Greenbone

Manual

Greenbone Cloud Service

Greenbone

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

Status: March 6, 2024

This is the manual for the Greenbone Cloud Service.
The Greenbone Cloud Service is under constant development. This manual attempts to always document the latest version. 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

Vulnerability Management

In IT security, the confluence of three basic elements forms the attack surface of an IT infrastructure.

1. Attackers with sufficient experience, equipment and money to carry out the attack.
2. Access to the IT infrastructure.
3. 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. The third element can be influenced, since 999 of 1,000 successfully exploited vulnerabilities are known for more than one year.

Vulnerability management is a core element in modern information technology (IT) compliance. IT compliance is defined as the adherence to legal, corporate and contractual rules and regulations related to IT infrastructures. Within its context IT compliance mainly relates to information security, availability, storage and privacy. Companies and agencies have to comply with many legal obligations in this area.

Controlling and improving IT security is an ongoing process consisting of at least the following steps:

- Discovery of the current state
- Improving the current state
- Reviewing the taken measures

Greenbone Cloud Service

The Greenbone Cloud Service offers an easy-to-use high-quality service for vulnerability management. It checks the IT infrastructure for security gaps and delivers a report containing all found vulnerabilities, sorted by severity.

For this purpose, the Greenbone Cloud Service offers the possibility to individually define the number of IP addresses to be scanned. Commercial and public entities of any size can use the Greenbone Cloud Service in self-service to address their specific security needs.

Users log in using their access data and are able to work with the Greenbone Cloud Service independent of their location. While doing so, both public IP services (WWW server, e-mail server, etc.) and internal networks can be scanned. The packages are structured as subscriptions and can be terminated or edited on a monthly basis.

The Greenbone Cloud Service discovers vulnerabilities through different perspectives of an attacker:

External
The Greenbone Cloud Service can simulate an external attack to identify outdated or misconfigured firewalls.

Demilitarized Zone (DMZ)
The Greenbone Cloud Service can identify actual vulnerabilities that may be exploited by attackers that get past the firewall.

Internal
The Greenbone Cloud Service 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.

For DMZ and internal scans, a distinction can be made between authenticated and unauthenticated scans. When performing an authenticated scan, the Greenbone Cloud Service uses credentials and can discover vulnerabilities in applications that are not running as a service but have a high risk potential. This includes web browsers, office applications or PDF viewers. For the advantages and disadvantages of authenticated scans see Chapter *6.3.1* (page 45).

Due to new vulnerabilities being discovered on a daily basis, regular updates and testing of systems are required. The Greenbone Enterprise Feed ensures that the Greenbone Cloud Service is provided with the latest testing routines and can discover the latest vulnerabilities reliably. Greenbone analyzes CVE[1] messages and security bulletins of vendors and develops new vulnerability tests daily.

When performing a vulnerability scan using the Greenbone Cloud Service, the personnel responsible will receive a list of vulnerabilities that have been identified in the target systems. For the selection of remediation measures a prioritization is required. The most important measures are those that protect the system against critical risks and eliminate the corresponding security holes.

The Greenbone Cloud Service utilizes the Common Vulnerability Scoring System (CVSS). CVSS is an industry standard for the classification and rating of vulnerabilities. It assists in prioritizing the remediation measures.

Fundamentally, there are two options to deal with vulnerabilities:

- Eliminating the vulnerability by updating the software, removing the component or changing the configuration.
- Implementing a rule in a firewall or a 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 attacker 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.

The Greenbone Cloud Service also supports the testing of the implemented remediation measures. With its help responsible personnel can document the current state of IT security, recognize changes and record these changes in reports.

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

CHAPTER 2

Read Before Use

The Greenbone Cloud Service uses 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. This includes probes via different protocols (e.g., HTTP, FTP) to all exposed services for service detection.

Note: It is the fundamental task of the Greenbone Cloud Service to find and identify otherwise undetected vulnerabilities. To a certain extent the scanner has to behave like a real attacker 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.

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.
- 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 included in the list of allowed connections on the affected system. Information on creating such a 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 an attacker can do the very same at unplanned times and to an unplanned extent. Finding out about it earlier than the attacker 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 Cloud Service to scan the target systems.

CHAPTER 3

Guideline for Using the Greenbone Cloud Service

The following steps are fundamental in using the Greenbone Cloud Service:

- Creating a user account for logging in → Chapter *4.1* (page 12)
- Selecting a subscription plan → Chapter *5.5* (page 22)
- Performing a scan → Chapter *6* (page 27)
- Performing an authenticated scan → Chapter *6.3* (page 44)
- Reading and using a report → Chapter *7.1* (page 72)

CHAPTER 4

Getting to Know and Accessing the Platform

4.1 Creating a User Account

For using the Greenbone Cloud Service, a user account must be created.

- If self-service is not enabled (= managed-service), the vMSP must create the user accounts.
- If self-service is enabled, users are able to create their own account as described in the following. Nevertheless, the vMSP can also create the user accounts.
- The created user account is a main user account.
- The main user can invite other users to their team (see Chapter *5.4* (page 21)).

Note: By default, all newly created accounts are free trial accounts that can be converted to paid accounts later (see Chapter *5.5* (page 22)).

A new user account can be created as follows:

1. Open the web browser.
2. Enter the URL of the Greenbone Cloud Service.
3. Click *Register*.
4. Enter the e-mail address for the account in the input box *E-mail address*.
5. Enter the password for the account in the input box *New password* and repeat it in the input box *Repeat new password*.
6. Activate the checkboxes regarding the agreement with the terms of use and the privacy policy.
7. Click *Test for free*.

   Note: For selecting a subscription see Chapter *5.5* (page 22).

4.2 Logging into the Platform

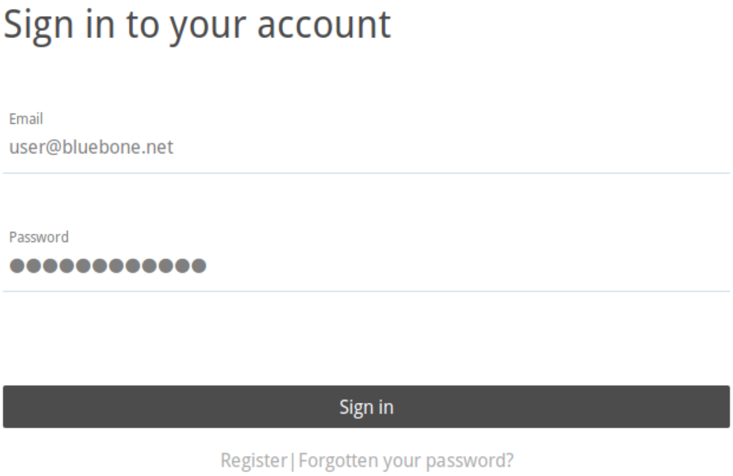
The Greenbone Cloud Service can be accessed as follows:

1. Open the web browser.
2. Enter the URL of the Greenbone Cloud Service.

Tip: The language of the platform can be selected in the upper right or upper left corner.

3. Log in using the e-mail address and password of the Greenbone Cloud Service account (see Chapter *4.1* (page 12)).

   → The page *Scan Management* is displayed.



Sign in to your account

Email
user@bluebone.net

Password
●●●●●●●●●●●●

Fig. 4.1: Logging in to the platform

Note: If the password is forgotten, a link for resetting it can be requested by clicking *Forgotten your password?*.

4.3 Structure of the Platform

4.3.1 List Pages

List pages show an overview of all existing objects of one kind (see Fig. 4.2). They are available for scans, scan tasks, targets, login credentials, schedules and gateways.

A list page can be opened by selecting the desired page in the menu panel, e.g., selecting *Targets* in the category *Scan Configuration* in the menu panel opens the list page *Targets*.

The list of objects (see Fig. 4.2/5) provides information such as name, status, type or possible actions for single objects (see Fig. 4.2/2). The information shown in the table depends on the object type.

1 – Searching for the name of a specific object.

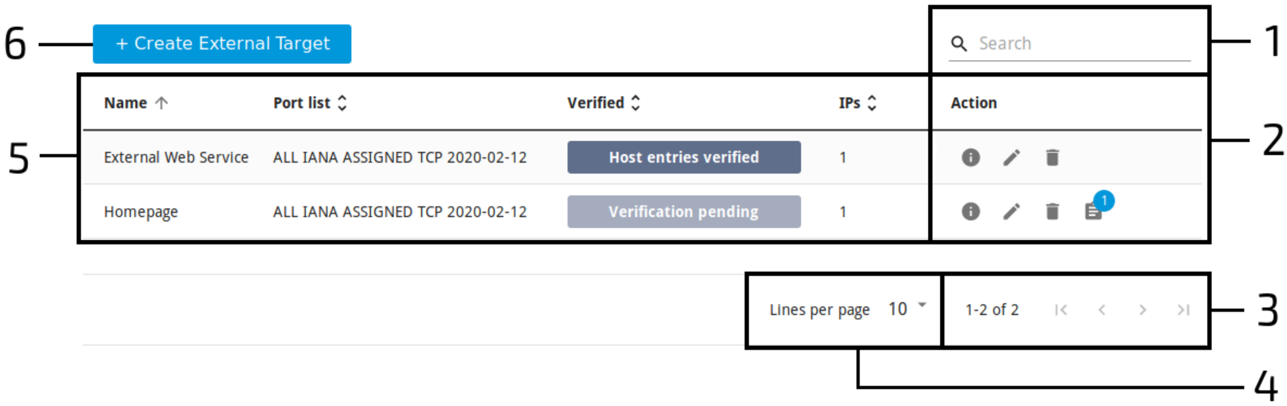
2 – Actions for single objects, depending on page content.

3 – Switching between pages.

4 – Selecting the number of objects displayed on one page.

5 – List of all existing objects of the selected object type.

6 – Creating a new object of the selected object type.



Name ↑	Port list ⇕	Verified ⇕	IPs ⇕	Action
External Web Service	ALL IANA ASSIGNED TCP 2020-02-12	Host entries verified	1	
Homepage	ALL IANA ASSIGNED TCP 2020-02-12	Verification pending	1	

Fig. 4.2: Structure of list pages

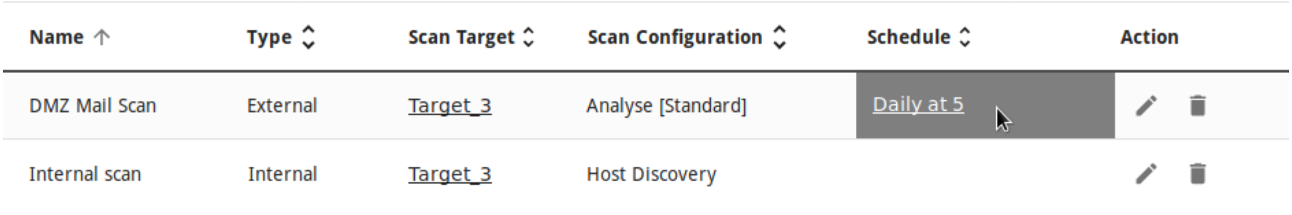
The list content can be sorted by a chosen column by clicking on the column title. The content can be sorted ascending or descending:

- ↑ in the column title shows that the objects are sorted ascending.
- ↓ in the column title shows that the objects are sorted descending.

4.3.2 Detail Overlays

For some objects an overlay containing detailed information can be opened, e.g., by clicking on the schedule name in the list of scan task (see Fig. 4.3), information about the used schedule is shown.

Note: If an overlay is available, the object's name is underlined.



Name ↑	Type ⇕	Scan Target ⇕	Scan Configuration ⇕	Schedule ⇕	Action
DMZ Mail Scan	External	Target_3	Analyse [Standard]	Daily at 5	
Internal scan	Internal	Target_3	Host Discovery		

Fig. 4.3: Opening the overlay

4.4 Getting Support

The menu item *Help* offers the following support issues and information:

Overview
Explanation of the basic terms of the Greenbone Cloud Service.

User Manual
Comprehensive user manual including step-by-step instructions for all activities related to the platform.

Legal Information
General terms of use and privacy policy of the Greenbone Cloud Service.

CHAPTER 5

Configuring the User, Team, and Account Settings

All users of the Greenbone Cloud Service can manage their own settings for scans and the platform.

5.1 Changing the Language

The language of the platform can be changed in the upper right corner.

Note: Alternatively, the language can be selected when logging in (see Chapter *4.2* (page 13)).

5.2 Setting up Notifications

Users can receive summaries of all run scans or notifications including reports when scans are finished.

Scan Summaries

Notifications including scan summaries can be set up as follows:

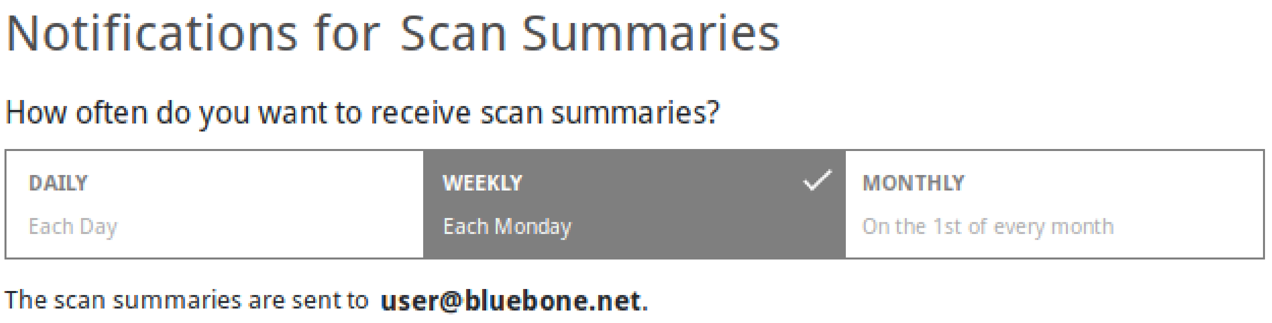
1. Select *Notifications* (category *User Settings*) in the menu panel.
2. Select the interval at which notifications should be received (see Fig. 5.1).

   Note: The setting for each interval is predefined.

   Multiple intervals can be selected at the same time.

   If no interval is selected, scan summaries are disabled.

   → The selection is applied immediately. The notifications are sent to the e-mail address that is used for logging in.



Notifications for Scan Summaries

How often do you want to receive scan summaries?

DAILY Each Day	WEEKLY ✓ Each Monday	MONTHLY On the 1st of every month

The scan summaries are sent to **user@bluebone.net**.

Fig. 5.1: Setting up scan summaries

Completed Scans

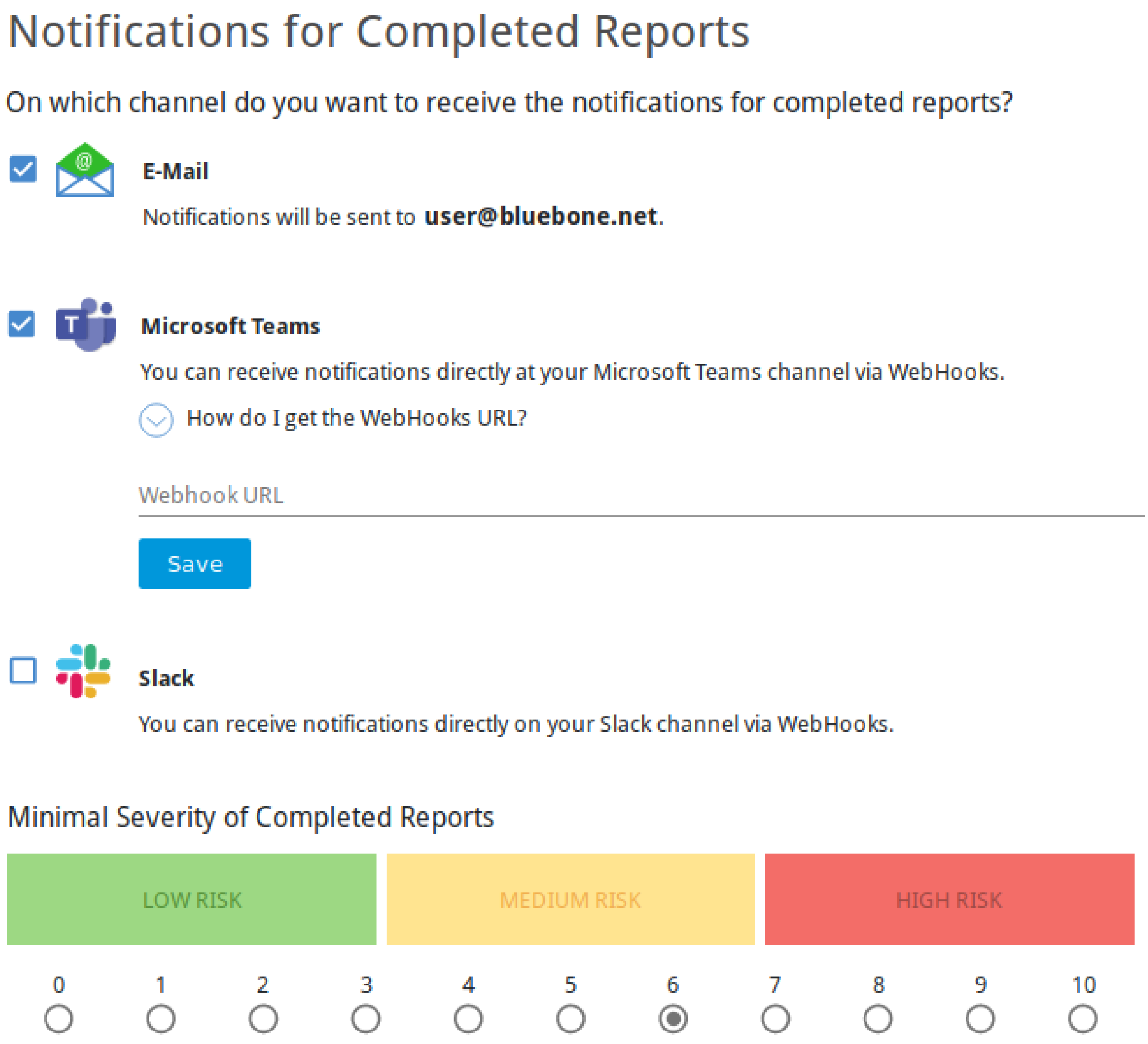
Notifications for completed scans can be set up as follows:

1. Select *Notifications* (category *User Settings*) in the menu panel.
2. Select the channel on which the notifications should be received and provide further details if necessary (see Fig. 5.2).

   Note: Multiple channels can be selected at the same time.

3. Select the minimum overall severity that a report must have for a notification to be sent.

   → The selection is applied immediately.



Notifications for Completed Reports

On which channel do you want to receive the notifications for completed reports?

☑ **E-Mail**

Notifications will be sent to **user@bluebone.net**.

☑ **Microsoft Teams**

You can receive notifications directly at your Microsoft Teams channel via WebHooks.

How do I get the WebHooks URL?

Webhook URL

Save

□ **Slack**

You can receive notifications directly on your Slack channel via WebHooks.

Minimal Severity of Completed Reports

LOW RISK	MEDIUM RISK	HIGH RISK

0	1	2	3	4	5	6	7	8	9	10
○	○	○	○	○	○	●	○	○	○	○

Fig. 5.2: Setting up notifications for completed scans

5.3 Changing the Security Settings

5.3.1 Changing the User Password

The password used for logging in can be changed as follows:

1. Select *Security* (category *User Settings*) in the menu panel.
2. Enter the current password in the input box *Password*.
3. Enter the new password in the input box *New Password*.
4. Repeat the password in the input box *Confirmation*.
5. Click *Save*.

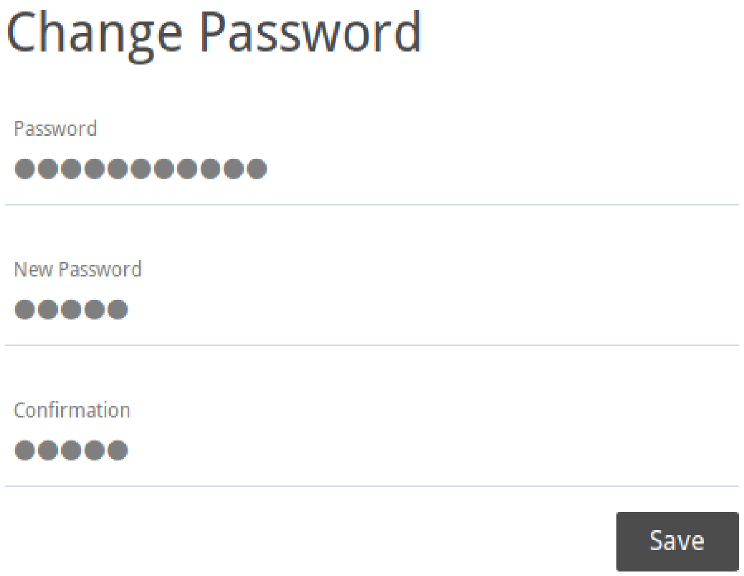
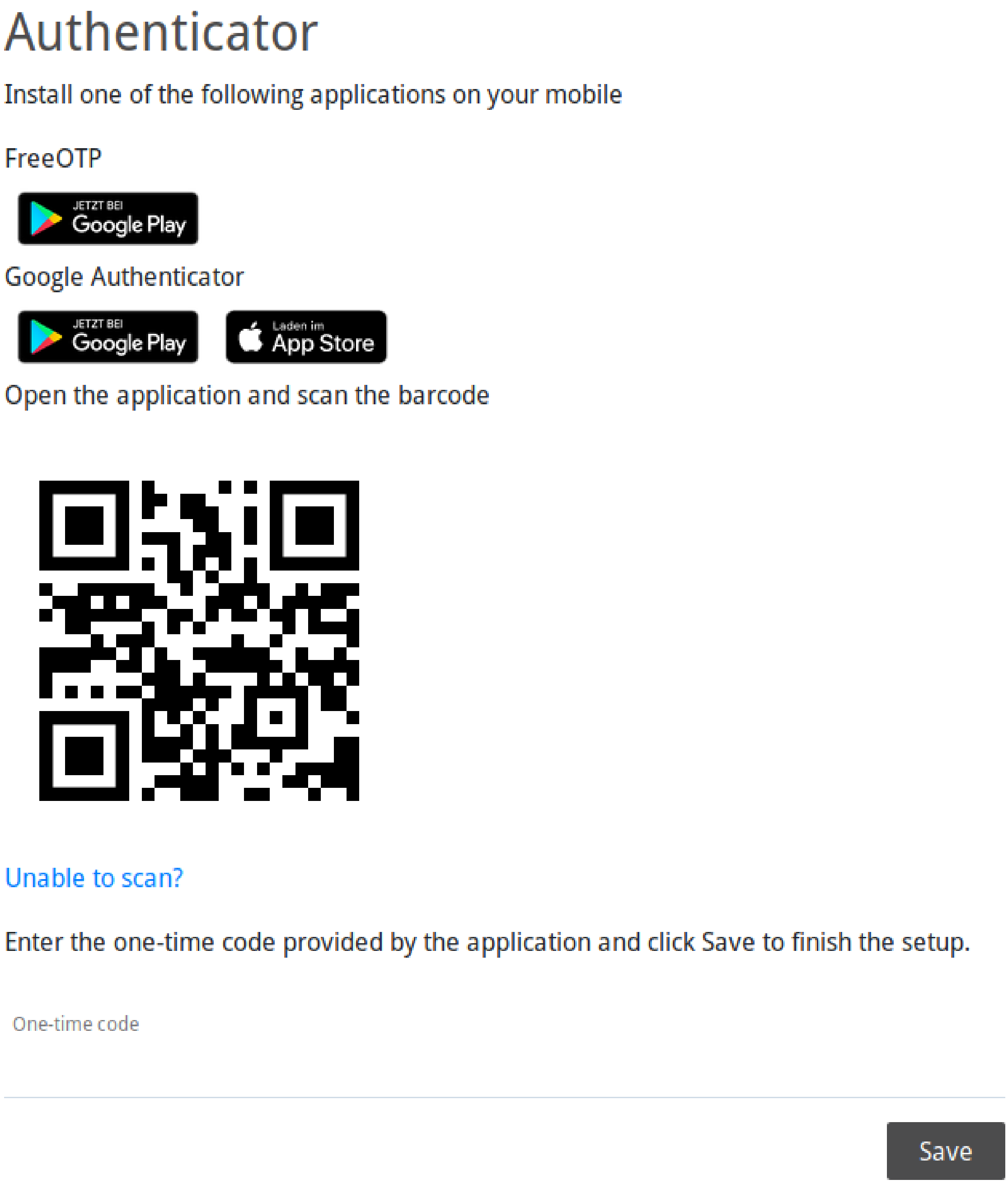


Fig. 5.3: Changing the user password

5.3.2 Setting up a Two-Factor Authentication

To make logging in more secure, a two-factor authentication can be set up as follows:

1. Download one of the following apps for smartphones:
   - *FreeOTP* (available for Android)
   - *Google Authenticator* (available for Android and iOS)
2. Finish the initial setup of the app.
3. Select *Security* (category *User Settings*) in the menu panel.
4. Scan the QR code displayed in the section *Authenticator* (see Fig. 5.4).
5. Enter the one-time code provided by the authenticator app in the input box *One-time code*.
6. Click *Save*.



