



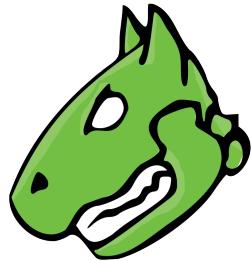
Greenbone
Sustainable Resilience

User Manual

Greenbone Security Manager



with Greenbone OS 21.04



Greenbone
Sustainable Resilience

Greenbone Networks GmbH
Neumarkt 12
49074 Osnabrück
Germany
<https://www.greenbone.net>

GOS version: GOS 21.04.1, 2021-05-25

This is the manual for the Greenbone Security Manager with Greenbone OS (GOS) version 21.04. Due to the numerous functional differences between GOS 21.04 and previous versions, this manual should not be used with older versions of GOS.

The Greenbone Security Manager is under constant development. This manual attempts to always document the latest software release. It is, however, possible that latest functionalities have not been captured in this manual.

Should you have additional notes or error corrections for this manual please send an e-mail to the Greenbone Networks support (<mailto:support@greenbone.net>).

The copyright for this manual is held by the company Greenbone Networks GmbH. Greenbone and the Greenbone logo are registered trademarks of Greenbone Networks GmbH. Other logos and registered trademarks used within this manual are the property of their respective owners and are used only for explanatory purposes.

Contents

1	Introduction	14
2	Read Before Use	16
3	Greenbone Security Manager – Overview	18
3.1	Physical Appliances	18
3.1.1	Enterprise Class – GSM 5400/6500	18
3.1.2	Midrange Class – GSM 400/450/600/650	19
3.1.3	SME (Small Enterprise) Class – GSM 150	19
3.1.4	Sensor – GSM 35	20
3.2	Virtual Appliances	22
3.2.1	Midrange Class – GSM DECA/TERA/PETA/EXA	22
3.2.2	SME (Small Enterprise) Class – GSM CENO	22
3.2.3	Sensor – GSM 25V	22
3.2.4	Entry Class – GSM ONE	23
4	Guideline for Using the Greenbone Security Manager	25
5	Setting up the Greenbone Security Manager	26
5.1	GSM 5400/6500	27
5.1.1	Installing the Appliance	27
5.1.2	Utilizing the Serial Port	27
5.1.3	Starting the Appliance	28
5.1.4	Performing a General System Setup	29
5.1.5	Logging into the Web Interface	39
5.2	GSM 400/450/600/650	40
5.2.1	Installing the Appliance	40
5.2.2	Utilizing the Serial Port	40
5.2.3	Starting the Appliance	41
5.2.4	Performing a General System Setup	42
5.2.5	Logging into the Web Interface	52
5.3	GSM 150	53
5.3.1	Installing the Appliance	53
5.3.2	Utilizing the Serial Port	53
5.3.3	Starting the Appliance	54
5.3.4	Performing a General System Setup	55
5.3.5	Logging into the Web Interface	65

5.4	GSM 35	66
5.4.1	Installing the Appliance	66
5.4.2	Utilizing the Serial Port	66
5.4.3	Starting the Appliance	67
5.4.4	Performing a General System Setup	68
5.5	GSM CENO/DECA/TERA/PETA/EXA	78
5.5.1	Setup Requirements	78
5.5.1.1	Resources	78
5.5.1.2	Supported Hypervisor	79
5.5.1.3	Verification of Integrity	79
5.5.2	Deploying the Appliance	80
5.5.3	Performing a General System Setup	82
5.5.4	Logging into the Web Interface	89
5.6	GSM 25V	90
5.6.1	Setup Requirements	90
5.6.1.1	Resources	90
5.6.1.2	Supported Hypervisor	90
5.6.1.3	Verification of Integrity	91
5.6.2	Deploying the Appliance	91
5.6.3	Performing a General System Setup	93
5.7	GSM ONE	101
5.7.1	Setup Requirements	101
5.7.1.1	Resources	101
5.7.1.2	Supported Hypervisor	101
5.7.1.3	Verification of Integrity	102
5.7.2	Deploying the Appliance	102
5.7.3	Performing a General System Setup	104
5.7.4	Logging into the Web Interface	112
6	Upgrading from GOS 20.08 to GOS 21.04	113
6.1	Upgrading the Greenbone Security Manager	113
6.2	Upgrading the Flash Partition to the Latest Version	116
6.3	Reloading the Web Interface After an Upgrade	116
6.4	New Features and Changes of Default Behavior	116
6.4.1	Reports	116
6.4.2	CVSS	116
6.4.3	Boreas Alive Scanner	117
6.4.4	Hardware Appliances	117
6.4.4.1	New Hardware Models for Midrange Class	117
6.4.4.2	Preparation for Upgrading a GSM 5300/6400	117
6.4.5	Virtual Appliances	117
6.4.6	Scanning Through a VPN	118
6.4.7	HTTPS	118
6.4.8	Sensors	118
6.4.9	Network Backend	118
6.4.10	Web Interface	119
6.4.10.1	Auto False Positives	119
6.4.10.2	Severity Class Scheme	119
6.4.10.3	Simultaneous Scanning via Multiple IP Addresses	119
6.4.11	Greenbone Management Protocol (GMP)	119
7	Managing the Greenbone Operating System	120
7.1	General Information	120
7.1.1	Greenbone Security Feed (GSF) Subscription Key	120
7.1.2	Authorization Concept	120
7.1.2.1	User Level Access	121

7.1.2.2	System Level Access	121
7.1.3	Using the GOS Administration Menu	122
7.2	Setup Menu	124
7.2.1	Managing Users	124
7.2.1.1	Changing the System Administrator Password	124
7.2.1.2	Managing Web Users	125
7.2.1.3	Creating a Web Administrator	126
7.2.1.4	Enabling a Guest User	126
7.2.1.5	Creating a Super Administrator	127
7.2.1.6	Deleting a User Account	128
7.2.1.7	Changing a User Password	129
7.2.1.8	Changing the Password Policy	129
7.2.1.9	Configuring the Settings for Data Objects	130
7.2.2	Configuring the Network Settings	132
7.2.2.1	Updating the Networking Mode to <i>gnm</i>	132
7.2.2.2	General Information About Namespaces	132
7.2.2.3	Switching an Interface to Another Namespace	133
7.2.2.4	Configuring Network Interfaces	134
7.2.2.5	Configuring the DNS Server	139
7.2.2.6	Configuring the Global Gateway	140
7.2.2.7	Setting the Host Name and the Domain Name	141
7.2.2.8	Restricting the Management Access	141
7.2.2.9	Displaying the MAC and IP Addresses and the Network Routes	142
7.2.3	Configuring a Virtual Private Network (VPN) Connection	143
7.2.3.1	Setting up a VPN Connection	144
7.2.3.2	Editing or Deleting a VPN Connection	145
7.2.4	Configuring Services	145
7.2.4.1	Configuring HTTPS	146
7.2.4.2	Configuring the Greenbone Management Protocol (GMP)	153
7.2.4.3	Configuring the Open Scanner Protocol (OSP)	153
7.2.4.4	Configuring SSH	154
7.2.4.5	Configuring SNMP	157
7.2.4.6	Configuring a Port for the Temporary HTTP Server	158
7.2.5	Configuring Periodic Backups	158
7.2.6	Configuring the Feed Synchronization	161
7.2.6.1	Adding a Greenbone Security Feed (GSF) Subscription Key	162
7.2.6.2	Enabling or Disabling Synchronization	163
7.2.6.3	Configuring the Synchronization Port	163
7.2.6.4	Setting the Synchronization Proxy	164
7.2.6.5	Deleting the Greenbone Security Feed (GSF) Subscription Key	165
7.2.7	Configuring the GSM as an Airgap Master/Sensor	166
7.2.7.1	Using the Airgap USB Stick	166
7.2.7.2	Using the Airgap FTP Server	167
7.2.8	Configuring the Time Synchronization	169
7.2.9	Selecting the Keyboard Layout	170
7.2.10	Configuring Automatic E-Mails	171
7.2.10.1	Configuring the Mail Server	171
7.2.10.2	Configuring SMTP Authentication for the Mail Server	172
7.2.10.3	Configuring the Size of Included or Attached Reports	173
7.2.11	Configuring the Collection of Logs	173
7.2.11.1	Configuring the Logging Server	174
7.2.11.2	Managing HTTPS Certificates for Logging	175
7.2.12	Setting the Maintenance Time	177
7.3	Maintenance Menu	178
7.3.1	Performing a Self-Check	178
7.3.2	Performing and Restoring a Backup	179

7.3.2.1	Performing a Backup Manually	179
7.3.2.2	Restoring a Backup Manually	180
7.3.2.3	Performing a Backup Using a USB Stick	181
7.3.2.4	Restoring a Backup Using a USB Stick	182
7.3.3	Copying Data and Settings to Another GSM with Beaming	183
7.3.3.1	Beaming Directly from Another GSM	183
7.3.3.2	Beaming via Remote File System	186
7.3.4	Performing a GOS Upgrade	188
7.3.5	Performing a GOS Upgrade on Sensors	188
7.3.6	Performing a Feed Update	189
7.3.7	Performing a Feed Update on Sensors	189
7.3.8	Upgrading the Flash Partition	190
7.3.9	Shutting down and Rebooting the Appliance	191
7.3.9.1	Rebooting the Appliance	191
7.3.9.2	Shutting down the Appliance	192
7.4	Advanced Menu	193
7.4.1	Displaying Log Files of the GSM	193
7.4.2	Performing Advanced Administrative Work	193
7.4.2.1	Managing the Superuser Account	193
7.4.2.2	Generating and Downloading a Support Package	195
7.4.2.3	Accessing the Shell	197
7.4.3	Displaying the Greenbone Security Feed (GSF) Subscription Key	198
7.4.4	Displaying the Copyright File	198
7.5	Displaying Information about the Appliance	199
8	Getting to Know the Web Interface	200
8.1	Logging into the Web Interface	200
8.2	List Pages and Details Pages	200
8.3	Dashboards and Dashboard Displays	203
8.3.1	Adding and Deleting Dashboard Displays	203
8.3.2	Editing a Dashboard Display	204
8.3.3	Organizing Displays in Dashboards	204
8.3.3.1	Adding a New Dashboard	206
8.3.3.2	Editing a Dashboard	207
8.3.3.3	Deleting a Dashboard	207
8.4	Filtering the Page Content	207
8.4.1	Adjusting the Filter Parameters	207
8.4.2	Syntax of the Powerfilter	209
8.4.2.1	Global Keywords	209
8.4.2.2	Operators	210
8.4.2.3	Text Phrases	211
8.4.2.4	Time Specifications	211
8.4.3	Examples for Powerfilters	212
8.4.4	Managing Powerfilters	212
8.5	Using Tags	214
8.5.1	Linking a Tag to a Single Object	214
8.5.2	Linking a Tag to Multiple Objects	214
8.5.3	Creating a Tag	215
8.5.4	Managing Tags	215
8.6	Using the Trashcan	216
8.7	Displaying the Feed Status	218
8.8	Changing the User Settings	218
8.9	Opening the User Manual	220
8.10	Logging Out of the Web Interface	220
9	Managing the Web Interface Access	221

