menu of the master displays the fingerprint of the key for verification.

Important: Do not confirm the fingerprint until the key is uploaded to the sensor.

8. In the GOS administration menu of the sensor, select *Setup* and press `Enter`.
9. Select *Sensor* and press `Enter`.
10. Select *Configure Master* and press `Enter` (see Fig. 16.2).

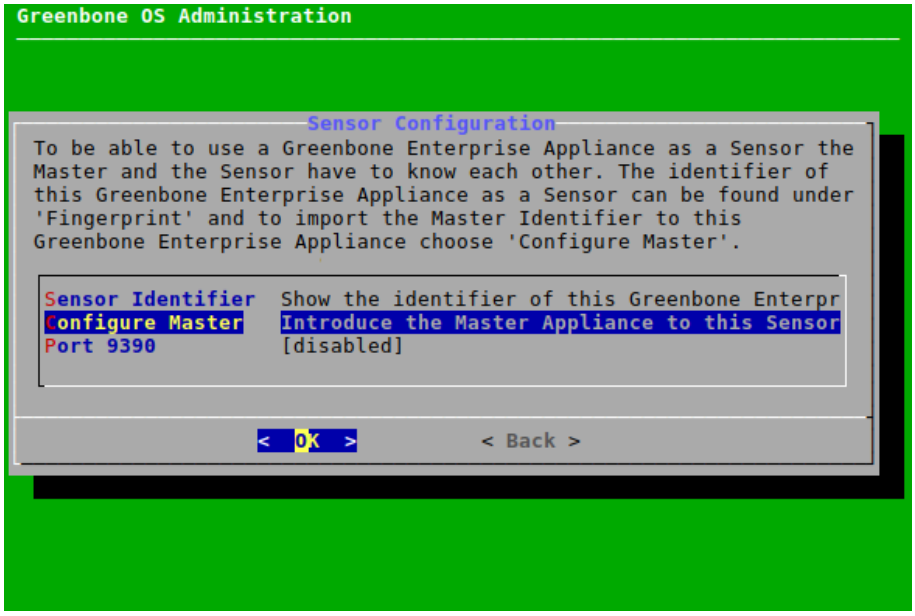


Fig. 16.2: Configuring the sensor

11. Select *Upload* and press `Enter`.
12. Open the web browser and enter the displayed URL.
13. Click *Browse...*, select the previously downloaded PUB file and click *Upload*.

    → When the key is uploaded, the GOS administration menu of the sensor displays the fingerprint of the key for verification.
14. Compare the fingerprint to the fingerprint displayed in the GOS administration menu of the master.

    If the fingerprints match, press `Enter` in both GOS administration menus.
15. In the GOS administration menu of the sensor, select *Save* and press `Enter`.
16. Perform twice: press `Tab` and press `Enter`.
17. Select *Services* and press `Enter`.
18. Select *SSH* and press `Enter`.
19. Select *SSH State* and press `Enter`.

    → SSH is enabled on the sensor.
20. Select *Save* and press `Enter`.
21. Press `Tab` to select *Back* and press `Enter`.
22. Select *OSP* and press `Enter`.
23. Press `Enter` to enable OSP.

    → A message informs that the changes have to be saved (see Chapter *7.1.3* (page 70)).

24. Press `Enter` to close the message.
25. Select *Save* and press `Enter`.

    → OSP is enabled on the sensor.
26. In the GOS administration menu of the master, select *Setup* and press `Enter`.
27. Select *Master* and press `Enter`.
28. Select *Sensors* and press `Enter`.
29. Select *Add a new sensor* and press `Enter`.
30. Enter the IP address or the host name of the sensor in the input box and press `Enter`.

    → Additional menu options for the sensor configuration are shown (see Fig. 16.3, see Chapter *16.2* (page 375)).

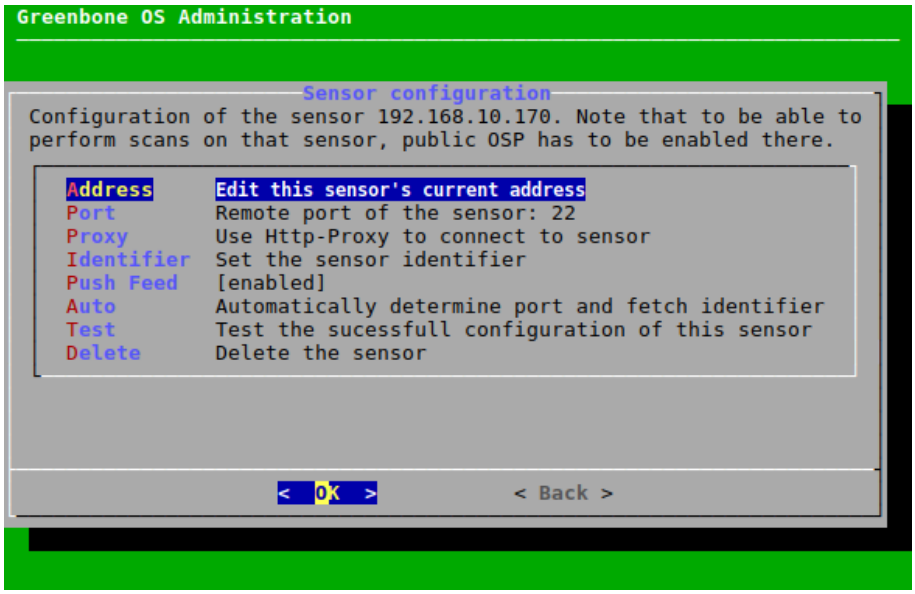


Fig. 16.3: Sensor configuration menu

31. Select *Auto* and press `Enter`.

    → The master connects to the sensor automatically and retrieves the identifier.

    The fingerprint of the identifier is displayed in the GOS administration menu of the master.
32. In the GOS administration menu of the sensor, select *Setup* and press `Enter`.
33. Select *Sensor* and press `Enter`.
34. Select *Sensor Identifier* and press `Enter`.
35. Select *Fingerprint* and press `Enter`.
36. Compare the fingerprint to the fingerprint displayed in the GOS administration menu of the master.

    If the fingerprints match, press `Enter` in the GOS administration menu of the master.
37. Select *Save* and press `Enter`.
38. Select *Test* and press `Enter`.

    → The configuration of the sensor is tested.

    If the test fails, a warning with instructions is displayed (see Fig. 16.4).

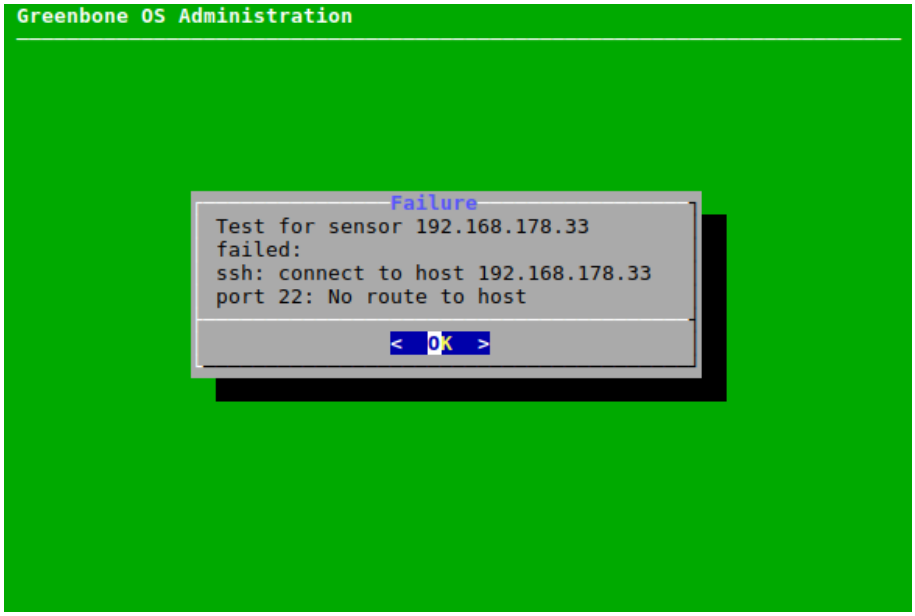


Fig. 16.4: Testing the sensor configuration

Note: Once configured successfully, sensors can be managed directly on the master using the GOS administration menu (see Chapters *7.3.5* (page 150) and *7.3.7* (page 151)).

16.2 Managing all Configured Sensors

All sensors configured on a master can be displayed as follows:

1. Select *Setup* and press `Enter`.
2. Select *Master* and press `Enter`.
3. Select *Sensors* and press `Enter`.

   → Actions for all configured sensors are displayed (see Fig. 16.5).

The following actions are available:

Testing all sensor connections Test whether all sensors are configured correctly. If the test fails, a warning with instructions is displayed.

Update all sensor protocols Update all sensor protocol configurations on the master.

Edit/Delete the sensor ... Open the menu for configuring a specific sensor (see Fig. 16.3). The following actions are available:

- Setting the address of the sensor.
- Setting the remote port of the sensor.
- Setting the proxy for the sensor.
- Setting the sensor identifier.
- Enabling/disabling automatic feed updates on the sensor if the feed is updated on the master.
- Setting the port and the identifier automatically.

- Testing the correct configuration of the sensor.
- Deleting the sensor.

Add a new sensor Configure a new sensor (see Chapter *16.1* (page 372)).

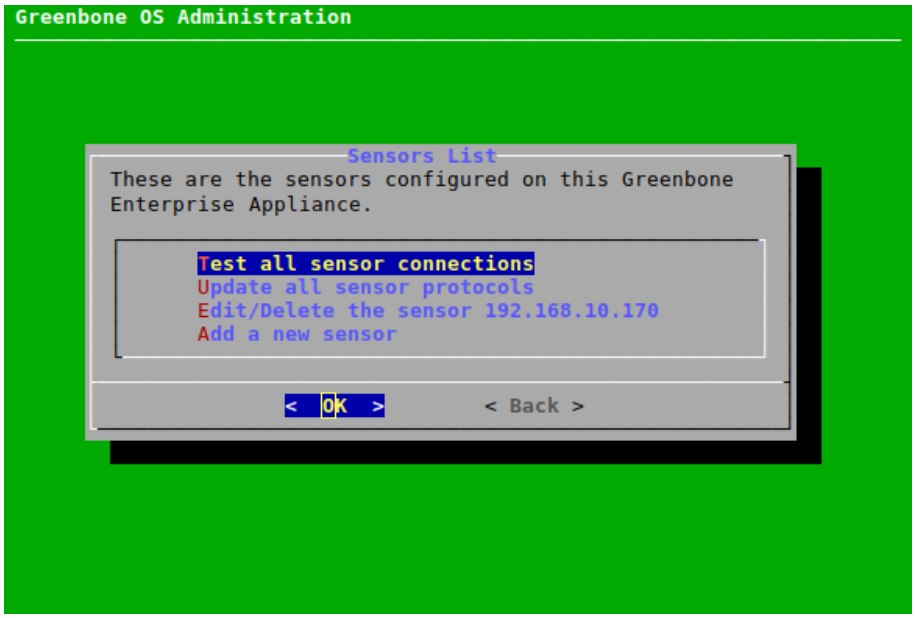


Fig. 16.5: Managing all configured sensors

16.3 Deploying Sensors in Secure Networks

For master-sensor setups the master stores all vulnerability information and credentials. A sensor does not store any information permanently (except for VTs).

Due to this the master needs to be placed in the highest security zone with communication to the outside (to the sensors). All communication is initiated from the master in the higher security zone down to the sensor in the lower security zone.

Note: A firewall separating the different zones only needs to allow connections from the master to the sensor. No additional connections need to be allowed into the higher security zone.

Master and sensor appliances communicate via the SSH protocol. Port 22/TCP is used by default. For backward compatibility port 9390/TCP can be used. This can be configured as follows:

1. In the GOS administration menu of the sensor, select *Setup* and press `Enter`.
2. Select *Sensor* and press `Enter`.
3. Select *Port 9390* and press `Enter`.
4. Select *Save* and press `Enter`.

On sensors, Greenbone Enterprise Feed updates and GOS upgrades can be downloaded either directly from the Greenbone servers or using the master. In the second case, only the master contacts the Greenbone servers and distributes the corresponding files to all connected sensors.

To prevent the sensor from contacting the Greenbone servers, automatic synchronization can be disabled as follows:

1. In the GOS administration menu of the sensor, select *Setup* and press `Enter`.
2. Select *Feed* and press `Enter`.
3. Select *Synchronisation* and press `Enter`.
4. Select *Save* and press `Enter`.

Tip: As an additional layer of security a source and destination NAT rule on a firewall using stateful packet inspection (SPI) can be used to avoid the need of default routes on the appliances.

16.4 Configuring a Sensor as a Remote Scanner

Note: In order to configure a sensor as a remote scanner, all steps in Chapter *16.1* (page 372) have to be completed first.

Sensors can be used as remote scanning engines (scanners) on the master in addition to the default OpenVAS and CVE scanners. For this, the sensor must be configured as a remote scanner using the web interface of the master.

A new remote scanner can be configured as follows:

1. Log into the web interface of the master.
2. Select *Configuration* > *Scanners* in the menu bar.
3. Create a new scanner by clicking .
4. Enter the name of the remote scanner in the input box *Name* (see Fig. 16.6).

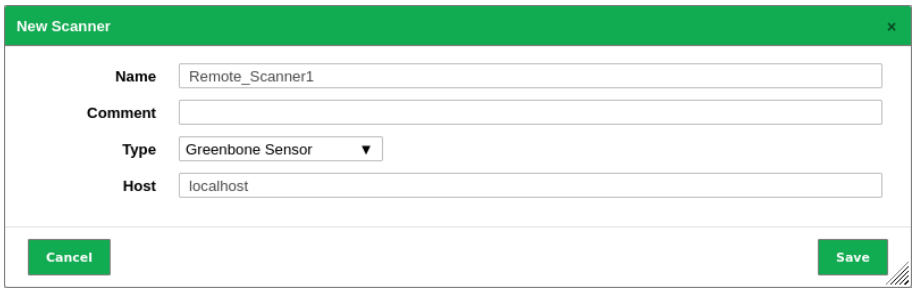


Fig. 16.6: Configuring the remote scanner on the master

5. Select *Greenbone Sensor* in the drop-down list *Type*.

   Note: It is mandatory to select *Greenbone Sensor*. The type *OSP Scanner* must not be used.

6. Enter the IP address or the host name of the sensor in the input box *Host*.
7. Click *Save* to create the remote scanner.

   → The scanner is created and displayed on the page *Scanners*.

8. In the row of the newly created remote scanner, click to verify the scanner.

   → If the setup is correct, the scanner is successfully verified.

Tip: Scanners are configured on a per-user basis. Scanners can be created for each user or permissions can be used to grant usage rights to other users (see Chapter *9.4* (page 193)).

16.5 Using a Remote Scanner

After a sensor is configured as a remote scanner, it can be selected as the scanner when creating a new scan task or a new audit (see Chapters *10.2.2* (page 215) and *12.2* (page 317)).

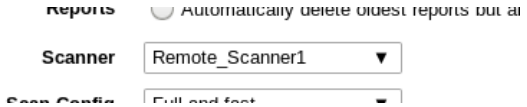


Fig. 16.7: Selecting the remote scanner for a task or audit

Tip: There are two options for using the remote scanner for an existing task or audit:

- If the task/audit is marked as alterable in the column *Name* (see Chapters *10.8* (page 254) and *12.2.3* (page 319)), change the scanner of the task/audit.
- Clone the task/audit and change the scanner of the clone.

CHAPTER 17

Managing the Performance

When operating the Greenbone Enterprise Appliance, significant amounts of data can be transferred between the appliance, the scan targets and any sensor appliances. In addition to that, the scan results have to be analyzed, filtered and processed by the appliance. Depending on the appliance model, the number of users and the configuration of the scan tasks, many of these processes will run concurrently.

17.1 Monitoring the Appliance Performance

The overall performance of the Greenbone Enterprise Appliance can be monitored by selecting *Administration > Performance* in the menu bar (see Fig. 17.1).

The resource utilization of the appliance for the last hour, day, week, month or year can be displayed.

Note: The performance of a configured sensor can be displayed on the master as well.