Authenticator

Install one of the following applications on your mobile

FreeOTP

Google Authenticator

Open the application and scan the barcode

Unable to scan?

Enter the one-time code provided by the application and click Save to finish the setup.

One-time code

Fig. 5.4: Setting up a two-factor authentication

5.4 Creating and Managing Teams

A main user whose account was created either by a vMSP or by the user themselves (see Chapter *4.1* (page 12)) can invite other users to their team. All users of a team are operating with the same permissions and use the subscription of the main user.

5.4.1 Adding Users to the Team

1. Select *Team* (category *Team Settings*) in the menu panel.
2. Select *Invites*.
3. Click *+ Create New Invite*.
4. Enter the e-mail address of a user who should be invited.
5. Click *Send Invite*.

   → Invited users receive an e-mail, can create an account and join the team.

   Joined users are displayed when *Members* is selected.

Note: The invite expires after 24 hours.

If a user does not receive the e-mail or the invite has expired, the e-mail can be resend by clicking ↻ in the column *Actions*.

5.4.2 (De)activating Team Members

Deleting individual users or the main user of a team is not possible. Users can only be deactivated.

Note: Only the main user can (de)activate other users.

A user can be activated or deactivated as follows:

1. Select *Team* (category *Team Settings*) in the menu panel.
2. Click the slider in the column *Status*.

   → The change is applied immediately.

   A deactivated user is no longer able to log in.

5.4.3 Changing the Main User

The main user of a team, i.e., the account whose subscription is used, can be changed, for example, in case the respective employee is leaving the company.

The new main user must be an active user, deactivated users cannot be set as the main user (see Chapter *5.4.2* (page 21)).

Note: Only the main user can change the main user.

Alternatively, the vMSP can be contacted for changing the main user.

The main user can be changed as follows:

1. Select *Team* (category *Team Settings*) in the menu panel.

   Note: The current main user is indicated by 👤 in front of the e-mail address.

   ---

2. In the row of the user who should be the main user, click 👤 in the column *Action*.

   → A message is displayed, asking to confirm the change.

3. Click *Ok*.

5.4.4 Deleting the Account

Deleting individual users or the main user of a team is not possible, they can only be deactivated (see Chapter *5.4.2* (page 21)). Deleting an account will result in the following:

- The main user as well as all other users of the team are deleted.
- The main user as well as all other users will no longer be able to log in and use the Greenbone Cloud Service.
- All user, team and customer data are deleted permanently.
- All targets and reports are deleted.
- Active subscriptions expire at the end of the current billing period.

Note: Only the main user can delete an account.

Alternatively, the vMSP can be contacted for deleting the account.

---

1. Select *Team* (category *Team Settings*) in the menu panel.
2. In the section *Delete Account*, click *Delete Account*.

   → A message is displayed, asking to confirm the deletion.

3. Click *Ok*.

   → An e-mail is sent to the e-mail address of the main user, containing a link for confirming the deletion.

5.5 Configuring the Subscription

The current subscription is displayed by selecting *Subscription* (category *Team Settings*) in the menu panel (see Fig. 5.5).

Note: In case of a managed-service account, changing or terminating the subscription is not supported. In this case, the vMSP must be contacted.

5.5.1 Changing the Subscription Scope

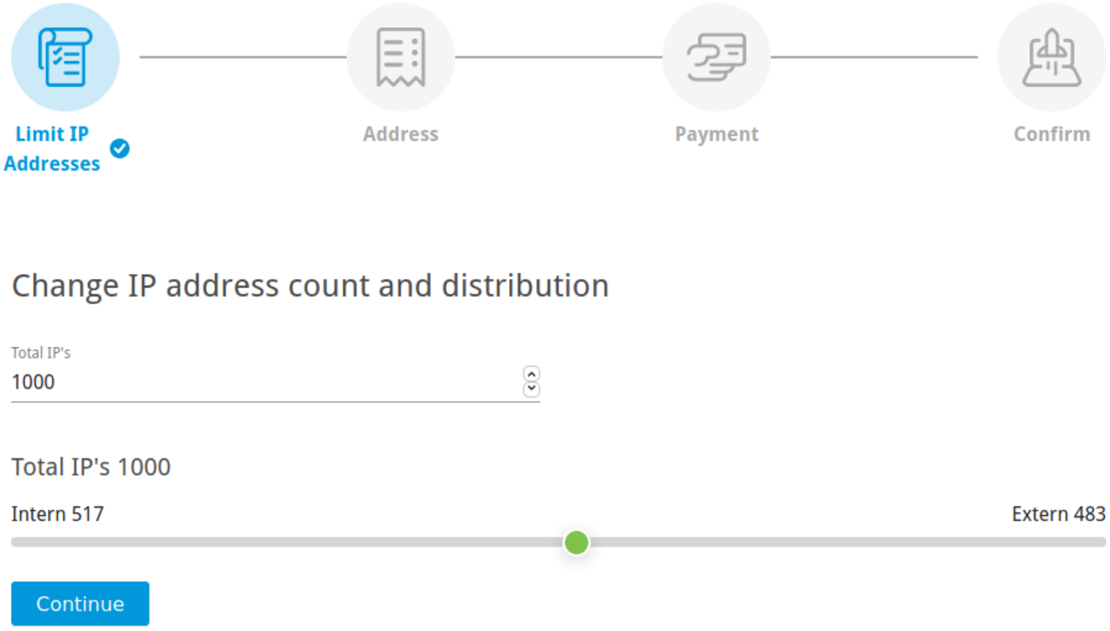
Shifting to a less extensive subscription is only possible by the end of the current posting month.

Upgrading to a more extensive subscription is possible immediately.

The subscription can be changed as follows:

1. Select *Subscription* (category *Team Settings*) in the menu panel.
2. Click *Upgrade*.
3. Enter the desired total number of IP addresses (sum of external and internal) in the input box *Total IP's* (see Fig. 5.5).
4. Move the slider to distribute the total number between internal and external IP addresses as desired.

   → The composition of the price is displayed in the overview.



Change IP address count and distribution

Total IP's
1000

Total IP's 1000

Intern 517

Extern 483

Fig. 5.5: Changing the subscription

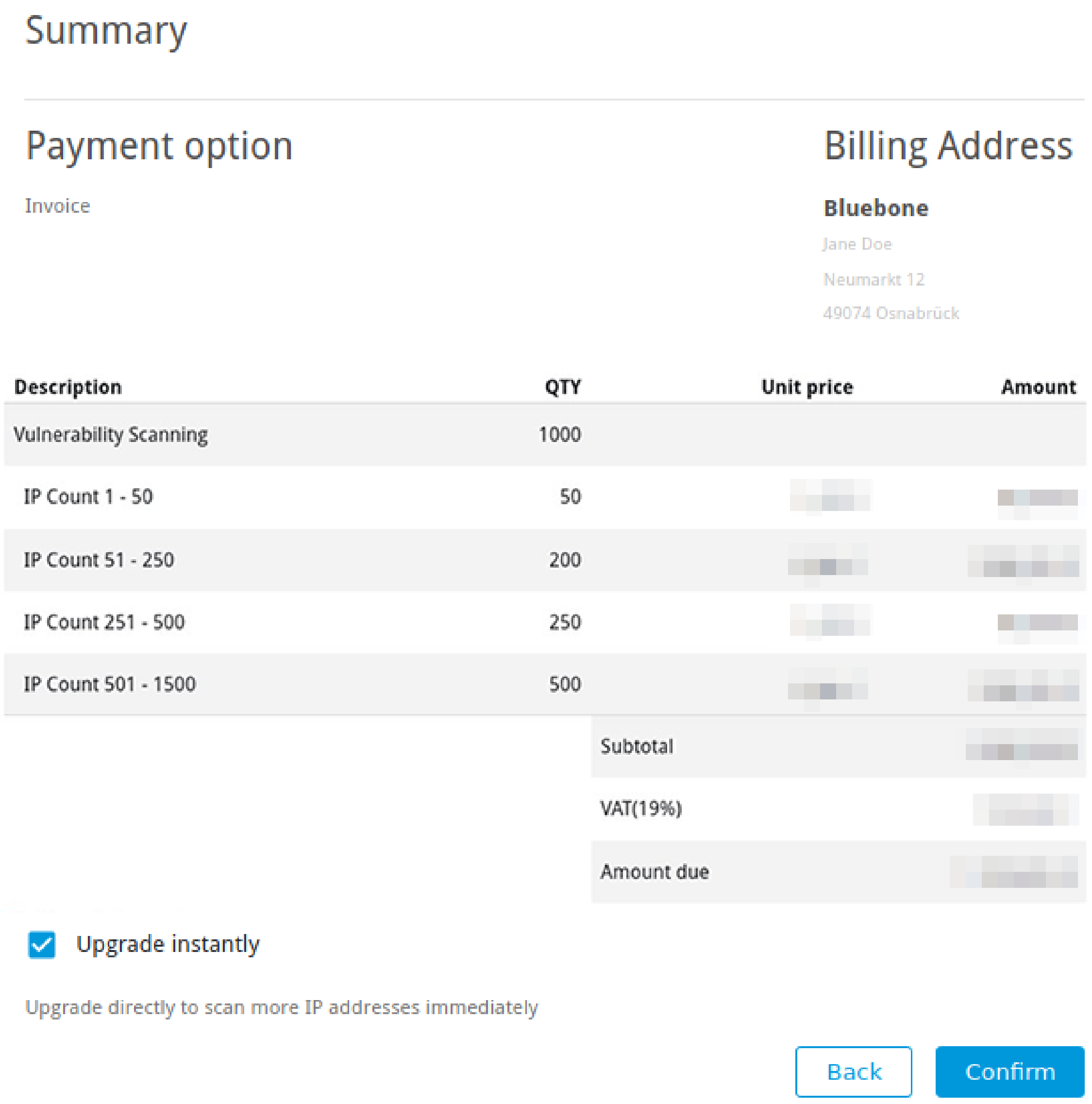
5. Click *Continue*.
6. Enter the contact data in the according input boxes.

   Tip: A different address for billing can be used, see step 8.

7. Enter the VAT number in the input box *Value Added Tax Identification (VAT-ID)*.
8. Optional: select the checkbox *Use a Different Billing Address* and enter the data in the according input boxes.
9. Click *Continue*.
10. Select the radio button of the desired payment method. If necessary, provide further payment details, e.g., credit card information.
11. Click *Continue*.

    → The order summary is displayed (see Fig. 5.6).

12. Optional: activate the checkbox *Upgrade instantly* if the new subscription should be used immediately.
13. Click *Confirm*.



Summary

Payment option

Invoice

Billing Address

Bluebone
Jane Doe
Neumarkt 12
49074 Osnabrück

Description	QTY	Unit price	Amount
Vulnerability Scanning	1000		
IP Count 1 - 50	50	[redacted]	[redacted]
IP Count 51 - 250	200	[redacted]	[redacted]
IP Count 251 - 500	250	[redacted]	[redacted]
IP Count 501 - 1500	500	[redacted]	[redacted]
		Subtotal	[redacted]
		VAT(19%)	[redacted]
		Amount due	[redacted]

☑ Upgrade instantly

Upgrade directly to scan more IP addresses immediately

Fig. 5.6: Confirming the subscription

5.5.2 Terminating the Subscription

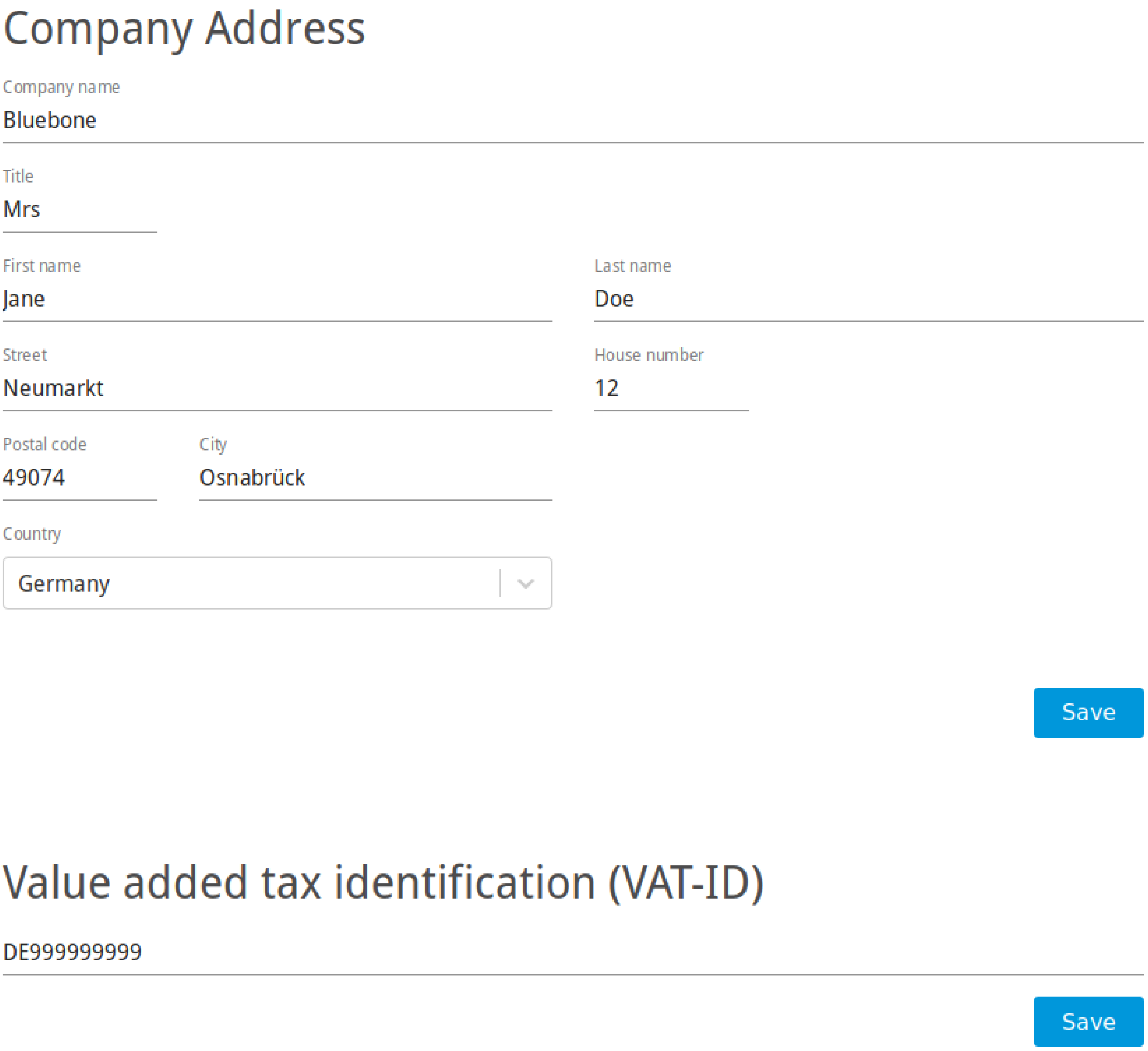
An active subscription can be terminated as follows:

1. Select *Billing* (category *Team Settings*) in the menu panel.
2. Click *Terminate Subscription*.

5.6 Changing the Billing Information

The client data can be changed as follows:

1. Select *Billing* (category *Team Settings*) in the menu panel.
2. In the section *Company Address*, enter the data in the according input boxes (see Fig. 5.7).
3. Click *Save*.



Company Address

Company name: Bluebone

Title: Mrs

First name: Jane

Last name: Doe

Street: Neumarkt

House number: 12

Postal code: 49074

City: Osnabrück

Country: Germany

Value added tax identification (VAT-ID)

DE999999999

Fig. 5.7: Changing the billing information

The VAT number can be added or changed as follows:

1. Select *Billing* (category *Team Settings*) in the menu panel.
2. In the section *Value Added Tax Identification (VAT-ID)*, enter the VAT number in the according input box (see Fig. 5.7).
3. Click *Save*.

5.7 Downloading Invoices

Note: Downloading invoices is only available for self-service accounts and subscriptions paid by credit card.

All invoices of current and former subscriptions can be downloaded by selecting *Invoices* (category *Team Settings*) in the menu panel and clicking PDF in the row of the respective invoice.

5.8 Configuring the Managed-Security Settings

In case of a managed-service account, the vMSP can be granted access to some report data or full access (“Managed Security”).

1. Select *Managed Security* (category *Team Settings*) in the menu panel.
2. Click the slider for *Report Access* to grant the vMSP report access.

   This includes access to the severity of the reports and tasks during the last two weeks and the amount of *High*, *Medium*, *Low* and *Log* results.

   or/and
3. Click the slider for *Full Access* to grant the vMSP full access to the settings and reports.

CHAPTER 6

Scanning a System

6.1 Using the Task Wizard for a Scan

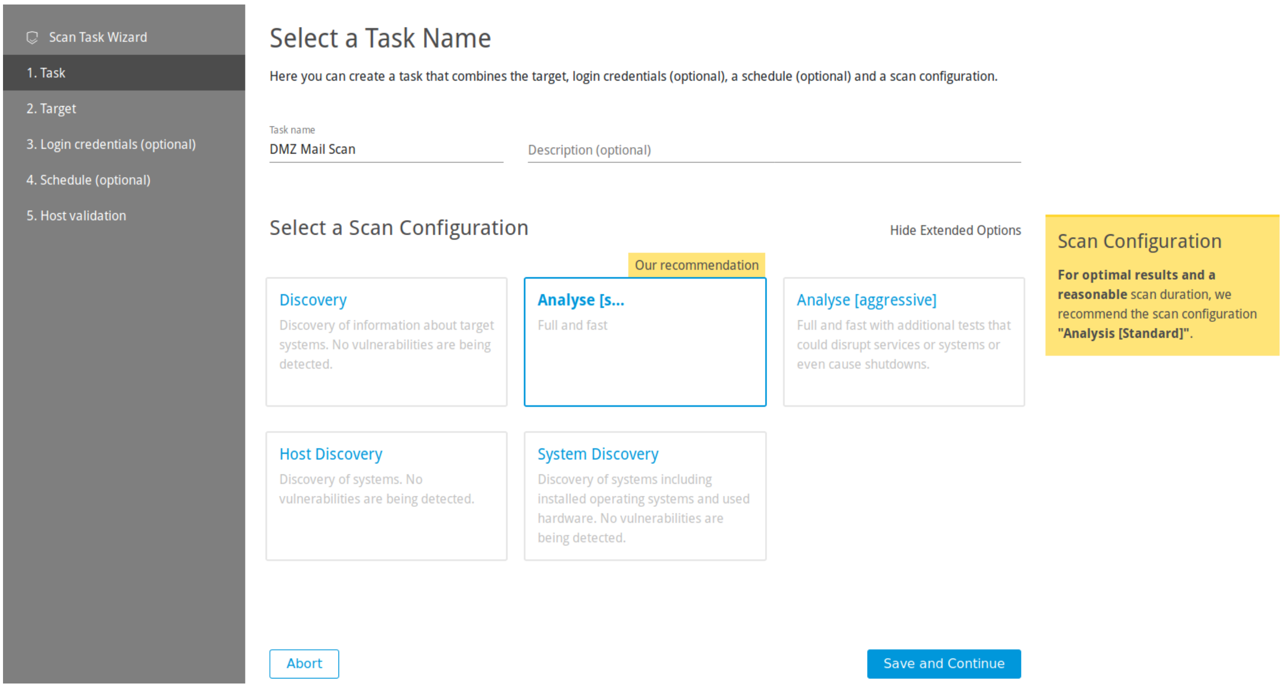
The task wizard can configure and start a scan with minimal user input.

1. Select *Scan Management* in the menu panel.
2. Click *+ Prepare New Scan Task with Wizard*.

   → An information message is displayed.
3. Click *Let's go!*.

   Note: If the message should not be displayed again, activate the checkbox *Do not show again* before clicking *Let's go!*.
4. Enter the name for the task in the input box *Task name* (see Fig. 6.1).
5. Optional: enter a description for the task in the input box *Description (optional)*.
6. Select the scan configuration.

   Note: The scan configuration *Analysis [standard]* is recommended.
7. Click *Save and Continue*.



Select a Task Name

Here you can create a task that combines the target, login credentials (optional), a schedule (optional) and a scan configuration.

Task name: DMZ Mail Scan

Description (optional)

Select a Scan Configuration

Discovery – Discovery of information about target systems. No vulnerabilities are being detected.

Analyse [s... – Full and fast

Analyse [aggressive] – Full and fast with additional tests that could disrupt services or systems or even cause shutdowns.

Host Discovery – Discovery of systems. No vulnerabilities are being detected.

System Discovery – Discovery of systems including installed operating systems and used hardware. No vulnerabilities are being detected.

Scan Configuration

For optimal results and a reasonable scan duration, we recommend the scan configuration **"Analysis [Standard]"**.

Fig. 6.1: Using the wizard

Note: When the wizard is used, only external target can be scanned.

8. Select an already available target from the list.

   or

8. Click *+ Create New Target* to create a new target.

   Tip: For the information to enter in the input boxes see Chapter *6.2.1* (page 30).

9. Click *Save and Continue*.

10. Optional: select already available credentials for Microsoft Windows login (SMB), SSH, or VMware ESXi from the list.

    or

10. Optional: click *+ Create New Login Credentials* to create new credentials.

    Tip: For the information to enter in the input boxes see Chapter *6.3.2.1* (page 46).

11. Click *Save and Continue*.

12. Optional: select an already available schedule from the list.

    or

12. Optional: click *+ Create New Schedule* to create a new schedule.

    Tip: For the information to enter in the input boxes see Chapter *6.4.1* (page 60).

13. Click *Save and Continue*.

Note: If an external target was chosen and the host(s) have not been validated yet, *Request Host Validation* is displayed for the host(s) (see Fig. 6.2).

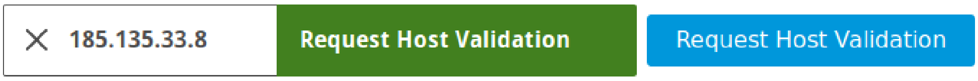


Fig. 6.2: Host(s) not validated yet

14. To carry out the host validation, click *Request Host Validation*.

→ The contacts for the configured host(s) are collected from RIPE NCC. For more information see Chapter *6.2.2* (page 34).

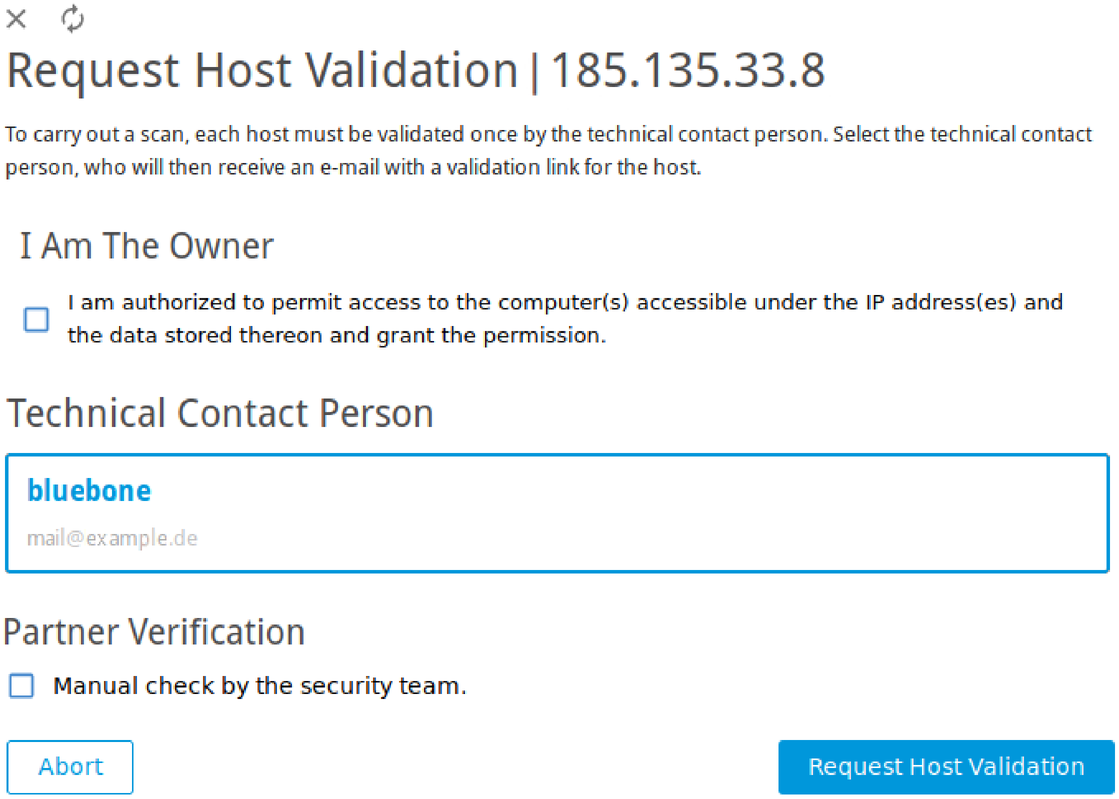
When this process is finished, an overlay displays the found contact (see Fig. 6.3).