9.1	Users	221
9.1.1	Creating and Managing Users	222
9.1.1.1	Creating a User	222
9.1.1.2	Managing Users	223
9.1.2	Simultaneous Login	225
9.1.3	Creating a Guest Login	225
9.2	Roles	225
9.2.1	Cloning an Existing Role	226
9.2.2	Creating a Role	227
9.2.3	Managing Roles	227
9.2.4	Assigning Roles to a User	228
9.2.5	Creating a Super Administrator	229
9.3	Groups	229
9.3.1	Creating a Group	229
9.3.2	Managing Groups	230
9.4	Permissions	231
9.4.1	Creating and Managing Permissions	231
9.4.1.1	Creating a Permission	231
9.4.1.2	Creating Permissions from the Resource Details Page	232
9.4.1.3	Managing Permissions	233
9.4.2	Granting Super Permissions	234
9.4.3	Granting Read Access to Other Users	236
9.4.3.1	Requirements for Granting Read Access	236
9.4.3.2	Granting Read Access	239
9.5	Using a Central User Management	240
9.5.1	LDAP	240
9.5.2	LDAP with SSL/TLS	242
9.5.3	RADIUS	243
10	Scanning a System	245
10.1	Using the Task Wizard for a First Scan	245
10.1.1	Using the Task Wizard	245
10.1.2	Using the Advanced Task Wizard	246
10.1.3	Using the Wizard to Modify a Task	247
10.2	Configuring a Simple Scan Manually	248
10.2.1	Creating a Target	248
10.2.2	Creating a Task	251
10.2.3	Starting the Task	253
10.3	Configuring an Authenticated Scan Using Local Security Checks	253
10.3.1	Advantages and Disadvantages of Authenticated Scans	254
10.3.2	Using Credentials	255
10.3.2.1	Creating a Credential	255
10.3.2.2	Managing Credentials	257
10.3.3	Requirements on Target Systems with Microsoft Windows	259
10.3.3.1	General Notes on the Configuration	259
10.3.3.2	Configuring a Domain Account for Authenticated Scans	260
10.3.3.3	Restrictions	266
10.3.3.4	Scanning Without Domain Administrator and Local Administrator Permissions	266
10.3.4	Requirements on Target Systems with ESXi	267
10.3.5	Requirements on Target Systems with Linux/Unix	270
10.3.6	Requirements on Target Systems with Cisco OS	272
10.3.6.1	SNMP	272
10.3.6.2	SSH	273
10.3.7	Requirements on Target Systems with Huawei VRP	274
10.3.7.1	SNMP	274
10.3.7.2	SSH	276

10.3.8 Requirements on Target Systems with EulerOS	278
10.3.9 Requirements on Target Systems with GaussDB	280
10.3.9.1 Requirements for System User <i>root</i>	280
10.3.9.2 Requirements for Database Administrator Accounts (e.g., <i>gaussdba</i>)	280
10.3.9.3 Requirements for a Regular User Accounts	280
10.3.9.4 Requirements for a Regular Database User Accounts (e.g., <i>gauss</i>)	280
10.4 Configuring a Prognosis Scan	281
10.5 Using Container Tasks	283
10.5.1 Creating a Container Task	283
10.5.2 Managing Container Tasks	283
10.6 Managing Targets	284
10.7 Creating and Managing Port Lists	285
10.7.1 Creating a Port List	286
10.7.2 Importing a Port List	286
10.7.3 Managing Port Lists	287
10.8 Managing Tasks	288
10.8.1 Granting Permissions for a Task	290
10.9 Configuring and Managing Scan Configurations	291
10.9.1 Default Scan Configurations	291
10.9.2 Creating a Scan Configuration	292
10.9.3 Importing a Scan Configuration	295
10.9.4 Editing the Scanner Preferences	295
10.9.4.1 Description of Scanner Preferences	296
10.9.5 Editing the VT Preferences	297
10.9.5.1 Description of VT Preferences	297
10.9.6 Managing Scan Configurations	299
10.10 Performing a Scheduled Scan	301
10.10.1 Creating a Schedule	301
10.10.2 Managing Schedules	302
10.11 Creating and Managing Scanners	303
10.11.1 Creating a Scanner	303
10.11.2 Managing Scanners	304
10.12 Using Alerts	305
10.12.1 Creating an Alert	305
10.12.2 Assigning an Existing Alert to a Task	310
10.12.3 Managing Alerts	310
10.13 Obstacles While Scanning	313
10.13.1 Hosts not Found	313
10.13.2 Long Scan Periods	313
10.13.3 VT not Used	314
10.13.4 Scanning vhosts	314
11 Reports and Vulnerability Management	315
11.1 Configuring and Managing Report Formats	315
11.1.1 Default Report Formats	316
11.1.2 Managing Report Formats	317
11.1.3 Adding a Report Format	318
11.2 Using and Managing Reports	319
11.2.1 Reading a Report	320
11.2.1.1 Results of a Report	321
11.2.1.2 Interpreting a Report	322
11.2.1.3 Filtering a Report	323
11.2.2 Exporting a Report	324
11.2.3 Importing a Report	325
11.2.4 Triggering an Alert for a Report	325
11.2.5 Creating a Delta Report	326

11.3	Displaying all Existing Results	328
11.4	Displaying all Existing Vulnerabilities	329
11.5	Trend of Vulnerabilities	330
11.6	Using Tickets	331
11.6.1	Creating a Ticket	331
11.6.2	Changing the Status of a Ticket	332
11.6.3	Setting an Alert for a Ticket	333
11.6.4	Managing Tickets	334
11.7	Using Notes	335
11.7.1	Creating a Note	335
11.7.1.1	Creating a Note Through a Scan Result	335
11.7.1.2	Creating a Note on the Page <i>Notes</i>	337
11.7.2	Managing Notes	337
11.8	Using Overrides and False Positives	338
11.8.1	Creating an Override	338
11.8.1.1	Creating an Override Through a Scan Result	338
11.8.1.2	Creating an Override on the Page <i>Overrides</i>	340
11.8.2	Managing Overrides	340
11.8.3	Disabling and Enabling Overrides	341
11.9	Using Business Process Maps	341
11.9.1	Navigating the Business Process Map	342
11.9.2	Creating a Business Process Map	342
11.9.3	Editing a Business Process Map	345
11.9.3.1	Editing a Process	345
11.9.3.2	Deleting Elements	345
12	Performing Compliance Scans and Special Scans	346
12.1	Configuring and Managing Policies	347
12.1.1	Creating a Policy	347
12.1.2	Importing a Policy	350
12.1.3	Managing Policies	350
12.2	Configuring and Managing Audits	352
12.2.1	Creating an Audit	352
12.2.1.1	Creating an Audit on the Page <i>Audits</i>	352
12.2.1.2	Creating an Audit Through a Policy	353
12.2.2	Starting an Audit	354
12.2.3	Managing Audits	354
12.3	Using and Managing Policy Reports	357
12.3.1	Using a Policy Report	357
12.3.2	Exporting a Policy Report	357
12.4	Generic Policy Scans	357
12.4.1	Checking File Content	357
12.4.1.1	Checking File Content Patterns	358
12.4.1.2	Changing the Severity	360
12.4.2	Checking Registry Content	360
12.4.2.1	Checking Registry Content Patterns	361
12.4.2.2	Changing the Severity	362
12.4.3	Checking File Checksums	363
12.4.3.1	Checking File Checksum Patterns	363
12.4.3.2	Changing the Severity	365
12.4.3.3	Checking File Checksum Patterns for Microsoft Windows	365
12.4.4	Performing CPE-Based Checks	367
12.4.4.1	Simple CPE-Based Checks for Security Policies	367
12.4.4.2	Detecting the Presence of Problematic Products	367
12.4.4.3	Detecting the Absence of Important Products	369
12.5	Checking Standard Policies	372