The following sections are important:

Processes A high amount of processes is not critical. However, primarily only sleeping and running processes should be displayed.

System Load An ongoing high utilization is critical. A load of 4 on a system with 4 cores is considered acceptable.

CPU Usage Especially a high Wait-IO is critical.

Memory Usage The appliance uses aggressive caching. The usage of most of the memory as cache is acceptable.

Swap Usage A use of the swap memory points to a potential system overload.

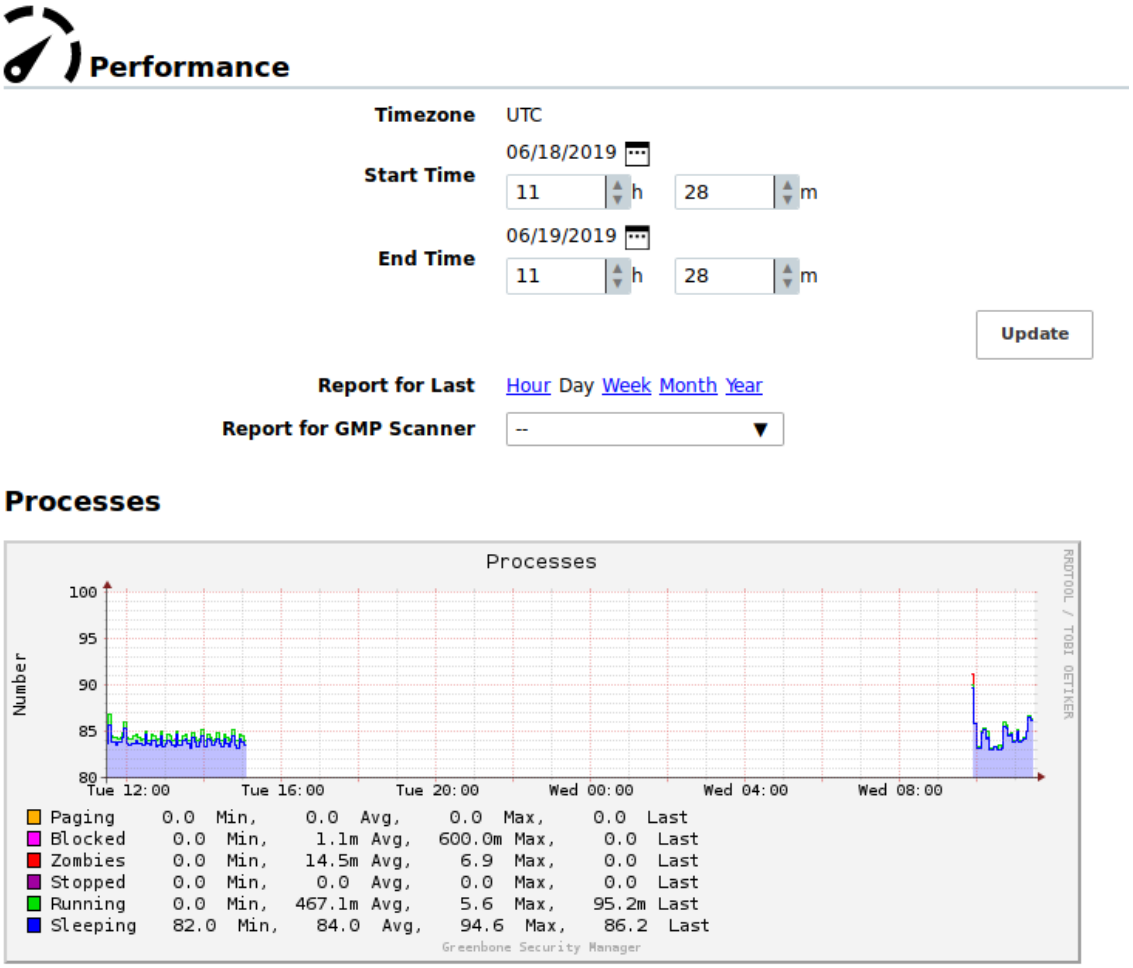


Fig. 17.1: Displaying the performance of the appliance

17.2 Optimizing the Scan Performance

The speed of a scan depends on many parameters:

- Selected ports
- Selected scan configuration
- Scanning order of targets

17.2.1 Selecting a Port List for a Task

The port list configured for a target has a large impact on the duration of the alive test and the vulnerability scan of this target.

17.2.1.1 General Information about Ports and Port Lists

Ports are the connection points of network communication. Each port of a system connects with the port on another system.

Transmission Control Protocol (TCP) ports

- 65535 TCP ports for each system
- Data transmission occurs in both directions between two TCP ports.
- The scan of TCP ports is usually performed simply and fast.

User Datagram Protocol (UDP) ports

- 65535 UDP ports for each system
- Data transmission occurs only in one directions between two UDP ports.
- Data received by UDP are not necessarily confirmed, so the testing of UDP ports usually takes longer.

Ports 0 to 1023 are privileged or system ports and cannot be opened by user applications[72].

The Internet Assigned Numbers Authority (IANA)[70] assigns ports to standard protocols, e.g., port 80 to “http” or port 443 to “https”. Over 5000 ports are registered.

Scanning all ports takes too long in many cases and many ports are usually not used. To overcome this, port lists can be used.

All ports of all systems of all internet accessible systems were analyzed and lists of the most used ports were created. Those do not necessarily reflect the IANA list because there is no obligation to register a specific service type for a respective port. Nmap[71], an open-source port scanner, and the OpenVAS scanner use different lists by default and do not check all ports either.

For most scans it is often enough to scan the ports registered with the IANA.

The following port lists are predefined on the appliance:

- All IANA assigned TCP: all TCP ports assigned by the Internet Assigned Numbers Authority (IANA), continuously updated
- All IANA assigned TCP and UDP: all TCP and UDP ports assigned by the Internet Assigned Numbers Authority (IANA), continuously updated
- All privileged TCP

[72] On Unix-like systems, access to privileged ports is restricted to privileged users (i.e., root). Ports starting at 1024 are also available to non-privileged users.

[70] https://www.iana.org/

[71] https://nmap.org/

- All privileged TCP and UDP
- All TCP
- All TCP and Nmap top 100 UDP: all TCP ports and the top 100 UDP ports according to the Nmap network scanner, continuously updated
- All TCP and Nmap top 1000 UDP: all TCP ports and the top 1000 UDP ports according to the Nmap network scanner, continuously updated
- Nmap top 2000 TCP and top 100 UDP: the top 2000 TCP ports and the top 100 UDP ports according to the Nmap network scanner, continuously updated
- OpenVAS Default: the TCP ports which are scanned by the OpenVAS scanner when passing the default port range preference

Note: Additional port lists can be created as described in Chapter *10.7* (page 252).

17.2.1.2 Selecting the Right Port List

When choosing a port list discovery performance and scan duration have to be taken into account.

The duration of a scan is mostly determined by the network configuration and the amount of ports to be tested.

Services not bound to ports on the list are not tested for vulnerabilities. Additionally, malicious applications that are bound to such ports will not be discovered. Malicious applications mostly use open ports that are usually not used and are far from the system ports.

Other criteria are the defense mechanisms that are activated by exhaustive port scans and initiate countermeasures or alerts. Even with normal scans, firewalls can simulate that all 65535 ports are active and as such slow down the actual scan with so called time-outs.

Additionally, for each port that is queried the service behind it reacts at least with one log entry. For organizational reasons some services may only be scanned at a specific time.

Scan Duration

In some situations with port throttling, scanning all TCP and UDP ports can take up to 24 hours or more for a single system. Since the scans are performed in parallel, two systems will only take marginally more time than a single system. However, the parallelizing has its limits due to system resources and network performance.

All IANA TCP ports usually require only a couple of minutes to be scanned.

Since some countermeasures can increase the duration of a scan, throttling can be prevented by making configuration changes on the defense system.

In suspected cases of a compromise or highest security breaches a fully inclusive scan is unavoidable.

Total Security

For port scans total security does not exist, i.e., even when all TCP and all UDP ports are scanned the preset timeout of the port testing can be too short to force a hidden malicious application to respond.

If an initial suspicion exists, an experienced penetration tester should be consulted.

17.2.2 Selecting a Scan Configuration for a Task

The scan configuration has an impact on the scan duration as well. The appliance offers four different scan configurations for vulnerability scans:

- Full and fast
- Full and fast ultimate
- Full and very deep
- Full and very deep ultimate

The scan configurations *Full and fast* and *Full and fast ultimate* optimize the scan process by using information found earlier in the scan. Only VTs that are useful are executed, resulting in a reduced scan duration.

Scans using the scan configurations *Full and very deep* and *Full and very deep ultimate* ignore already discovered information and execute all available VTs without exception.

17.2.3 Selecting the Scanning Order of Targets

During a scan the correspconding status bar on the page *Tasks* reflects the progress of the scan in percent (see Chapter *10.8* (page 254)).

In most cases this progress is a rough estimation since it is difficult for the appliance to project how the systems or services that have not been scanned yet behave compared to the already scanned systems and services.

Example A target network `192.168.0.0/24` that has only 5 alive hosts with the IP addresses `192.168.0.250-254` should be scanned. When creating a task with default settings for this target, the scanner will try to scan all possible hosts in the target network sequentially.

Since no hosts can be scanned for the IP addresses `192.168.0.1-249`, the scanner skips these hosts and the scan progress reaches 95 % very quickly, indicating that the scan is almost finished.

Then the hosts with the IP addresses `192.168.0.250-254` are scanned and for each host, the vulnerability tests take some time. As a consequence, the scan progress is noticeably slower between 95 % and 100 %.

In order to improve the progress estimation, the setting *Order for target hosts* can be adjusted when creating a new task (see Chapter *10.2.2* (page 215)).

The setting *Random* is recommended (see Fig. 17.2).

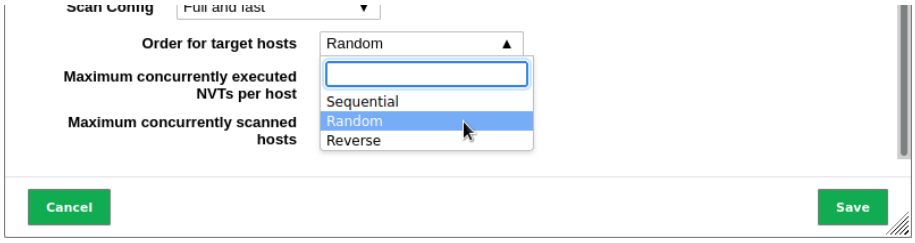


Fig. 17.2: Selecting the order for targets

17.3 Scan Queuing

When ▷ is clicked for a task or an audit, it is added to a waiting queue and gets the status *Queued*. The scanner only begins the scan if sufficient system resources are available. The available resources depend on the appliance model, the GOS version used, and the current workload of the system. Additionally, the queued scans are started at 1 minute intervals to avoid overloading the system.

The most relevant resource for scanning is random-access memory (RAM). Each scan requires a certain minimum of RAM to be executed properly because the same scan process cannot handle multiple scans from different users or even from the same user. RAM has physical limits and cannot be shared in a satisfactory way.

CPU, network connection and disk I/O are relevant system resources as well. However, unlike RAM, they can be shared at the cost of slower scan execution.

The system performance charts provide detailed information about the RAM over time (see Chapter *17.1* (page 379)).

In some cases, tasks/audits remain in the waiting queue:

- Too many tasks/audits are started and running at the same time and not enough RAM is available.
- The appliance is performing a feed update and is currently loading new VTs.
- The appliance was just started and is currently loading the VTs.

When the required RAM is available again, or the loading of the VTs is finished, tasks/audits from the waiting queue are started, following the principle “first in, first out”.

The workload management is subject to the scanner. If a master-sensor setup is used, each sensor manages its available resources on its own. Sensor scans affect the scanning capacity of the master only minimally.

CHAPTER 18

Connecting the Greenbone Enterprise Appliance to Other Systems

The Greenbone Enterprise Appliance can be connected to other systems.

Some systems have already been integrated into the appliance by Greenbone:

- verinice ITSM system (see Chapter *18.1* (page 386))
- Nagios Monitoring System (see Chapter *18.2* (page 390))
- Cisco Firepower Management Center (see Chapter *18.3* (page 394))

The appliance offers numerous interfaces that allow for the communication with other systems:

Greenbone Management Protocol (GMP) The Greenbone Management Protocol allows to remote control the appliance completely. The protocol supports the creating of users, creating and starting of scan tasks and exporting of reports.

Report format The appliance can present the scan results in any format. To do so, the appliance already comes with a multitude of pre-installed report formats (see Chapter *11.1* (page 283)). Additional report formats may be developed in collaboration with Greenbone.

Alert via Syslog, e-mail, SNMP trap or HTTP (see Chapter *10.12* (page 272))

Automatic result forwarding through connectors These connectors are created by Greenbone, verified and integrated into the appliance.

Monitoring via SNMP The webpage https://docs.greenbone.net/API/SNMP/snmp-gos-22.04.en.html provides the current Management Information Base (MIB) file. MIB files describe the files that can be queried by SNMP about the equipment.

18.1 Using Verinice

Verinice[73] is a free open-source Information Security Management System (ISMS) developed by SerNet[74].

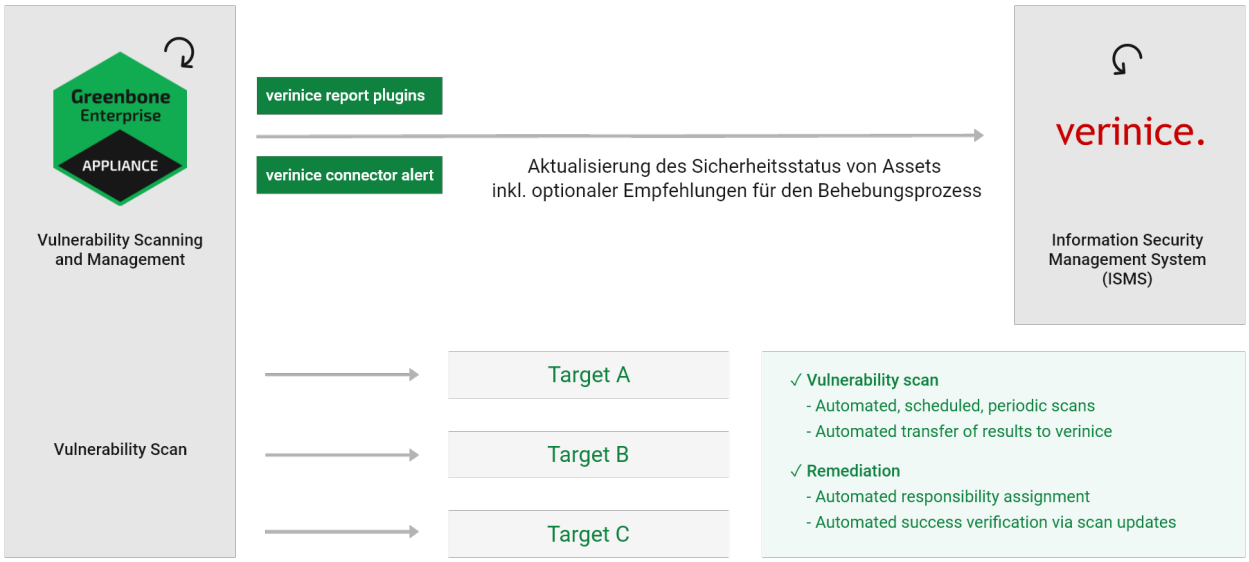


Fig. 18.1: Integrating the appliance with verinice

Verinice is suitable for:

- Vulnerability remediation workflow
- Performing risk analysis based on ISO 27005
- Operating an ISMS based on ISO 27001
- Performing an IS assessment per VDA specifications
- Proof of compliance with standards such as ISO 27002, IDW PS 330

The appliance can support the operation of an ISMS. For this, Greenbone offers two report formats for exporting the data from the appliance into verinice:

- Verinice ISM
- Verinice ISM all results

It is possible to transfer data completely automated from the appliance to verinice.PRO, the server extension of verinice.

Note: For support with the use of the connector, contact SerNet or the Greenbone Enterprise Support[75].