Note: If no contact was found, the hosts have to be checked manually by the vMSP's security team.

15. Select the contact person from the list.

or

15. Activate the checkbox *Manual check by the security team*.



Request Host Validation | 185.135.33.8

To carry out a scan, each host must be validated once by the technical contact person. Select the technical contact person, who will then receive an e-mail with a validation link for the host.

I Am The Owner

□ I am authorized to permit access to the computer(s) accessible under the IP address(es) and the data stored thereon and grant the permission.

Technical Contact Person

bluebone
mail@example.de

Partner Verification

□ Manual check by the security team.

Fig. 6.3: Selecting contact for the host validation

16. Click *Request Host Validation*.

→ An e-mail is sent to the contact person or the security team. The status of the host validation is displayed on the page *Targets*.

17. Click *Prepare Scan*.

    → The page *Scan Management* is opened. The new task has the status *Available*.

18. In the row of the created task click ⏵.

For the status of a task see Chapter *6.7* (page 66).

Tip: The report of a task can be displayed as soon as the task has been started by clicking 🗎 for the respective task on the page *Scan Management*.

For reading, managing and downloading reports see Chapter *7* (page 72).

As soon as the status changes to *Done* the complete report is available. At any time the intermediate results can be reviewed (see Chapter *7.1* (page 72)).

Note: It can take a while for the scan to complete. The page is refreshing automatically if new data is available.

6.2 Configuring a Simple Scan Manually

Generally speaking, the Greenbone Cloud Service can use two different approaches to scan a target:

- Simple scan
- Authenticated scan using local security checks (see Chapter *6.3* (page 44))

The following steps have to be executed to configure a simple scan:

- Creating a target (see Chapter *6.2.1* (page 30))
- Validating the host(s) (see Chapter *6.2.2* (page 34)) or creating a gateway (see Chapter *6.2.3* (page 37))
- Creating a task (see Chapter *6.2.4* (page 42))
- Starting the task (see Chapter *6.2.5* (page 44))

6.2.1 Creating a Target

The first step is to define an external or an internal scan target.

6.2.1.1 Creating an External Target

1. Select *Targets* (category *Scan Configuration*) in the menu panel.
2. Click *External Targets*.
3. Create a new target by clicking *+ Create New External Target*.

4. Select the target mode by clicking *IP Address* or *Hostname*. It defines the form in which the target is specified.

Note: The target mode cannot be changed after initially creating the target.

A mixed target mode is not possible.

5. Define the target (see Fig. 6.4).
6. Click *Create Target*.

Note: A host validation is necessary for scanning an external target (see Chapter *6.2.2* (page 34)).

The following information can be entered:

Target name
The name can be chosen freely. A descriptive name should be chosen if possible.

Description (optional)
The optional comment allows specifying background information. It simplifies understanding the configured targets later.

Hosts to Be Scanned (for target mode *IP Address*)
Manual entry of the hosts that should be scanned, separated by commas.

Note: The IP address or the host name is required. In both cases it is necessary that the Greenbone Cloud Service can connect to the system. If using the host name, the Greenbone Cloud Service must also be able to resolve the name.

For entering the following options are available:

- Single IPv4 address, e.g., 192.168.15.5
- Domain name, e.g., example.com
- IPv4 address range, e.g., 192.168.15.5-192.168.15.27
- IPv4 address range in CIDR notation, e.g., 192.168.15.0/24
- Single IPv6 address, e.g., fe80::222:64ff:fe76:4cea
- IPv6 address range in CIDR notation, e.g., fe80::222:64ff:fe76:4cea/120

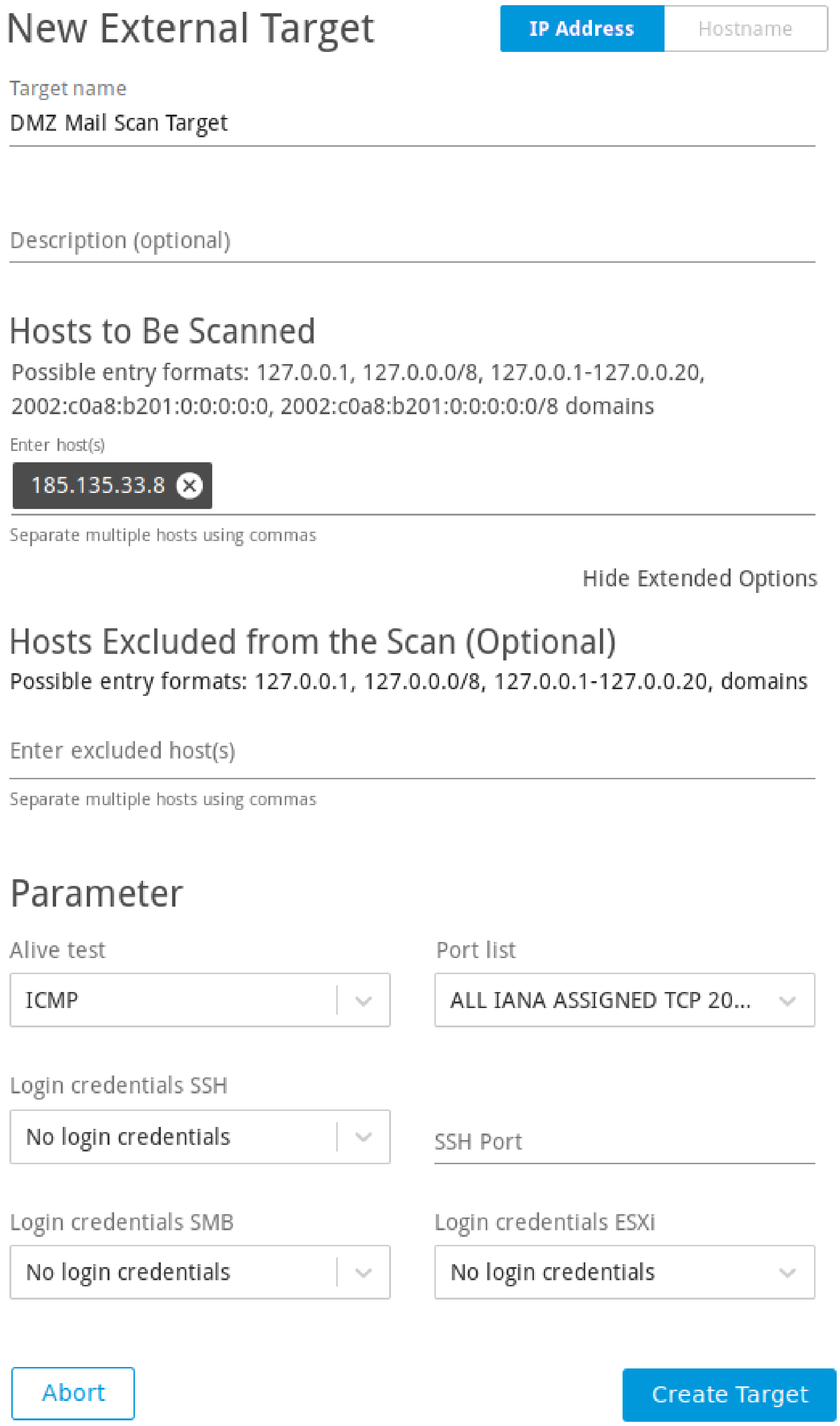
Multiple options can be mixed.

Hosts Excluded from the Scan (Optional) (for target mode *IP Address*)
Manual entry of the hosts that should be excluded from the list mentioned above, separated by commas.

The same specifications as for *Hosts to Be Scanned* apply.

Hostnames to be Scanned (for target mode *Hostname*)
Manual entry of the hosts that should be scanned, separated by commas.

Note: The host name is required. It is necessary that the Greenbone Cloud Service can connect to the system. The Greenbone Cloud Service must also be able to resolve the host name.



New External Target

Target name: DMZ Mail Scan Target

Description (optional)

Hosts to Be Scanned

Possible entry formats: 127.0.0.1, 127.0.0.0/8, 127.0.0.1-127.0.0.20, 2002:c0a8:b201:0:0:0:0:0, 2002:c0a8:b201:0:0:0:0:0/8 domains

Enter host(s): 185.135.33.8

Separate multiple hosts using commas

Hosts Excluded from the Scan (Optional)

Possible entry formats: 127.0.0.1, 127.0.0.0/8, 127.0.0.1-127.0.0.20, domains

Enter excluded host(s)

Separate multiple hosts using commas

Parameter

Alive test: ICMP

Port list: ALL IANA ASSIGNED TCP 20...

Login credentials SSH: No login credentials

SSH Port

Login credentials SMB: No login credentials

Login credentials ESXi: No login credentials

Fig. 6.4: Creating a new target

Alive test
This options specifies the method to check if a target is reachable. Options are:

- TCP ack service
- ICMP
- Consider alive
- TCP syn service

Port list
Port list used for the scan (see Chapter *6.9* (page 70)).

Login credentials SSH
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 Chapter *6.3* (page 44)).

Login credentials SMB
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 Chapter *6.3* (page 44)).

Login credentials ESXi
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 Chapter *6.3* (page 44)).

6.2.1.2 Creating an Internal Target

1. Select *Targets* (category *Scan Configuration*) in the menu panel.
2. Click *Internal Targets*.
3. Create a new target by clicking *+ Create New Internal Target*.
4. Define the target.
5. Click *Create Target*.

Note: A gateway has to be used for scanning an internal target (see Chapter *6.2.3* (page 37)).

The following information can be entered:

Target name
The name can be chosen freely. A descriptive name should be chosen if possible.

Description (optional)
The optional comment allows specifying background information. It simplifies understanding the configured targets later.

Hosts to Be Scanned
Manual entry of the hosts that should be scanned, separated by commas.

Note: The IP address or the host name is required. In both cases it is necessary that the Greenbone Cloud Service can connect to the system. If using the host name, the Greenbone Cloud Service must also be able to resolve the name.

For entering the following options are available:

- Single IPv4 address, e.g., 192.168.15.5
- Domain name, e.g., example.com

- IPv4 address range, e.g., 192.168.15.5-192.168.15.27
- IPv4 address range in CIDR notation, e.g., 192.168.15.0/24

Multiple options can be mixed.

Hosts Excluded from the Scan (Optional)
Manual entry of the hosts that should be excluded from the list mentioned above, separated by commas.

The same specifications as for *Hosts to Be Scanned* apply.

Alive test
This options specifies the method to check if a target is reachable. Options are:

- TCP ack service
- ICMP
- Consider alive
- TCP syn service

Port list
Port list used for the scan (see Chapter *6.9* (page 70)).

Login credentials SSH
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 Chapter *6.3* (page 44)).

Login credentials SMB
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 Chapter *6.3* (page 44)).

Login credentials ESXi
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 Chapter *6.3* (page 44)).

6.2.2 For External Targets: Validating the Hosts

If an external target is created, the defined hosts must be validated. Scanning targets without host validation is not possible.

A host can be validated by the following persons:

- By the users themselves if they are the owner of the host(s)
- By the person responsible for the host(s)
- By the security team of the vMSP

6.2.2.1 Validation by the User as the Owner

The host can be validated by the user.

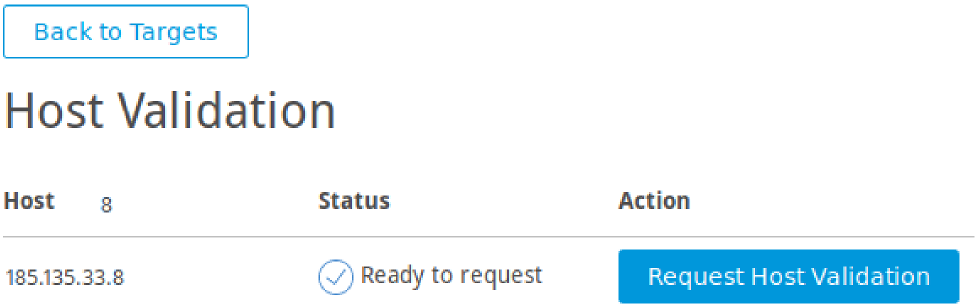
Note: The user must confirm that they are authorized to permit access to the computer(s) accessible under the IP address(es) and the data stored on them. By accepting this, the user assumes all responsibility for vulnerability scans performed against the corresponding computer(s) as well as for all effects and consequences that may arise from the scans. Any third-party complaints or requests will be forwarded directly to the user by Greenbone, and Greenbone will not further process nor provide any assistance in case of complaints or requests.

1. Select *Targets* (category *Scan Configuration*) in the menu panel.

2. Click *External Targets*.

   → If the validation has not been completed yet, Verification pending is displayed in the column *Verified*.

3. In the row of the target click 📋.
4. Click *Request Host Validation* (see Fig. 6.5).

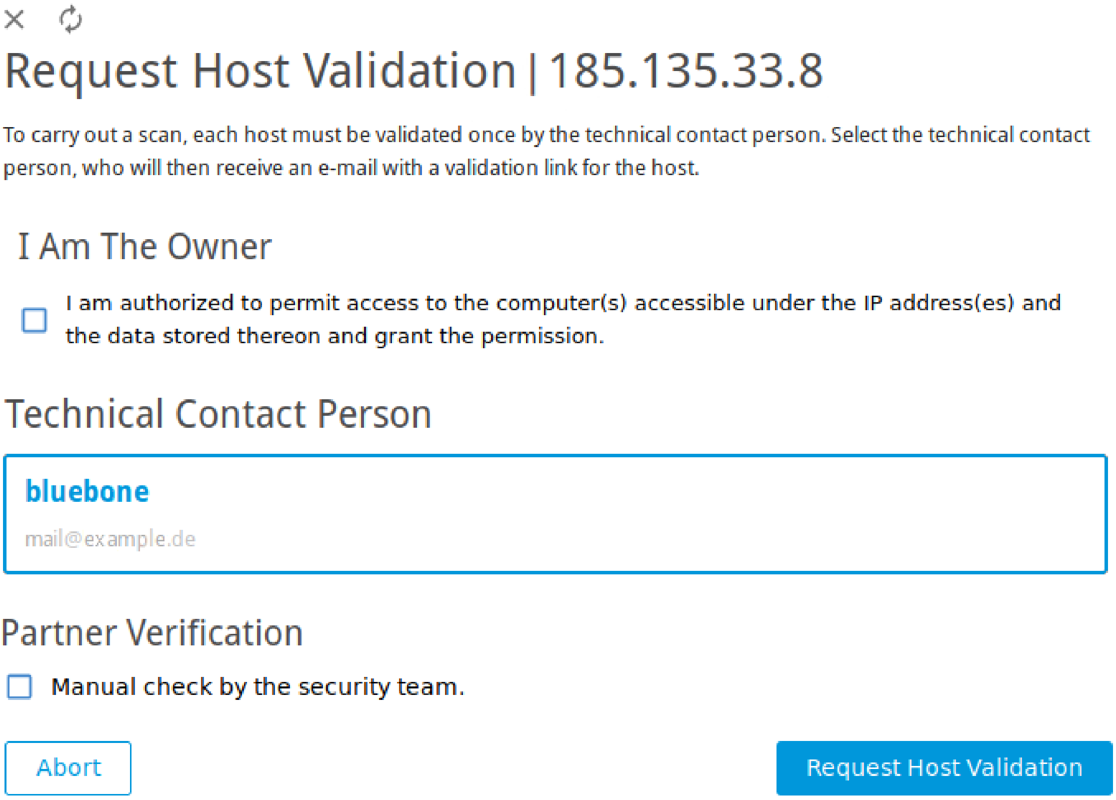


Host Validation

Host 8	Status	Action
185.135.33.8	✓ Ready to request	Request Host Validation

Fig. 6.5: Requesting the host validation

5. Activate the checkbox *I Am The Owner* (see Fig. 6.6).



Request Host Validation | 185.135.33.8

To carry out a scan, each host must be validated once by the technical contact person. Select the technical contact person, who will then receive an e-mail with a validation link for the host.

I Am The Owner

□ I am authorized to permit access to the computer(s) accessible under the IP address(es) and the data stored thereon and grant the permission.

Technical Contact Person

bluebone
mail@example.de

Partner Verification

□ Manual check by the security team.

Fig. 6.6: Selecting contact for the host validation

6. Click *Validate Host*.

   → When the hosts are validated, Host entries verified is displayed in the column *Verified* on the page *Targets*.

6.2.2.2 Validation by the Contact Person or by the vMSP’s Security Team

The responsible contact person – if available – is obtained from RIPE NCC[2]. RIPE NCC is the Regional Internet Registry (RIR) for Europe, the Middle East and parts of Central Asia and allocates and registers IP address ranges.

If no contact is found, the hosts can be checked manually by the vMSP’s security team.

1. Select *Targets* (category *Scan Configuration*) in the menu panel.
2. Click *External Targets*.

   → If the validation has not been completed yet, Verification pending is displayed in the column *Verified*.
3. In the row of the target click 📋.
4. Click *Request Host Validation* (see Fig. 6.5).

   → The contacts for the configured host are collected from RIPE NCC.

   When this process is finished, an overlay displays the found contact (see Fig. 6.6).
5. Select the contact person from the list.

   or

5. If no contact person was found, activate the checkbox *Manual check by the security team*.
6. Click *Request Host Validation*.

   → An e-mail is sent to the contact person or the security team.

Note: By clicking *Reset Contact Selection* the selected contact is rejected.

If the hosts are validated, Host entries verified is displayed in the column *Verified* on the page *Targets*.

If the host validation is rejected, Verification rejected is displayed in the column *Verified* on the page *Targets*.

[2] https://www.ripe.net/

6.2.3 For Internal Targets: Creating a Gateway

If an internal target in the customer's network should be scanned, a gateway must be used.

Resources

The gateway requires at least the following resources:

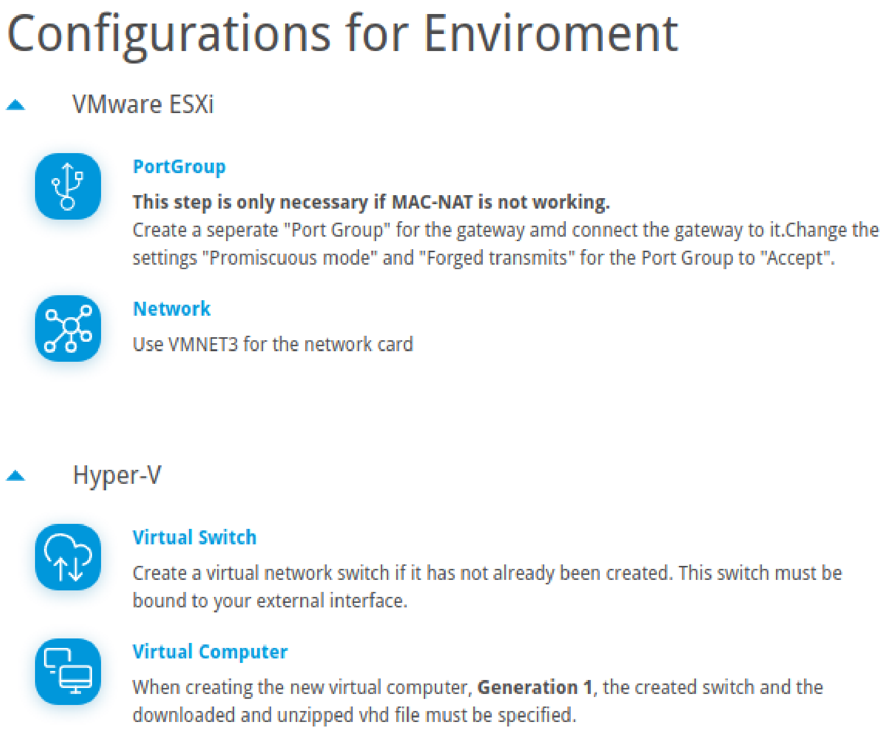
- 1 virtual CPU
- 512 MB RAM
- 8 GB hard disk

Supported Hypervisors

The following hypervisors are officially supported for running the gateway:

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

Note: Depending on the used virtual environment, the settings described under *Configurations for Environment* have to be configured (see Fig. 6.7).



Configurations for Enviroment

VMware ESXi

PortGroup

This step is only necessary if MAC-NAT is not working.

Create a seperate "Port Group" for the gateway amd connect the gateway to it.Change the settings "Promiscuous mode" and "Forged transmits" for the Port Group to "Accept".

Network

Use VMNET3 for the network card

Hyper-V

Virtual Switch

Create a virtual network switch if it has not already been created. This switch must be bound to your external interface.

Virtual Computer

When creating the new virtual computer, **Generation 1**, the created switch and the downloaded and unzipped vhd file must be specified.

Fig. 6.7: Advanced virtual environment settings

A gateway can be created as follows:

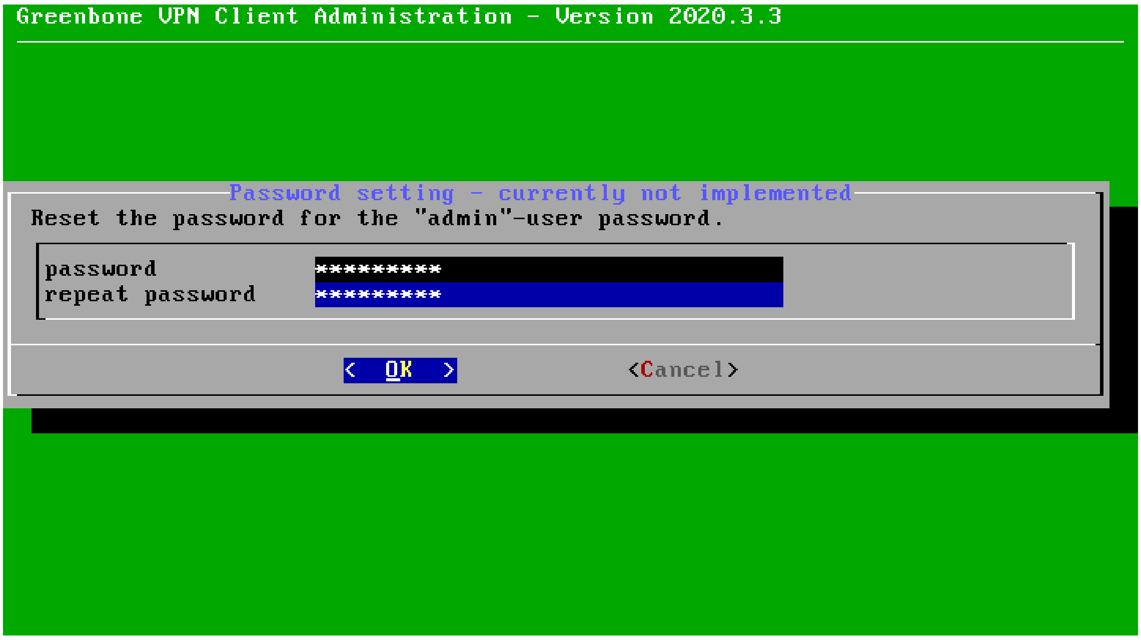
1. Select *Gateways* (category *Scan Configuration*) in the menu panel.
2. Select the desired virtual environment in the drop-down list *Download* and click ⤓.
3. Import the gateway to the virtual environment.
4. Start the gateway in the virtual environment.