12.5.1	IT-Grundschutz	372
12.5.2	BSI TR-03116: Kryptographische Vorgaben für Projekte der Bundesregierung	373
12.5.3	BSI TR-02102: Kryptographische Verfahren: Empfehlungen und Schlüssellängen	374
12.6	Running a TLS Map Scan	376
12.6.1	Checking for TLS and Exporting the Scan Results	376
13	Managing Assets	378
13.1	Creating and Managing Hosts	378
13.1.1	Creating a Host	378
13.1.2	Managing Hosts	379
13.1.3	Creating a Target from Hosts	380
13.2	Managing Operating Systems	381
13.3	Managing TLS Certificates	382
14	Managing SecInfo	384
14.1	Vulnerability Tests (VT)	385
14.2	Security Content Automation Protocol (SCAP)	386
14.2.1	CVE	387
14.2.2	CPE	389
14.2.3	OVAL Definitions	390
14.2.4	CVSS	393
14.2.4.1	CVSS Version 2.0	394
14.2.4.2	CVSS Version 3.0/3.1	395
14.3	CERT-Bund Advisories	396
14.4	DFN-CERT Advisories	397
15	Using the Greenbone Management Protocol	399
15.1	Changes to GMP	399
15.2	Activating GMP	399
15.3	Using gvm-tools	400
15.3.1	Accessing with gvm-cli.exe	400
15.3.1.1	Configuring the Client	402
15.3.1.2	Starting a Scan Using the Command gvm-cli	402
15.3.2	Accessing with gvm-pyshell.exe	404
15.3.2.1	Starting a Scan Using the Command gvm-pyshell	404
15.3.3	Example Scripts	407
15.4	Status Codes	407
16	Using a Master-Sensor Setup	409
16.1	Configuring a Master-Sensor Setup	410
16.1.1	Connecting a Master to a Sensor	410
16.1.2	Creating a Scan User Account	413
16.2	Managing all Configured Sensors	413
16.3	Deploying Sensors in Secure Networks	414
16.4	Configuring a Sensor as a Remote Scanner	415
16.5	Using a Remote Scanner	416
17	Managing the Performance	417
17.1	Monitoring the Appliance Performance	417
17.2	Optimizing the Scan Performance	419
17.2.1	Selecting a Port List for a Task	419
17.2.1.1	General Information about Ports and Port Lists	419
17.2.1.2	Selecting the Right Port List	420
17.2.2	Selecting a Scan Configuration for a Task	421
17.2.3	Selecting the Scanning Order of Targets	421
17.3	Scan Queueing	422

18 Connecting the Greenbone Security Manager to Other Systems	423
18.1 Using an OSP Scanner	424
18.2 Using Verinice	424
18.2.1 IT Security Management	425
18.2.1.1 Importing the ISM Scan Report	425
18.2.1.2 Creating Tasks	427
18.2.1.3 Remediating Vulnerabilities	428
18.3 Using Nagios	428
18.3.1 Configuring the GSM User	429
18.3.2 Configuring the Script	429
18.3.3 Caching and Multiprocessing	431
18.4 Using the Cisco Firepower Management Center	432
18.4.1 Configuring the Host-Input-API Clients	432
18.4.2 Configuring a Sourcefire Connector Alert	433
18.5 Using Alemba vFire	434
18.5.1 Prerequisites for Alemba vFire	434
18.5.2 Configuring an Alemba vFire Alert	435
18.6 Using Splunk	436
18.6.1 Setting up the Greenbone-Splunk App	436
18.6.1.1 Installing the App	436
18.6.1.2 Configuring the Greenbone-Splunk App	437
18.6.2 Configuring a Splunk Alert	438
18.6.2.1 Creating the Splunk Alert	438
18.6.2.2 Adding the Splunk Alert to a Task	439
18.6.2.3 Testing the Splunk Alert	439
18.6.3 Using the Greenbone-Splunk App	440
18.6.3.1 Accessing the Information in Splunk	440
18.6.3.2 Performing a Search	440
18.6.3.3 Creating a Dashboard for the Top 5 Affected Hosts and for Incoming Reports	442
19 Architecture	444
19.1 GOS Architecture	444
19.2 Protocols	446
19.2.1 GSM as a Client	446
19.2.2 GSM as a Server	449
19.2.3 Master-Sensor Setup	450
19.3 Security Gateway Considerations	450
19.3.1 Stand-Alone/Master GSM	450
19.3.2 Sensor GSM	451
20 Frequently Asked Questions	452
20.1 Why is the Scanning Process so Slow?	452
20.2 Why Is a Service/Product Not Detected?	452
20.3 Why Is a Vulnerability Not Detected?	453
20.4 Why Is It Not Possible to Edit Scan Configurations, Port Lists, Compliance Policies, or Report Formats?	454
20.5 Why Is It Not Possible to Delete Scan Configurations, Port Lists, Compliance Policies, or Report Formats?	454
20.6 Why Does a VNC Dialog Appear on the Scanned Target System?	454
20.7 Why Does the Scan Trigger Alarms on Other Security Tools?	455
20.8 How Can a Factory Reset of the GSM Be Performed?	456
20.9 Why Does Neither Feed Update nor GOS Upgrade Work After a Factory Reset?	456
20.10 How Can an Older, Newer or Unsupported Backup Be Restored?	456
20.11 What Can Be Done if the GOS Administration Menu Is not Displayed Correctly in PuTTY?	456
20.12 How Can the GMP Status Be Checked Without Using Credentials?	457



21 Glossary	458
21.1 Alert	458
21.2 Asset	458
21.3 CERT-Bund Advisory	458
21.4 Compliance Audit	458
21.5 Compliance Policy	458
21.6 CPE	459
21.7 CVE	459
21.8 CVSS	459
21.9 DFN-CERT Advisory	459
21.10 Filter	459
21.11 Group	459
21.12 Host	460
21.13 Note	460
21.14 Vulnerability Test (VT)	460
21.15 OVAL Definition	460
21.16 Override	460
21.17 Permission	460
21.18 Port List	460
21.19 Quality of Detection (QoD)	461
21.20 Remediation Ticket	462
21.21 Report	462
21.22 Report Format	462
21.23 Result	462
21.24 Role	462
21.25 Scan	462
21.26 Scanner	463
21.27 Scan Configuration	463
21.28 Schedule	463
21.29 Severity	463
21.30 Solution Type	463
21.31 Tag	464
21.32 Target	464
21.33 Task	464
21.34 TLS Certificate	464
Index	465

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 Security Manager – GSM

The Greenbone Security Manager (GSM) is an appliance for the vulnerability management of IT infrastructures, available as physical or virtual models.

It assists companies and agencies with automated and integrated vulnerability assessment and management. Its task is to discover vulnerabilities and security gaps before a potential attacker does.

The GSM consists of the Greenbone Operating System (GOS) on which the Greenbone Security Feed (GSF) is installed, a scan service, the web interface and, in case of a physical appliance, a special hardware.

The scan service uses over 78,000 Vulnerability Tests (VTs) to detect existing vulnerabilities on the inspected network. The found vulnerabilities are evaluated based on their severity which enables the setting of priorities for eliminating the vulnerabilities.



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

The GSM discovers vulnerabilities through different perspectives of an attacker:

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

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

Internal The GSM 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 GSM 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 10.3.1 (page 254).

Due to new vulnerabilities being discovered on a daily basis, regular updates and testing of systems are required. The Greenbone Security Feed ensures that the GSM is provided with the latest testing routines and can discover the latest vulnerabilities reliably. Greenbone Networks analyzes CVE¹ messages and security bulletins of vendors and develops new vulnerability tests daily.

When performing a vulnerability scan using the GSM, 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 GSM 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 GSM 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 Security Manager (GSM) includes a full-featured vulnerability scanner. While the vulnerability scanner has been designed to minimize any adverse effects on the network environment, it still needs to interact and communicate with the target systems being analyzed during a scan.

Note: It is the fundamental task of the GSM 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 firewalls and intrusion detection and prevention systems. Intrusion prevention measures may be triggered.
 - Scans may increase latency on the target and/or the scanned network, in extreme cases resulting in situations similar to a denial of service (DoS) attack.
 - Scans may trigger bugs in fragile or insecure applications resulting in faults or crashes.
 - Scans may result in user accounts being locked due to the testing of default user name/password combinations.
 - Logins (e.g., via SSH or FTP) are done against the target systems for banner grabbing purposes.
 - Embedded systems and elements of operational technology with weak network stacks are especially subject to possible crashes or even broken devices.
-

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 GSM to scan the target systems.

CHAPTER 3

Greenbone Security Manager – Overview

The Greenbone Security Manager (GSM) is a dedicated appliance for vulnerability scanning and vulnerability management. It is offered in different performance levels.



The specifications of the physical and virtual appliances are explained in two videos:

- Specifications of physical appliances²
- Specifications of virtual appliances³

3.1 Physical Appliances

3.1.1 Enterprise Class – GSM 5400/6500

The GSM 6500 and GSM 5400 are designed for the operation in large companies and agencies.



Fig. 3.1: GSM of the Enterprise Class

The appliances of the Enterprise Class can control other appliances as sensors. The appliances themselves can be controlled as remote scanners by another appliance.

² <https://youtu.be/4Qhl-Be3gJQ>

³ <https://youtu.be/4WRMquNEOo4>



The appliances in the Enterprise Class come in a 2U 19" chassis for easy integration into the data center. For easy installation and monitoring they are equipped with a two line LC display with 16 characters per line. For uninterrupted operation they have redundant, hot swappable power supplies, hard drives and fans.

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

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

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

3.1.2 Midrange Class – GSM 400/450/600/650

The GSM 400, GSM 450, GSM 600 and GSM 650 are designed for medium-sized companies and agencies as well as larger branch offices.



Fig. 3.2: GSM of the Midrange Class

The appliances of the Midrange Class can control other appliances as sensors. The appliances themselves can be controlled as remote scanners by another appliance.

The appliances in the Midrange Class come in a 1U 19" chassis for easy integration into the data center. For easy installation and monitoring they are equipped with a two line LC display with 16 characters per line. For uninterrupted operation the appliances come with redundant fans.

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

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

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

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

3.1.3 SME (Small Enterprise) Class – GSM 150

The GSM 150 is designed for small companies and agencies as well as small to medium branch offices. Controlling sensors in other security zones is not considered. However, the GSM 150 itself can be controlled as a remote scanners by another appliance.

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

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



Fig. 3.3: GSM of the SME Class

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

3.1.4 Sensor – GSM 35

The GSM 35 is designed as a sensor for smaller companies and agencies as well as small branches.



Fig. 3.4: Physical sensor

The GSM 35 can only be used in sensor mode and has to be managed via a GSM master. No web interface is available on the GSM 35. GSMS of the Midrange Class and the Enterprise Class (GSM 400/GSM DECA and beyond) can be utilized as masters for the GSM 35.