[73] https://verinice.com/en/
[74] https://www.sernet.de/en/
[75] https://www.greenbone.net/en/technical-support/

18.1.1 IT Security Management

The report formats *Verinice ISM* and *Verinice ISM all results* for verinice are available via the Greenbone Enterprise Feed. With these report formats, Greenbone supports the vulnerability remediation workflow in verinice.

Verinice ISM When using the report format *Verinice ISM*, verinice uses the notes feature (see Chapter *11.7* (page 305)) to create objects for processing. A note must be attached to each scan results that should be transferred to verinice. If this report format is used and there are no notes in a task, only the assets as well as the complete vulnerability report will be imported.

Verinice ISM all results When using the report format *Verinice ISM all results*, all results are transferred by default. It is not necessary, to attach a note to the results that should be transferred to verinice.

After the scan is completed, the report must be exported using one of the report formats explained above (see Chapter *11.2.2* (page 292)). A VNA file is created. This is a ZIP file containing the scan data.

Note: For the following example SerNet verinice 1.18.1 was used.

If another version is used, the steps may differ. Contact the verinice support for help.

18.1.1.1 Importing the ISM Scan Report

The report can be imported in verinice as follows:

1. Start verinice.
2. Select *View > Show Perspective > Information Security Management* in the menu bar (see Fig. 18.2).

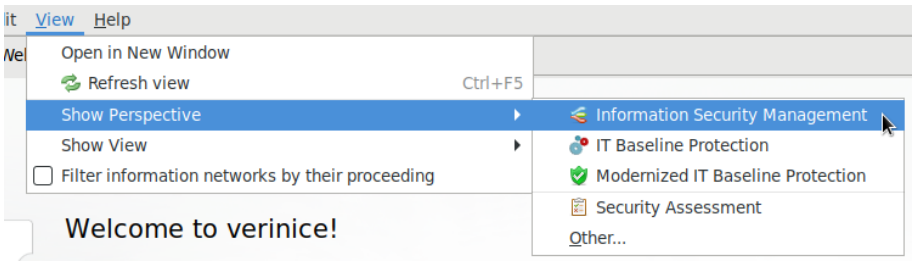


Fig. 18.2: Opening the perspective *Information Security Management*

3. Click in the window *Catalogs* to import the desired catalog.
4. Create an organization by clicking (see Fig. 18.3).

Note: The window for defining the details of the organization can simply be closed.

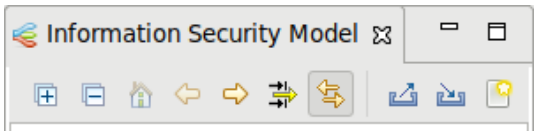


Fig. 18.3: Creating a new organization

5. In the window *Information Security Model* click .

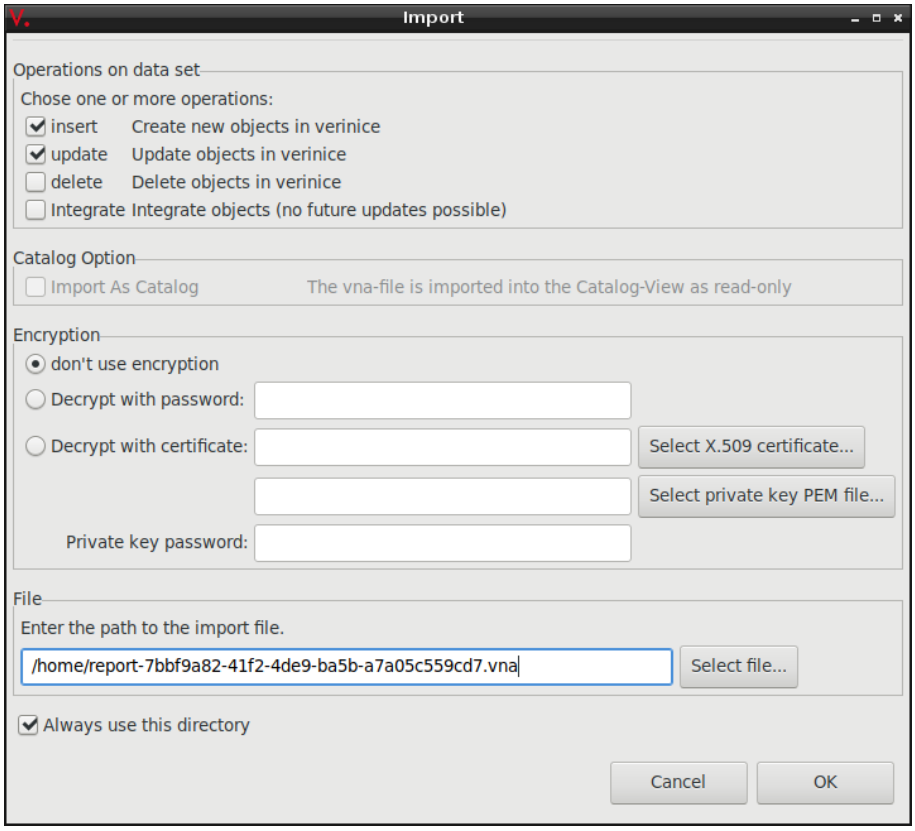


Fig. 18.4: Selecting the ISM report

6. Click *Select file...* and select the ISM report. The remaining parameters can be kept with their default settings (see Fig. 18.4).
7. Click *OK*.

   → The results of the ISM report are imported and can be unfolded in verinice (see Fig. 18.5).

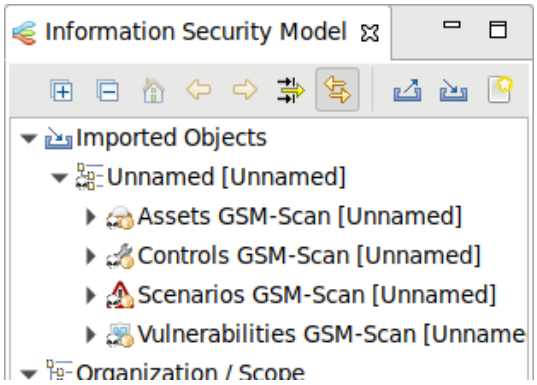


Fig. 18.5: Unfolding the results of the ISM report

The process to track vulnerabilities for the imported organization can be separated into two sub processes:

- Creation of tasks
- Remediation of vulnerabilities

18.1.1.2 Creating Tasks

Before creating tasks the data for the organization must be prepared as follows:

1. After the first import of an organization it must be moved from the group of imported objects to the top level.

   Right click on the organization and select *Cut*. Click right in the top level in the window *Information Security Model* and select *Paste*.

2. The assets and controls must be grouped.

   Right click on *Assets GSM-Scan* and select *Group by Tags...* (see Fig. 18.6).

   Confirm the message by clicking *OK*.

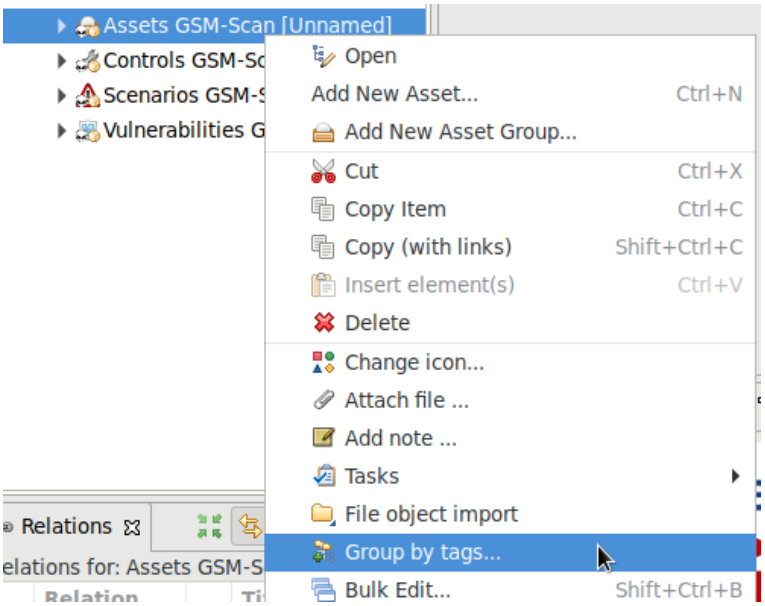


Fig. 18.6: Grouping the assets

3. Right click on *Controls GSM-Scan* and select *Group by Tags...*.

   Confirm the message by clicking *OK*.

4. All assets groups must be assigned a responsible person.

   Expand the organization, right click on *Persons* and select *Add Person...*.

5. Assign the newly created person per drag and drop to the assets group.

   → The successful assignment can be displayed in the window *Relations* by clicking *Assets GSM-Scan* (see Fig. 18.7).

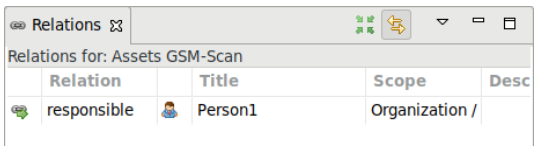


Fig. 18.7: Displaying the relations for a group

6. Right click on the organization and select *Tasks > Greenbone: Start vulnerability process...*.

   → It is verified whether all assets and controls are grouped and whether all asset groups are assigned to a person. A message displays the result of the verification.

7. Continue with creating a task or cancel the creation.

   The task to remediate vulnerabilities is called “Remediate Vulnerabilities”.

18.1.1.3 Remediating Vulnerabilities

The created tasks can be managed with the help of the view *Task* (*View* > *Show View* > *Tasks* in the menu bar) or the web frontend of the verinice.PRO version (under: ISO 27000 tasks).

A task contains controls, scenarios and assets that are connected to a control group and are assigned to a responsible person. The responsible person remediates the vulnerabilities for all assets.

Note: If the deadline for the task “Remediate Vulnerabilities” expires, a reminder e-mail is sent to the responsible person.

After the task is completed all connections between assets and scenarios that were assigned to a task are deleted.

The following states of a control are possible:

- Implemented: no asset is assigned to the scenario anymore.
- Partly: other connections to assets still exist.

18.2 Using Nagios

Nagios can integrate the scan results as an additional test in its monitoring tasks. The scanned systems are automatically matched with the monitored systems. With this the scan results are eventually available for the alert rules and other processes of Nagios.

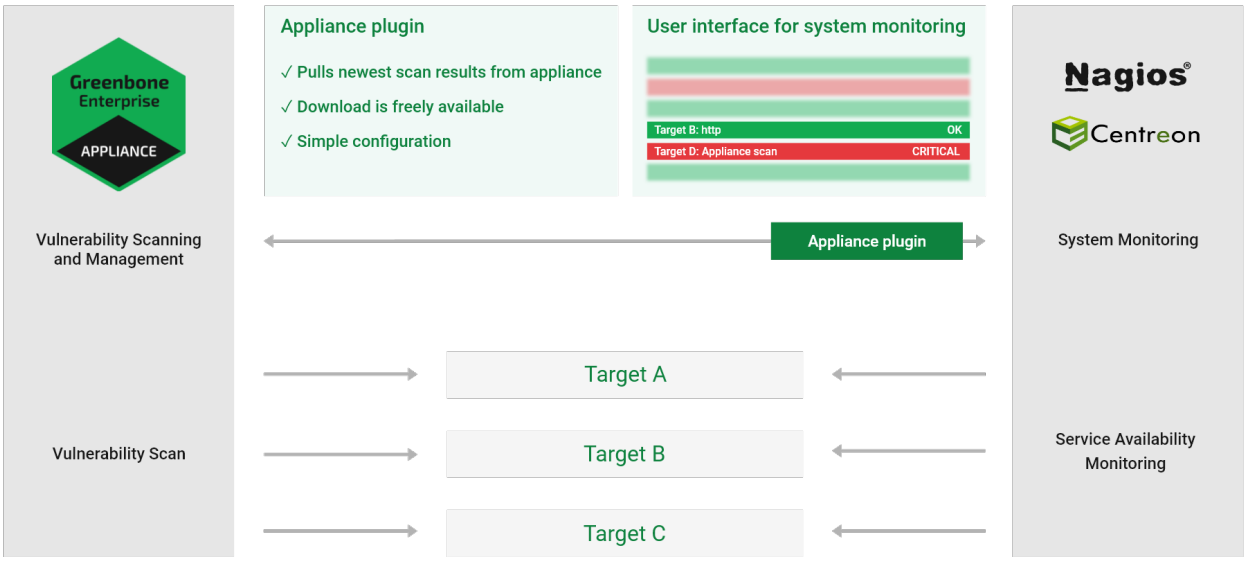


Fig. 18.8: Linking Nagios with the appliance

When linking Nagios with the appliance, Nagios will assume the controlling role.

Nagios retrieves the newest scan results from the appliance regularly and automatically. This is done via a Nagios command which uses the tool `gvm-script` to call the script `check-gmp.gmp.py`.

Note: Other products compatible with Nagios such as Open Monitoring Distribution, Icinga, Centreon etc. should generally work but may require small adjustments to the described steps.

18.2.1 Configuring the Appliance User

For access, Nagios requires a user to log in to the appliance. For this user a scan target (or multiple scan targets) has to be set up with all hosts of which the security status should be monitored.

Note: The sample configuration used here assumes that there is only one relevant target but technically it is possible to link complex setups with multiple targets and multiple appliances.

The appliance user account provided for queries by the GMP script must be owner of the relevant scan targets or at least have unrestricted reading access to them.

The tasks should be run as scheduled scans regularly.

Additionally, network access via GMP to the appliance must be possible. Therefore, the GMP access must be activated in the GOS administration menu (see Chapter *15.2* (page 361)).

18.2.2 Configuring the Script

Greenbone provides the script `check-gmp.gmp.py` as part of the script collection of the gvm-tools (see Chapter *15.3* (page 362)). This script can be called by the monitoring solution using `gvm-script`.

Note: The following assumes Nagios is installed in `/usr/local/nagios/`, afterwards referred to as `/.../`.

Adjust the file location if necessary.

1. Copy the plug-in to `/.../libexec/`.
2. Check if the script can reach the appliance through the network, GMP was activated and the user was created properly:

   Note: In the following command, replace the IP address with the appliance's IP address and provide the user name and the created password.

```
nagios-host# gvm-script --gmp-username="user name" --gmp-password="password" \
ssh --hostname 192.168.10.169 /.../libexec/check-gmp.gmp.py --ping \
GMP OK: Ping successful
```

3. Check whether there is access to the data:

```
nagios-host# gvm-script --gmp-username="user name" --gmp-password="password" \
ssh --hostname 192.168.10.169 /.../libexec/check-gmp.gmp.py \
-F 192.168.10.130 --last-report -T "Scan Suspect Host" --status
GMP CRITICAL: 284 vulnerabilities found - High: 118 Medium: 153 Low: 13
Report did contain 1 errors for IP 192.168.10.130
|High=118 Medium=153 Low=13
```

The script supports several command line switches. These can be displayed using:

```
nagios-host# gvm-script -c /.../etc/gvm-tools.conf ssh --hostname
  192.168.10.169 scripts/check-gmp.gmp.py -H
usage: check-gmp [-H] [-V] [--cache [CACHE]] [--clean] [-F HOSTADDRESS] [-T TASK]
...

Check-GMP Nagios Command Plugin 2.0.0 (C) 2017-2019 Greenbone Networks GmbH
...


optional arguments:
-H                    Show this help message and exit.
-V, --version         Show program's version number and exit
--cache [CACHE]       Path to cache file. Default: /tmp/check_gmp/reports.db.
--clean               Activate to clean the database.
...
```

4. If the tests were successful the check can be integrated into Nagios monitor.

   Add the host to be monitored to the section `HOST DEFINITIONS` in the Nagios configuration file `/.../etc/objects/localhost.cfg`.

   In this example the host is a Metasploitable Linux.

```
define host{
     use                     linux-server
     host_name               metasploitable
     alias                   metasploitable
     address                 192.168.10.130
     }
```

5. In the same configuration file, in the section `SERVICE DEFINITIONS`, define a new service which calls the Nagios command `check_gmp_status`.