5. After the boot process is completed, the login prompt is shown. The default login information is:
   - Login name: `admin`
   - Password: `admin`

   → The gateway administration menu is opened.
6. Select *Gateway configuration* and press `Enter`.
7. Select *Set web password* and press `Enter`.
8. Enter the password twice and press `Tab` (see Fig. 6.8).

Note: The password has to fulfill the following criteria:

- At least 8 characters
- Contains upper and lower cases
- Contains at least one special character
- Contains at least one number



```
Greenbone VPN Client Administration - Version 2020.3.3

Password setting - currently not implemented
Reset the password for the "admin"-user password.

password          **********
repeat password   **********
```

Fig. 6.8: Setting the password for the gateway web interface

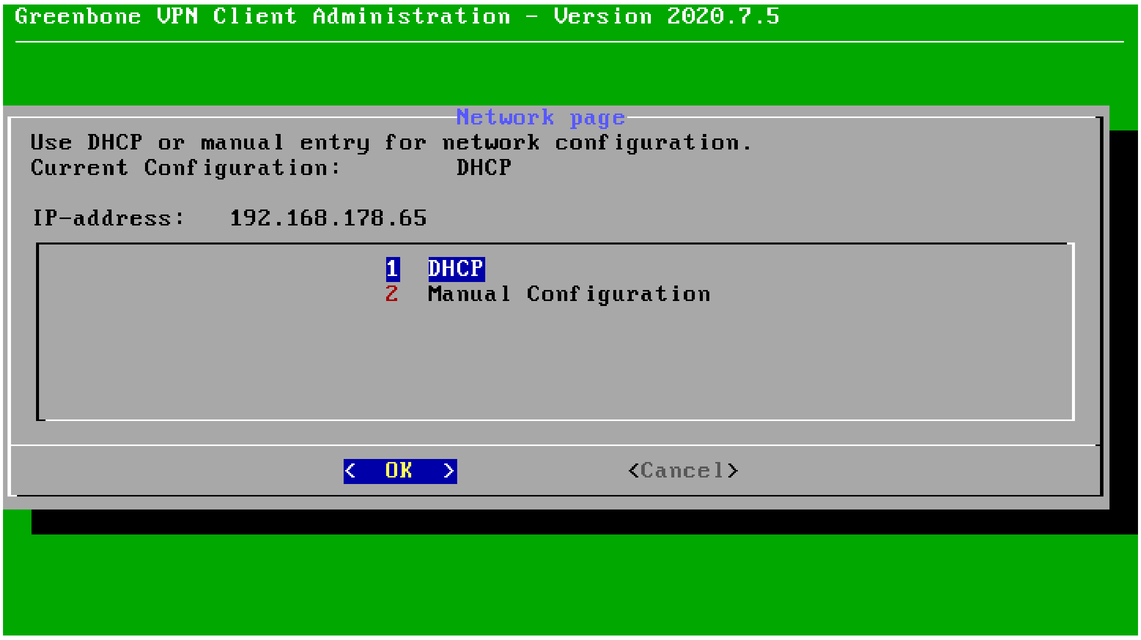
9. Press `Enter`.
10. Select *Save changes* and press `Enter`.

    → A message is displayed, informing that the gateway has been configured successfully.
11. Press `Enter` to close the message.
12. Select *Network configuration* and press `Enter`.

Note: For all configuration options see Chapter *6.6.2* (page 64).

---

13. Note the displayed IP address of the gateway (see Fig. 6.9). It is needed for accessing the gateway web interface.

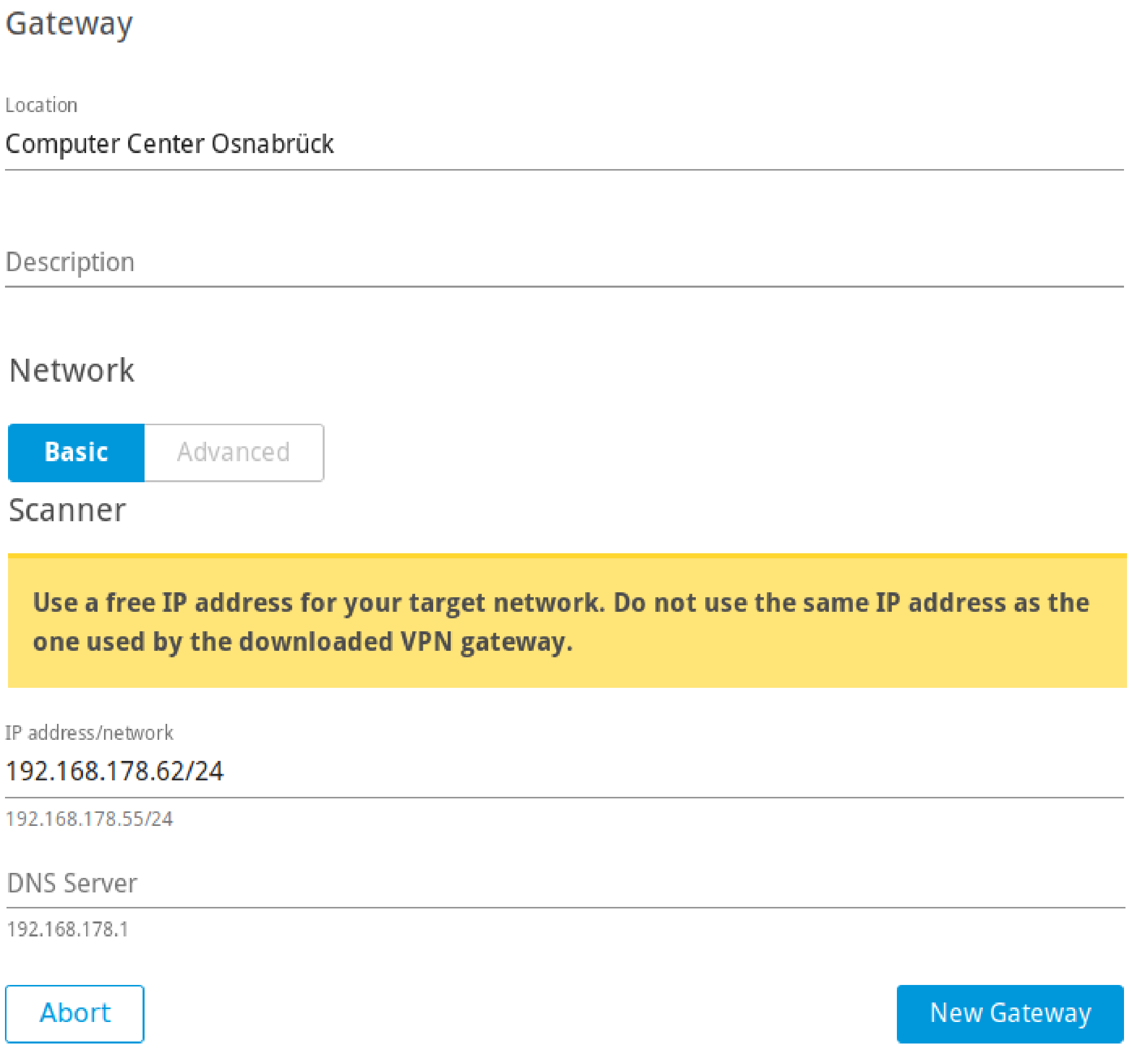


```
Greenbone VPN Client Administration - Version 2020.7.5

                          Network page
 Use DHCP or manual entry for network configuration.
 Current Configuration:        DHCP

 IP-address:    192.168.178.65

                          1  DHCP
                          2  Manual Configuration

                 <  OK  >            <Cancel>
```

Fig. 6.9: IP address of the gateway

14. On the platform, click *+ Create New Gateway*.

15. Enter a textual description of the gateway's location in the input box *Location* (see Fig. 6.10).



Gateway

Location

Computer Center Osnabrück

Description

Network

Scanner

Use a free IP address for your target network. Do not use the same IP address as the one used by the downloaded VPN gateway.

IP address/network

192.168.178.62/24

192.168.178.55/24

DNS Server

192.168.178.1

Fig. 6.10: Creating a new gateway

16. Optional: enter a description for the gateway in the input box *Description*.
17. Enter a free IP address from the network that should be scanned including the prefix length in the input box *IP address/network*.

Note: The entered IP address must differ from the IP address of the gateway.

18. Enter the IP address of a DNS server located in the target network in the input box *DNS Server*.

Note: By default, MAC-NAT is enabled.

19. If MAC-NAT does not work, click *Advanced* and deactivate the checkbox *Use MAC-NAT*.

Note: If VMware ESXi is the virtual environment in use, configure the settings displayed on the page *Gateways* under *Configurations for Environment*.

Note: If a network is to be scanned in which the scanner is not located, network routing can be used.

20. Click *+ Create New Route*.
21. Define the route by entering the network and the gateway located in the network in the respective input boxes.
22. Enter the metric information in the input box *Metric*.

    The metric is important if there are multiple routes for the same target network. In this case, the best route is the one with the smallest metric value.
23. Click *Save*.

    → The route is displayed in the table.
24. Click *New Gateway*.

    → The gateway is created and displayed on the page *Gateways*.

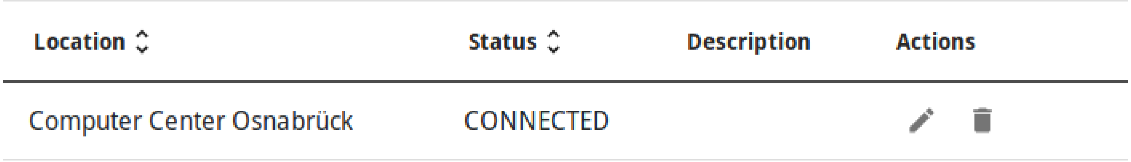
Registering the Gateway

The gateway has to be registered either via gateway web interface or via gateway administration menu (CLI).

The registration via gateway web interface is carried out as follows:

1. In the row of the gateway click ✎.
2. Select *WEB*.
3. Click *Copy to Clipboard* to copy the API key.
4. Open the web browser and enter the following URL: `https://<ip>`. Replace `<ip>` with the IP address of the gateway (see step 13).
5. Log in using the user name `admin` and the password defined in steps 6 – 9.
6. Select *Settings* in the menu panel.
7. Paste the API key in the input box *API-Key*.
8. Click *Save*.

    → On the page *Gateways* on the platform, the column *Status* displays *CONNECTED* (see Fig. 6.11).

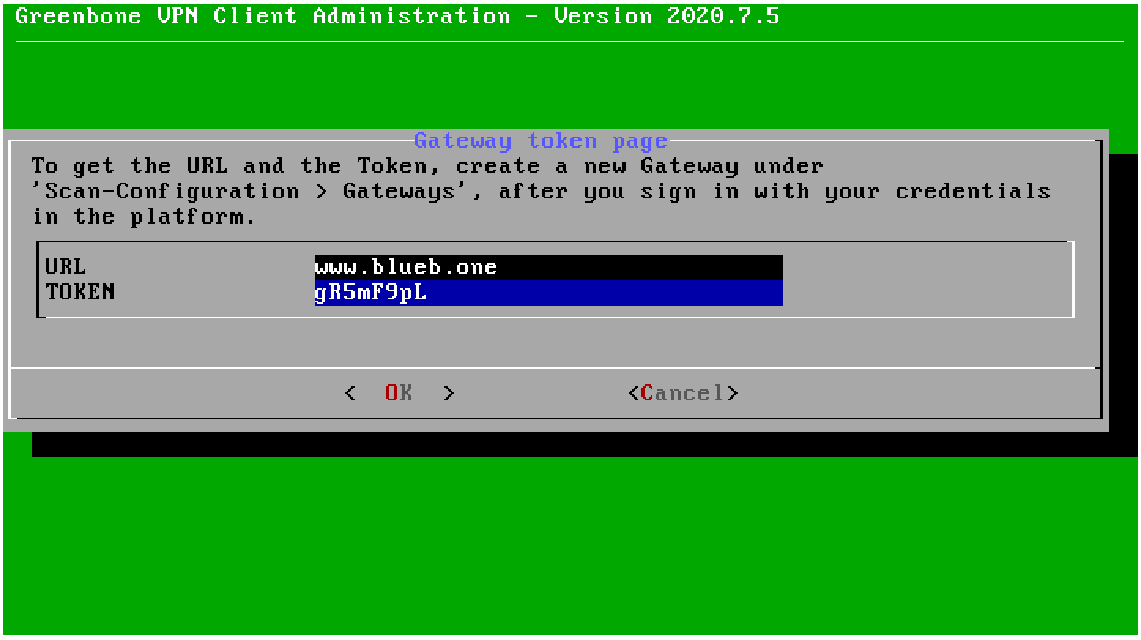


Location ⇕	Status ⇕	Description	Actions
Computer Center Osnabrück	CONNECTED		✎ 🗑

Fig. 6.11: Connecting the gateway

The registration via gateway administration menu (CLI) is carried out as follows:

1. In the row of the gateway click ✎.
2. Select *CLI*.
3. Note the URL and the token.
4. In the CLI, select *Gateway configuration* and press `Enter`.
5. Select *Enter connection token (Optional)* and press `Enter`.
6. Enter the URL and the token in the respective input boxes (see Fig. 6.12).



Greenbone VPN Client Administration - Version 2020.7.5

Gateway token page

To get the URL and the Token, create a new Gateway under
'Scan-Configuration > Gateways', after you sign in with your credentials
in the platform.

URL www.blueb.one
TOKEN gR5mF9pL

Fig. 6.12: Connecting the gateway

7. Press `Tab` and `Enter`.

   → On the page *Gateways* on the platform, the column *Status* displays *CONNECTED* (see Fig. 6.11).

6.2.4 Creating a Task

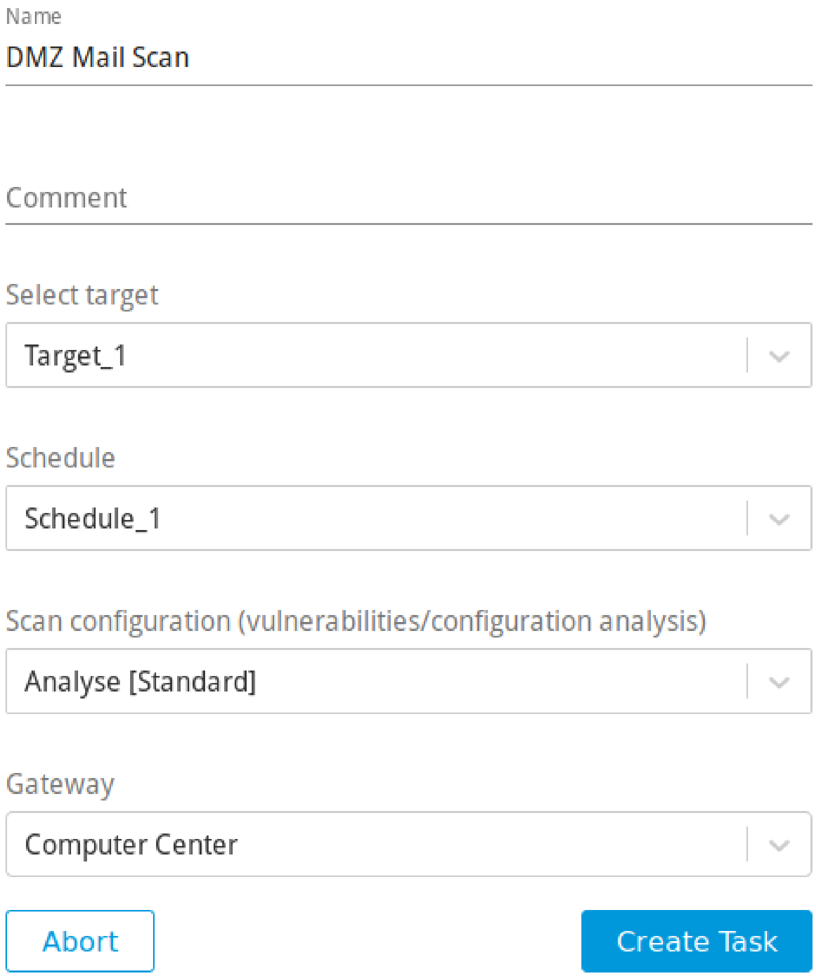
The next step is to create a task.

The Greenbone Cloud Service controls the execution of a scan using tasks. These tasks can be repeated regularly or run at specific times (see Chapter *6.4* (page 60)).

A task can be created as follows:

1. Select *Scan Configuration* in the menu panel.
2. Create a new task by clicking *+ Create New Task*.
3. Define the task (see Fig. 6.13).
4. Click *Create Task*.

   → The task is created and displayed on the page *Scan Configuration*.



Name
DMZ Mail Scan

Comment

Select target
Target_1

Schedule
Schedule_1

Scan configuration (vulnerabilities/configuration analysis)
Analyse [Standard]

Gateway
Computer Center

Fig. 6.13: 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.

Comment

The optional comment allows for the entry of background information. It simplifies understanding the configured task later.

Select target

Select a previously configured target from the drop-down list (see Chapter *6.2.1* (page 30)).

Schedule

Select a previously configured schedule from the drop-down list (see Chapter *6.4* (page 60)). The task can be run once or repeatedly at a predetermined time, e.g., every Monday morning at 6:00 a.m.

Selecting a schedule is optional. If no schedule should be used, select *Do not use a schedule*.

Scan configuration

The scan configuration specifies which vulnerability tests are performed during a scan.

The Greenbone Cloud Service comes with various predefined scan configurations (see Chapter *6.8* (page 69)).

The following option is only visible if an internal target is selected:

Gateway

Select a previously configured gateway from the drop-down list (see Chapter *6.2.3* (page 37)).

6.2.5 Starting the Task

Select *Scan Management* in the menu panel. In the row of the desired task, click ▷.

→ The scan is running. For the status of a task see Chapter *6.7* (page 66).

Tip: The report of a task can be displayed as soon as the task has been started by clicking 🗎. For reading, managing and downloading reports see Chapter *7* (page 72).

As soon as the status changes to *Done* the complete report is available. At any time the intermediate results can be reviewed (see Chapter *7.1* (page 72)).

Note: It can take a while for the scan to complete. The page is refreshing automatically if new data is available.

6.3 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 Greenbone Cloud Service 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 Greenbone Cloud Service was able to log into the target system. The local security check VTs in the resulting scan are minimally invasive.

The Greenbone Cloud Service only determines the risk level but does not introduce any changes on the target system. However, the login by the Greenbone Cloud Service is probably logged in the protocols of the target system.

The Greenbone Cloud Service can use different credentials based on the nature of the target. The most important ones are:

- **SMB**
  On Microsoft Windows systems, the Greenbone Cloud Service 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.

6.3.1 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 Greenbone Cloud Service 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 Greenbone Cloud Service 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 Greenbone Cloud Service itself. During the test, the Greenbone Cloud Service 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 *Analysis [Standard]*, 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). 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 if VTs that may cause damage to the host system are disabled 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 Greenbone Cloud Service does not evaluate the leaked information. The information is immediately discarded.

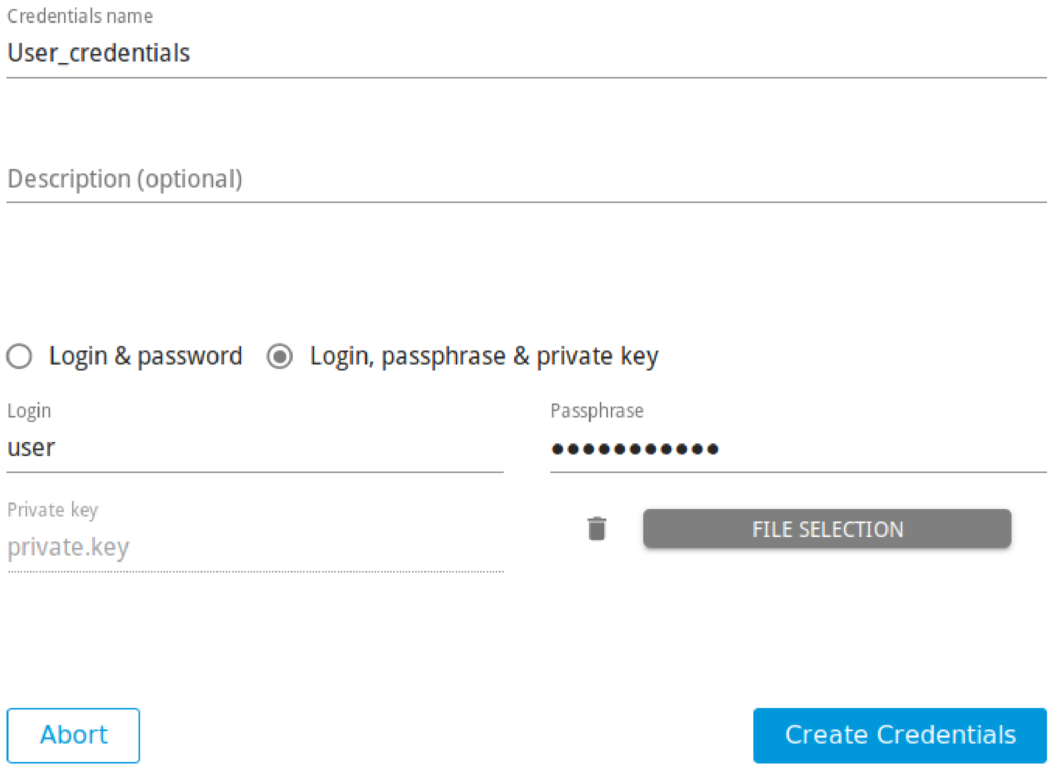
6.3.2 Using Credentials

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.

6.3.2.1 Creating Credentials

New credentials can be created as follows:

1. Select *Login Credentials* (category *Scan Configuration*) in the menu panel.
2. Create new credentials by clicking *+ Create New Login Credentials*.
3. Define the credentials (see Fig. 6.14).



Credentials name
User_credentials

Description (optional)

○ Login & password ● Login, passphrase & private key

Login
user

Passphrase
●●●●●●●●●●●

Private key
private.key

Fig. 6.14: Creating new credentials

4. Click *Create Credentials*.

The following details of the credentials can be defined:

Note: If the details contain German umlauts, the login does not work. The umlauts have to be replaced as follows:

- “ß” → “ss”
- “ä” → “a”
- “ö” → “o”
- “ü” → “u”

Credentials name
Definition of the name. The name can be chosen freely.

Description (optional)
An optional comment can contain additional information.

Login & password/Login, passphrase & private key
Selection of the credential type.

Depending on the selected type, further options are shown:

Login & password

- **Login**
  Definition of the login name used by the Greenbone Cloud Service to authenticate on the scanned target system.
- **Password**
  Definition of the password used by the Greenbone Cloud Service to authenticate on the scanned target system.

Login, passphrase & private key

- **Login**
  Definition of the login name used by the Greenbone Cloud Service to authenticate on the scanned target system.
- **Passphrase**
  Definition of the passphrase of the private SSH key.
- **Private key**
  Upload of the private SSH key by clicking *FILE SELECTION*.

  An uploaded file can be deleted by clicking 🗑.

6.3.2.2 Managing Credentials

All existing credentials can be displayed by selecting *Login Credentials* in the menu panel.

For all credentials the following information is displayed:

Name
Name of the credentials.

Login Name
User name for the credentials.

Comment
Optional additional information about the credentials.

For all credentials the following actions are available:

- ✎ Edit the credentials.
- 🗑 Delete the credentials. Only credentials which are currently not used can be deleted.

6.3.3 Requirements on Target Systems with Microsoft Windows

6.3.3.1 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 Greenbone Cloud Service 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 *6.3.3.2* (page 48).
- 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 Greenbone Cloud Service 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 IP address of the Greenbone Cloud Service. If the entry is confirmed, the firewall rule is configured. The service *File and Printer Sharing* will be enabled in the firewall rules.

6.3.3.2 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.