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

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

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



	Appliance							Sensor
	GSM 6500	GSM 5400	GSM 650 Rev. 2	GSM 600 Rev. 2	GSM 450 Rev. 2	GSM 400 Rev. 2	GSM 150	GSM 35
Use Case	Large enterprise/service providers	Large enterprise/service providers	Medium enterprise/branch location	Medium enterprise/branch location	Medium enterprise/branch location	Medium enterprise/branch location	Small and medium enterprise/small branch location	Sensor for managed services/branch scans
Support Level	Platinum	Platinum	Platinum	Platinum	Platinum	Platinum	Platinum	Platinum (managed via master)
Scan Capacity (IP Addresses per 24 h)	9,000 – 80,000	4,000 – 40,000	1,000 – 10,000	500 – 6,000	500 – 4,000	300 – 2,000	50 – 500	20 – 300
Weight (kg)	22 kg	22 kg	7 kg	7 kg	7 kg	7 kg	4 kg	4 kg
Dimension (WxDxH)	437/481x550x88 mm	437/481x550x88 mm	430/481x300x44 mm	430/481x300x44 mm	430/481x300x44 mm	430/481x300x44 mm	430/480x200x45 mm	430/480x200x45 mm
Ports								
Management/Feed	2 out of band management	2 out of band management	1	1	1	1	1	1
Scan GbE-Base-TX	0 – 32 ports	0 – 32 ports	8 ports	8 ports	8 ports	8 ports	4 ports	4 ports
Scan 1 GbE SFP	0 – 32 ports	0 – 32 ports	✓	✓	✓	✓	✗	✗
Scan 10 GbE SFP+	0 – 8 ports	0 – 8 ports	2 ports	2 ports	2 ports	2 ports	✗	✗
Port Roles	2 management, others dynamic	2 management, others dynamic	10 ports dynamic	10 ports dynamic	10 ports dynamic	10 ports dynamic	4 ports dynamic	4 ports dynamic
VLAN Support	128 per Ethernet Port	64 per Ethernet Port	64 per Ethernet Port	64 per Ethernet Port	16 per Ethernet Port	16 per Ethernet Port	8 per Ethernet Port	8 per Ethernet Port
Hardware								
Fan Speed Control	✗	✗	✓	✓	✓	✓	✓	✓
Redundant Fan	✓	✓	✓	✓	✓	✓	✗	✗
Redundant Power Supply	✓	✓	✗	✗	✗	✗	✗	✗
Redundant Hard Disk	✓	✓	✗	✗	✗	✗	✗	✗
Hot Swap Power Supply	✓	✓	✗	✗	✗	✗	✗	✗
Hot Swap Hard Disk	✓	✓	✗	✗	✗	✗	✗	✗
Hot Swap Fan	✓	✓	✗	✗	✗	✗	✗	✗
LCD	✓	✓	✓	✓	✓	✓	✗	✗
Power Supplies/Outlets	2	2	1	1	1	1	1	1
Max. Power Consumption per Supply	500 W	500 W	300 W	300 W	300 W	300 W	40 W	40 W
Networks								
Master Mode (Scan & Management)	Up to 80 sensors	Up to 40 sensors	Up to 20 sensors	Up to 12 sensors	Up to 6 sensors	Up to 2 sensors	✗	✗
Sensor Mode (Managed via Master)	✓	✓	✓	✓	✓	✓	✓	✓
Airgap Master	USB, FTP	USB, FTP	USB, FTP	USB, FTP	USB, FTP	USB, FTP	✗	✗
Airgap Sensor	USB, FTP	USB, FTP	USB, FTP	USB, FTP	USB, FTP	USB, FTP	FTP	✗
Greenbone OS								
SSH v2	✓	✓	✓	✓	✓	✓	✓	✓
NTP	✓	✓	✓	✓	✓	✓	✓	✓
GMP (API)	✓	✓	✓	✓	✓	✓	✓	✗
Web Interface (G), Report Plugins (P), Alerts (A), Scheduling (S)	G, P, A, S	G, P, A, S	G, P, A, S	G, P, A, S	G, P, A, S	G, P, A, S	G, P, A, S	✗
LDAP/RADIUS	✓	✓	✓	✓	✓	✓	✓	✗
SNMP v2	✓	✓	✓	✓	✓	✓	✗	✗
Syslog (UDP/TCP/TLS)	✓	✓	✓	✓	✓	✓	✓	✓
IPv6 Support	✓	✓	✓	✓	✓	✓	✓	✓
RAID6	✓	✓	✗	✗	✗	✗	✗	✗
Certificate Management	✓	✓	✓	✓	✓	✓	✓	✗
Network Namespaces	✓	✓	✓	✓	✓	✓	✗	✗
Remediation Workflow	✓	✓	✓	✓	✓	✓	✗	✗
Backup/Restore	Remote/USB, periodic	Remote/USB, periodic	Remote/USB, periodic	Remote/USB, periodic	Remote/USB, periodic	Remote/USB, periodic	USB	✗



3.2 Virtual Appliances

3.2.1 Midrange Class – GSM DECA/TERA/PETA/EXA

The GSM DECA, GSM TERA, GSM PETA and GSM EXA are designed for medium-sized companies and agencies as well as larger branch offices.



Fig. 3.5: GSM of the virtual Midrange Class

The appliances of the Midrange Class can control other appliances as sensors. The appliances themselves can be controlled as remote scanners by another appliance.

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

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

One of these ports is also used as management port.

3.2.2 SME (Small Enterprise) Class – GSM CENO

The GSM CENO is designed for small companies and agencies as well as small to medium branch offices. Controlling sensors in other security zones is not considered. However, the GSM CENO itself can be controlled as a remote scanner by another appliance.



Fig. 3.6: GSM of the virtual SME Class

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

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

One of these ports is also used as management port.

3.2.3 Sensor – GSM 25V

The GSM 25V is designed as a sensor for smaller companies and agencies as well as small branches. It provides a simple and cost effective option to monitor virtual infrastructures.

The GSM 25V can be deployed using VMware ESXi on Microsoft Windows, MacOS and Linux systems.



Fig. 3.7: Virtual sensor

The GSM 25V can only be used in sensor mode and has to be managed via a GSM master. No web interface is available on the GSM 25V. GSMS of the Midrange Class and the Enterprise Class (GSM 400/GSM DECA and beyond) can be utilized as masters for the GSM 25V.

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

One of these ports is also used as management port.

3.2.4 Entry Class – GSM ONE

The GSM ONE is designed for specific requirements such as audit using a laptop or educational purposes. It can neither control other sensors nor be controlled as a sensor by another appliance.



Fig. 3.8: GSM ONE

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

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

The GSM ONE has all the functions of the Midrange and Enterprise Class except for the following:

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

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



Appliance							Sensor
	GSM EXA	GSM PETA	GSM TERA	GSM DECA	GSM CENO	GSM ONE	GSM 25V
Use Case	Medium enterprise/ branch location	Medium enterprise/ branch location	Medium enterprise/ branch location	Medium enterprise/ branch location	Small and medium enterprise/small branch location	Special use/training/ audit-via-laptop	Sensor for managed services/ branch scans
Support Level	Platinum	Platinum	Platinum	Platinum	Platinum	Platinum	Platinum (managed via master)
Scan Capacity (IP Addresses per 24 h)	2,000 – 18,000	1,000 – 9,000	300 – 3,000	50 – 1,500	50 – 500	20 – 300	20 – 300
Required Memory on Hypervisor (GB)	24	16	8	8	8	6	4
vCPUs	12	8	6	4	2	2	2
Ports							
Virtual Ports	8	8	8	4	4	1	4
Port Roles	8 ports dynamic	8 ports dynamic	8 ports dynamic	4 ports dynamic	4 ports dynamic	1 port management/ scan/update	4 ports dynamic
GSM Networks							
Master Mode (Scan & Management)	Up to 24 sensors	Up to 12 sensors	Up to 6 sensors	Up to 2 sensors	✗	✗	✗
Sensor Mode (Managed via Master)	✓	✓	✓	✓	✓	✗	✓
Airgap Master	✗	✗	✗	✗	✗	✗	✗
Airgap Sensor	FTP	FTP	FTP	FTP	FTP	✗	✗
Open VM Tools	✓	✓	✓	✓	✓	✗	✓
Supported Hypervisors	Microsoft Hyper-V, VMware vSphere Hypervisor (ESXi), Huawei FusionCompute	Microsoft Hyper-V, VMware vSphere Hypervisor (ESXi)	Oracle VirtualBox, VMware Workstation Pro, VMware Workstation Player	Microsoft Hyper-V, VMware vSphere Hypervisor (ESXi), Huawei FusionCompute			
Cloud Support	Azure	Azure	Azure	Azure	Azure	✗	✗
Greenbone OS							
SSH v2	✓	✓	✓	✓	✓	✓	✓
NTP	✓	✓	✓	✓	✗	✗	✗
GMP (API)	✓	✓	✓	✓	✓	✓	✗
HTTPS GUI (G), Report Plugins (P), Alerts (A), Scheduling (S)	G, P, A, S	G, P, A, S	G, P, A, S	✗			
LDAP/RADIUS	✓	✓	✓	✓	✓	✗	✗
SNMP v2	✓	✓	✓	✓	✗	✗	✗
Remediation Workflow	✓	✓	✓	✓	✗	✗	✗
Syslog (UDP/TCP/TLS)	✓	✓	✓	✓	✓	✗	✗
IPv6 Support	✓	✓	✓	✓	✓	✓	✓
Certificate Management	✓	✓	✓	✓	✓	✓	✗
Backup/Restore	Remote, periodic, VM snapshot	Remote, periodic, VM snapshot	Remote, periodic, VM snapshot	Remote, periodic, VM snapshot	VM snapshot	VM snapshot	VM snapshot

CHAPTER 4

Guideline for Using the Greenbone Security Manager

The following steps are fundamental in using the Greenbone Security Manager (GSM):

- Setting up the GSM → Chapter 5 (page 26)
- Upgrading the Greenbone operating system (GOS) → Chapter 6 (page 113) and Chapter 7.3.4 (page 188)
- Performing a scan → Chapter 10 (page 245)
- Reading and using a report → Chapter 11.2.1 (page 320)
- Using notes to manage the results → Chapter 11.7 (page 335)
- Using overrides to manage false positives → Chapter 11.8 (page 338)

The following steps are more advanced:

- Setting up a central authentication using LDAP → Chapter 9.5 (page 240)
- Connecting verinice to the GSM → Chapter 18.2 (page 424)
- Connecting Nagios to the GSM → Chapter 18.3 (page 428)

CHAPTER 5

Setting up the Greenbone Security Manager

This chapter provides specific setup guides for all current GSM appliances:

- GSM 5400/6500 → Chapter 5.1 (page 27)
- GSM 400/450/600/650 → Chapter 5.2 (page 40)
- GSM 150 → Chapter 5.3 (page 53)
- GSM 35 → Chapter 5.4 (page 66)
- GSM CENO/DECA/TERA/PETA/EXA → Chapter 5.5 (page 78)
- GSM 25V → Chapter 5.6 (page 90)
- GSM ONE → Chapter 5.7 (page 101)



5.1 GSM 5400/6500

This setup guide shows the steps required to put a GSM 5400 or 6500 appliance into operation.