   As the example shows, the name of the task where to fetch the report from is passed to the command as an argument.

```
define service{
     use                     local-service    ; Name of service template to use
     host_name               metasploitable
     service_description     GMP task last report status
     check_command           check_gmp_status!metasploitable
     }
```

6. Create the `check_gmp_status` command in the file `/.../etc/objects/commands.cfg`.

```
define command{
    command_name    check_gmp_status
    command_line    gvm-script -c /.../etc/gvm-tools.conf ssh
       --hostname 192.168.10.169 $USER1$/check-gmp.gmp.py -F $HOSTADDRESS$
         --last-report -T $ARG1$ --status
    }
```

Note: In the command line it can be seen that no user name and password options but a configuration file are passed to the tool `gvm-script` (see Chapter *15.3* (page 362)).

7. Restart the Nagios service to apply the new configuration.

```
nagios-host# systemctl restart nagios
```

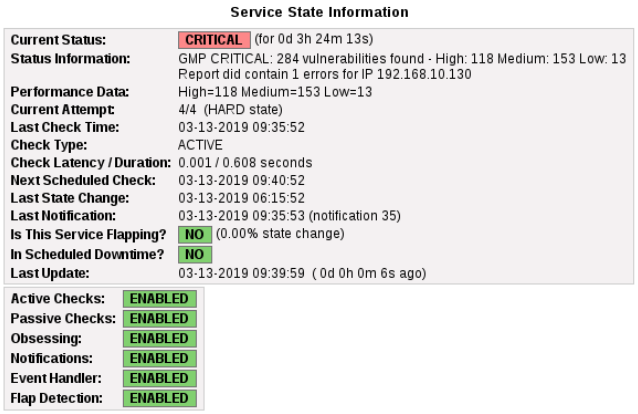


Fig. 18.9: Nagios displaying the monitored host status

18.2.3 Caching and Multiprocessing

The script `check-gmp.gmp.py` supports caching. All new reports will be cached in a SQLite database. The first call with an unknown host will take longer because the report needs to be retrieved from the appliance. Subsequent calls will only retrieve the current report from the appliance if the end time of the scan differs. Otherwise, the information from the database is used. This will greatly reduce the load both on the monitoring server and the appliance.

The cache file is written to `/tmp/check_gmp/reports.db` by default. A different location of the database can be specified using the command line switch `--cache`.

To further reduce the load both on the monitoring server and the appliance, the plug-in can restrict the maximum number of simultaneously running plug-in instances. Additionally started instances are stopped and wait for their continuation. The default value of `MAX_RUNNING_INSTANCES` is 10. The default can be modified using the command line switch `-I`.

18.3 Using the Cisco Firepower Management Center

The Cisco Firepower Management Center (former Sourcefire Intrusion Prevention System (IPS)) is one of the leading solutions for intrusion detection and defense in computer networks. As a Network Intrusion Detection System (NIDS) it is tasked with the discovery, alerting and the defense against attacks on the network.

To identify and classify attacks correctly, the Firepower Management Center requires as much information as possible about the systems in the network, the applications installed on them, and the potential vulnerabilities for both. For this purpose the Firepower Management Center has its own asset database that can be augmented with information from the appliance. Additionally, the Firepower Management Center can start an automatic scan if it suspects anything.

The following connection methods are available:

Automatic data transfer from the appliance to the NIDS/IPS If the appliance and NIDS/IDS are configured respectively, the data transfer from the appliance to the NIDS/IPS can be utilized easily, like any other alert functionality of the appliance. After completion of the scan, the report will be forwarded as an alert to the NIDS/IPS with respect to the desired criteria. If the scan task is run automatically on a weekly basis, a fully automated alerting and optimization system is obtained.

Active control of the appliance by the NIDS/IPS In the operation of the NIDS/IPS, suspected incidents on systems with high risk can occur. In such a case, the NIDS/IPS can instruct the appliance to check the system[78].

Note: To use the connection methods, the option to receive the data must be enabled in the Firepower Management Center.

18.3.1 Configuring the Host-Input-API Clients

The Host-Input-API is an interface through which the Firepower Management Center accepts data from other applications for its asset database.

1. Log into the Firepower Management Center.
2. Select *System* > *Integration* in the menu bar.
3. Select the register *Host Input Client*.
4. Enter the IP address of the appliance in the input box *Hostname* (see Fig. 18.10).

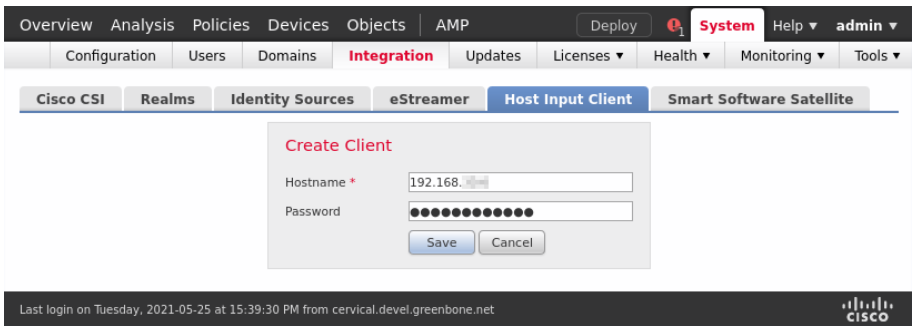


Fig. 18.10: Creating a host input client

5. Enter the password in the input box *Password*.

[78] This control does not exist as a finalized *Remediation* for the Firepower Management Center but it can be implemented via GMP (see Chapter *15* (page 361)).

6. Click *Save*.

   Note: The connection is TLS encrypted.

   → The Firepower Management Center creates a private key and certificate automatically.

   In the certificate the IP address entered above will be used as common name and verified when the client is establishing a connection. If the client uses a different IP address, the connection fails.

   The created PKCS#12 file is optionally secured by a password.

   Afterwards the certificate and the key are created and made available as a download.

7. Click to download the file (see Fig. 18.11).

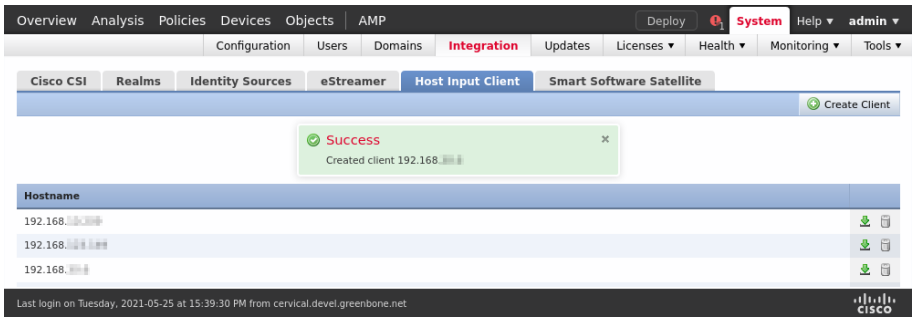


Fig. 18.11: Downloading the created PKCS#12 file

18.3.2 Configuring a Sourcefire Connector Alert

Now the respective alert must be set up on the appliance.

1. Select *Configuration > Alerts* in the menu bar.
2. Create a new alert by clicking .
3. Define the alert (see Fig. 18.12).

   Tip: For the information to enter in the input boxes see Chapter *10.12* (page 272).

4. Choose *Sourcefire Connector* in the drop-down list *Method*.

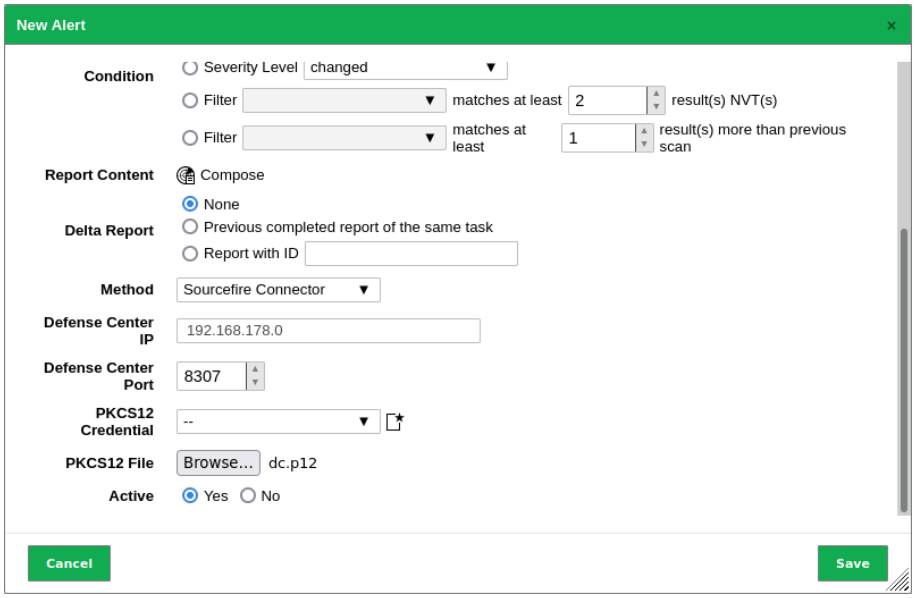


Fig. 18.12: Creating an alert with Sourcefire Connector

5. Enter the IP address of the Management Center in the input box *Defense Center IP*, and the port used to connect to it in the input box *Defense Center Port*.

   Note: If a password was assigned when the client was created, the password for the PKCS#12 file must be provided as a credential (see Chapter *10.3.2.1* (page 219)).

6. Select the credential in the drop-down list *PKCS12 Credential*.

   Note: A new credential can be created by clicking .

7. Provide the PKCS#12 file by clicking *Browse...*.
8. Click *Save*.

18.4 Using Alemba vFire

vFire is an Enterprise Service Management application, developed by Alemba[76].

The appliance can be configured to create tickets in an instance of vFire based on events like finished scans.

18.4.1 Prerequisites for Alemba vFire

For the integration to work properly, the following prerequisites must be met on the vFire system:

- The vFire installation must support the RESTful Alemba API, which has been added in vFire version 9.7. The legacy API of older versions is not supported by the Greenbone connector.
- An Alemba API client with the correct session type (analyst/user) and password login must be enabled.
- The user account that should be used requires permissions to use the Alemba API.

18.4.2 Configuring an Alemba vFire Alert

To have the appliance automatically create tickets (called “calls”) in vFire, an alert must be set up as follows:

1. Select *Configuration > Alerts* in the menu bar.
2. Create a new alert by clicking .
3. Define the alert (see Fig. 18.13).

   Tip: For the information to enter in the input boxes see Chapter *10.12* (page 272).

4. Choose *Alemba vFire* in the drop-down list *Method*.
5. Click *Save*.

The following details of the alert can be defined:

Report Formats The report formats used for the attachments. Multiple report formats can be selected or the selection can be left empty if no attachments are wanted.

Base URL This is the URL of the Alemba instance including the server name and the virtual directory. For example, if the user interface is accessed via `https://alemba.example.com/vfire/core.aspx`, the base URL would be `https://alemba.example.com/vfire`.

Credential The user name and the password used for logging into Alemba vFire.

Session Type The type of session to use. It can be either “analyst” or “user”.

As an “analyst” it is possible to perform some actions not available to a “user”. The “user” requires special permissions for these actions and the number of concurrent logins may be limited.

Alemba Client ID This is the Alemba API client ID (see Chapter *18.4.1* (page 397)).

Partition The partition to create the ticket in. See the Alemba vFire help for more information about partitioning.

Call Description This is the template for the description text used for the newly created calls. The same placeholders as in the message input box of the e-mail alert method can be used (see Chapter *10.12* (page 272)).

Call Template The name of a call template to use for the calls created by the alert. A call template can be configured in vFire to fill in all the fields that cannot be specified directly in the alert.

[76] https://alemba.com/

Call Type The name of a call type to use for the calls created by the alert.

Impact The full name of an impact value.

Urgency The full name of an urgency value.

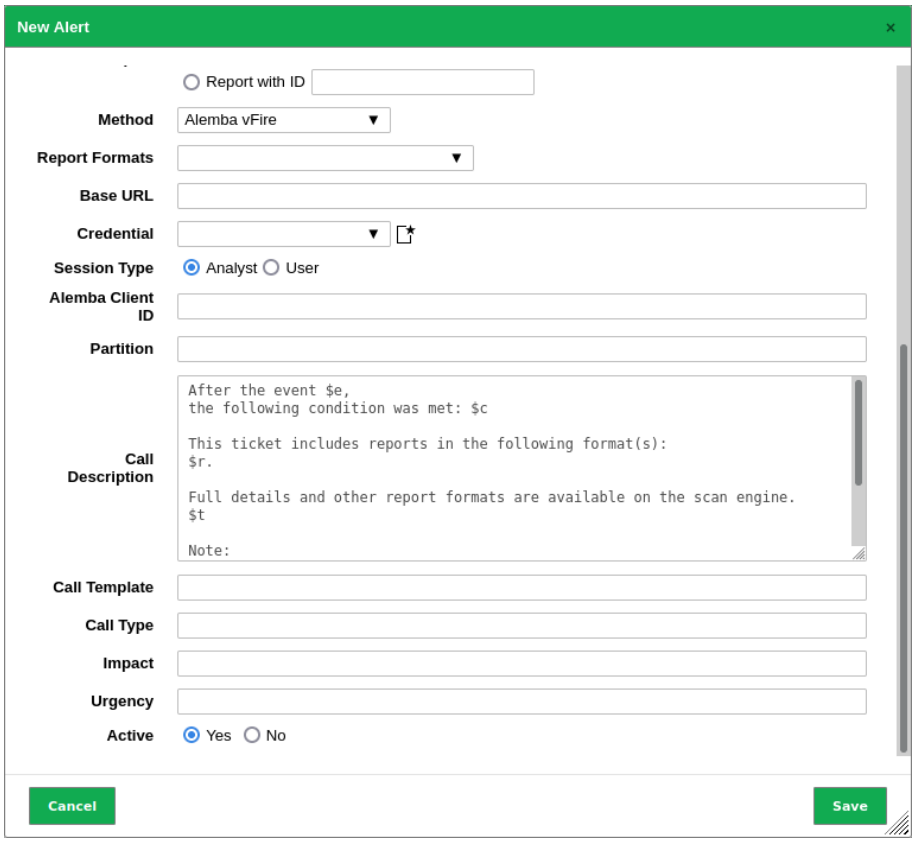


Fig. 18.13: Creating an alert with Alemba vFire

18.5 Using Splunk

The appliance can be configured to forward the scan results to a Splunk enterprise installation for further analysis and correlation.

Connecting an appliance to a Splunk solution is not part of the appliance's core functionality. As an add-on, Greenbone provides an app for the integration with Splunk Enterprise on-premise solutions. The app is currently available at https://download.greenbone.net/tools/Greenbone-Splunk-App-1.0.1.tar.gz.

Important: External links to the Greenbone download webpage are case-sensitive.

Note that upper cases, lower cases and special characters have to be entered exactly as they are written here.

Note: If there are problems with downloading or testing the app contact the Greenbone Enterprise Support[77].

In the following Splunk Enterprise version 8.5 is used. The installation of the app on Splunk Light is not supported. Connecting an appliance to Splunk Cloud is not supported.

18.5.1 Setting up the Greenbone-Splunk App

18.5.1.1 Installing the App

The Greenbone-Splunk app can be installed as follows:

1. Open Splunk Enterprise.
2. Click ⚙ in the left menu panel (see Fig. 18.14).

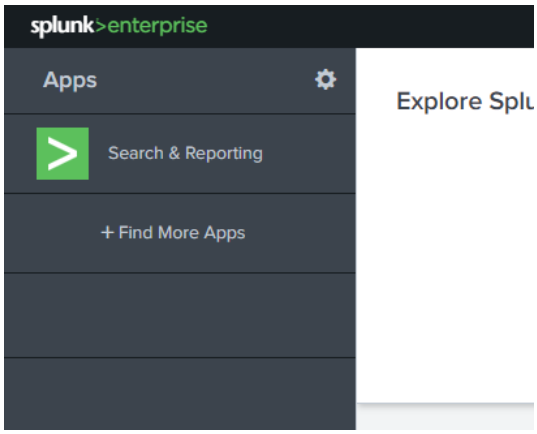


Fig. 18.14: Installing the Splunk app

3. Click *Install app from file*.
4. Click *Browse...*.
5. Select the TAR file of the Greenbone-Splunk app.
6. Click *Upload*.