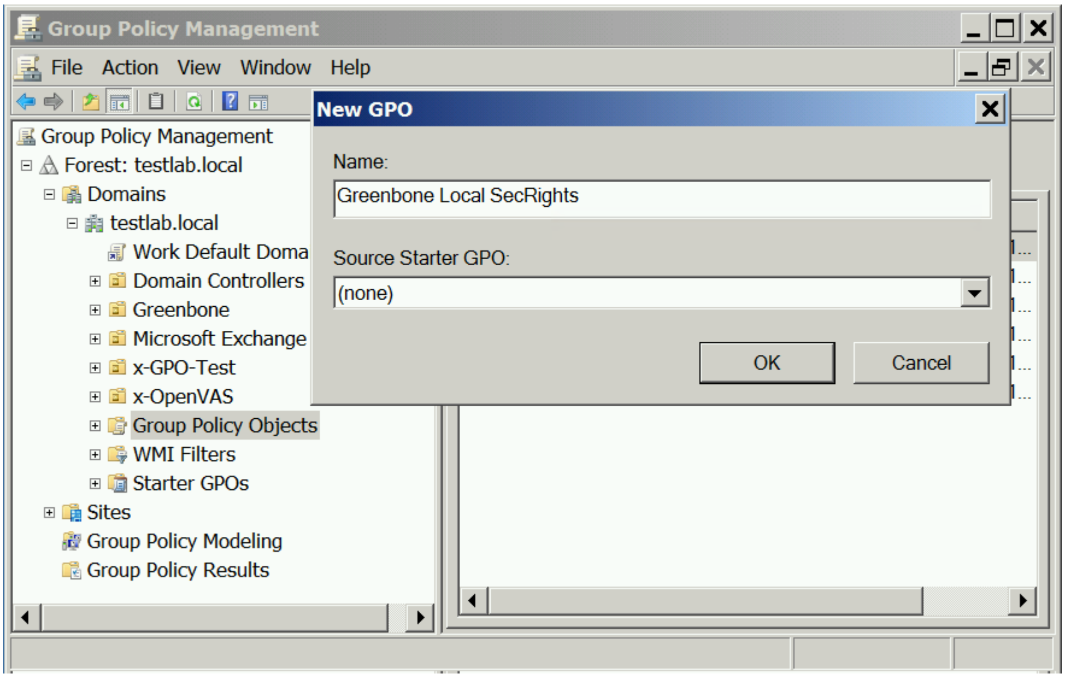
In order to use a domain account for host based remote audits on a Microsoft Windows target, the following configuration must be made under Windows XP Professional, Windows Vista, Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows 7, Windows 8, Windows 8.1 or 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 by the Greenbone Cloud Service for the local authenticated scans 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. 6.15).



Name: Greenbone Local SecRights

Source Starter GPO: (none)

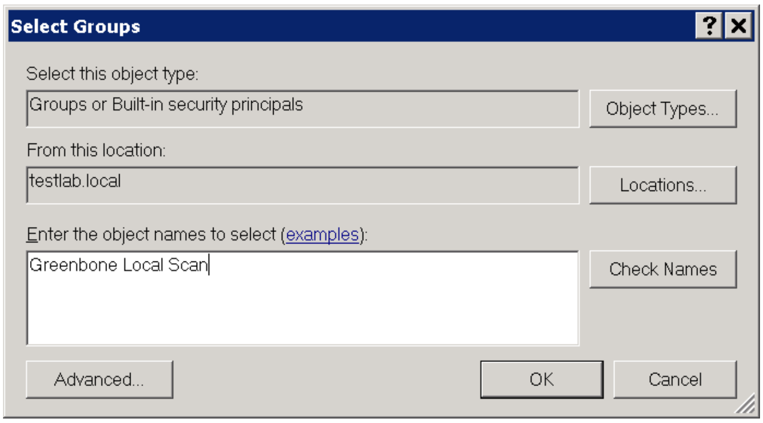
Fig. 6.15: Creating a new Microsoft Windows group policy object for Greenbone scans

4. Click *OK*.

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. 6.16).



Select this object type:
Groups or Built-in security principals

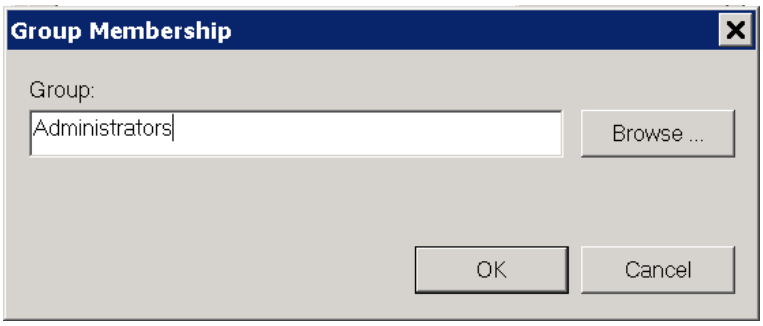
From this location:
testlab.local

Enter the object names to select (examples):
Greenbone Local Scan

Fig. 6.16: 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. 6.17) and click *OK* twice to close the open windows.

Note: On non-English systems enter the respective name of the local administrator group.

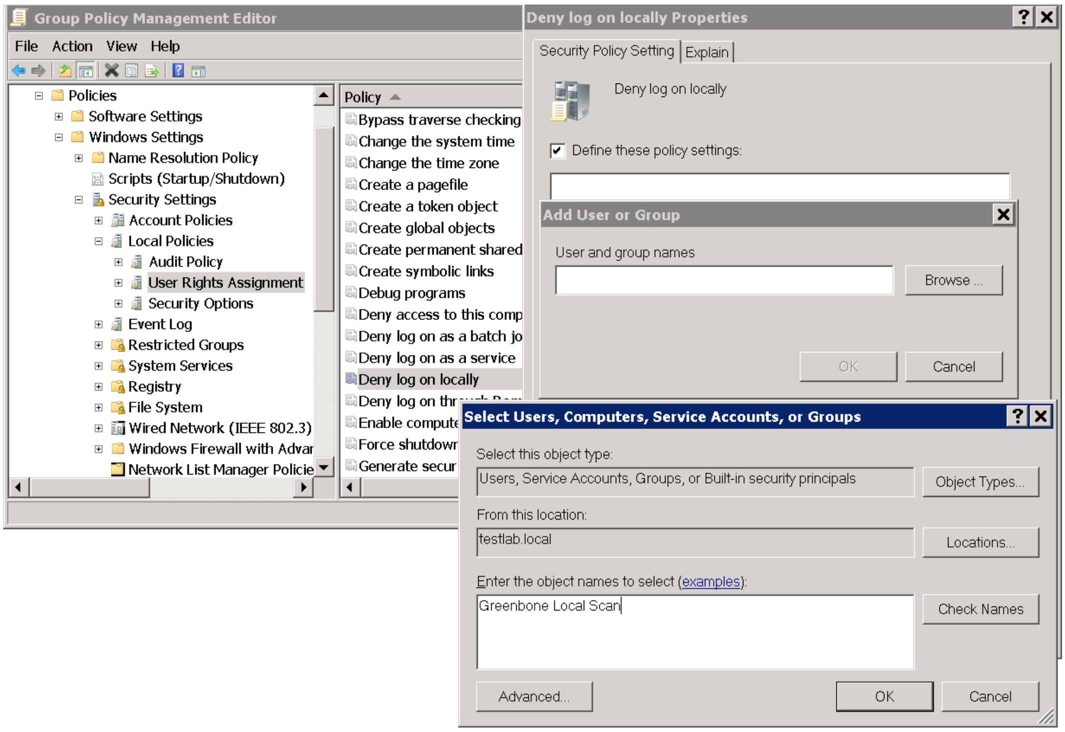


Group:
Administrators

Fig. 6.17: 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. 6.18).
6. Click *Check Names*.
7. Click *OK* three times to close the open windows.



☑ Define these policy settings:

Select this object type:
Users, Service Accounts, Groups, or Built-in security principals

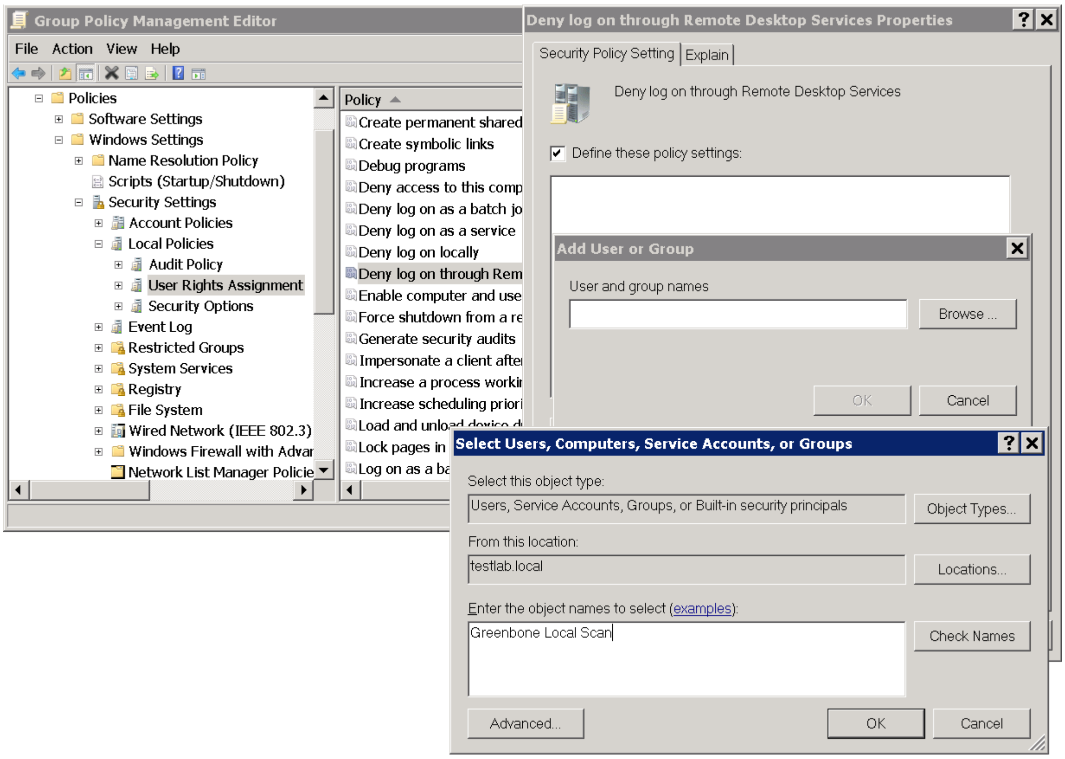
From this location:
testlab.local

Enter the object names to select (examples):
Greenbone Local Scan

Fig. 6.18: Editing the policy

Configuring the Policy to Deny the Group Greenbone Local Scan Logging into the System Remotely

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 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. 6.19).
6. Click *Check Names*.
7. Click *OK* three times to close the open windows.



☑ Define these policy settings:

Select this object type: Users, Service Accounts, Groups, or Built-in security principals

From this location: testlab.local

Enter the object names to select (examples): Greenbone Local Scan

Fig. 6.19: Editing the policy

Configuring the Policy to Give Read Permissions Only to the Registry for the Group Greenbone Local Scan

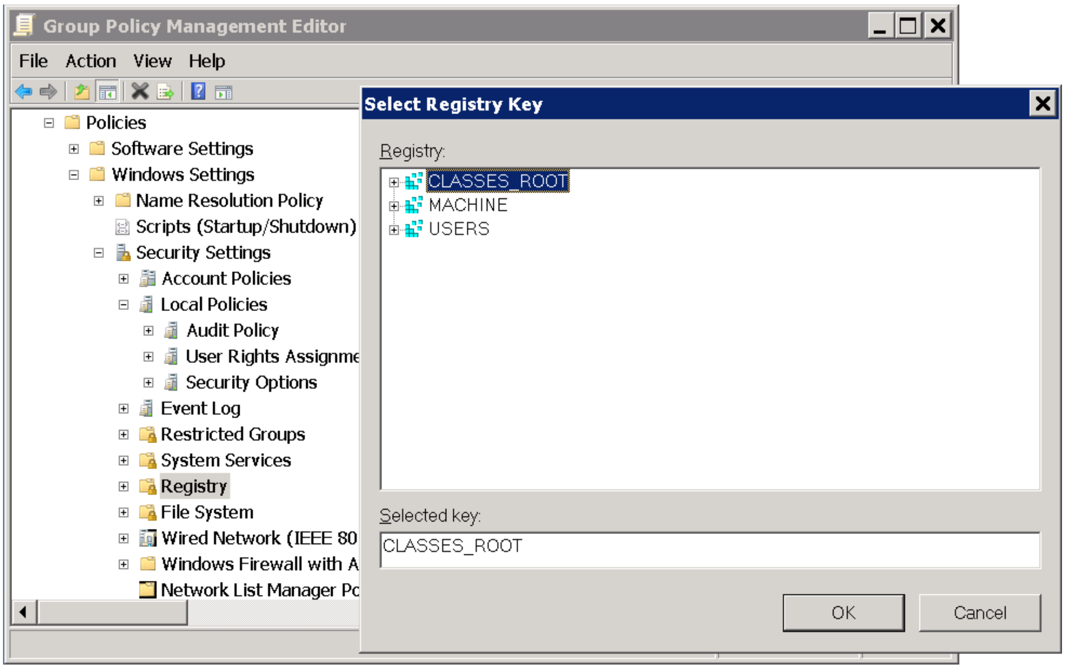
Important: This setting still exists after the GPO has been removed ("tattooing GPO").

This changes fundamental privileges which may not be simply reversed by removing the GPO.

Research whether the settings are compatible with the environment.

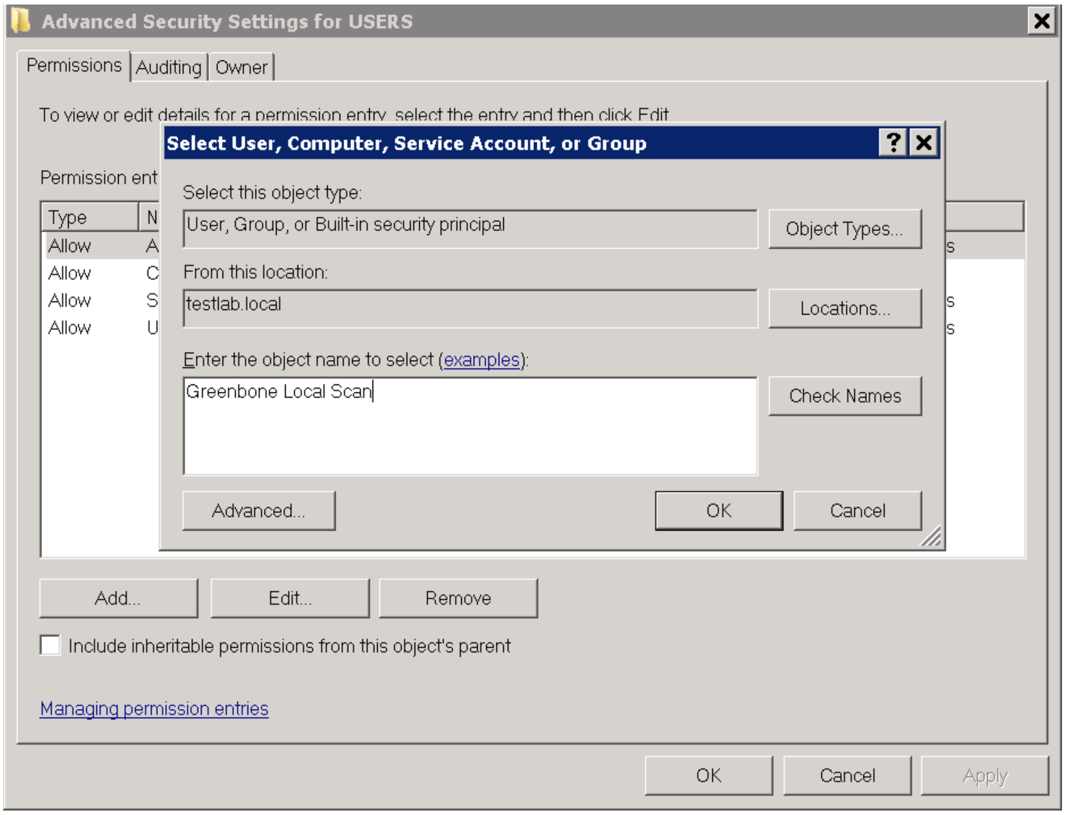
Note: The following steps are optional.

1. In the left panel right click *Registry* and select *Add Key*.
2. Select *USERS* and click *OK* (see Fig. 6.20).
3. Click *Advanced* and *Add*.
4. Enter `Greenbone Local Scan` in the input box and click *OK* (see Fig. 6.21).
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. 6.22).
7. Click *OK* twice and confirm the warning message by clicking *Yes*.
8. Click *OK*.
9. Select the radio buttons *Configure this key then* and *Propagate inheritable permissions to all subkeys* and click *OK* (see Fig. 6.23).
10. Repeat the steps 2 to 9 for *MACHINE* and *CLASSES_ROOT*.



Selected key: CLASSES_ROOT

Fig. 6.20: Selecting the registry key


Advanced Security Settings for USERS
Permissions
Auditing
Owner
To view or edit details for a permission entry, select the entry and then click Edit.
Permission ent
Type
N
Allow
Allow
Allow
Allow
Select User, Computer, Service Account, or Group
Object Types...
Locations...
Check Names
Advanced...
OK
Cancel
Add...
Edit...
Remove
Managing permission entries
OK
Cancel
Apply

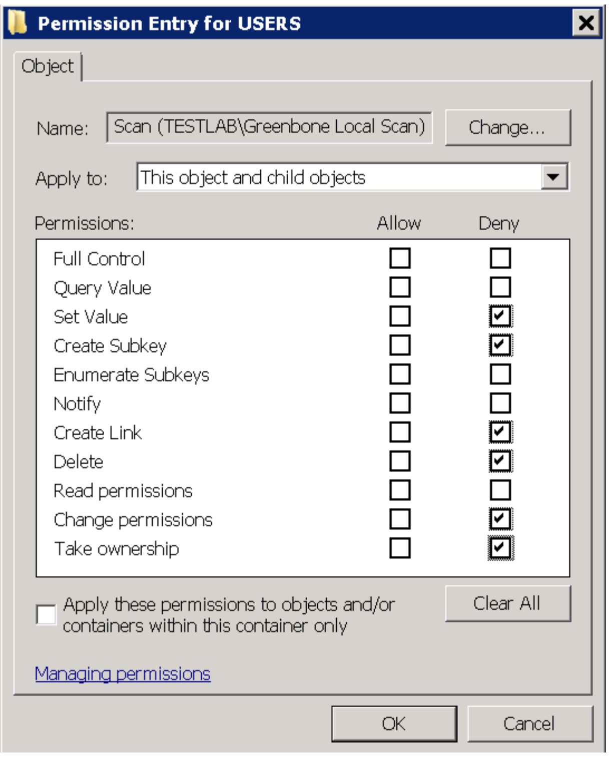
Select this object type: User, Group, or Built-in security principal

From this location: testlab.local

Enter the object name to select (examples): Greenbone Local Scan

□ Include inheritable permissions from this object's parent

Fig. 6.21: Selecting the group *Greenbone Local Scan*



Permission Entry for USERS

Object

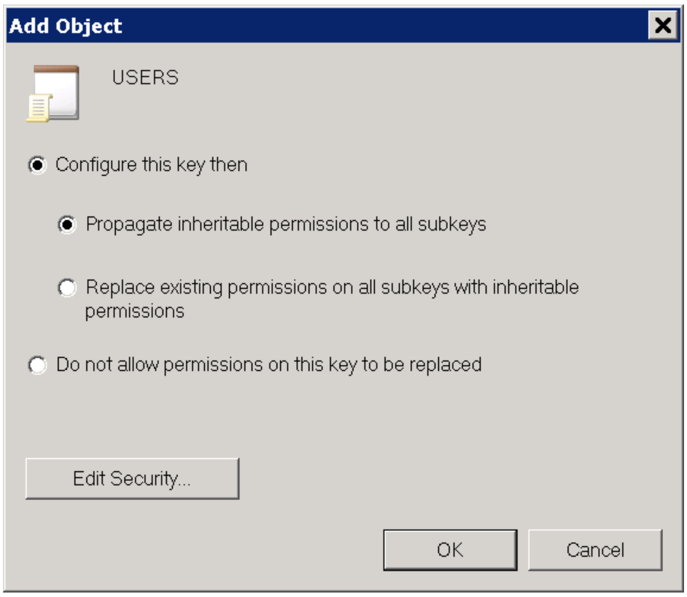
Name: Scan (TESTLAB\Greenbone Local Scan)

Apply to: This object and child objects

Permissions:	Allow	Deny
Full Control	□	□
Query Value	□	□
Set Value	□	☑
Create Subkey	□	☑
Enumerate Subkeys	□	□
Notify	□	□
Create Link	□	☑
Delete	□	☑
Read permissions	□	□
Change permissions	□	☑
Take ownership	□	☑

□ Apply these permissions to objects and/or containers within this container only

Fig. 6.22: Disallowing edition of the registry



Add Object

USERS

● Configure this key then

● Propagate inheritable permissions to all subkeys

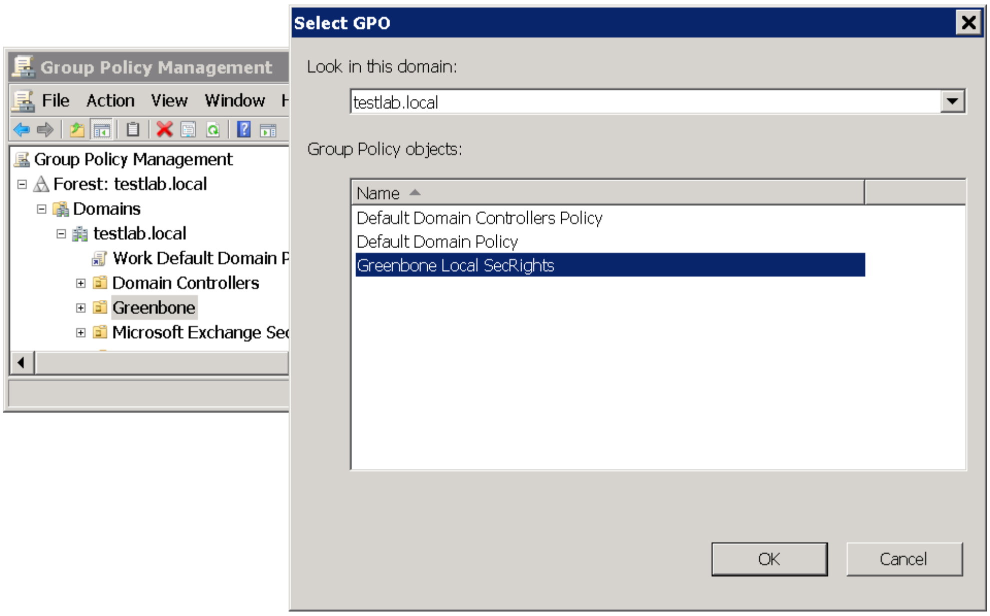
○ Replace existing permissions on all subkeys with inheritable permissions

○ Do not allow permissions on this key to be replaced

Fig. 6.23: Making the permissions recursive

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. 6.24).



Select GPO

Look in this domain: testlab.local

Group Policy objects:

Name
Default Domain Controllers Policy
Default Domain Policy
Greenbone Local SecRights

Fig. 6.24: Linking the policy

6.3.3.3 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.

6.3.3.4 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.

6.3.4 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 an SSH key stored on the Greenbone Cloud Service.
- 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 keys may also be used. SSH keys can be generated with OpenSSH by using the command `ssh-keygen` on Linux or `puttygen.exe` if using PuTTY on Microsoft Windows. The formats Ed25519 or RSA are recommended. All SSH keys must correspond to RFC 4716[3].
- 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.