The following checklist can be used to monitor the progress:

Step	Done
Power supply established (2 connectors)	
Networking cables connected	
Console access established	
Keyboard layout selected	
IP address configured	
DNS server configured	
SSH service enabled (optional)	
SSL certificate created	
Web user account created	
GOS selfcheck run	

5.1.1 Installing the Appliance

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

For cabling GSM 5400 and GSM 6500 appliances have corresponding connectors at the front and back:

- **Front**

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

- **Back**

- 1 VGA port
- 2 USB 3.0 ports
- 2 USB 2.0 ports
- 2 power supplies

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

5.1.2 Utilizing the Serial Port

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

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



In Linux the command `screen` can be used in the command line to access the serial port by passing the device providing the serial port as parameter:

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

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

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

In Microsoft Windows the PuTTY⁴ application can be used. After starting it, the options as shown in Fig. 5.1 and the appropriate serial port have to be selected.

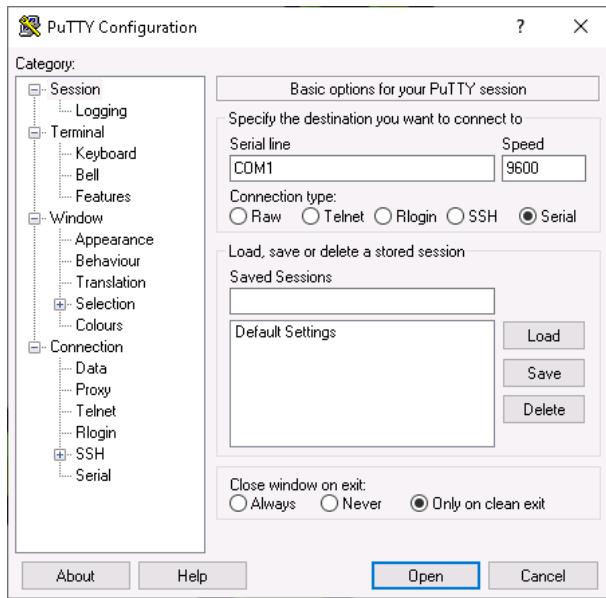


Fig. 5.1: Setting up the serial port in PuTTY

5.1.3 Starting the Appliance

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

The appliance will boot and after short time – depending on the exact model – the first messages will be displayed in the terminal application.

⁴ <https://www.chiark.greenend.org.uk/~sgtatham/putty/>



5.1.4 Performing a General System Setup

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

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

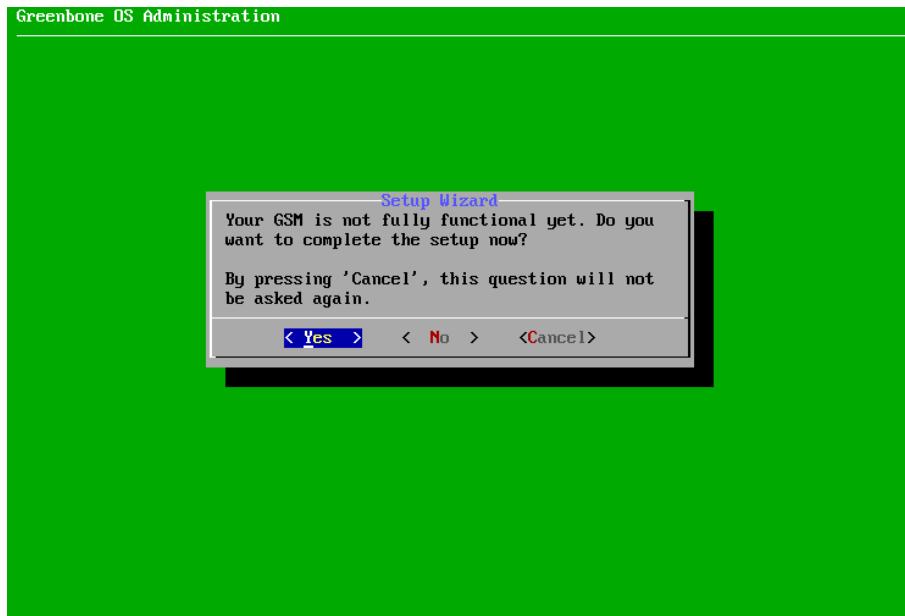


Fig. 5.2: Using the first setup wizard

By selecting *Yes* and pressing `Enter` the first setup wizard is opened and can be used as follows:

Note: By selecting *No* and pressing `Enter` the wizard can be closed. Steps which have not been completed yet are displayed when logging in again.

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

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

In case of a factory reset, all steps have to be carried out (see 20.8 (page 456)).

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

1. Configuring the Network

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

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

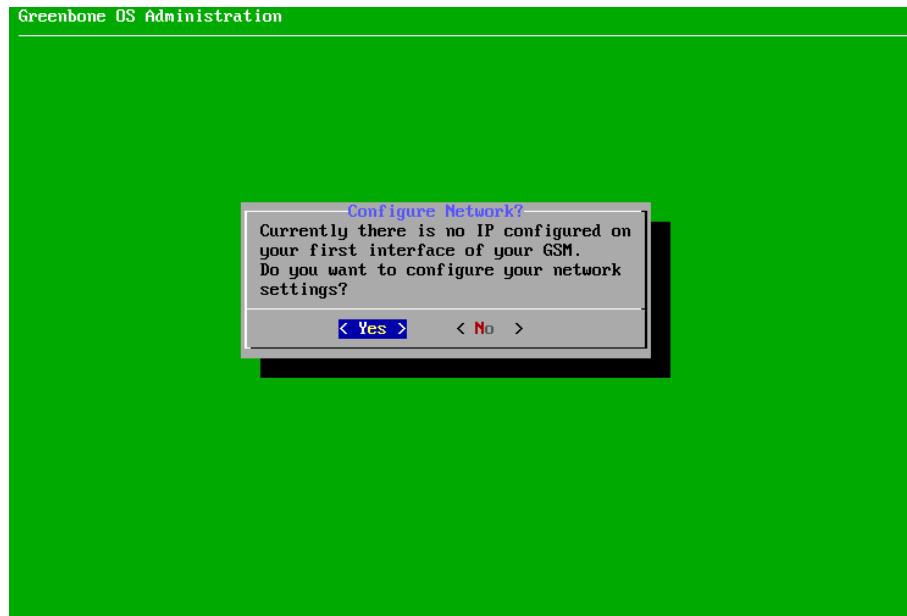


Fig. 5.3: Configuring the network settings

3. Select the desired interface and press Enter.

Note: Using interface eth0 is recommended.

If there is only one interface, the configuration of this interface is opened directly.

→ The interface can be configured.

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

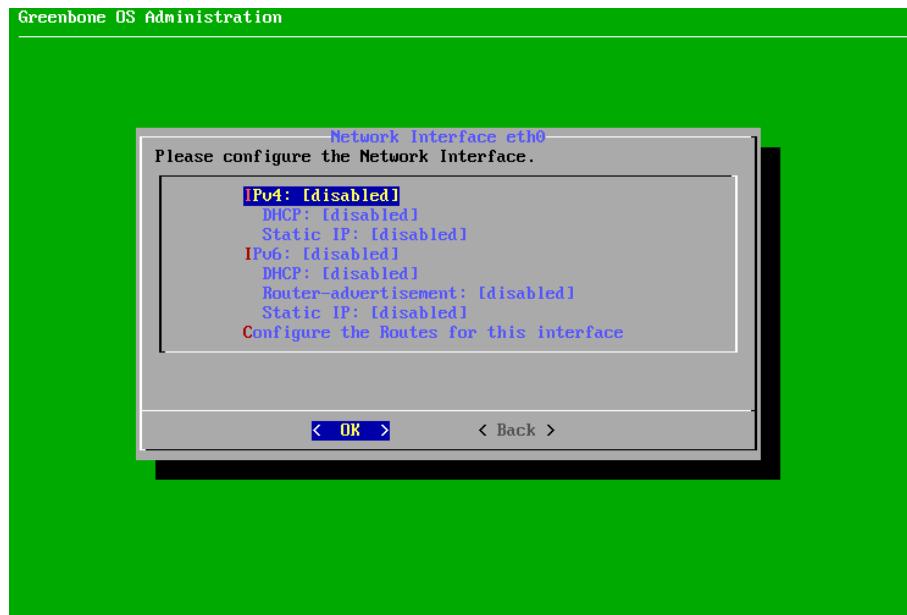


Fig. 5.4: Configuring the network interface

5. Select *Save* and press Enter.



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

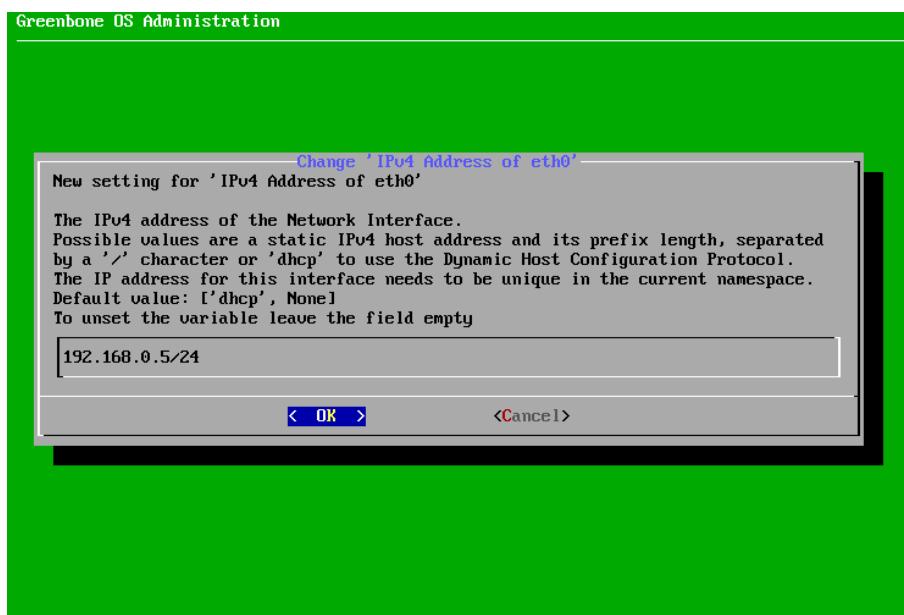


Fig. 5.5: Entering a static IP address

6. Press *Enter*.
→ A message informs that the changes have to be saved.
7. Press *Enter* to close the message.
8. Select *Save* and press *Enter*.
9. Select *Back* and press *Enter*.
10. Select *Ready* and press *Enter*.