[77] https://www.greenbone.net/en/technical-support/

18.5.1.2 Configuring the Greenbone-Splunk App

The port of the Greenbone-Splunk app is required for the configuration on the appliance.

Check the port of the Greenbone-Splunk app as follows:

1. Select the Greenbone-Splunk app in the left menu panel.
2. Select *Settings* > *Data inputs* in the menu bar.
3. Click *TCP* (see Fig. 18.15).

Note: The Greenbone-Splunk app sets up a data input on port 7680/tcp (default port) and tags the incoming data to *Greenbone Scan Results* and places it in the index *default*.

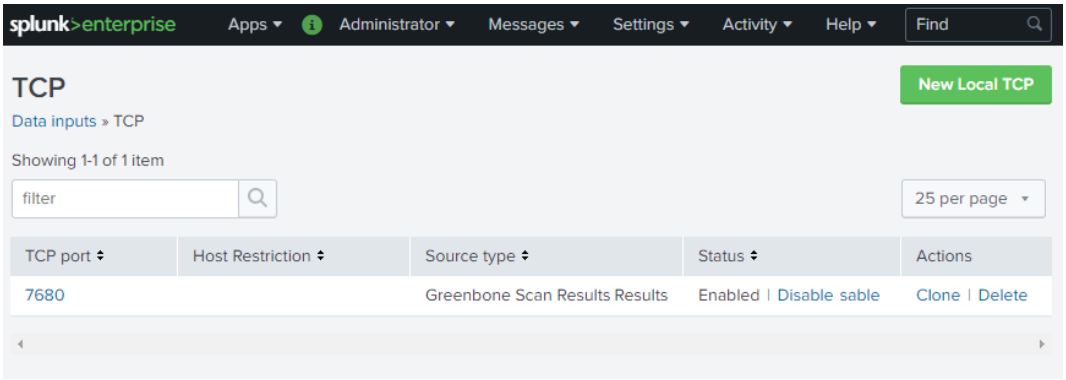


Fig. 18.15: Checking the port of the Greenbone-Splunk app

To make the data more user-friendly, the field names can be replaced as follows:

1. Click  in the left menu panel.
2. In the row of *Greenbone*, click *View objects*.
3. Click *Greenbone Scan Results: FIELDALIAS-reportfields*.
4. Enter the field name aliases in the respective input boxes (see Fig. 18.16).

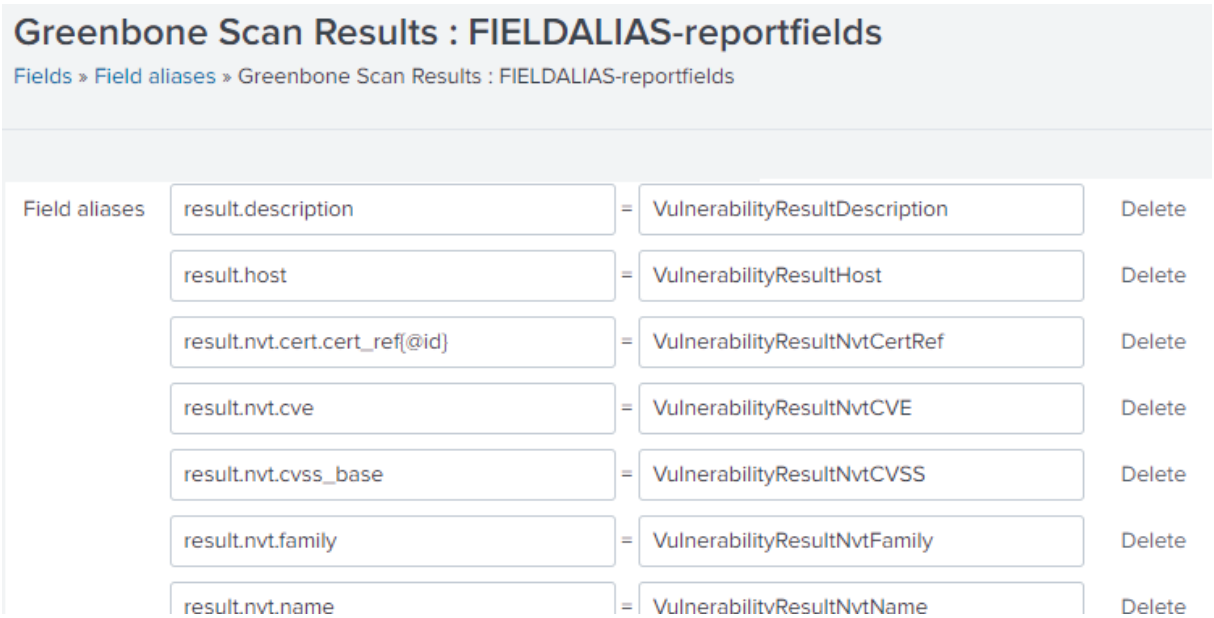


Fig. 18.16: Changing the field name aliases

18.5.2 Configuring a Splunk Alert

The appliance transfers the scan results in the form of an XML report via an alert directly to the Splunk main server.

Note: The dashboard of the Greenbone-Splunk app only shows results from reports less than 7 days old.

If a report older than 7 days is sent, the dashboard will not display the results. However, the results are in the main index of the Splunk server.

18.5.2.1 Creating the Splunk Alert

The alert is created as follows:

1. Select *Configuration* > *Alerts* in the menu bar.
2. Create a new alert by clicking .
3. Define the alert (see Fig. 18.17).

   Tip: For the information to enter in the input boxes see Chapter *10.12* (page 272).

   ---

4. Choose *Send to host* in the drop-down list *Method*.
5. Enter the IP address of the Splunk server in the input box *Send to host* and `7680` in the input box *on port*.

   Note: The TCP port is 7680 by default.

   This setting can be checked in the Greenbone-Splunk app as described in Chapter *18.5.1.2* (page 400).

   ---

6. Choose *XML* in the drop-down list *Report*.

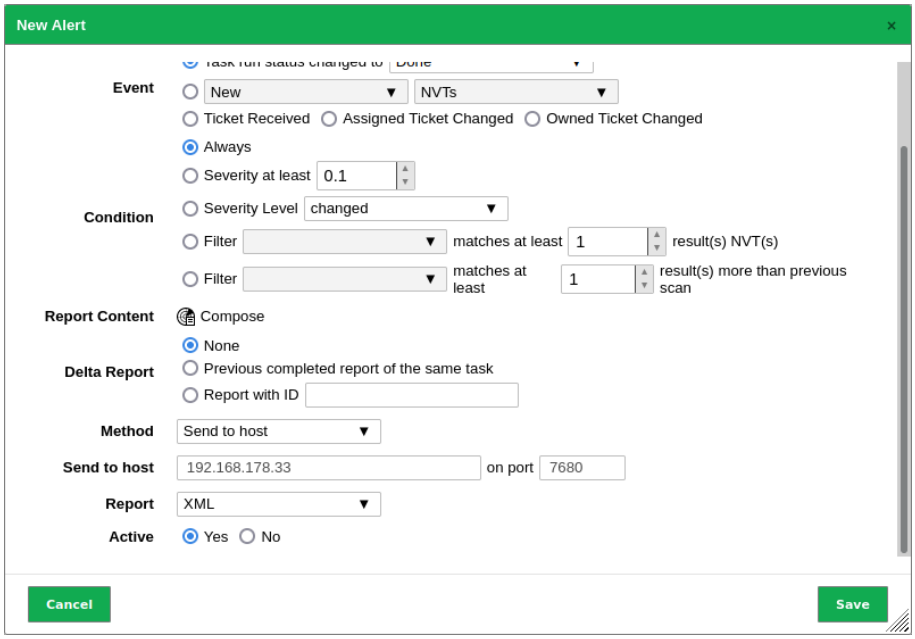


Fig. 18.17: Configuring the Splunk alert

7. Click *Save*.

18.5.2.2 Adding the Splunk Alert to a Task

The alert can now be selected when creating a new task (see Chapter *10.2.2* (page 215)) or be added to an existing task (see Chapter *10.12.2* (page 278)).

18.5.2.3 Testing the Splunk Alert

For testing purposes existing reports may be processed by the alert.

1. Select *Scans* > *Reports* in the menu bar.
2. Click on the date of a report.
3. Click ▷.
4. Select the alert in the drop-down list *Alert* (see Fig. 18.18).

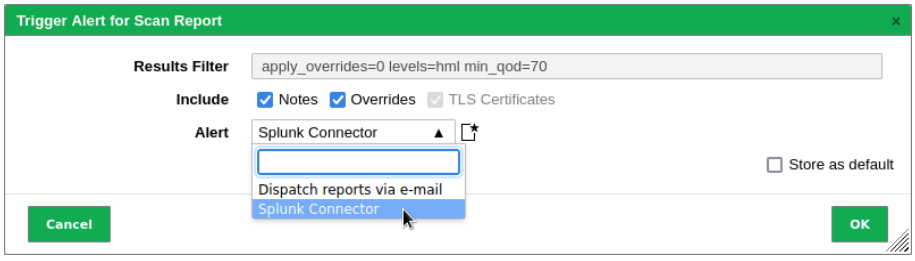


Fig. 18.18: Triggering the alert

5. Click *OK*.

18.5.3 Using the Greenbone-Splunk App

18.5.3.1 Accessing the Information in Splunk

To access the information in Splunk open the Greenbone dashboard as follows:

1. Open Splunk Enterprise.
2. Select the Greenbone-Splunk app in the left menu panel.
3. Select *Dashboards* in the menu bar.
4. Click *Greenbone Dashboard*.

Note: The dashboard of the Greenbone-Splunk app only shows results from reports less than 7 days old.

If a report older than 7 days is sent, the dashboard will not display the results. However, the results are in the main index of the Splunk server.

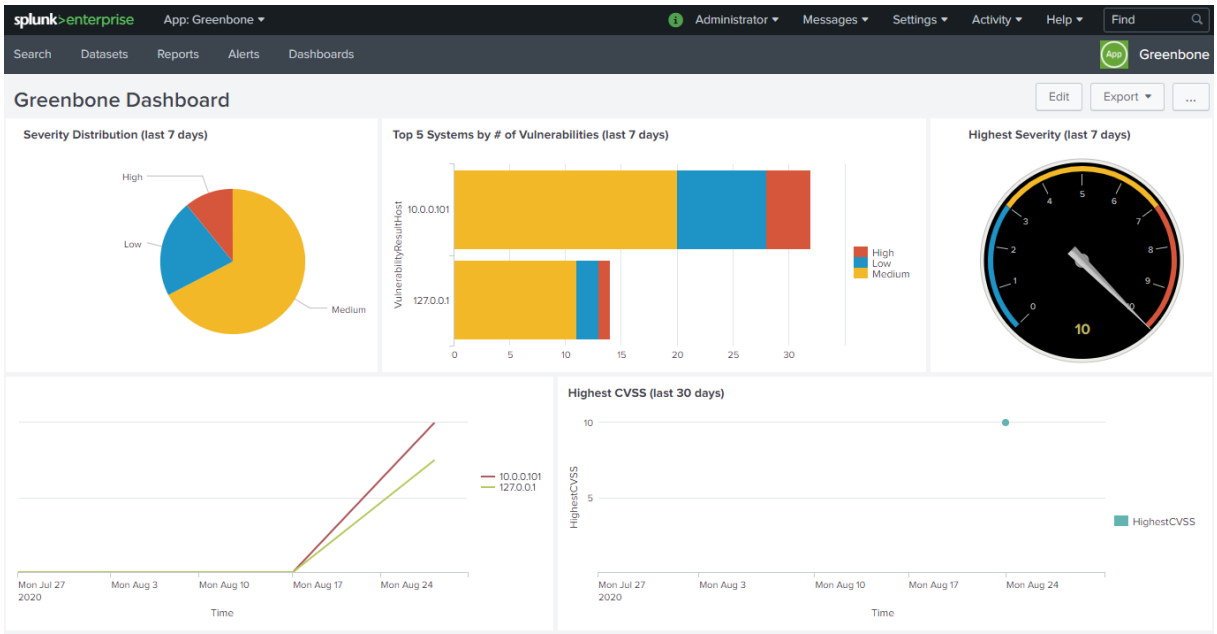


Fig. 18.19: Greenbone dashboard within the Greenbone-Splunk app

The input field *CVE-ID* below the dashboard can be used to display the number of hosts affected by a certain CVE over time.

Note: If the input box is left empty and `Enter` is pressed, the number of hosts affected by all CVEs is displayed.

18.5.3.2 Performing a Search

Since the information forwarded by the appliance is indexed by Splunk, the search view can be used to search for any data as follows:

1. Open Splunk Enterprise.
2. Select the Greenbone-Splunk app in the left menu panel.
3. Select *Search* in the menu bar.
4. Enter the index and the value that should be searched in the input box.
5. Select the time window in the drop-down list right of the input box.
6. Click .

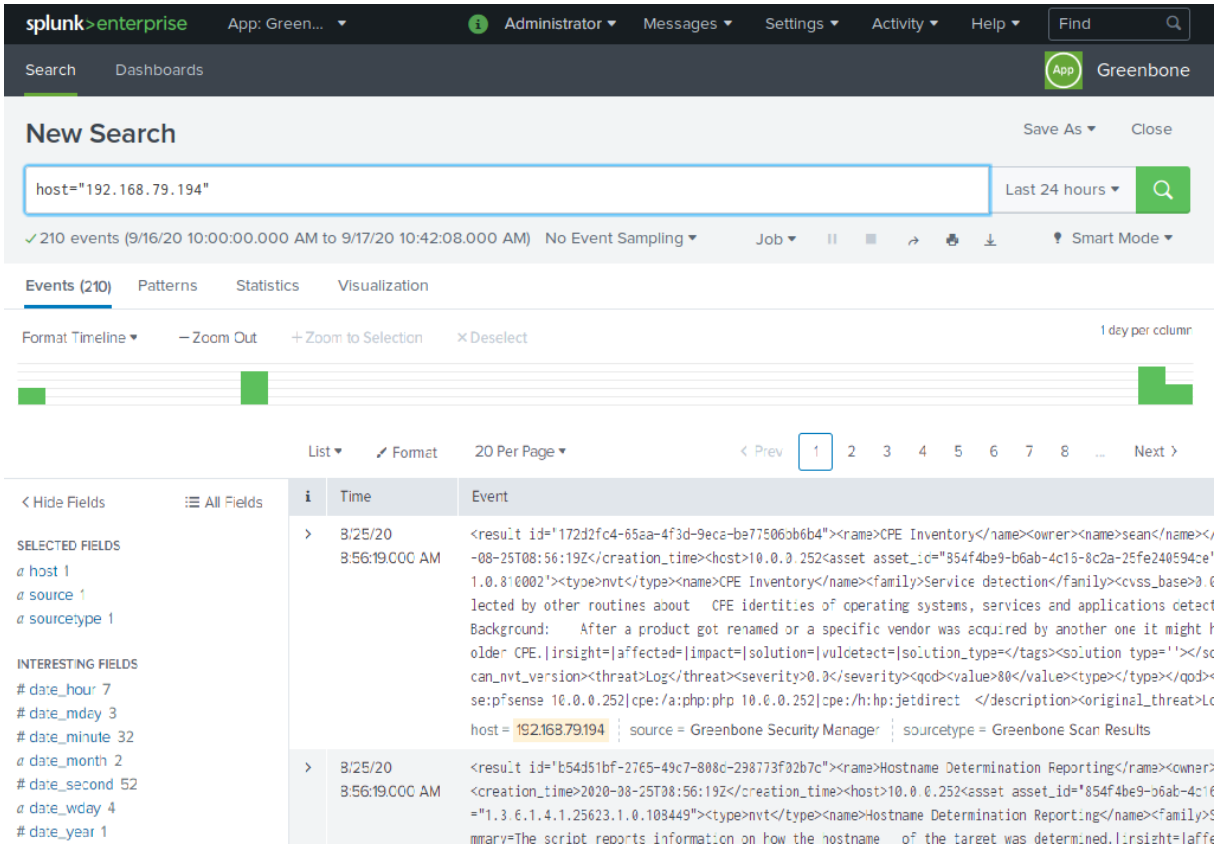


Fig. 18.20: Carrying out a search in the Greenbone-Splunk app

Some supported indexes are:

- host
- source, sourcetype
- date_hour, date_minute, date_month, date_year, date_mdate, date_wday, date_zone
- VulnerabilityResultNvtCVE
- VulnerabilityResultNvtCVSS
- VulnerabilityResultQod
- VulnerabilityResultSeverity
- VulnerabilityResultThreat

18.5.3.3 Creating a Dashboard for the Top 5 Affected Hosts and for Incoming Reports

A new dashboard can be created to show the top 5 affected hosts of all time and the incoming reports from the appliance. The dashboard will show each time a new report comes in to the Splunk server for the past year.