[3] https://datatracker.ietf.org/doc/html/rfc4716

6.3.5 Requirements on Target Systems with ESXi

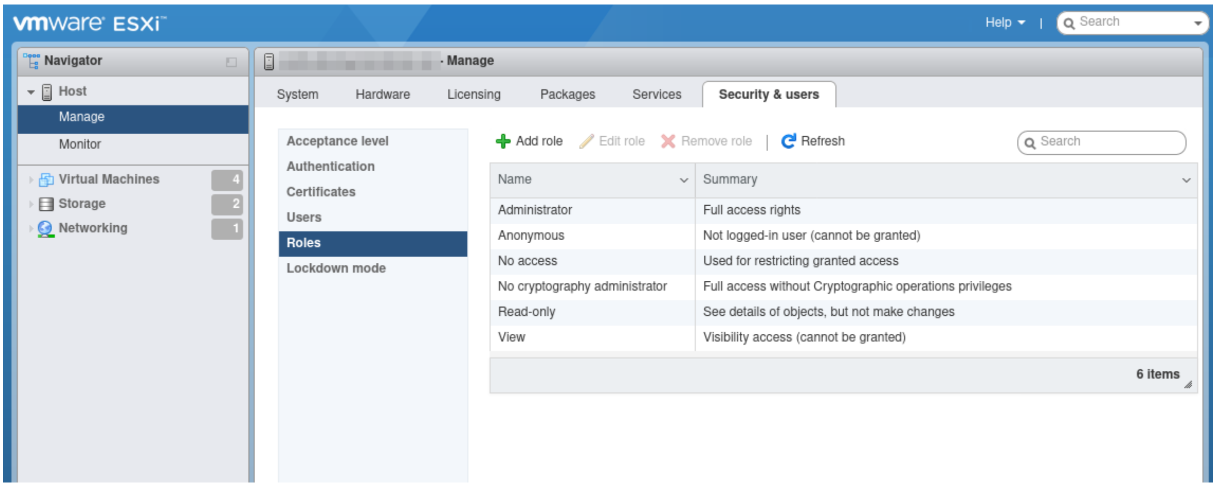
Note: If a vCenter Server Appliance (VCSA) is used to control ESXi hosts and users are created on the VCSA, they are only known on the VCSA and not on the ESXi hosts.

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. 6.25).

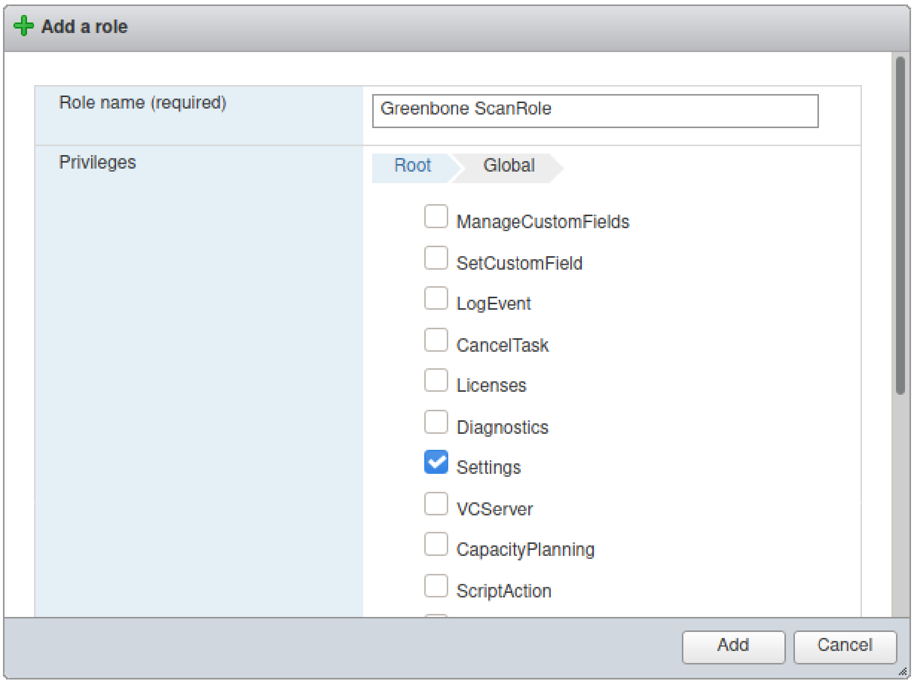


Name	Summary
Administrator	Full access rights
Anonymous	Not logged-in user (cannot be granted)
No access	Used for restricting granted access
No cryptography administrator	Full access without Cryptographic operations privileges
Read-only	See details of objects, but not make changes
View	Visibility access (cannot be granted)

6 items

Fig. 6.25: Displaying the roles

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. 6.26).
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 Greenbone Cloud Service.
12. Click *Assign role*.
13. Select the previously created role in the drop-down list (see Fig. 6.27).
14. Click *Assign role*.
15. Click *Close*.



Add a role

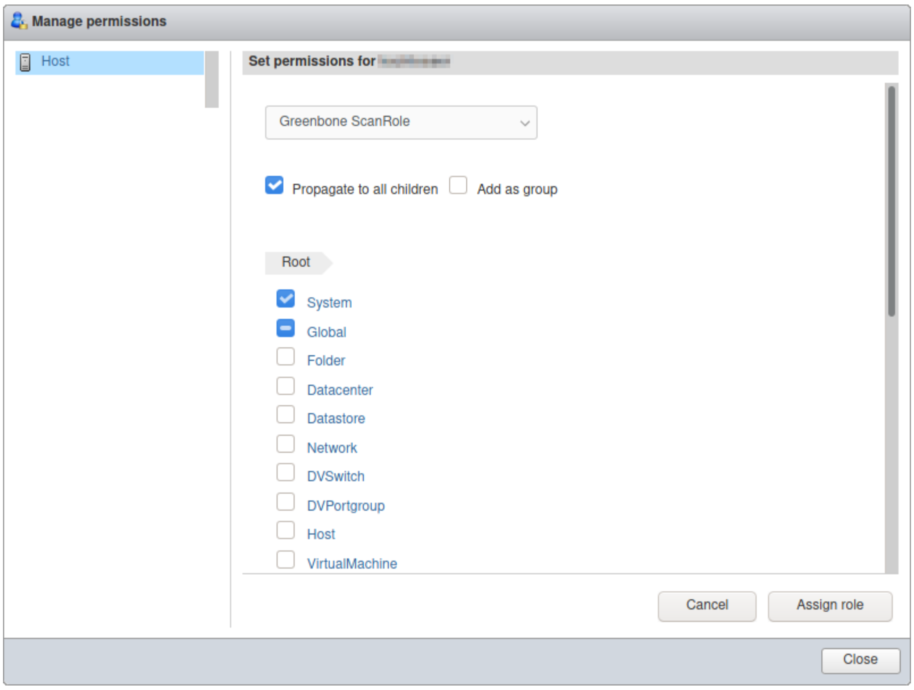
Role name (required): Greenbone ScanRole

Privileges

Root > Global

☐ ManageCustomFields
☐ SetCustomField
☐ LogEvent
☐ CancelTask
☐ Licenses
☐ Diagnostics
☑ Settings
☐ VCServer
☐ CapacityPlanning
☐ ScriptAction

Fig. 6.26: Creating a role



Manage permissions

Host

Set permissions for [redacted]

Greenbone ScanRole

☑ Propagate to all children ☐ Add as group

Root

☑ System
⊟ Global
☐ Folder
☐ Datacenter
☐ Datastore
☐ Network
☐ DVSwitch
☐ DVPortgroup
☐ Host
☐ VirtualMachine

Fig. 6.27: Assigning the role to the scan user

6.3.6 Requirements on Target Systems with Cisco OS

The Greenbone Cloud Service 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 Greenbone Cloud Service can use SSH.

The Greenbone Cloud Service currently only requires the command `show version` to retrieve the current version of the firmware of the device.

To set up a less privileged user which is only able to run this command, several approaches are possible. The following example uses the role based access control feature.

Tip: 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 gcs-view
(config-view)# secret 0 view-pw
(config-view)# commands exec include show version
(config-view)# exit
```

Now the user `gcs-user` with the password `gcs-pw` is created and linked to the view `gcs-view`:

```
(config)# username gcs-user view gcs-view password 0 gcs-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
```

The credentials of the user need to be entered on the platform. Select *Login Credentials* (category *Scan Configuration*) in the menu panel and create the appropriate user (see Chapter *6.3.2* (page 46)).

Link the credentials to the target to be used as SSH credentials.

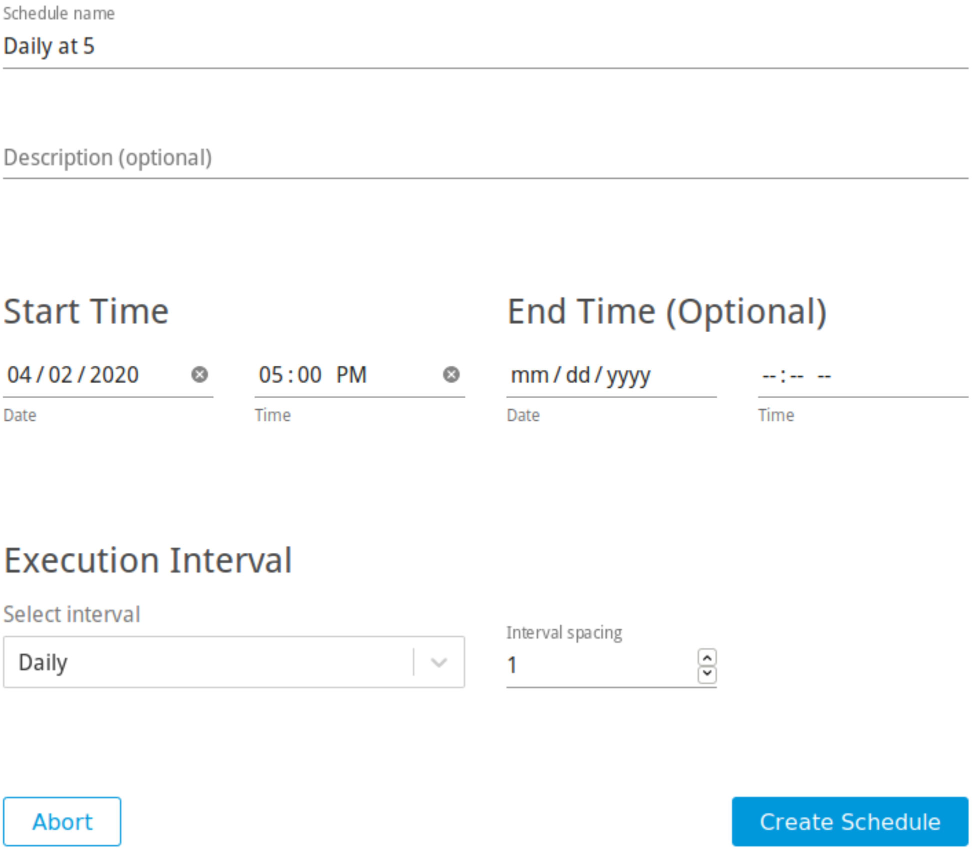
6.4 Performing a Scheduled Scan

For continuous vulnerability management, the manual execution of task is tedious. The Greenbone Cloud Service supports the scheduling of tasks for their automation and refer to schedules as automatic scans at a specific time. They can be run once or repeatedly.

6.4.1 Creating a Schedule

A new schedule can be created as follows:

1. Select *Schedules* (category *Scan Configuration*) in the menu panel.
2. Create a new schedule by clicking *+ Create New Schedule*.
3. Define the schedule (see Fig. 6.28).



Schedule name: Daily at 5

Description (optional):

Start Time — Date: 04 / 02 / 2020, Time: 05 : 00 PM

End Time (Optional) — Date: mm / dd / yyyy, Time: -- : -- --

Execution Interval — Select interval: Daily, Interval spacing: 1

Fig. 6.28: Creating a new schedule

4. Click *Create Schedule*.

   → The schedule is created and can be selected when creating a new task (see Chapter *6.2.4* (page 42)).

The following details of the schedule can be defined:

Schedule name
Definition of the name. The name can be chosen freely.

Description (optional)
An optional comment can contain additional information.

Start Time
Definition of the date and time for the first scan to start.

End Time (Optional)
Definition of the date and time for the first scan to end.

By setting no end time, the scan runs indefinitely until it is finished.

Execution Interval
Definition of the repetition rate of the task. It can be selected between *Daily*, *Weekly* and *Monthly*. Additionally, the space between intervals is set.

Example: a scheduled task with an interval of *Weekly* and an interval spacing of *2* runs every two weeks.

6.4.2 Managing Schedules

All existing schedules can be displayed by selecting *Schedules* (category *Scan Configuration*) in the menu panel.

For all schedules the following information is displayed:

Name
Name of the schedule.

Comment
Optional description of the schedule.

Start Time
Start time of the first run of the task.

End Time
Optional end time of the first run of the task.

Interval Type
Time period between two runs of the task.

Interval Spacing
Space between intervals.

For all schedules the following actions are available:

- ✎ Edit the schedule.
- 🗑 Delete the schedule. Only schedules which are currently not used can be deleted.

6.5 Managing Targets

All existing targets can be displayed by selecting *Targets* (category *Scan Configuration*) in the menu panel.

Internal Targets

For all internal targets the following information is displayed:

Name
Name of the target.

Port list
Port list used if the target is used for a scan (see Chapter *6.2.4* (page 42)).

IP Addresses
Number of scanned hosts.

For all targets the following actions are available:

- ⓘ Open an overlay with detailed information about the target.
- ✎ Edit the target.
- 🗑 Delete the target. Only targets which are currently not used can be deleted.

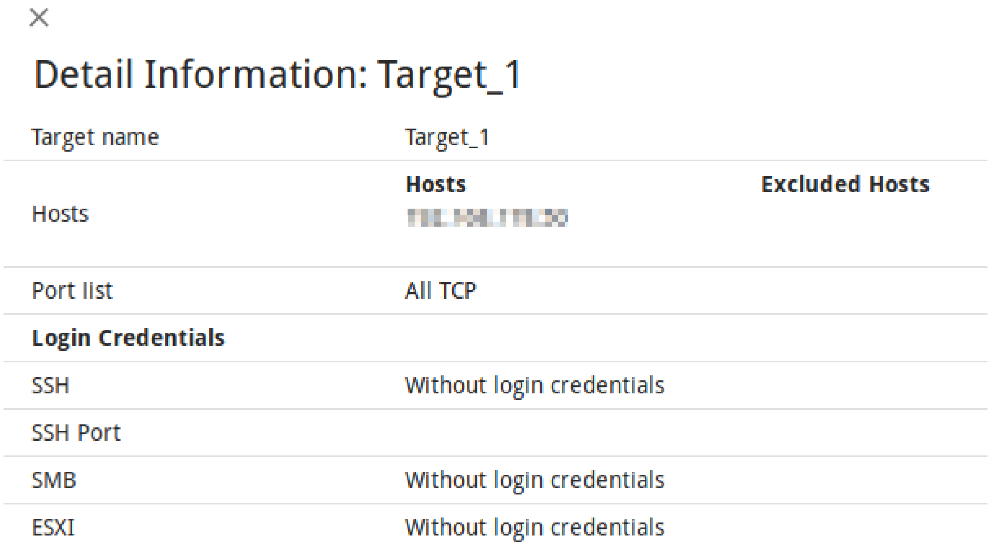
Clicking ⓘ opens an overlay (see Fig. 6.29) containing the following information:

Target name
Name of the target.

Hosts
Hosts that are scanned if the target is used for a scan (see Chapter *6.2.4* (page 42)).

Port list
Port list used if the target is used for a scan (see Chapter *6.2.4* (page 42)).

Login Credentials
Credentials configured for the target.



Detail Information: Target_1

Target name	Target_1	
Hosts	**Hosts** [redacted]	**Excluded Hosts**
Port list	All TCP	
Login Credentials		
SSH	Without login credentials	
SSH Port		
SMB	Without login credentials	
ESXI	Without login credentials	

Fig. 6.29: Overlay containing information about the target

External Targets

For all external targets the following information is displayed:

Name
Name of the target.

Port list
Port list used if the target is used for a scan (see Chapter *6.2.4* (page 42)).

Verified
Status of the validation of the configured hosts.

IP Addresses
Number of scanned hosts.

For all targets the following actions are available:

- ⓘ Open an overlay with detailed information about the target.
- ✎ Edit the target.
- 🗑 Delete the target. Only targets which are currently not used can be deleted.
- 📋 Show pending host validations.

Clicking ⓘ opens an overlay (see Fig. 6.29) containing the following information:

Target name
Name of the target.

Hosts
Hosts that are scanned if the target is used for a scan (see Chapter *6.2.4* (page 42)).

Port list
Port list used if the target is used for a scan (see Chapter *6.2.4* (page 42)).

Login Credentials
Credentials configured for the target.

6.6 Managing Gateways

6.6.1 Page *Gateways*

All existing gateways can be displayed by selecting *Gateways* (category *Scan Management*) in the menu panel.

For all gateways the following information is displayed:

Location
Textual description of the location of the gateway.

Status
Status of the connection with the scanner.

Description (optional)
Optional description of the gateway.

For all gateways the following actions are available:

- ✎ Edit the gateway.
- 🗑 Delete the gateway.

6.6.2 Gateway Administration Menu (CLI)

Note: The gateway can be imported to Microsoft Hyper-V or VMware ESXi.

Network settings of the gateway are managed using the gateway administration menu:

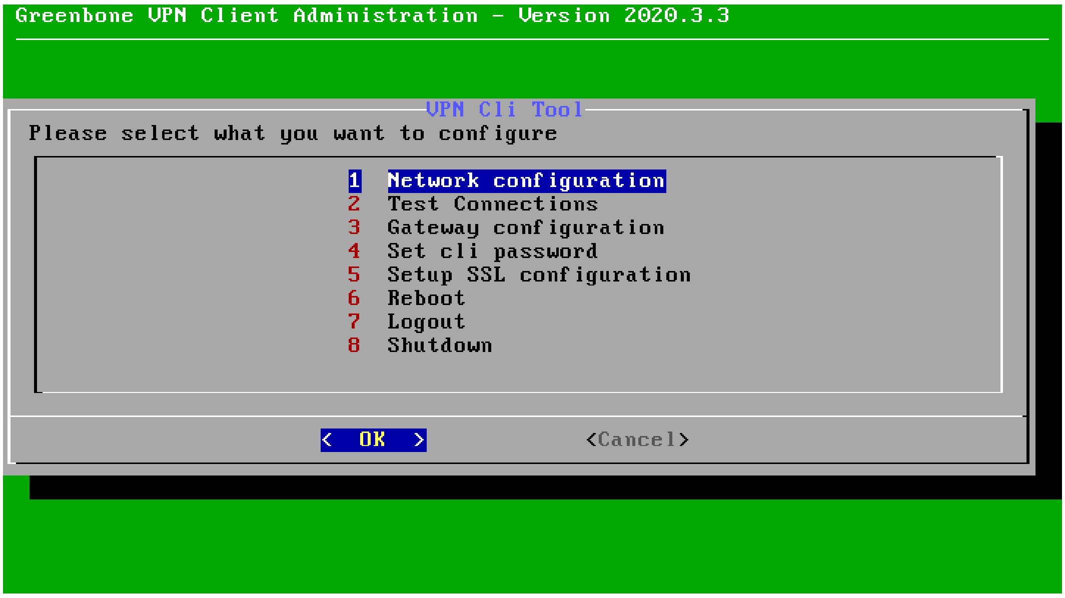
1. Start the gateway in the virtual environment.
2. After the boot process is completed, log in to the gateway administration menu. The default login information is:
   - Login name: `admin`
   - Password: `admin`

   → Actions for the gateway are displayed (see Fig. 6.30).

The following actions are available:

Network configuration
Set up the network of the gateway using DHCP or by entering IP address, netmask, DNS and gateway manually.

Test connections
Check whether all gateway connections work as intended.



```
Greenbone VPN Client Administration - Version 2020.3.3

                         VPN Cli Tool
 Please select what you want to configure

                    1  Network configuration
                    2  Test Connections
                    3  Gateway configuration
                    4  Set cli password
                    5  Setup SSL configuration
                    6  Reboot
                    7  Logout
                    8  Shutdown