2. Importing or Generating an HTTPS Certificate

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

1. Select *Import* and press *Enter* (see Fig. 5.6).
→ A message informs that a PKCS#12 file can be imported.
2. Select *Continue* and press *Enter*.
3. Open the web browser and enter the displayed URL.
4. Click *Browse...*, select the PKCS#12 file and click *Upload*.
→ When the certificate is retrieved by the GSM, the GOS administration menu displays the fingerprint of the certificate for verification.
5. Check the fingerprint and confirm the certificate by pressing *Enter*.

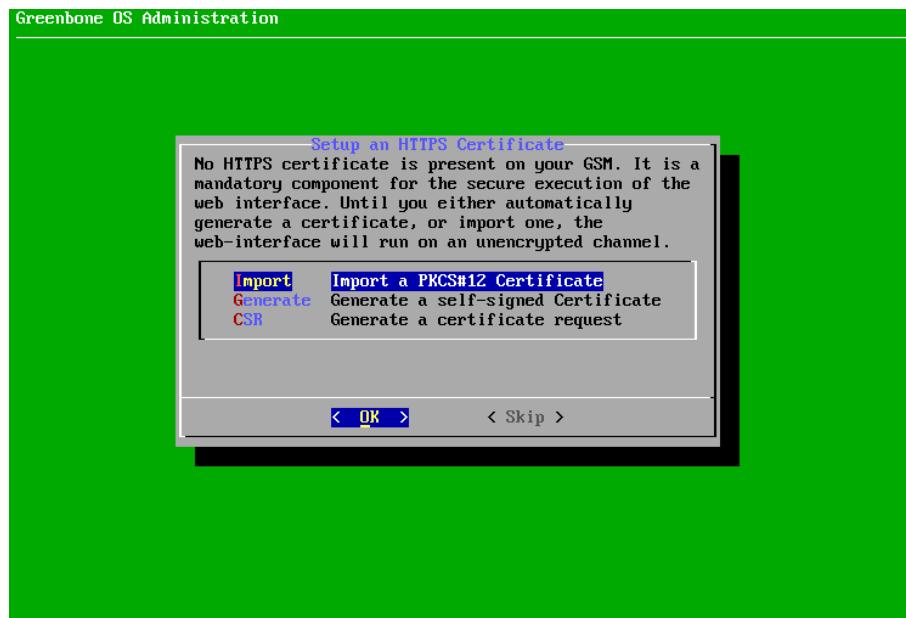


Fig. 5.6: Importing or generating an HTTPS certificate

or

1. Select *Generate* and press *Enter*.
→ A message informs that parameters have to be entered to generate the certificate.
2. Select *Continue* and press *Enter*.
3. Provide the settings for the certificate (see Fig. 5.7).

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

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

4. Select *OK* and press *Enter*.
→ A message informs that the certificate is created and can be downloaded (see Fig. 5.8).

Note: The download is not done in the first setup wizard, but in the later GOS administration menu as described in Chapter 7.2.4.1.4.1 (page 149), steps 1 – 4 and 9 – 13.

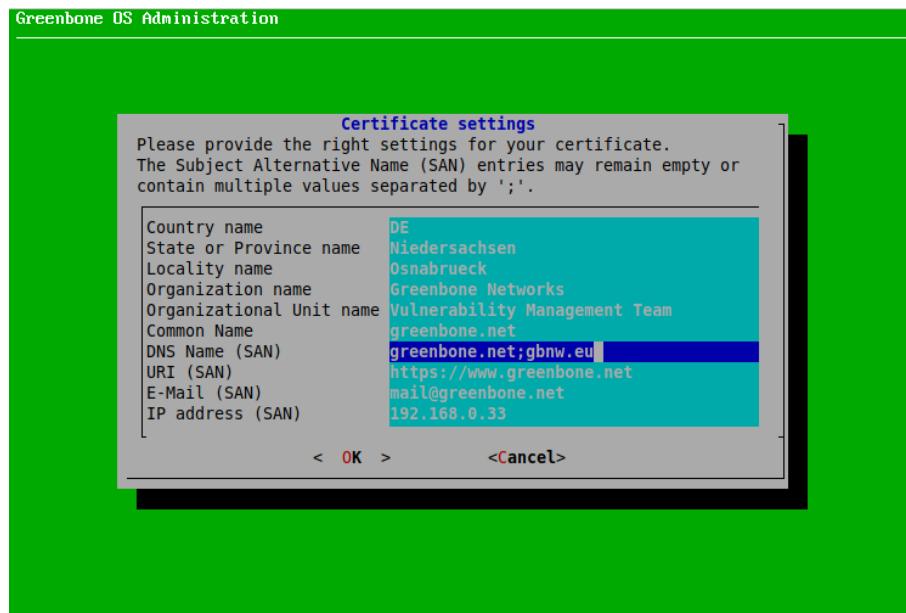


Fig. 5.7: Entering information for the certificate

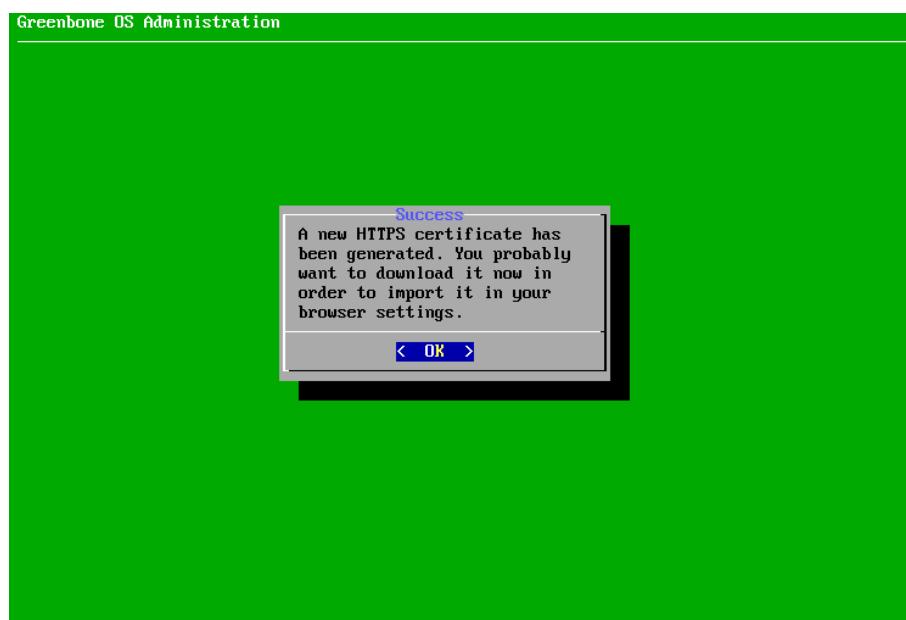


Fig. 5.8: Completing the HTTPS certificate



or

1. Select *CSR* and press *Enter*.
→ A message informs that a key pair and a certificate request are created.
2. Select *Continue* and press *Enter*.
3. Provide the settings for the certificate.

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

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

4. Select *OK* and press *Enter*.
5. Open the web browser and enter the displayed URL.
6. Download the PEM file.
→ The GOS administration menu displays a message to verify that the CSR has not been tampered with.
7. Verify the information by pressing *Enter*.

Note: When the certificate is signed it has to be uploaded to the GSM. The upload is not done in the first setup wizard, but in the later GOS administration menu as described in Chapter 7.2.4.1.4.2 (page 150), steps 1 – 4 and 11 – 14.



3. Creating a Web Administrator

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

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

The first web administrator (web user) that is created is automatically the Feed Import Owner (see Chapter 7.2.1.9 (page 130)).