1. Open Splunk Enterprise.
2. Select the Greenbone-Splunk app in the left menu panel.
3. Select *Dashboards* in the menu bar.
4. Click *Create New Dashboard*.
5. Enter a title in the input box *Title*, e.g., `Greenbone incoming stats`.
6. Click *Create Dashboard*.
7. Click *Source*.
8. Copy and paste the following into the input field (replacing all):

```
<dashboard>
  <label>Greenbone incoming stats</label>
  <row>
        <panel>
          <title>Top 5 all time</title>
          <chart>
                <search>
                  <query>sourcetype = "Greenbone Scan Results"␣
↪VulnerabilityResultSeverity &gt; 0 | chart count over VulnerabilityResultHost by␣
↪VulnerabilityResultThreat | fillnull High | fillnull Medium | fillnull Low | eval␣
↪_count= High+Low+Medium | sort by _count desc | head 5</query>
                  <earliest>0</earliest>
                  <latest></latest>
                </search>
                <option name="charting.axisLabelsX.majorLabelStyle.overflowMode">
↪ellipsisNone</option>
                <option name="charting.axisLabelsX.majorLabelStyle.rotation">0</
↪option>
                <option name="charting.axisTitleX.visibility">visible</option>
                <option name="charting.axisTitleY.visibility">visible</option>
                <option name="charting.axisTitleY2.visibility">visible</option>
                <option name="charting.axisX.scale">linear</option>
                <option name="charting.axisY.scale">linear</option>
                <option name="charting.axisY2.enabled">0</option>
                <option name="charting.axisY2.scale">inherit</option>
                <option name="charting.chart">bar</option>
                <option name="charting.chart.bubbleMaximumSize">50</option>
                <option name="charting.chart.bubbleMinimumSize">10</option>
                <option name="charting.chart.bubbleSizeBy">area</option>
                <option name="charting.chart.nullValueMode">gaps</option>
                <option name="charting.chart.showDataLabels">none</option>
                <option name="charting.chart.sliceCollapsingThreshold">0.01</option>
                <option name="charting.chart.stackMode">stacked</option>
                <option name="charting.chart.style">shiny</option>
                <option name="charting.drilldown">all</option>
                <option name="charting.fieldColors">{"High":0xD6563C,"Medium
↪":0xF2B827, "Low":0x1E93C6}</option>
                <option name="charting.layout.splitSeries">0</option>
                <option name="charting.layout.splitSeries.allowIndependentYRanges">0
↪</option>
                <option name="charting.legend.labelStyle.overflowMode">
↪ellipsisMiddle</option>
```

(continues on next page)

(continued from previous page)

```
                <option name="charting.legend.placement">right</option>
                <option name="refresh.display">progressbar</option>
          </chart>
        </panel>
  </row>
  <row>
        <panel>
          <chart>
                <title>Incoming feed to Greenbone App</title>
                <search>
                  <query>| tstats count where sourcetype = "Greenbone Scan Results"␣
↪by sourcetype _time | timechart span=1d count by  sourcetype</query>
                  <earliest>@y</earliest>
                  <latest>now</latest>
                </search>
                <option name="charting.chart">line</option>
                <option name="refresh.display">progressbar</option>
          </chart>
        </panel>
  </row>
</dashboard>
```

9. Click *Save*.

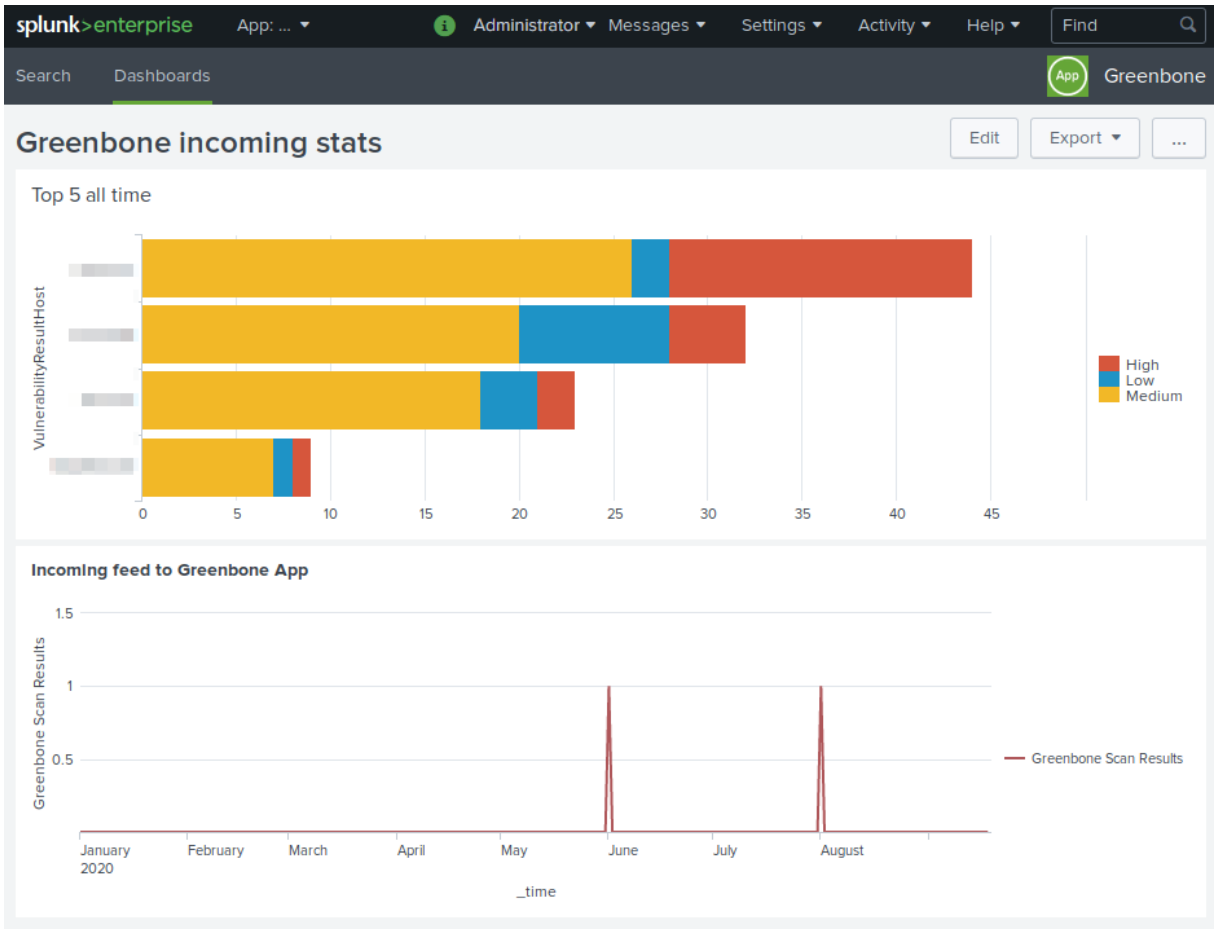


Fig. 18.21: Dashboard for the top 5 affected hosts and for incoming reports

CHAPTER 19

Architecture

19.1 GOS Architecture

The Greenbone Operating System (GOS) is the operating system of the Greenbone Enterprise Appliance. Here is an architecture overview for GOS 22.04.

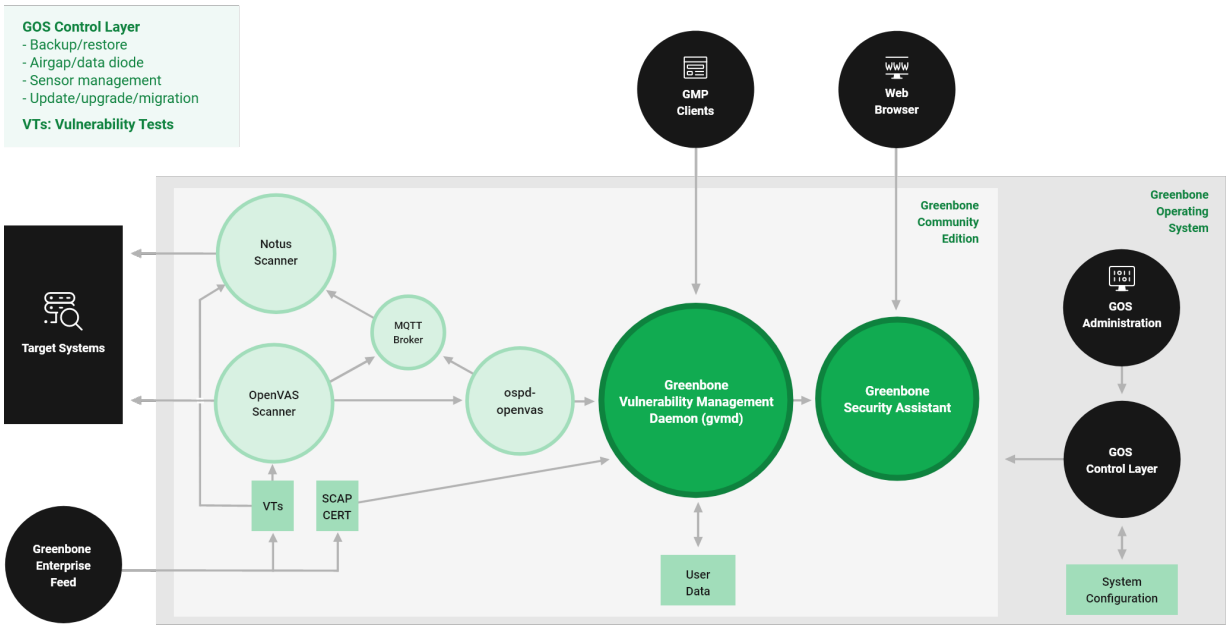


Fig. 19.1: GOS 22.04 architecture

The GOS control layer provides access to the administration of the Greenbone Operating System (GOS). Only a single system administrator account is supported. The system administrator cannot modify system files directly but can instruct the system to change configurations.

GOS is managed using a menu-based graphical interface (GOS administration menu). The system administrator is not required to use the command line (shell) for configuration or maintenance tasks. Shell access is provided for support and troubleshooting purposes only.

Accessing the system level requires either console access (serial, hypervisor or monitor/keyboard) or a connection via SSH.

GOS allows users to configure, start, and stop all services of the Greenbone Community Edition.

Greenbone Community Edition

The Greenbone Community Edition consists of a framework with several services. It is developed as part of the Greenbone Enterprise products.

The Greenbone Community Edition was originally built as a community project named “OpenVAS” and is primarily developed and forwarded by Greenbone. It consists of the Greenbone Vulnerability Management Daemon (gvmd), the Greenbone Security Assistant (GSA) with the Greenbone Security Assistant Daemon (gsad) and the executable scan application that runs vulnerability tests (VT) against target systems.

The Greenbone Community Edition is released under open-source licenses. By using it, Linux distributions can create and provide the software components in the form of installation packages.

Greenbone Vulnerability Management Daemon (gvmd)

The Greenbone Vulnerability Management Daemon (gvmd)[79] – also called Greenbone Vulnerability Manager – is the central service that consolidates plain vulnerability scanning into a full vulnerability management solution. gvmd controls the OpenVAS Scanner via Open Scanner Protocol (OSP)[80]. It is XML-based, stateless and does not require a permanent connection for communication.

The service itself offers the XML-based Greenbone Management Protocol (GMP)[81]. gvmd also controls an SQL database (PostgreSQL) where all configuration and scan result data is centrally stored. Furthermore, gvmd also handles user management including permissions control with groups and roles. And finally, the service has an internal runtime system for scheduled tasks and other events.

Greenbone Security Assistant (GSA)

The Greenbone Security Assistant (GSA)[82] is the web interface that a user controls scans and accesses vulnerability information with. It is the main contact point for a user with the appliance. It connects to gvmd via the web server Greenbone Security Assistant Daemon (gsad) to provide a full-featured web application for vulnerability management. The communication occurs using the Greenbone Management Protocol (GMP) with which the user can also communicate directly by using different tools.

OpenVAS Scanner

The main scanner OpenVAS Scanner[83] is a full-featured scan engine that executes vulnerability tests (VTs) against target systems. For this, it uses the daily updated and comprehensive feeds: the full-featured, extensive, commercial Greenbone Enterprise Feed or the free available Greenbone Community Feed[84].

The scanner consists of the components ospd-openvas[85] and openvas-scanner[86]. The OpenVAS Scanner is controlled via OSP. The OSP Daemon for the OpenVAS Scanner (ospd-openvas) communicates with gvmd via OSP: VT data is collected, scans are started and stopped, and scan results are transferred to gvmd via ospd.

[79] https://github.com/greenbone/gvmd
[80] https://docs.greenbone.net/API/OSP/osp-22.4.html
[81] https://docs.greenbone.net/API/GMP/gmp-22.4.html
[82] https://github.com/greenbone/gsa
[83] https://github.com/greenbone/openvas-scanner
[84] https://www.greenbone.net/en/feed-comparison/
[85] https://github.com/greenbone/ospd-openvas
[86] https://github.com/greenbone/openvas-scanner

Notus Scanner

The Notus scanner scans during every regular scan, so no user interaction is necessary. It offers better performance due to less system resource consumption and thus, faster scanning.

The Notus scanner replaces the logic of potentially all NASL-based local security checks (LSCs). A comparison of installed software on a host against a list of known vulnerable software is done instead of running a VT script for each LSC.

The regular OpenVAS Scanner loads each NASL LSC individually and executes it one by one for every host. A single known vulnerability is then compared with the installed software. This is repeated for all LSCs.

With the Notus scanner, the list of installed software is loaded in the same way, but is directly compared with all known vulnerable software for the operating system of the scanned host. This eliminates the need to run the LSCs because the information about the known vulnerable software is collected in one single list and not distributed in individual NASL scripts.

GMP Clients

The Greenbone Vulnerability Management Tools (gvm-tools)[87] are a collection of tools that help with remote controlling a Greenbone Enterprise Appliance and its underlying Greenbone Vulnerability Management Daemon (gvmd). The tools aid in accessing the communication protocols GMP (Greenbone Management Protocol) and OSP (Open Scanner Protocol).

This module is comprised of interactive and non-interactive clients. The programming language Python is supported directly for interactive scripting. But it is also possible to issue remote GMP/OSP commands without programming in Python.

[87] https://github.com/greenbone/gvm-tools

19.2 Protocols

There are mandatory and optional protocols. Some protocols are only used in specific setups.

The appliance requires several protocols to fully function. These protocols provide the feed updates, Domain Name System (DNS) resolution, time, etc.