                 <  OK  >            <Cancel>
```

Fig. 6.30: Managing a gateway

Gateway configuration
Set the password for the gateway web interface and register the gateway.

Set cli password
Set the password for the gateway administration menu (CLI)

Setup SSL configuration
Set up a new SSL certificate.

Reboot
Reboot the gateway.

Logout
Log out from the gateway administration menu.

Shutdown
Shut down the gateway.

6.6.3 Gateway Web Interface

1. Open the web browser and enter the following URL: `https://<ip>`. Replace `<ip>` with the IP address of the gateway.

   Tip: The IP address can be displayed in the gateway administration menu by selecting *Network configuration* and pressing `Enter` (see Chapter *6.6.2* (page 64)).

2. Log in using the user name `admin` and the password defined in the gateway administration menu (see Chapter *6.6.2* (page 64)).
3. Select *Overview* in the menu panel to display the status and the ports of the gateway.

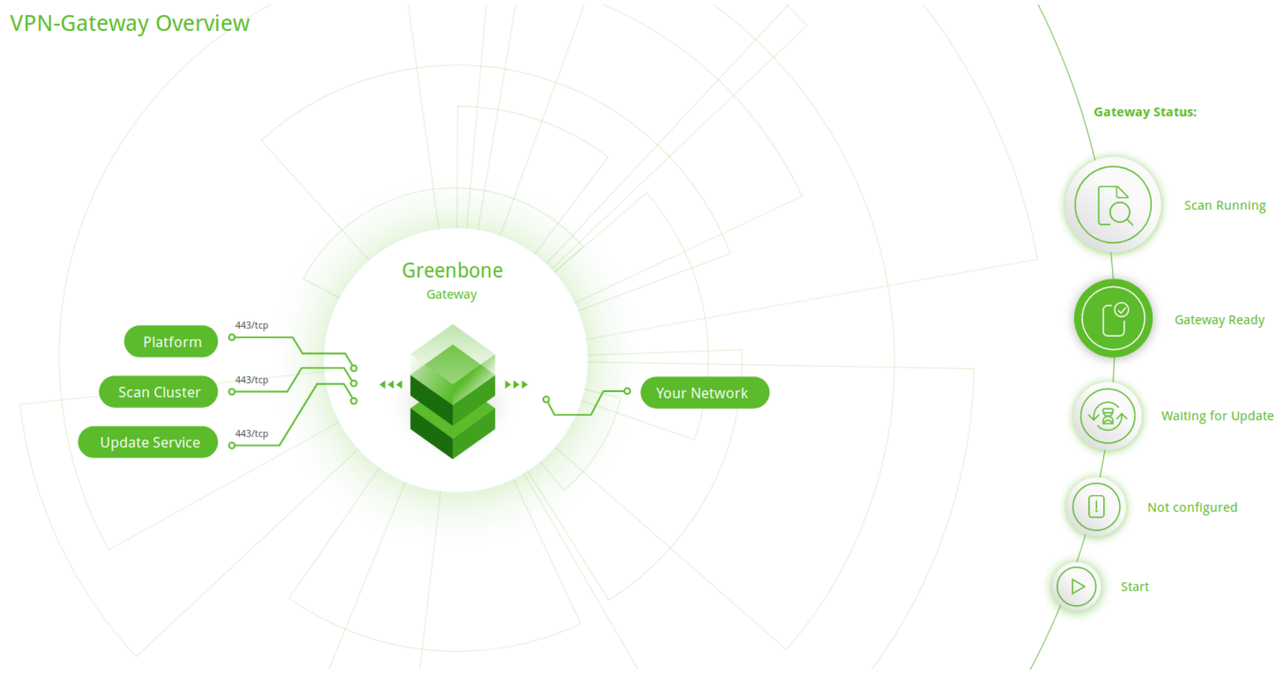


Fig. 6.31: Gateway overview

4. Select *Settings* in the menu panel.

   → The following actions are available:

   - Setting the API key of the gateway (see Chapter *6.2.3* (page 37)).
   - Setting the password for logging in to the gateway web interface.
   - Enabling/disabling error reporting.

6.7 Managing Tasks

All existing tasks can be displayed and managed on the pages *Scan Management* and *Scan Configuration*.

6.7.1 Page *Scan Management*

Select *Scan Management* in the menu panel.

For all tasks the following information is displayed:

📄

Open the latest report of the scan. For reading, managing and downloading reports see Chapter *7* (page 72).

Task

Name of the task.

By clicking on the name of a task, an overlay with details is opened.

Status

Current status of the task. The following status bars are possible:

Available The task has not been run since it was created.

Export requested The export of the task to the scan engine was requested.

Exported The task was successfully exported to the scan engine.

Export failed The export of the task to the scan engine failed.

Scan requested The task was just started. The Greenbone Cloud Service is preparing the scan.

Running The scan is currently running. The column *Progress* provides further details.

Delete requested The task was deleted. The actual deletion process can take some time as reports need to be deleted as well.

Stop requested The task was requested to stop recently. However, the scan engine has not yet reacted to this request yet.

Stopped The task was stopped. The latest report is possibly not yet complete. Other reasons for this status could be the reboot of the scan engine or a power outage. After restarting the scanner, the task will be resumed automatically.

Done The task has been completed successfully.

Internal error An error has occurred and the task was interrupted. The latest report is possibly not complete yet or is missing completely.

Progress

When the scan was started, further information about the scan status are displayed.

A percent value shows the completion of the scan based on the number of VTs executed on the selected hosts. For this reason, the value does not necessarily correlate with the time spent.

Reports

Number of reports for the task. By clicking on the number, an overview of all reports is opened.

Last Scan

Date and time of the last scan of the task.

Target

Scan target that is examined when the task is run.

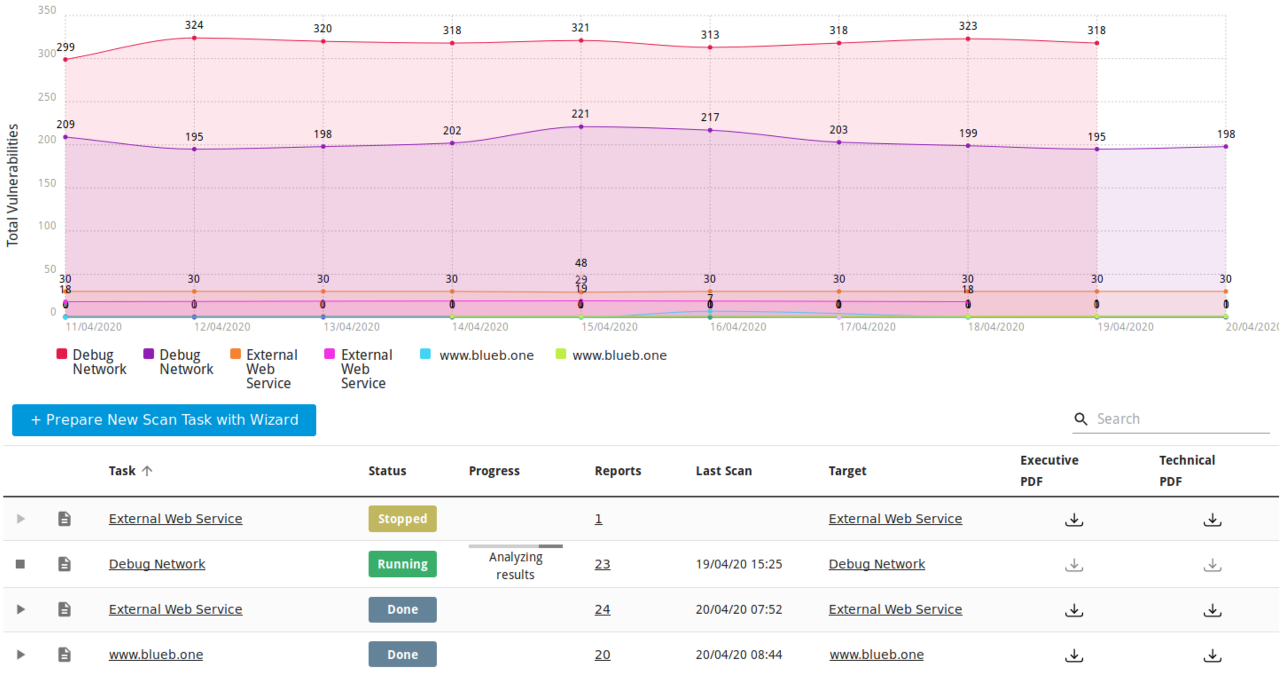
By clicking on the name of a target, an overlay with details is opened.

Executive PDF

By clicking ⤓ the “Executive Report” can be downloaded. It contains general information about the scan and lists of hosts sorted by severity.

Technical PDF

By clicking ⤓ the “Technical Report” can be downloaded. It contains general information about the scan as well as about the scanned hosts and details for each found vulnerability.



		Task ↑	Status	Progress	Reports	Last Scan	Target	Executive PDF	Technical PDF
▶	🗎	External Web Service	Stopped		1		External Web Service	⤓	⤓
■	🗎	Debug Network	Running	Analyzing results	23	19/04/20 15:25	Debug Network	⤓	⤓
▶	🗎	External Web Service	Done		24	20/04/20 07:52	External Web Service	⤓	⤓
▶	🗎	www.blueb.one	Done		20	20/04/20 08:44	www.blueb.one	⤓	⤓

Fig. 6.32: Page *Scan Management*

6.7.2 Page *Scan Configuration*

Select *Scan Configuration* in the menu panel.

For all tasks the following information is displayed:

Name
Name of the task.

Type
Type of the target: internal or external.

Scan Target
Scan target that is examined when the task is run.

By clicking on the name of a target, an overlay providing details is opened.

Scan Configuration
Scan configuration that is used for the task.

Schedule
Schedule for this task (see Chapter *6.4* (page 60)).

By clicking on the name of a schedule, an overlay providing details is opened.

For all targets the following actions are available:

- ✎ Edit the target.
- 🗑 Delete the target. Only targets which are currently not used can be deleted.

6.8 Scan Configurations

The scan configuration specifies which vulnerability tests are performed during a scan. The Greenbone Cloud Service comes with various predefined scan configurations.

The following configurations are available:

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 dynamic, i.e., new VTs of the chosen VT families are 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 scanners are *Ping Host* and *Nmap* which detect whether a host is alive.

The VT families are dynamic, i.e., new VTs of the chosen VT families are added and used automatically.

Analysis [standard]

For many environments this is one of the best options 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 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.

Analysis [aggressive]

This scan configuration expands the scan configuration *Analyze [Standard]* 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.

Analyse [standard] without Brute force attacks and Default Accounts

For many environments this is one of the best options 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 VT families are dynamic, i.e., new VTs of the chosen VT families are added and used automatically.

Exchange ZeroDay CVE-2021-26855

This scan configuration checks for CVE-2021-26855 which is related to Microsoft Exchange Server. CVE-2021-26855 is a server-side request forgery (SSRF) vulnerability in Exchange that allows an attacker to send HTTP requests and authenticate to the Exchange server.

Log4j Zero Day CVE-2021-44228
This scan configuration checks for CVE-2021-44228 in the logging library Log4j. The vulnerability listed in CVE-2021-44228 could allow a remote code execution.

6.9 Port Lists

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.

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[6].

The Internet Assigned Numbers Authority (IANA)[4] 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[5], 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 Greenbone Cloud Service:

- All IANA assigned TCP 2012-02-10: all TCP ports assigned by IANA on 10th of February 2012
- All privileged TCP
- All privileged TCP and UDP
- All TCP
- OpenVAS Default: the TCP ports which are scanned by the OpenVAS scanner when passing the default port range preference
- All IANA assigned TCP and UDP 2012-02-10: all TCP and UDP ports assigned by IANA on 10th of February 2012
- All TCP and Nmap 5.51 top 100 UDP: all TCP ports and the top 100 UDP ports according to Nmap 5.51

[6] 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.

[4] https://www.iana.org/

[5] https://nmap.org/

- All TCP and Nmap 5.51 top 1000 UDP: all TCP ports and the top 1000 UDP ports according to Nmap 5.51
- Nmap 5.51 top 2000 TCP and top 100 UDP: the top 2000 TCP ports and the top 100 UDP ports according to Nmap 5.51
- Web services

6.10 Using Notifications

The user can receive summaries about the configured scans and alerts for completed scans (see Chapter *5.2* (page 16)).

6.11 Obstacles While Scanning

There are several typical problems which might occur during a scan using the default values of the Greenbone Cloud Service. While the default values are valid for most environments and customers, depending on the actual environment and the configuration of the scanned hosts they might require some tweaking.

6.11.1 Hosts not Found

During a typical scan (either *Discovery* or *Analysis [Standard]*) the scanner will first use the ping command to check the availability of the configured targets by default. 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 Chapter *6.2.1* (page 30)).

If the target does not respond to a ping request, a TCP ping may be tested.

6.11.2 Long Scan Periods

Once the target is discovered to be alive using the ping command, the scanner 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.

CHAPTER 7

Reports and Vulnerability Management

The results of a scan are summarized in a report. Reports can be displayed and downloaded in different formats.

The Greenbone Cloud Service saves not only the latest report of a scan 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.

7.1 Reading a Report

An overview of all existing reports of a task can be displayed by selecting *Scan Management* in the menu panel and clicking on the number of reports in the column *Reports* (see Fig. 7.1).

The following information is displayed:

Date
Date and time of report creation.

Unfinished scans are marked with ⚠.

Severity
Highest severity found on the target.

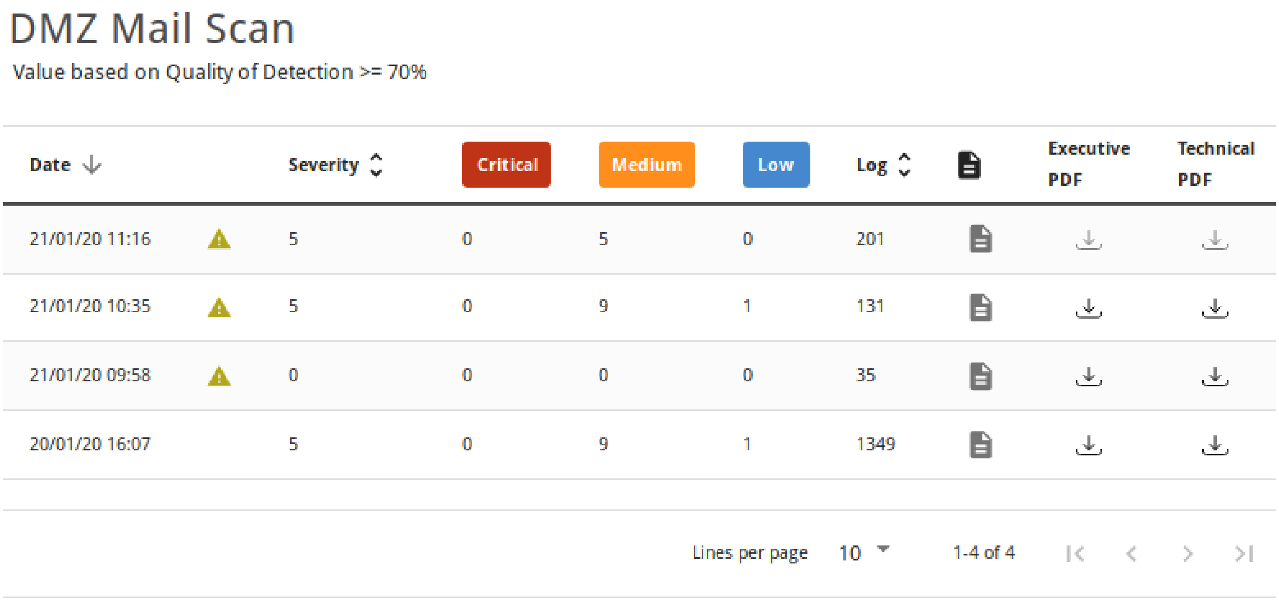
Critical/Medium/Low/Log
Number of found vulnerabilities for each severity class.

🗎
Show all results for the respective report.

Executive PDF
By clicking ⤓ the “Executive Report” can be downloaded. It contains general information about the scan and lists of hosts sorted by severity.

Technical PDF

By clicking ⤓ the “Technical Report” can be downloaded. It contains general information about the scan as well as about the scanned hosts and details for each found vulnerability.



DMZ Mail Scan

Value based on Quality of Detection >= 70%

Date ↓		Severity ⇕	Critical	Medium	Low	Log ⇕	🗎	Executive PDF	Technical PDF
21/01/20 11:16	⚠	5	0	5	0	201	🗎	⤓	⤓
21/01/20 10:35	⚠	5	0	9	1	131	🗎	⤓	⤓
21/01/20 09:58	⚠	0	0	0	0	35	🗎	⤓	⤓
20/01/20 16:07		5	0	9	1	1349	🗎	⤓	⤓

Fig. 7.1: Summary of all reports of a scan

7.1.1 Interpreting a Report

To interpret the results, note the following information:

- **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.

- **Critical** Critical **and Medium** Medium

  Findings of the severity levels *Critical* and *Medium* are most important and should be addressed with priority. Before addressing medium level findings, critical 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.

  Note: VTs that are terminated by timeout before a result is received are reported with the severity *Low* and a Quality of Detection (QoD) of 0 (see Chapter *7.1.2* (page 74)). More information about this error can be found in the details of such results.

7.1.2 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 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, 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.
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.

QoD	QoD Type	Description
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.
1 %	general_note	General note on potential vulnerability without finding any present application.
0 %	timeout	The test was unable to determine a result before it was ended by timeout.

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 *7.3* (page 80)).

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.

7.2 Results of a Report

A report can be opened by clicking 📄 for the desired report in the report overview (see Fig. 7.1).

Tip: The latest report of a scan can be displayed by selecting *Scan Management* in the menu panel and clicking 📄 in the row of the scan.

The name, date and time of the scan as well as the highest found severity are displayed at the top.

The following registers are available:

- Dashboard
- Grid Overview
- Table Overview

7.2.1 Dashboard

The dashboard provides a summarizing overview of the found vulnerabilities, their severities and their possible solutions.

The following information is displayed:

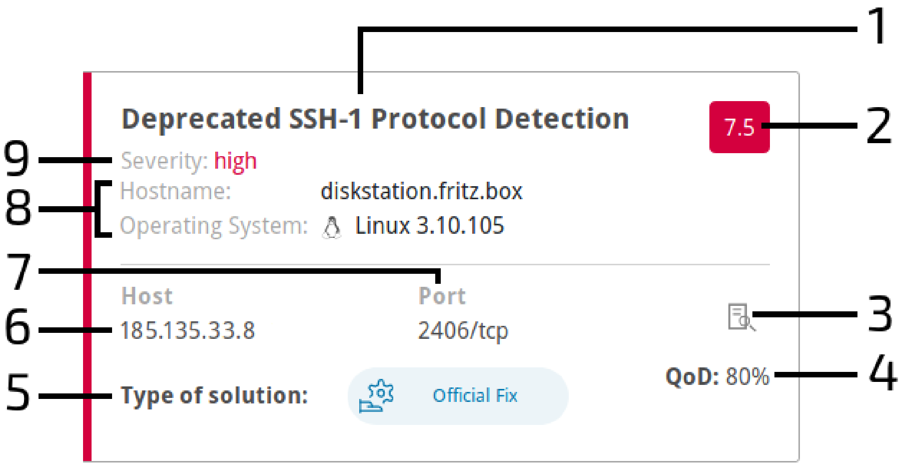
- Total number of detected vulnerabilities
- Number of detected vulnerabilities for each solution type
- Number of detected vulnerabilities for each severity level
- The two solutions with the highest fix percentage
- Risk level (highest found severity)

- Top 10 hosts with number of found vulnerabilities and distribution of severities (sorted by number of vulnerabilities or by severity)

7.2.2 Grid Overview

The grid overview shows all found vulnerabilities sorted from highest to lowest severity.

By clicking *Filter +* the results can be filtered (see Chapter *7.3* (page 80)).



Deprecated SSH-1 Protocol Detection

Severity: high

Hostname: diskstation.fritz.box

Operating System: Linux 3.10.105

Host 185.135.33.8

Port 2406/tcp

Type of solution: Official Fix

QoD: 80%

Fig. 7.2: Result of a scan

For every result the following information is displayed:

1 – Name of the found vulnerability.

2 – Severity of the vulnerability.

3 – Open an overlay showing details of the vulnerability.

4 – QoD is short for “Quality of Detection” and shows the reliability of the detection of a vulnerability (see Chapter *7.1.2* (page 74)).

5 – Solution type for the found vulnerability. The following the solutions are possible:

- Official Fix: an official vendor patch is available. Unless otherwise noted, it is assumed that this fix fully resolves the vulnerability.
- Temporary Fix: a workaround (information about a configuration or a specific deployment scenario that can be used to avoid exposure to the vulnerability) is available to temporarily eliminate the vulnerability.

  There can be none, one or more workaround(s) available.

  This is usually the “first line of defense” against a new vulnerability before a risk reduction or official fix has been issued or even discovered.
- Risk Reduction: 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.
- No Fix Available: 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.
- Searching for Fix: there is currently no solution available to remediate the vulnerability but there may be a solution in the future.

6 – Host for which the result was found.

7 – Port number and protocol type used to find the vulnerability on the host.

8 – Host name and operating system of the host for which the result was found.

9 – Severity level of the vulnerability.

7.2.3 Table Overview

The table overview shows the results of the scan in the form of different tables.

There are three different tables that can be selected (see Fig. 7.3):

- Overview: all detected results
- Host: results grouped by host
- Vulnerability: results grouped by vulnerability

By clicking *Filter +* the results can be filtered (see Chapter *7.3* (page 80)).

Fig. 7.3: Different tables in the table overview

7.2.3.1 “Overview” Table

For every result the following information is displayed:

Name
Name of the corresponding vulnerability.

Severity
Severity of the corresponding vulnerability. It is displayed with the color according to the severity level to support the analysis of the results.

Host
Host for which the result was found.

Port
Port number and protocol type used to find the result on the host.

Solution
Solution for the corresponding vulnerability. The following the solutions are possible:

- Official Fix: an official vendor patch is available. Unless otherwise noted, it is assumed that this fix fully resolves the vulnerability.
- Temporary Fix: a workaround (information about a configuration or a specific deployment scenario that can be used to avoid exposure to the vulnerability) is available to temporarily eliminate the vulnerability.

  There can be none, one or more workaround(s) available.

  This is usually the “first line of defense” against a new vulnerability before a risk reduction or official fix has been issued or even discovered.
- Risk Reduction: 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.

- No Fix Available: 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.

- Searching for Fix: there is currently no solution available to remediate the vulnerability but there may be a solution in the future.

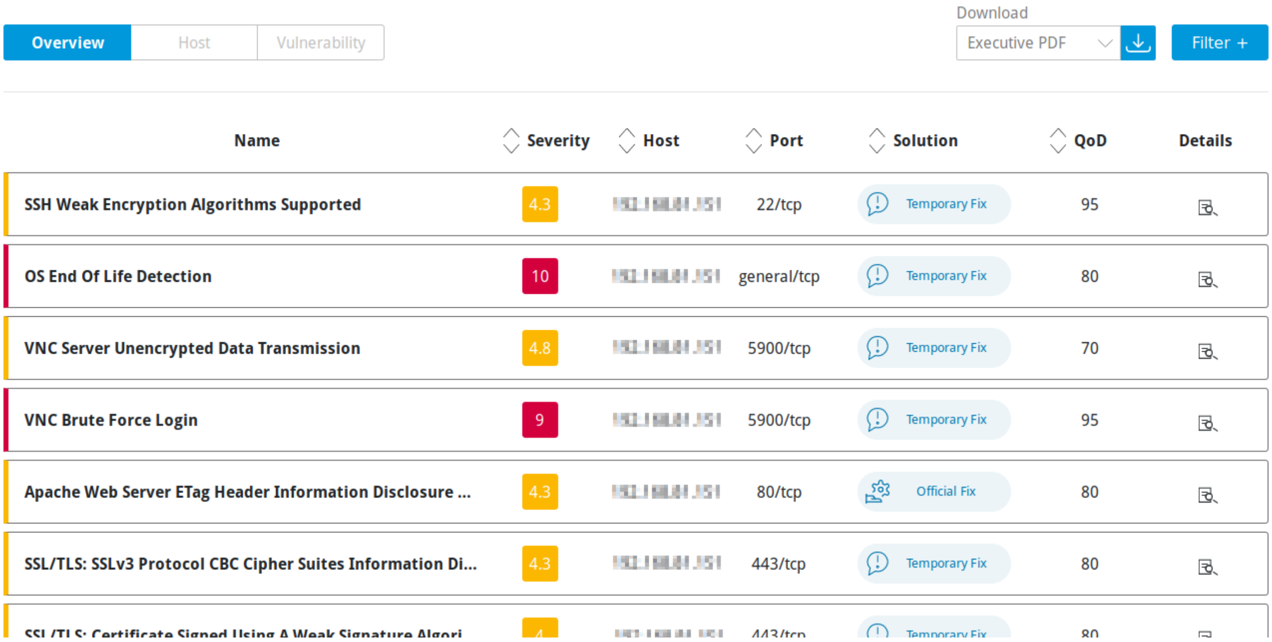
QoD

QoD is short for “Quality of Detection” and shows the reliability of the detection of a vulnerability (see Chapter *7.1.2* (page 74)).

By default, only results that were detected by a VT with a QoD of 70 % or higher are displayed. The possibility of false positives is thereby lower. The filter can be adjusted to show results with a lower QoD (see Chapter *7.3* (page 80)).

Details

By clicking 🔍 an overlay is opened showing details of the vulnerability.



Name	Severity	Host	Port	Solution	QoD	Details
SSH Weak Encryption Algorithms Supported	4.3	[redacted]	22/tcp	Temporary Fix	95	🔍
OS End Of Life Detection	10	[redacted]	general/tcp	Temporary Fix	80	🔍
VNC Server Unencrypted Data Transmission	4.8	[redacted]	5900/tcp	Temporary Fix	70	🔍
VNC Brute Force Login	9	[redacted]	5900/tcp	Temporary Fix	95	🔍
Apache Web Server ETag Header Information Disclosure ...	4.3	[redacted]	80/tcp	Official Fix	80	🔍
SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Di...	4.3	[redacted]	443/tcp	Temporary Fix	80	🔍
SSL/TLS: Certificate Signed Using A Weak Signature Algori	4	[redacted]	443/tcp	Temporary Fix	80	🔍

Fig. 7.4: Overview table

7.2.3.2 “Host” Table

For every host the following information is displayed:

Name

IP address of the host.

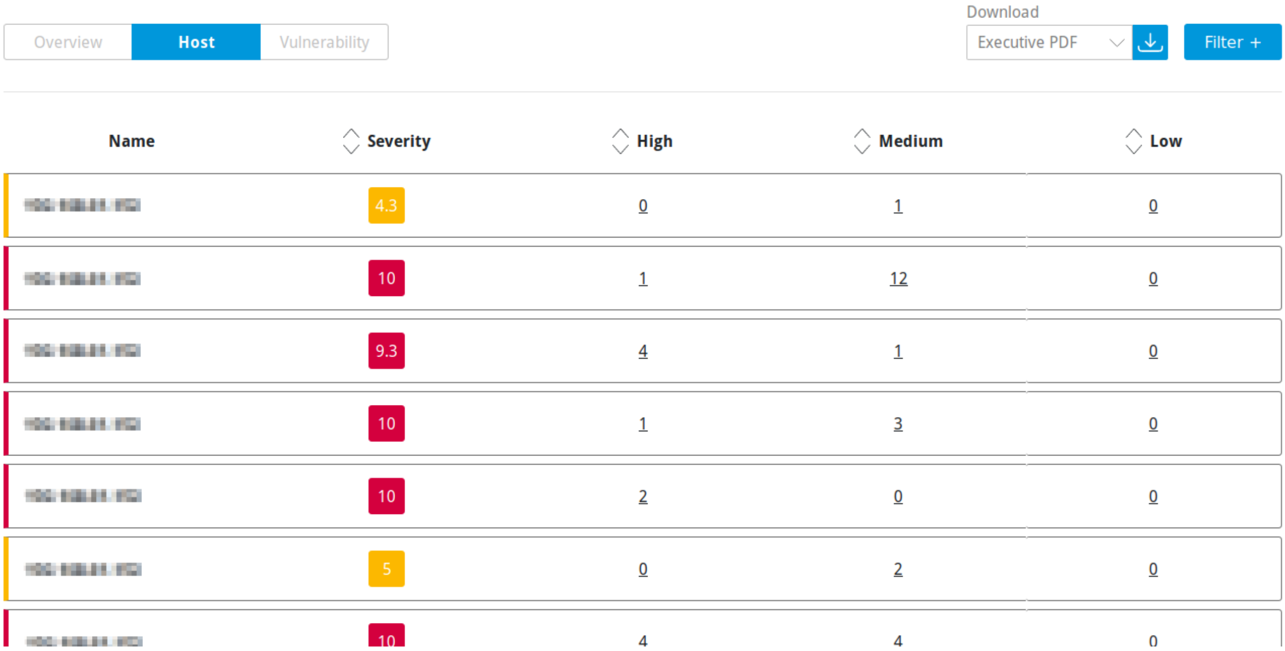
Severity

Highest severity found on the host.

High/Medium/Low

Number of found vulnerabilities for each severity.

By clicking on a number, the top 20 vulnerabilities for the selected severity found on the respective host are displayed.



Name	Severity	High	Medium	Low
[redacted]	4.3	0	1	0
[redacted]	10	1	12	0
[redacted]	9.3	4	1	0
[redacted]	10	1	3	0
[redacted]	10	2	0	0
[redacted]	5	0	2	0