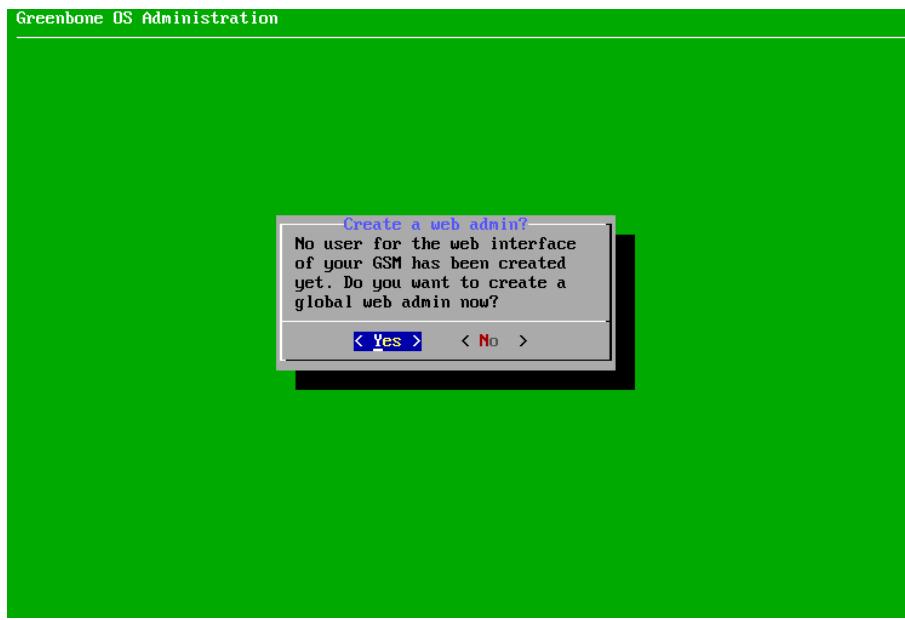


Fig. 5.9: Creating a web administrator

1. Select **Yes** and press **Enter**.
2. Enter the user name for the web administrator.
3. Enter the password for the web administrator twice.
4. Select **OK** and press **Enter**.
→ A message informs that the web administrator has been created.
5. Press **Enter** to close the message.



4. Entering or Uploading a Greenbone Security Feed (GSF) Subscription Key

If no valid GSF subscription key is stored on the appliance, the appliance only uses the public Greenbone Community Feed (GCF) and not the GSF. A GSF subscription key can be entered or uploaded as follows:

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

→ The editor is opened.



Fig. 5.10: Entering or uploading a GSF subscription key

2. Enter the subscription key.

3. Press **Ctrl + X**.

4. Press **Y** to save the changes.

5. Press **Enter**.

or

1. Select *HTTP Upload* and press **Enter**.

2. Open the web browser and enter the displayed URL.

3. Click *Browse...*, select the subscription key and click *Upload*.



5. Downloading the Feed

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

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



Fig. 5.11: Downloading the feed

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

2. Press Enter to close the message.

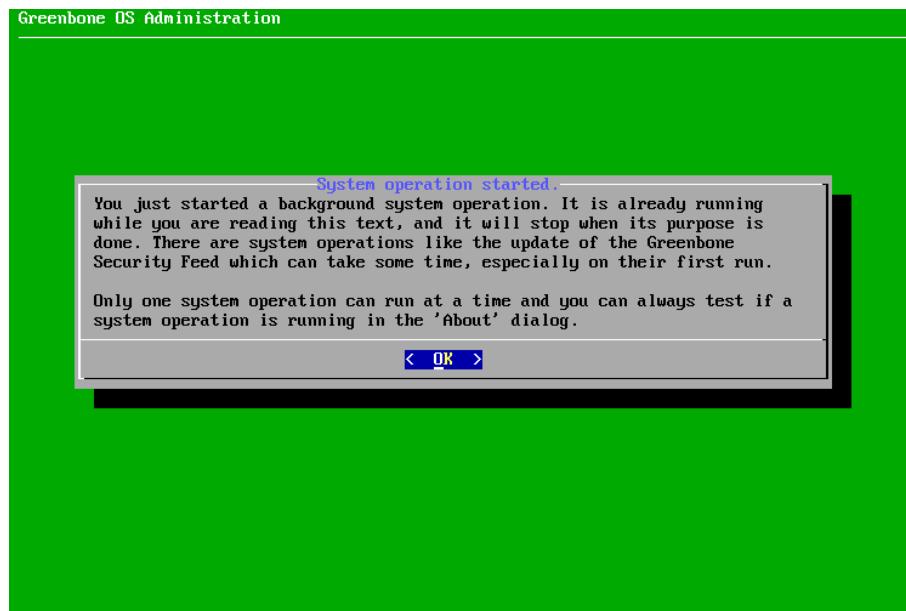


Fig. 5.12: Downloading the feed

6. Finishing the First Setup Wizard

Note: After the last step, a status check is performed. A message shows the result (see Fig. 5.13).

After closing the message by pressing **Enter** the GOS administration menu can be used as described in Chapter 7 (page 120).

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

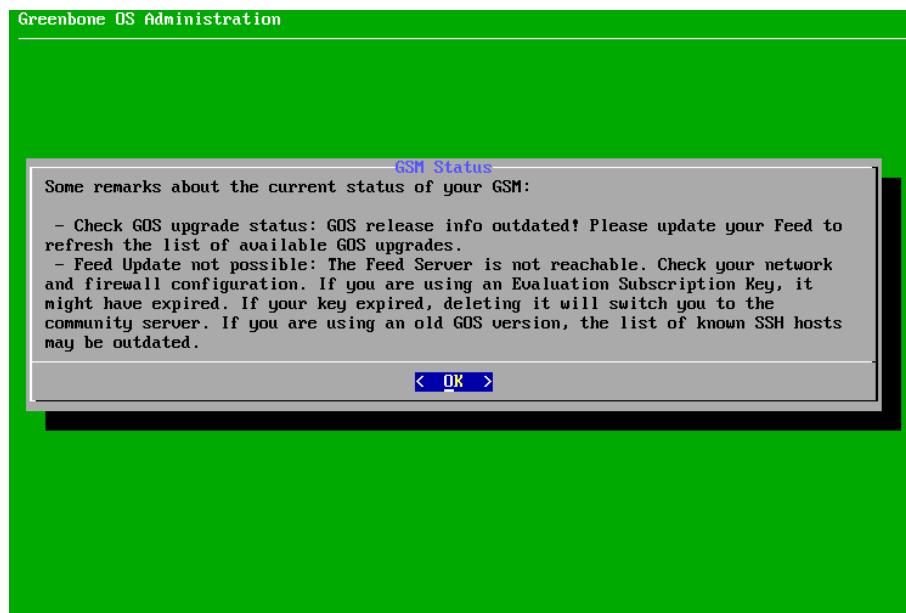


Fig. 5.13: Result of the status check



5.1.5 Logging into the Web Interface

The main interface of the GSM is the web interface, also called Greenbone Security Assistant (GSA). The web interface can be accessed as described in Chapter 8.1 (page 200).



5.2 GSM 400/450/600/650

This setup guide shows the steps required to put a GSM 400, GSM 450, GSM 600 or GSM 650 appliance into operation.

The following checklist can be used to monitor the progress:

Step	Done
Power supply established (1 connector)	
Networking cables connected	
Console access established	
Keyboard layout selected	
IP address configured	
DNS server configured	
SSH service enabled (optional)	
SSL certificate created	
Web user account created	
GOS selfcheck run	

5.2.1 Installing the Appliance

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

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

- **Front**

- 1 RS-232 serial port, Cisco compatible, suitable cable is enclosed
- 2 USB 3.0 ports
- 6 RJ45 Ethernet ports
- 2 SFP Ethernet ports

- **Back**

- 1 VGA port
- 1 power supply

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

5.2.2 Utilizing the Serial Port

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

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

In Linux the command `screen` can be used in the command line to access the serial port by passing the device providing the serial port as parameter:

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



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

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

In Microsoft Windows the PuTTY⁵ application can be used. After starting it, the options as shown in Fig. 5.14 and the appropriate serial port have to be selected.

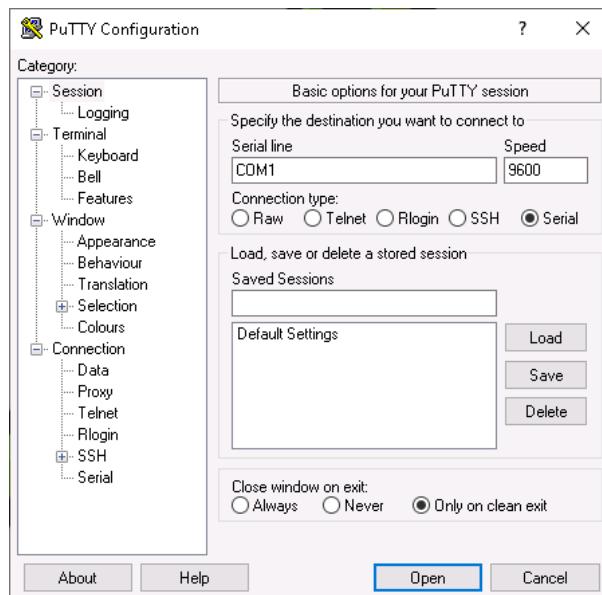


Fig. 5.14: Setting up the serial port in PuTTY

5.2.3 Starting the Appliance

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

The appliance will boot and after short time – depending on the exact model – the first messages will be displayed in the terminal application.

⁵ <https://www.chiark.greenend.org.uk/~sgtatham/putty/>



5.2.4 Performing a General System Setup

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

When the GSM is delivered by Greenbone Networks or after a factory reset, the GOS administration menu shows the first setup wizard after logging in to assist with the basic GOS configuration (see Fig. 5.15).

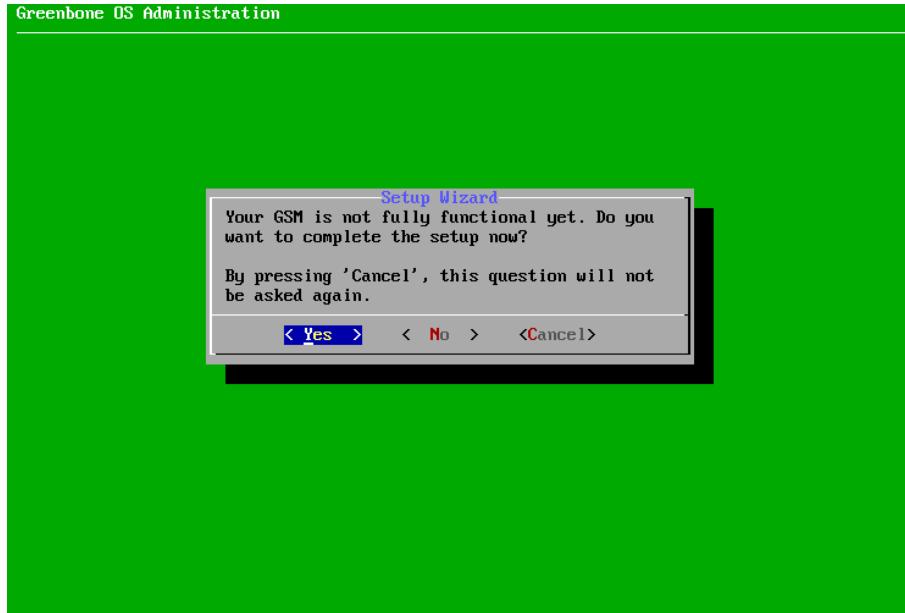


Fig. 5.15: Using the first setup wizard

By selecting *Yes* and pressing `Enter` the first setup wizard is opened and can be used as follows:

Note: By selecting *No* and pressing `Enter` the wizard can be closed. Steps which have not been completed yet are displayed when logging in again.