19.2.1 Appliance as a Client

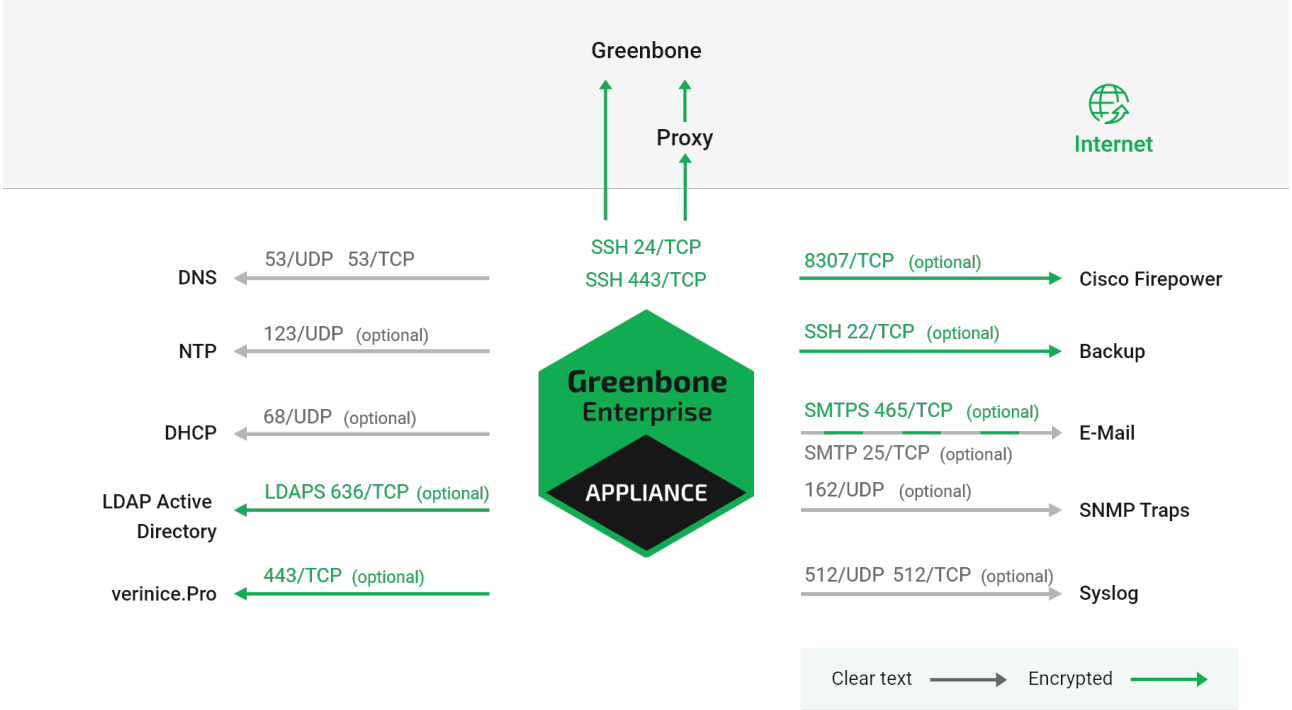


Fig. 19.2: Appliance acting as a client

The following protocols are used by a stand-alone system or a master appliance to initiate connections as a client:

DNS – Name resolution

- Connecting to 53/udp and 53/tcp
- Mandatory
- Not encrypted
- May use internal DNS server

NTP – Time synchronization

- Connecting to 123/udp
- Mandatory
- Not encrypted
- May use internal NTP server

Feeds (see below)

- Direct
  - Connecting to 24/tcp or 443/tcp
  - Direct internet access required
- Via proxy
  - Connecting to internal HTTP proxy supporting CONNECT method on configurable port
- Connecting to apt.greenbone.net and feed.greenbone.net
- Mandatory on stand-alone and master appliances
- Used protocol is SSH
- Encrypted and bidirectionally authenticated via SSH
  - Server: public key
  - Client: public key

DHCP

- Connecting to 67/udp and 68/udp
- Optional
- Not encrypted

LDAPS – User authentication

- Connecting to 636/tcp
- Optional
- Encrypted and authenticated via SSL/TLS
  - Server: certificate
  - Client: user name/password

Syslog – Remote logging and alerts

- Connecting to 512/udp or 512/tcp
- Optional
- Not encrypted

SNMP traps for alerts

- Connecting to 162/udp
- Optional
- Only SNMPv1
- Not encrypted

SMTP(S) for e-mail alerts

- Connecting to 465/tcp for SMTPS, 25/tcp for SMTP, alternatively connecting to 587/tcp
- Optional
- SMTPS can be enforced to always be used
- Encrypted via STARTTLS, if SMTPS is not enforced
- Not encrypted, if encryption via STARTTLS is not possible

SSH for backup

- Connecting to 22/tcp
- Optional
- Encrypted and bidirectionally authenticated via SSH
  - Server: public key
  - Client: public key

Cisco Firepower (Sourcefire) for IPS integration

- Connecting to 8307/tcp
- Optional
- Encrypted and bidirectionally authenticated via SSL/TLS
  - Server: certificate
  - Client: certificate

verinice.PRO

- Connecting to 443/tcp
- Optional
- Encrypted via SSL/TLS
  - Server: optional via certificate
  - Client: user name/password

TippingPoint SMS

- Connecting to 443/tcp
- Optional
- Encrypted via SSL/TLS
  - Server: certificate
  - Client: certificate, user name/password

19.2.2 Appliance as a Server

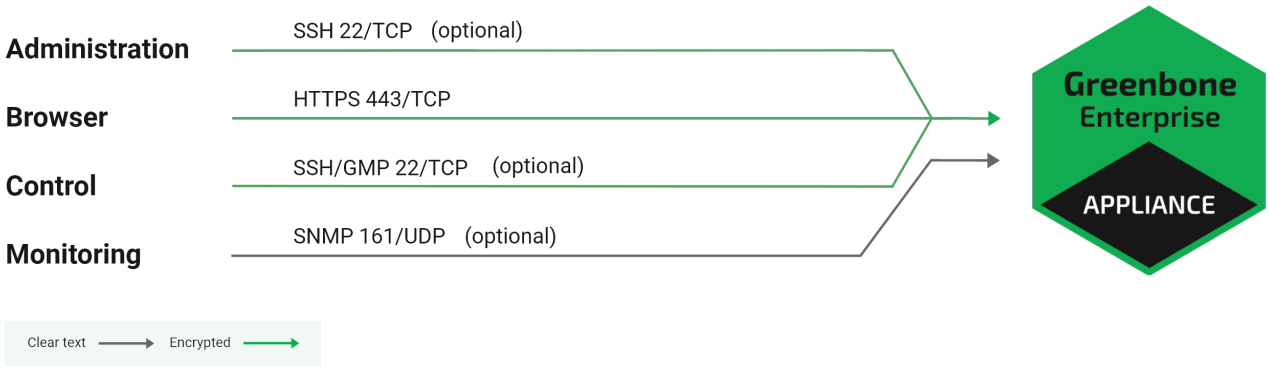


Fig. 19.3: Appliance acting as a server

The following connections are supported by an appliance acting as a server:

HTTPS – Web interface

- 443/tcp
- Mandatory on stand-alone and master appliances
- Encrypted and authenticated via SSL/TLS
  - Server: optional via certificate
  - Client: user name/password

SSH – CLI access and GMP

- 22/tcp
- Optional
- Encrypted and authenticated via SSH
  - Server: public key
  - Client: user name/password

SNMP

- 161/udp
- Optional
- Optionally encrypted when using SNMPv3

19.2.3 Master-Sensor Setup

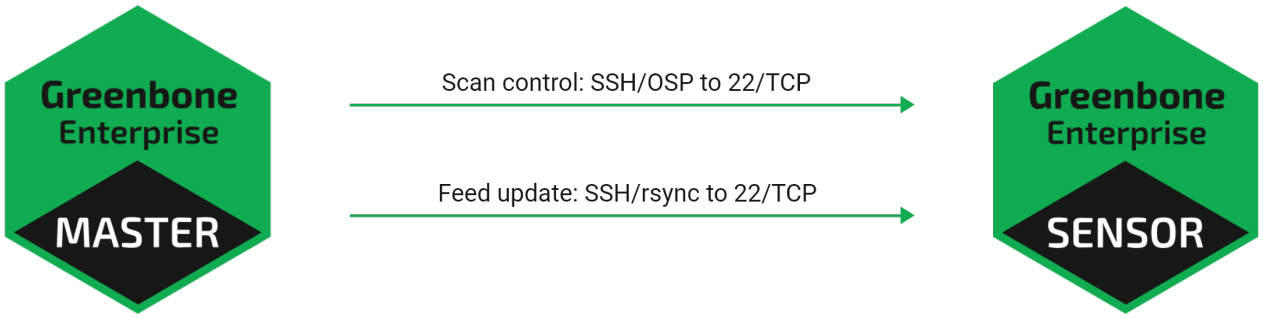


Fig. 19.4: Appliance master and sensor

In a master-sensor setup the following additional requirements apply. The master (server) initiates up to three additional connections to the sensor (client):

SSH for GOS upgrades, feed updates, GMP and OSP

- 22/tcp
- Mandatory
- Encrypted and bidirectionally authenticated via SSH
  - Server: public key
  - Client: public key

19.3 Security Gateway Considerations

Many enterprises deploy security gateways to restrict the internet access. These security gateways can operate as packet filters or application layer gateways.

Some products support deep inspection and try to determine the actual protocol used in the communication channels. They may even try to decrypt and analyze any encrypted communication.

19.3.1 Stand-Alone/Master Appliance

While many protocols used by the appliance are only used internally, some protocols require access to the internet. These protocols may be filtered by such a security gateway.

When deploying the appliance as a stand-alone appliance or as a master, the appliance must be able to access the Greenbone Enterprise Feed. The Greenbone Enterprise Feed can be access directly via port 24/tcp or 443/tcp or using a proxy.

Note: In all cases the used protocol is SSH, even when using the port 443/tcp or a HTTP proxy.

A deep inspection firewall may detect the usage of the SSH protocol running on port 443/tcp and drop or block the traffic.

If the security gateway tries to decrypt the traffic using man-in-the-middle techniques, the communication of the appliance and the feed server fails. The SSH protocol using bidirectional authentication based on public keys prevents any man-in-the-middle approaches by terminating the communication.

Additional protocols which need internet access are DNS and NTP. Both DNS and NTP can be configured to use internal DNS and NTP servers.

19.3.2 Sensor Appliance

If security gateways are deployed between the master and the sensor, the security gateway must permit SSH (22/tcp) connections from the master to the sensor.

CHAPTER 20

Frequently Asked Questions

20.1 Why Is the Scanning Process so Slow?

The performance of a scan depends on various aspects.

- Several port scanners were activated concurrently.

  If an individual scan configuration is used, select only a single port scanner in the VT family *Port scanners* (see Chapter *10.9.2* (page 259)). The VT *Ping Host* can still be activated.

- Unused IP addresses are scanned very time-consuming.

  As a first step, it is detected whether an active system is present or not for each IP address. In case it is not, this IP address will not be scanned. Firewalls and other systems can prevent a successful detection. The VT *Ping Host* (1.3.6.1.4.1.25623.1.0.100315) in the VT family *Port scanners* offers fine-tuning of the detection.

- The ports to be scanned resulted in port throttling, or UDP port scanning has been chosen.

  For more information, see Chapters *17.2.1.2* (page 382) and *17.2.1.2.1* (page 382).

20.2 What Influences the Scan Capacity?

The scan capacity – the scannable number of IP addresses per 24 hours – depends on the appliance model (see Chapter *3* (page 20)). However, the values provided for the estimated scan capacity can only be understood as guide values, as the scan capacity is influenced by many factors.

The following factors influence the scan capacity:

- **Complexity of the used scan configuration** In the same amount of time, many more discovery scans can be performed than vulnerability scans. For more information about scan configurations, see Chapter *10.9* (page 258).
- **Using the appliance outside its specifications** Starting too many scans or scanning too many targets at once can result in performance problems.

- **Performance of the network infrastructure and the target system(s)** If systems are slow to respond to network requests, the scanning process will be slower.
- **Type of the scanned target system(s)** The type determines which and how many vulnerability tests are executed during a scan. More vulnerability tests usually mean slower scans.

  Some scan scenarios increase resource usage, which can have an impact on performance, e.g., scanning of virtual hosts (vhosts) and scanning of web servers with CGI caching enabled. For more information about configuration options for those scenarios, see Chapter *10.9* (page 258).
- **Using the appliance in parallel while scanning** If other resource-intensive operations (e.g., feed updates, generation of large reports) are running, less system resources are available for scans.
- **Using sensors** Using sensors can increase the scanable IP addresses per 24 hours.

20.3 Why Is a Service/Product Not Detected?

- The target is not detected as online/reachable.

  Solution(s):

  - Fix the network setup/routing to the target.
  - Update the criteria/test configuration to detect the target as alive (see Chapter *10.2.1* (page 212)).
  - Ensure that the scan configuration includes the following VTs from the VT family *Port scanners*: * *Nmap (NASL wrapper)* (OID: 1.3.6.1.4.1.25623.1.0.14259) * *Ping Host* (OID: 1.3.6.1.4.1.25623.1.0.100315)
  - Verify and remove any network device (firewall, IDS/IPS, WAF, etc.) between the scanner and the target, or any security mechanisms on the target itself. Whitelist the scanner's IP address.
- The service/product is running on a specific port not included in the port list.

  Solution(s):

  - Create a suitable port list (see Chapter *10.7* (page 252)). This is especially important for UDP ports.
- There is a detection VT for an service/product available but the service/product is not found during a scan.

  Solution(s):

  - Fix the network setup/routing to the target.
  - Update the criteria/test configuration to detect the target as alive (see Chapter *10.2.1* (page 212)).
  - Verify and remove any network device (firewall, IDS/IPS, WAF, etc.) between the scanner and the target, or any security mechanisms on the target itself. Whitelist the scanner's IP address.
  - Create a suitable port list (see Chapter *10.7* (page 252)). This is especially important for UDP ports.
  - If the solutions above do not help, contact the Greenbone Enterprise Support[88] and provide more information about the service/product (product name, specific version running, etc.).

[88] https://www.greenbone.net/en/technical-support/

- The target is not stable/responds slowly during a scan.

  Solution(s):

  - Lower the concurrently executed VTs (see Chapter *10.2.2* (page 215)).
  - Update the service/product to a newer version (e.g., to fix triggered bugs).
  - Assign more resources (CPU, RAM, etc.) to the target to make it more stable during scans.

20.4 Why Is a Vulnerability Not Detected?

- The affected service/product is not detected at all.

  Solution(s):

  - See Chapter *20.3* (page 417).
- The service/product was detected but the a version extraction was not possible.

  Solution(s):

  - Perform an authenticated scan (see Chapter *10.3* (page 218)).
  - If the solutions above do not help, contact the Greenbone Enterprise Support[89] and provide more information about the service/product (product name, specific version running, etc.).
- There is only a version check with a lower Quality of Detection (QoD) and the vulnerability is not displayed by default.

  Solution(s):

  - Change the QoD value in the results filter (see Chapter *11.2.1.3* (page 291)).
  - Perform an authenticated scan (see Chapter *10.3* (page 218)).
- If an authenticated scan was carried out, the login has failed.

  Solution(s):

  - Check the correctness of the used credentials.
  - Verify that the user is not blocked.
  - Verify that the user is allowed to log in to the target.
  - If the solutions above do not help, contact the Greenbone Enterprise Support[90] and provide more information about the service/product (product name, specific version running, etc.).
- The service/product itself crashed or stopped to respond during the scan.

  Solution(s):

  - Lower the concurrently executed VTs (see Chapter *10.2.2* (page 215)).
  - Update the service/product to a newer version (e.g., to fix triggered bugs).
  - Assign more resources (CPU, RAM, etc.) to the target to make it more stable during scans.
- The vulnerability was only recently discovered and there is no VT for it yet.

  Solution(s):

  - Contact the Greenbone Enterprise Support[91] and ask for a new VT or whether a VT is already planned.

[89] https://www.greenbone.net/en/technical-support/
[90] https://www.greenbone.net/en/technical-support/
[91] https://www.greenbone.net/en/technical-support/

- The specific detection became outdated.

  Solution(s):

  - Contact the Greenbone Enterprise Support[92].

20.5 Why Do the Results for the Same Target Differ across Several Consecutive Scans?

The results of consecutive scans may differ due to the following reasons:

- There was a loss of connection over unreliable network connections (between the scanner host and the target).
- The network connection or equipment (between the scanner host and the target) was overloaded.
- An overloaded target host and/or service stopped responding.
- “Fragile” protocols (e.g., Remote Desktop Protocol) do not always respond as expected.
- A previous probe/attacking request caused the service to not respond for a short period of time.

Although the scanner tries to reduce the occurrence of such situations by internal retry routines, they cannot be ruled out completely.

20.6 Why Is It Not Possible to Edit Scan Configurations, Port Lists, Compliance Policies, or Report Formats?

Scan configurations, port lists, compliance policies and report formats by Greenbone (hereafter referred to as “objects”) are distributed via the feed. These objects must be owned by a user, the Feed Import Owner. The objects are downloaded and updated during a feed update, if a Feed Import Owner has been set.

The objects cannot be edited. This is by design to ensure that the objects function as intended by Greenbone.