[redacted]	10	4	4	0

Fig. 7.5: Host table

7.2.3.3 “Vulnerability” Table

For every vulnerability the following information is displayed:

Name
Name of the vulnerability.

Severity
Severity of the vulnerability. It is displayed with the color according to the severity level to support the analysis of the results.

Host
Number of hosts on which the vulnerability was found.

By clicking on the number, the top 20 hosts on which the vulnerability was found as well as additional details are displayed.

Port
Number of ports by which the vulnerability was found.

By clicking on the number of ports, the top 20 ports by which the vulnerability was found as well as additional details are displayed.

Solution
Solution for the corresponding vulnerability. The following the solutions are possible:

- Official Fix: an official vendor patch is available. Unless otherwise noted, it is assumed that this fix fully resolves the vulnerability.
- Temporary Fix: a workaround (information about a configuration or a specific deployment scenario that can be used to avoid exposure to the vulnerability) is available to temporarily eliminate the vulnerability.

  There can be none, one or more workaround(s) available.

  This is usually the “first line of defense” against a new vulnerability before a risk reduction or official fix has been issued or even discovered.

- Risk Reduction: 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.
- No Fix Available: 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.
- Searching for Fix: there is currently no solution available to remediate the vulnerability but there may be a solution in the future.

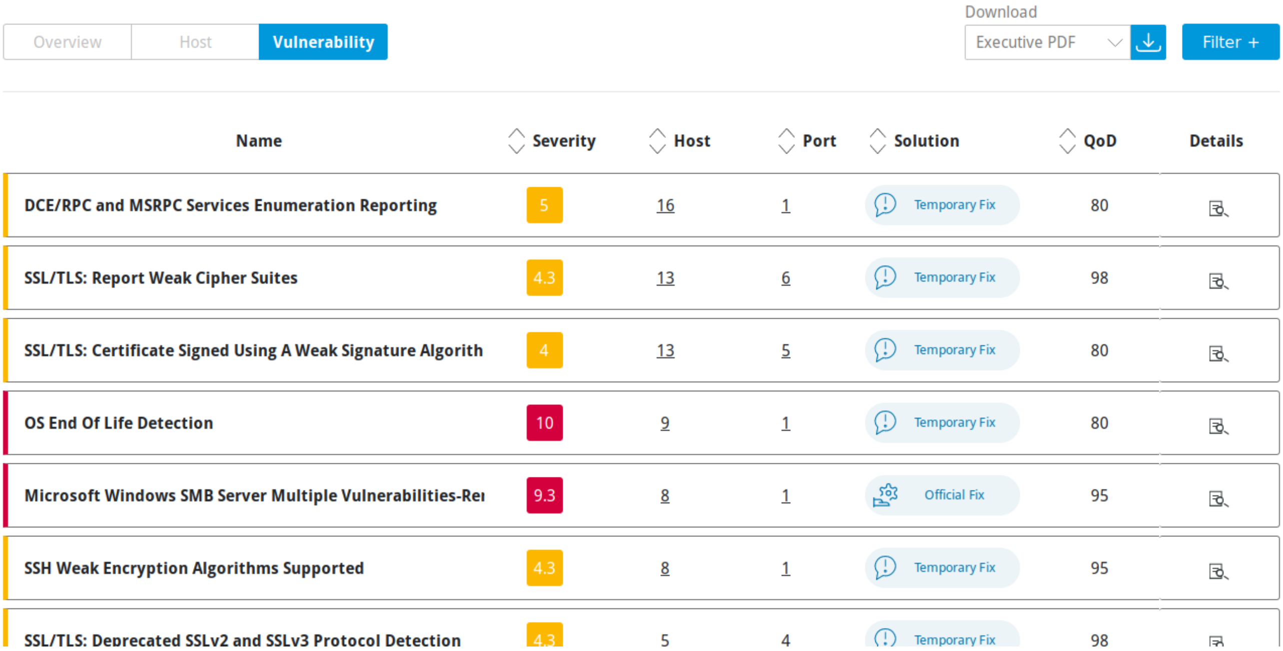
QoD

QoD is short for "Quality of Detection" and shows the reliability of the detection of a vulnerability (see Chapter *7.1.2* (page 74)).

By default, only results that were detected by a VT with a QoD of 70 % or higher are displayed. The possibility of false positives is thereby lower. The filter can be adjusted to show results with a lower QoD (see Chapter *7.3* (page 80)).

Details

By clicking 🔍 an overlay is opened showing details of the vulnerability.



Name	Severity	Host	Port	Solution	QoD	Details
DCE/RPC and MSRPC Services Enumeration Reporting	5	16	1	Temporary Fix	80	🔍
SSL/TLS: Report Weak Cipher Suites	4.3	13	6	Temporary Fix	98	🔍
SSL/TLS: Certificate Signed Using A Weak Signature Algorith	4	13	5	Temporary Fix	80	🔍
OS End Of Life Detection	10	9	1	Temporary Fix	80	🔍
Microsoft Windows SMB Server Multiple Vulnerabilities-Rei	9.3	8	1	Official Fix	95	🔍
SSH Weak Encryption Algorithms Supported	4.3	8	1	Temporary Fix	95	🔍
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	4.3	5	4	Temporary Fix	98	🔍

Fig. 7.6: Vulnerability table

7.3 Filtering a Report

Since a report often contains a lot of findings, the complete report as well as only filtered results can be displayed.

The grid overview or table overview of a report (see Chapter *7.2* (page 75)) can be filtered as follows:

1. Select *Scan Management* in the menu panel.
2. Click on the total number of reports in the column *Reports*.

   → The overview of all reports of a task is opened.
3. In the row of the desired report click 📄.

4. Select the register *Grid Overview* or *Table Overview*.
5. Click *Filter +*.
6. For *Quality Of Detection Range (QoD)* and *Severity* set the minimal and maximal values using the sliders (see Fig. 7.7).
7. For *Solution* select the buttons of the desired solution types.

   Tip: The selected solution types are highlighted by a border.

8. For *Port*, *Host*, *Hostname* and *Operating System* select the ports, hosts, host names and operating systems in the drop-down lists for which the found results should be displayed.
9. Click *Apply*.

7.4 Exporting a Report

A report can be exported in various formats:

Executive Report (PDF or JSON)
This report contains general information about the scan and lists of hosts sorted by severity.

Technical Report (PDF or JSON)
This report contains general information about the scan as well as about the scanned hosts and details for each found vulnerability.

XML

A report can be exported as follows:

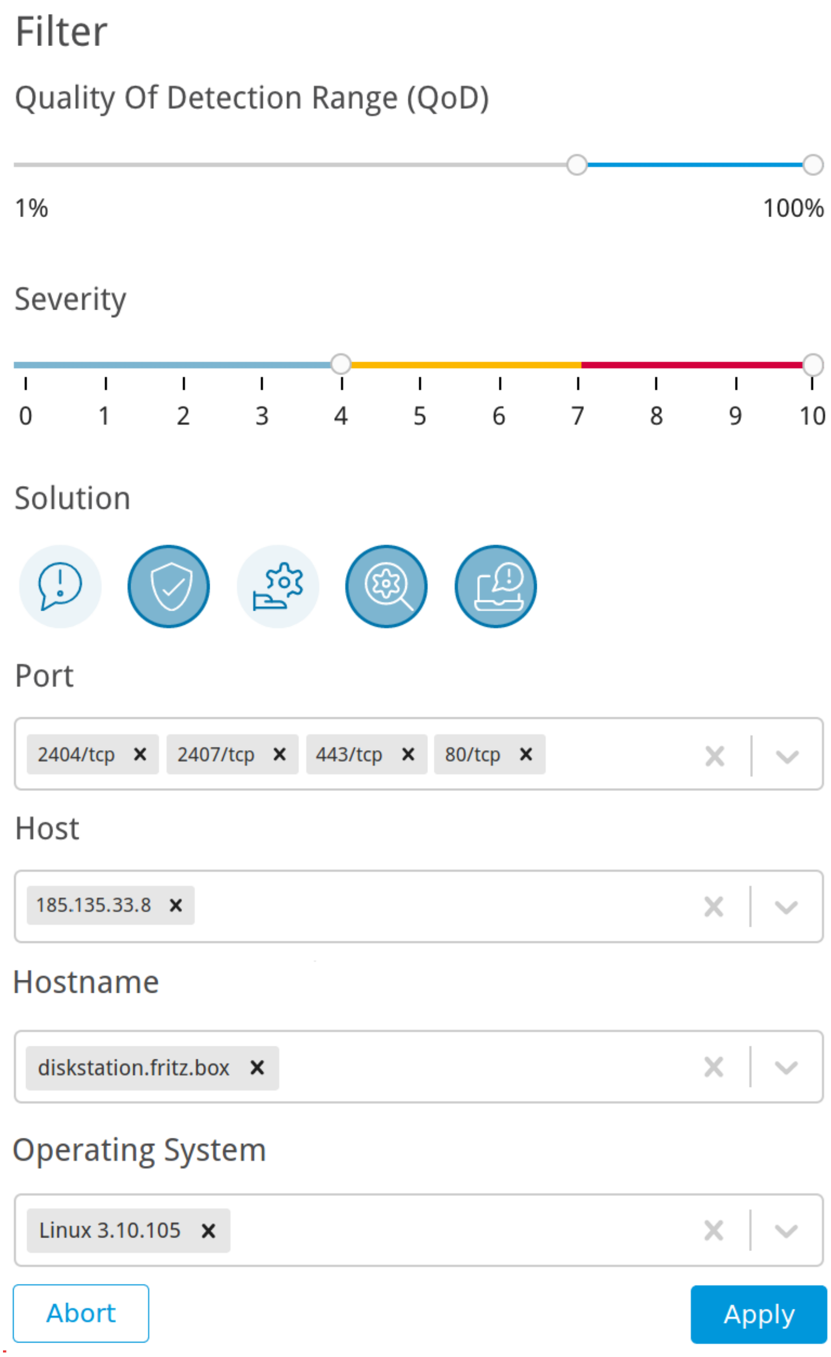
1. Select *Scan Management* in the menu panel.
2. Click on the total number of reports in the column *Reports*.

   → The overview of all reports of a scan is opened.
3. In the row of the desired report click ⤓ for *Executive PDF* or *Technical PDF*.
4. Save the report by clicking *OK*.

   or

1. Select *Scan Management* in the menu panel.
2. Click on the total number of reports in the column *Reports*.

   → The overview of all reports of a scan is opened.
3. In the row of the desired report click 🗎.
4. Select the register *Grid Overview* or *Table Overview*.
5. Select the desired report format in the drop-down list *Download* (see Fig. 7.8).
6. Click the slider *Anonymized* if IP addresses should be anonymized in the downloaded report.
7. Click ⤓.
8. Save the report by clicking *OK*.



Filter

Quality Of Detection Range (QoD)

Severity

Solution

Port: 2404/tcp ✕ 2407/tcp ✕ 443/tcp ✕ 80/tcp ✕

Host: 185.135.33.8 ✕

Hostname: diskstation.fritz.box ✕

Operating System: Linux 3.10.105 ✕

Fig. 7.7: Adjusting the filter for the report

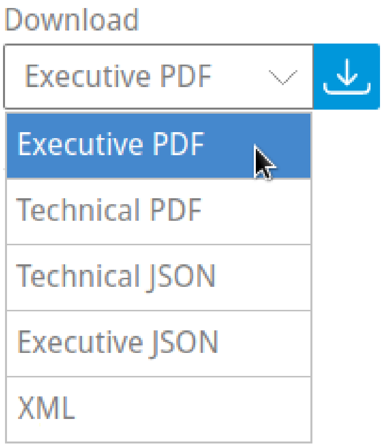


Fig. 7.8: Exporting a report

7.5 Notifications for Reports

Notifications can be sent regularly as a summary of scans or when a report is complete (see Chapter *5.2* (page 16)).

CHAPTER 8

Frequently Asked Questions

8.1 Which Firewall Access Rules Are Necessary for the Communication Between the Greenbone Scan Cluster (GSC) and the VPN Gateway?

The gateway uses the following outgoing connections:

- 443/tcp outgoing to GSC (45.135.106.140)
- 443/tcp outgoing to Greenbone Cloud Service (195.252.156.97)
- 443/tcp outgoing to update service (gpublic.azurecr.io)

8.2 Which Firewall Access Rules Are Necessary for the Communication Between the Greenbone Scan Cluster (GSC) and External Targets?

The Greenbone Scan Cluster (GSC) uses the IP address range 45.135.106.0/25 for scan traffic to external targets. The ports used are selected according to the port list configured when creating the target (see Chapters *6.2.1* (page 30) and *6.9* (page 70)).

8.3 Which Technology Is Used for the VPN Connection?

An SSH Layer 2 based VPN is used for the VPN connection.

8.4 What Has to Be Done if MAC-NAT Does Not Work?

With gateway version 1.5 or higher there are usually no problems.

If MAC-NAT does not work, the checkbox *Use MAC-NAT* has to be deselected when creating a gateway and the following settings have to be configured in VMware ESXi or Oracle VirtualBox:

In VMware ESXi:

- Create a separate *Port Group* for the gateway and connect the gateway to it.
- Change the settings *Promiscuous mode* and *Forged transmits* for the port group to *Accept*.

In Oracle VirtualBox:

- In the network settings, open *Advanced* and change the setting *Promiscuous Mode* to *Allow All*.

8.5 What Happens to the User Account When the Subscription Ends?

When the subscription ends, the user can still log in and see all completed reports. The starting of new scans is no longer possible.

If the account is not used anymore, it is deleted after a certain time. The user will receive a notification beforehand.

8.6 Why is the Scanning Process so Slow?

The performance of a scan depends on various aspects. One possible reason is the time-consuming scanning of unused IP addresses.

To avoid this, a “Discovery” scan should be performed before the actual scan. This scan detects for each IP address whether it is active or not. Inactive IP addresses will not be scanned during the actual scan. Firewalls and other systems can prevent a successful detection.

Additionally, the duration of a scan is mostly determined by the network configuration and the amount of ports to be tested. For each port that is queried, the service behind it reacts at least with one log entry. 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. 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 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.

8.7 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.

8.8 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).

8.9 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 VTs that may cause damage to the host system are enabled by the scan configuration. Otherwise the target system can be affected.

CHAPTER 9

Glossary

This section defines relevant terminology which is consistently used across the entire system.

9.1 CERT-Bund Advisory

The CERT-Bund[7], 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

Additionally, CERT-Bund operates the German IT Situation Centre[8].

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

[7] https://www.cert-bund.de/

[8] https://www.bsi.bund.de/EN/Topics/IT-Crisis-Management/IT-Situation-Centre/itsituationcentre_node.html

CERT-Bund offers a warning and information service (German: Warn- und Informationsdienst, abbreviated as "WID"). Currently this service offers the CERT-Bund 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.

9.2 CPE

The Common Platform Enumeration (CPE)[9] is modelled after CVE. It is a structured naming scheme for applications, operating systems and hardware devices.

CPE was initiated by MITRE[10] and is maintained by NIST as a part of the National Vulnerability Database (NVD)[11]. NIST has already maintained the official CPE dictionary and the CPE specifications for many years. CPE is based on the generic syntax of the Uniform Resource Identifier (URI) and 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 (see Fig. 9.1):

- 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

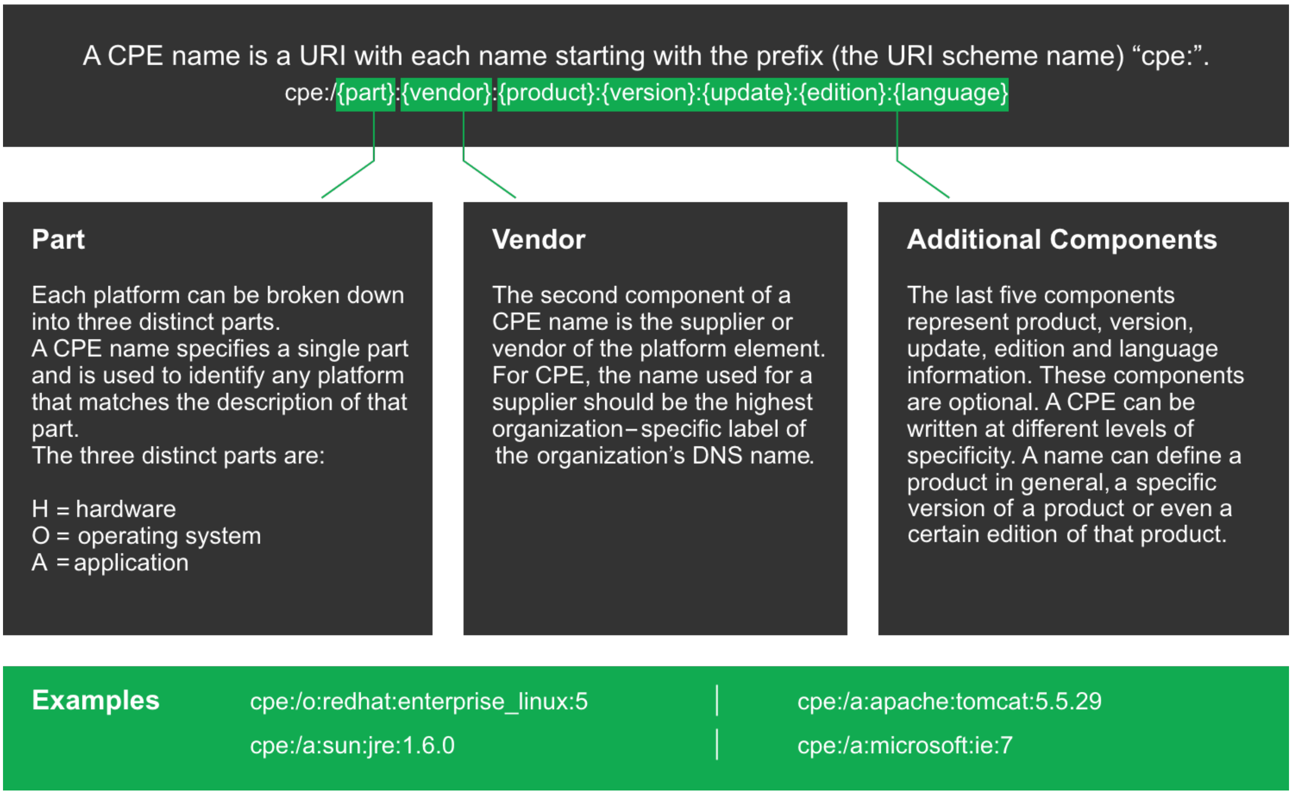
CPE is composed of the following components:

- **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.

[9] https://csrc.nist.gov/projects/security-content-automation-protocol/specifications/cpe

[10] https://www.mitre.org/

[11] https://nvd.nist.gov/



A CPE name is a URI with each name starting with the prefix (the URI scheme name) “cpe:”.

cpe:/{part}:{vendor}:{product}:{version}:{update}:{edition}:{language}

Part

Each platform can be broken down into three distinct parts.
A CPE name specifies a single part and is used to identify any platform that matches the description of that part.
The three distinct parts are:

H = hardware
O = operating system
A = application

Vendor

The second component of a CPE name is the supplier or vendor of the platform element. For CPE, the name used for a supplier should be the highest organization–specific label of the organization’s DNS name.

Additional Components

The last five components represent product, version, update, edition and language information. These components are optional. A CPE can be written at different levels of specificity. A name can define a product in general, a specific version of a product or even a certain edition of that product.

Examples

cpe:/o:redhat:enterprise_linux:5 | cpe:/a:apache:tomcat:5.5.29
cpe:/a:sun:jre:1.6.0 | cpe:/a:microsoft:ie:7

Fig. 9.1: Name structure of a CPE name

9.3 CVE

In the past, various organizations discovered and reported vulnerabilities at the same time and assigned them different names. This led to different scanners reporting the same vulnerability under different names making communication and comparison of the results complicated.

To address this, MITRE[12] founded the Common Vulnerabilities and Exposure (CVE) project[13]. Every vulnerability is assigned a unique identifier consisting of the release year and a simple number. This identifier serves as a central reference.

The CVE database of MITRE is not a vulnerability database. CVE was developed in order to connect the vulnerability database and other systems with each other enabling the comparison of security tools and services.

The CVE database does not contain detailed technical information or any information regarding risk, impact or elimination of the vulnerability. A CVE only contains the identification number with the status, a short description and references to reports and advisories.

The National Vulnerability Database (NVD)[14] refers to the CVE database and complements the content with information regarding the elimination, severity, possible impact and affected products of the vulnerability. Greenbone refers to the CVE database of the NVD.

[12] https://www.mitre.org/
[13] https://cve.mitre.org/
[14] https://nvd.nist.gov/

9.4 CVSS

To support the interpretation of a vulnerability, the Common Vulnerability Scoring System (CVSS) was invented. 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 counter measures.

CVSS is developed by the CVSS Special Interest Group (CVSS-SIG)[15] of the Forum of Incident Response and Security Teams (FIRST)[16]. The current CVSS score version is 3.1.

The CVSS score in version 2 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.

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.

9.5 DFN-CERT Advisory

While the individual VTs, CVEs, CPEs and OVAL definitions are created primarily to be processed by computer systems, DFN-CERT[17] publishes new advisories regularly.

DFN-CERT is responsible for hundreds of universities and research institutions that are associated with the German Research and Education Network[18] (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.

9.6 Greenbone Enterprise Feed

The content of the Greenbone Enterprise Feed, which provides the vulnerability tests (VTs) for scanning, can be viewed in Greenbone's SecInfo Portal[19].

[15] https://www.first.org/cvss/

[16] https://www.first.org/

[17] https://www.dfn-cert.de/

[18] https://www.dfn.de/en/

[19] https://www.greenbone.net/en/secinfo-portal/

9.7 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.

Hosts in scan targets and in scan reports are identified by their network address, either an IP address or a host name.

9.8 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 include information about development date, affected systems, impact of vulnerabilities and remediation.

9.9 OVAL Definition

The Open Vulnerability and Assessment Language (OVAL)[20] is a MITRE[21] project and maintained by the Center of Internet Security (CIS).

OVAL is a language to describe vulnerabilities, configuration settings (compliance), patches and applications (inventory).

The XML based definitions allow simple processing by automated systems and describe the discovery of individual systems and vulnerabilities.

9.10 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.

9.11 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.

While the QoD range allows to express the quality quite fine-grained, in fact most of the test routines use a standard methodology. Therefore, QoD types are associate with a QoD value. The current list of types might be extended over time.

[20] https://oval.cisecurity.org/

[21] https://www.mitre.org/

QoD in %	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 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		During system migration this value was assigned to any results obtained before QoD was introduced. However, some VTs eventually might own this value for some reason.
70	remote_analysis	Remote checks that do some analysis but which are not always fully reliable.
50	remote_probe	Remote checks in which intermediate systems such as firewalls might 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.
1	general_note	General note on potential vulnerability without finding any present application.

9.12 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.

9.13 Result

A single result generated by the scanner as part of a report, for example a vulnerability warning or a log message.

9.14 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 *Scan Management*.

When the scan is running, 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 *Scan Management* offers the option to stop a scan.

9.15 Scanner

A scanner is an OpenVAS Scanner daemon or compatible OSP daemon on which the scan will be run.

9.16 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.

9.17 Schedule

A schedule sets the time when a task should be started automatically, a period after which the task should run again and a maximum duration the task is allowed to take.

9.18 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* and *Critical*).

This concept is based on CVSS but is applied in case no full CVSS Base Vector is available as well. For example, arbitrary values in that range are applied for overrides and used by OSP scanners even without a vector definition.

Comparison, weighting and prioritisation 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 CVE does not offer one and any result of OSP scanners is assigned an adequate severity value even if the respective scanner uses a different severity scheme.

The severity classes *Log*, *Low*, *Medium* and *Critical* are defined by sub-ranges of the main range 0.0 – 10.0.

Scan results are assigned a severity while achieved. The severity of the related VT may change over time though.

9.19 Solution Type

This information shows possible solutions for the remediation of the vulnerability.

Temporary Fix
A workaround (information about a configuration or a specific deployment scenario that can be used to avoid exposure to the vulnerability) is available to temporarily eliminate the vulnerability. There can be none, one or more workaround(s) available. This is usually the “first line of defense” against a new vulnerability before a risk reduction or official fix has been issued or even discovered.

Risk Reduction
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.

Official Fix
An official vendor patch is available. Unless otherwise noted, it is assumed that this fix fully resolves the vulnerability.

Searching for Fix
There is currently no solution available to remediate the vulnerability but there may be a solution in the future.

No Fix Available
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.

9.20 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.

9.21 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.

Index