20.7 Why Is It Not Possible to Delete Scan Configurations, Port Lists, Compliance Policies, or Report Formats?

Scan configurations, port lists, compliance policies and report formats by Greenbone (hereafter referred to as “objects”) are distributed via the feed. These objects must be owned by a user, the Feed Import Owner. The objects are downloaded and updated during a feed update, if a Feed Import Owner has been set.

Only the Feed Import Owner, a super administrator and users who obtained respective rights are able to delete objects.

If objects are deleted, they will be downloaded again during the next feed update. If no objects should be downloaded, the Feed Import Owner must be unset.

[92] https://www.greenbone.net/en/technical-support/

20.8 Why Does a VNC Dialog Appear on the Scanned Target System?

When testing port 5900 or configuring a VNC port, a window appears on the scanned target system asking the user to allow the connection. This was observed for UltraVNC Version 1.0.2.

Solution: exclude port 5900 or other configured VNC ports from the target specification. Alternatively, upgrading to a newer version of UltraVNC would help (UltraVNC 1.0.9.6.1 only uses balloons to inform users).

20.9 Why Does the Scan Trigger Alarms on Other Security Tools?

For many vulnerability tests the behavior of real attacks is applied. Even though a real attack does not happen, some security tools will issue an alarm.

A known example is:

Symantec reports attacks regarding CVE-2009-3103 if the VT *Microsoft Windows SMB2 '_Smb2ValidateProviderCallback()' Remote Code Execution Vulnerability* (1.3.6.1.4.1.25623.1.0.100283) is executed. This VT is only executed if the radio button *No* is selected for *safe_checks* in the scanner preferences (see Fig. 20.1). Otherwise the target system can be affected.

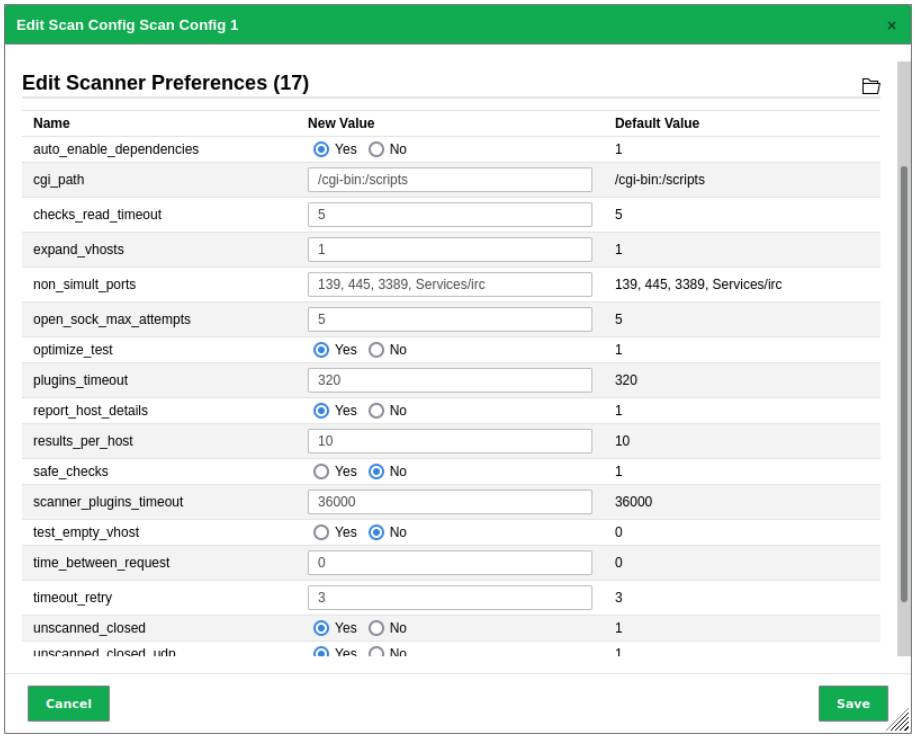


Fig. 20.1: Disabling the scanner preference *safe_checks*

20.10 How Can a Factory Reset of the Appliance Be Performed?

A factory reset can be performed to erase user data securely from the appliance.

Note: Contact the Greenbone Enterprise Support[93] to receive detailed instructions on how to perform a factory reset.

20.11 Why Does Neither Feed Update nor GOS Upgrade Work After a Factory Reset?

A factory reset deletes the whole system including the Greenbone Enterprise Feed subscription key. The subscription key is mandatory for feed updates and GOS upgrade.

1. Reactivate the subscription key:

   A backup key is delivered with each appliance (see Chapter *7.1.1* (page 67)). Use this key to reactivate the appliance. The activation is described in the setup guide of the respective appliance model (see Chapter *5* (page 28)).

2. Update the system to the current version:

   Depending on the GOS version, the respective upgrade procedure has to be executed.

20.12 How Can an Older Backup or Beaming Image Be Restored?

Only backups and beaming images created with the currently used GOS version or the previous GOS version can be restored. For GOS 22.04, only backups and beaming images from GOS 21.04 or GOS 22.04 can be imported. If an older backup or beaming image should be imported, e.g., from GOS 6 or GOS 20.08, an appliance with a matching GOS version has to be used.

Backups and beaming images from GOS versions newer than the currently used GOS version are not supported as well. If a newer backup or beaming image should be imported, an appliance with a matching GOS version has to be used.

If there are any questions, contact the Greenbone Enterprise Support[94].

20.13 What Can Be Done if the GOS Administration Menu Is not Displayed Correctly in PuTTY?

Check the settings in PuTTY by selecting *Window* > *Translation* in the left panel. *UTF-8* has to be selected in the drop-down list *Remote character set* (see Fig. 20.2).

[93] https://www.greenbone.net/en/technical-support/
[94] https://www.greenbone.net/en/technical-support/

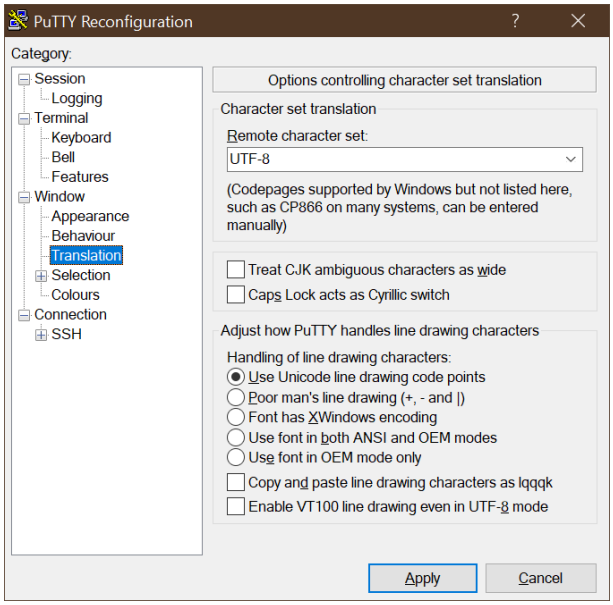


Fig. 20.2: Selecting the remote character set

20.14 How Can the GMP Status Be Checked Without Using Credentials?

1. Build an SSH connection to the appliance via command line using the GMP user:

   ```
   ssh gmp@<appliance>
   ```

   Replace `<appliance>` with the IP address or DNS name of the appliance.

   Note: No input prompt is displayed but the command can be entered nevertheless.

2. Enter `<get_version/>`.

   → If GMP is activated, the output should look like `<get_version_response status="200" status_text="OK"><version>8.0</version></get_version_response>`.

20.15 What Should Be Done if the Self-Check Shows “RAID Array degraded”?

The appliance models Greenbone Enterprise 6500/6400/5400/5300 use RAID (Redundant Array of Independent Disks) 6 as a software RAID. RAID is a data storage virtualization technology that combines multiple hard disk drive (HDD) components into one or more logical units for the purposes of data redundancy. For RAID 6, at least 4 HDDs are required for the RAID, and thus the data rendundancy, to function. The appliance itself will still function if up to 2 HDDs fail.

If one or more HDD(s) fail(s), GOS will show the self-check warnings `RAID Array degraded` with the hint `Replace the failed disk`, and `Check for system integrity status` with the hint `The system integrity may be endangered. Please contact the support.` The integrity check fails due to the failed HDD(s).

Failed HDDs must be replaced and the RAID must be repaired. Contact the Greenbone Enterprise Support[95] for assistance.

[95] https://www.greenbone.net/en/technical-support/

CHAPTER 21

Glossary

This section defines relevant terminology which is consistently used across the entire system.

21.1 Alert

An alert is an action which can be triggered by certain events. In most cases, this means the output of a notification, e.g., an e-mail in case of new found vulnerabilities.

21.2 Asset

Assets are discovered on the network during a vulnerability scan or entered manually by the user. Currently, assets include hosts and operating systems.

21.3 CERT-Bund Advisory

An advisory published by CERT-Bund. See https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/CERT-Bund/cert-bund_node.html for more information.

21.4 Compliance Audit

A compliance audit is a scan task with the flag *audit* and used to check the fulfillment of compliances.

21.5 Compliance Policy

A compliance policy is a scan configuration with the flag *policy* and used to check the fulfillment of compliances.

21.6 CPE

Common Platform Enumeration (CPE) is a structured naming scheme for information technology systems, platforms and packages. Based on the generic syntax for Uniform Resource Identifiers (URI), CPE includes a formal name format, a language for describing complex platforms, a method for checking names against a system and a description format for binding text and tests to a name.

A CPE name starts with “cpe:/”, followed by up to seven components separated by colons:

- Part (“h” for hardware, “o” for operating system or “a” for application)
- Vendor
- Product
- Version
- Update
- Edition
- Language

Example: cpe:/o:linux:kernel:2.6.0

21.7 CVE

Common Vulnerabilities and Exposures (CVE) is a dictionary of publicly known information security vulnerabilities and exposures.

21.8 CVSS

The Common Vulnerability Scoring System (CVSS) is an open framework to characterize vulnerabilities.

21.9 DFN-CERT Advisory

An advisory published by DFN-CERT. See https://www.dfn-cert.de/ for more information.

21.10 Filter

A filter describes how to select a certain subset from a group of resources.

21.11 Group

A group is a collection of users.

21.12 Host

A host is a single system that is connected to a computer network and that can be scanned. One or many hosts form the basis of a scan target.

A host is also an asset type. Any scanned or discovered host can be recorded in the asset database.

Hosts in scan targets and in scan reports are identified by their network address, either an IP address or a host name.

In the asset database the identification is independent of the actual network address, which however is used as the default identification.

21.13 Note

A note is a textual comment associated with a VT. Notes show up in reports, below the results generated by the VT. A note can be applied to a particular result, task, severity, port and/or host, so that the note appears only in certain reports.

21.14 Vulnerability Test (VT)

A Vulnerability Test (VT) is a routine that checks a target system for the presence of a specific known or potential security problem.

VTs are grouped into families of similar VTs. The selection of families and/or single VTs is part of a scan configuration.

21.15 Override

An override is a rule to change the severity of items within one or many report(s).

Overrides are especially useful to mark report items as False Positives (e.g., an incorrect or expected finding) or emphasize items that are of higher severity in the observed scenario.

21.16 Permission

A permission grants a user, role or group the right to perform a specific action.

21.17 Port List

A port list is a list of ports. Each target is associated with a port list. This determines which ports are scanned during a scan of the target.

21.18 Quality of Detection (QoD)

The Quality of Detection (QoD) is a value between 0 % and 100 % describing the reliability of the executed vulnerability detection or product detection. The value of 70 % is the default minimum used for filtering the displayed results in the reports.

For more information about the QoD see Chapter *11.2.6* (page 296).

21.19 Remediation Ticket

Remediation tickets are used to resolve the findings of vulnerabilities. Tickets can be assigned to the current user or other users. All valuable information to understand and resolve the problem is directly cross-linked and available for the assigned user.

All tickets have a specific status (e.g., open, fixed) to track the progress.

Additionally, alerts can be assigned for certain events considering tickets, e.g., a status change of an assigned ticket.

The ticket management system is capable of considering the repetition of scans automatically in order to verify that the problem has been solved.

21.20 Report

A report is the result of a scan and contains a summary of what the selected VTs detected for each of the target hosts.

A report is always associated with a task. The scan configuration that determines the extent of the report is part of the associated task and cannot be modified. Therefore, for any report it is ensured that its execution configuration is preserved and available.

21.21 Report Format

A format in which a report can be downloaded.

An example is TXT which has the content type “text/plain”, meaning that the report is a plain text document.

21.22 Result

A single result generated by the scanner as part of a report, for example a vulnerability warning or a log message.

21.23 Role

A role defines a set of permissions that can be applied to a user or a group.

21.24 Scan

A scan is a task in progress. For each task only one scan can be active. The result of a scan is a report.

The status of all active scans can be seen on the page *Tasks*.

The progress is shown as a percentage of total number of tests to be executed. The duration of a scan is determined by the number of targets and the complexity of the scan configuration and ranges from minutes to many hours or even days.

The page *Tasks* offers an option to stop a scan.

If a stopped or interrupted scan is resumed, all unfinished hosts are scanned completely anew. The data of hosts that were already fully scanned is kept.

21.25 Scanner

A scanner is an OpenVAS Scanner daemon or compatible OSP daemon on which the scan will be run.

21.26 Scan Configuration

A scan configuration covers the selection of VTs as well as general and very specific (expert) parameters for the scan server and for some of the VTs.

Not covered by a scan configuration is the selection of targets.

21.27 Schedule

A schedule sets the time when task should be automatically started, a period after which the task should run again and a maximum duration the task is allowed to take.

21.28 Severity

The severity is a value between 0.0 (no severity) and 10.0 (highest severity) and expresses also a severity class (*Log*, *Low*, *Medium* or *High*).

This concept is based on CVSS but is applied in case no full CVSS Base Vector is available as well.

Comparison, weighting and prioritization of any scan results or VTs is possible because the severity concept is strictly applied across the entire system. Any new VT is assigned with a full CVSS vector even if the CVE does not offer one.

The severity classes *Log*, *Low*, *Medium* and *High* are defined by sub-ranges of the main range 0.0 – 10.0. Users can select to use different classifications. The default is the NVD classification which is the most commonly used one.

Scan results are assigned a severity while achieved. The severity of the related VT may change over time though. If *Dynamic Severity* is selected in the user settings the system always uses the most current severities of VTs for the results.

21.29 Solution Type

This information shows possible solutions for the remediation of the vulnerability.

- Workaround: Information about a configuration or specific deployment scenario that can be used to avoid exposure to the vulnerability is available. There can be none, one or more workarounds available. This is usually the “first line of defense” against a new vulnerability before a mitigation or vendor fix has been issued or even discovered.

- Mitigation: Information about a configuration or deployment scenario that helps to reduce the risk of the vulnerability is available but that does not resolve the vulnerability on the affected product. Mitigations may include using devices or access controls external to the affected product. Mitigations may or may not be issued by the original author of the affected product and they may or may not be officially sanctioned by the document producer.
- Vendor fix: Information is available about an official fix that is issued by the original author of the affected product. Unless otherwise noted, it is assumed that this fix fully resolves the vulnerability.
- No fix available: Currently there is no fix available. Information should contain details about why there is no fix.
- Will not fix: There is no fix for the vulnerability and there never will be one. This is often the case when a product has been orphaned, is no longer maintained or otherwise deprecated. Information should contain details about why there will be no fix issued.

21.30 Tag

A tag is a short data package consisting of a name and a value that is attached to a resource of any kind and contains user defined information on this resource.

21.31 Target

A target defines a set of systems (hosts) that is scanned. The systems are identified either by their IP addresses, by their host names or with CIDR network notation.

21.32 Task

A task is initially formed by a target and a scan configuration. Executing a task initiates a scan. Each scan produces a report. As a result, a task collects a series of reports.

A task's target and scan configuration are static. Thus, the resulting sequence of reports describes the change of security status over time. However, a task can be marked as alterable when there are no reports present. For such a task the target and scan configuration can be changed at any time which may be convenient in certain situations.

A container task is a task with the function to hold imported reports. Running a container task is not possible.

21.33 TLS Certificate

A TLS (Transport Layer Security) certificate is a certificate used for authentication when establishing a connection secured by TLS.

The scan report contains all TLS certificates collected during a vulnerability scan.

Index

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

X