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

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

In case of a factory reset, all steps have to be carried out (see 20.8 (page 456)).

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

1. Configuring the Network

The network must be set up for the appliance to be fully functional. If there is no IP address configured, it is asked whether the network settings should be adjusted (see Fig. 5.16).

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

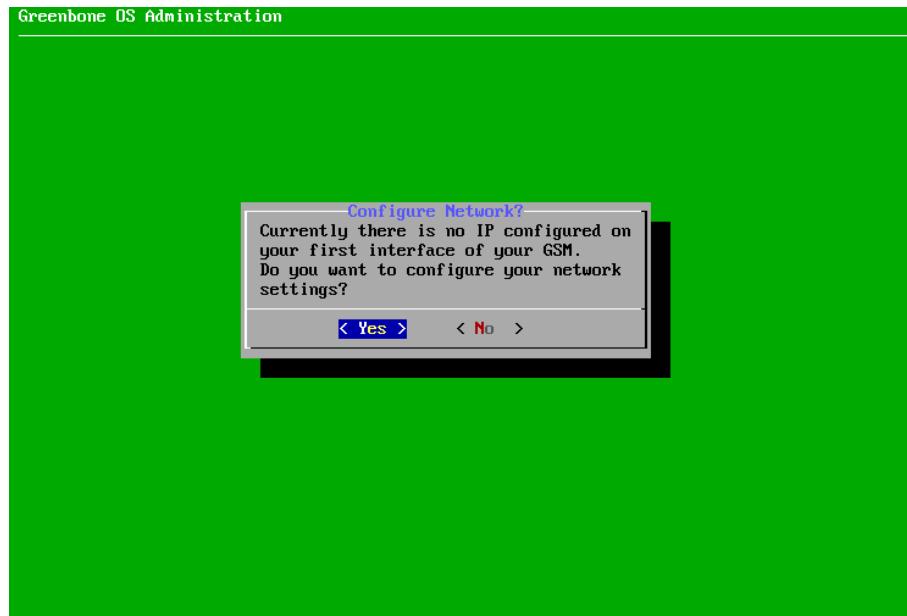


Fig. 5.16: Configuring the network settings

3. Select the desired interface and press Enter.

Note: Using interface eth0 is recommended.

If there is only one interface, the configuration of this interface is opened directly.

→ The interface can be configured.

4. If DHCP should be used, select *DHCP* (for IPv4 or IPv6) and press Enter (see Fig. 5.17).

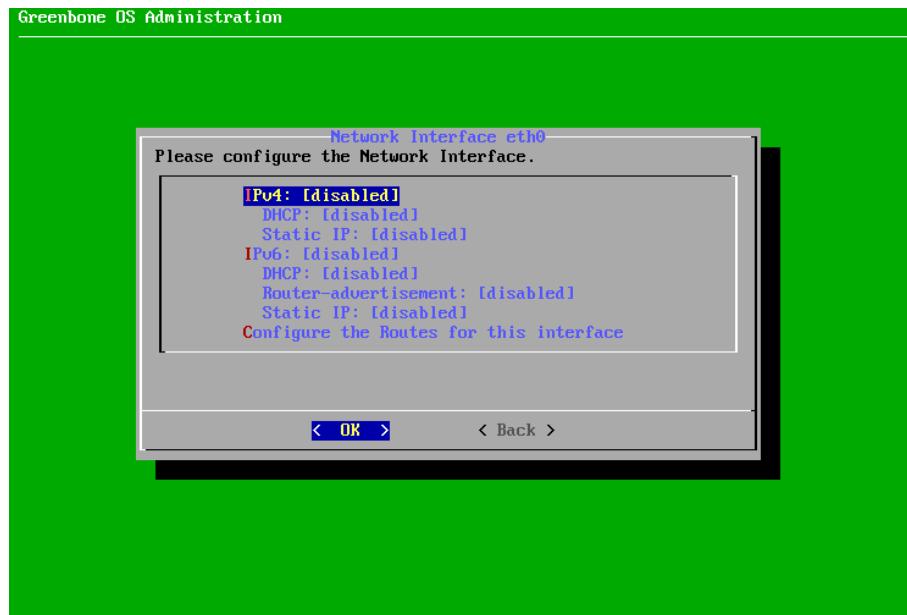


Fig. 5.17: Configuring the network interface

5. Select *Save* and press Enter.



6. Select *Back* and press *Enter*.
7. Select *Ready* and press *Enter*.
or
4. If a static IP address should be used, select *Static IP* (for IPv4 or IPv6) and press *Enter*.
5. Enter the IP address including the prefix length in the input box (see Fig. 5.18).

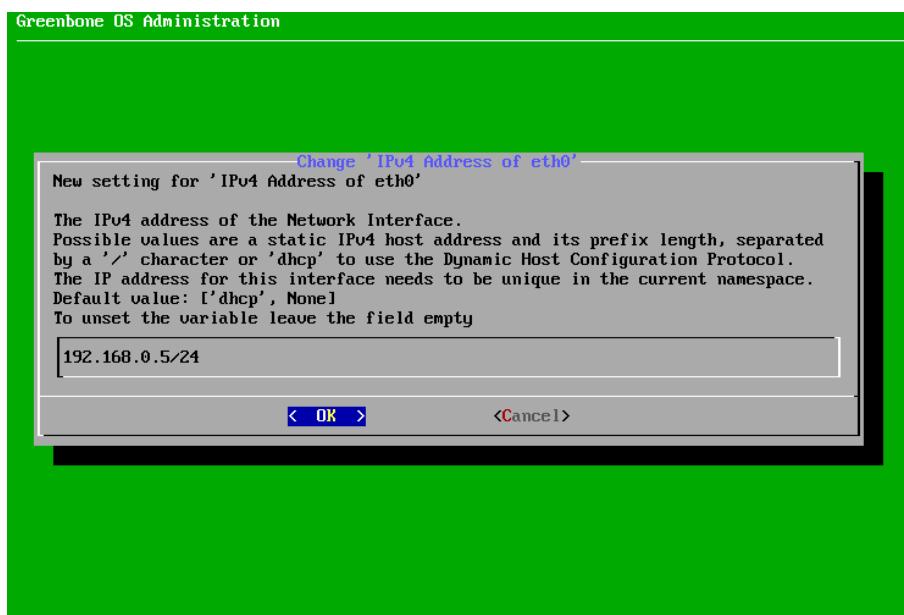


Fig. 5.18: Entering a static IP address

6. Press *Enter*.
→ A message informs that the changes have to be saved.
7. Press *Enter* to close the message.
8. Select *Save* and press *Enter*.
9. Select *Back* and press *Enter*.
10. Select *Ready* and press *Enter*.

2. Importing or Generating an HTTPS Certificate

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

1. Select *Import* and press *Enter* (see Fig. 5.19).
→ A message informs that a PKCS#12 file can be imported.
2. Select *Continue* and press *Enter*.
3. Open the web browser and enter the displayed URL.
4. Click *Browse...*, select the PKCS#12 file and click *Upload*.
→ When the certificate is retrieved by the GSM, the GOS administration menu displays the fingerprint of the certificate for verification.
5. Check the fingerprint and confirm the certificate by pressing *Enter*.
or

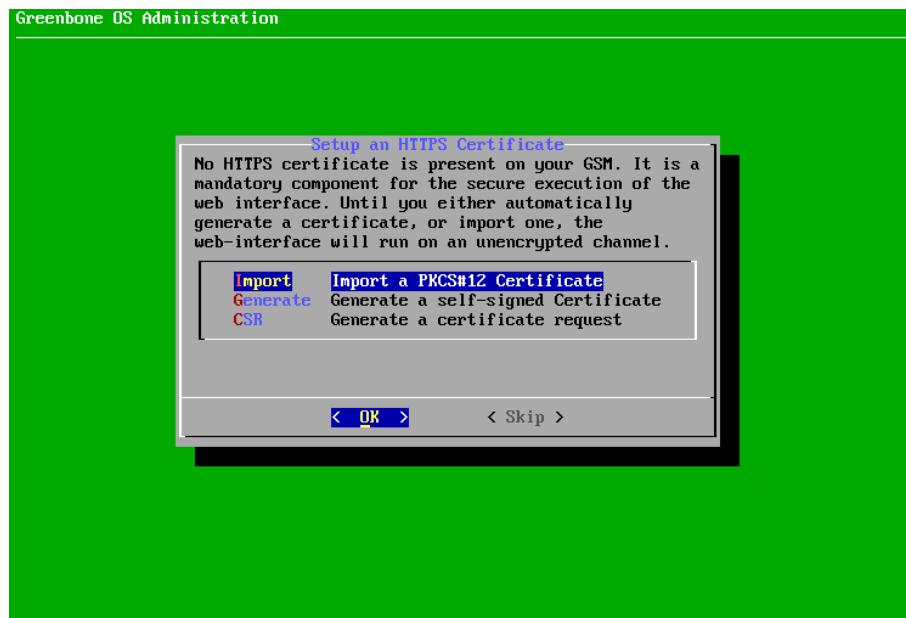


Fig. 5.19: Importing or generating an HTTPS certificate

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

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

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

3. Provide the settings for the certificate (see Fig. 5.20).

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

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

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

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

Note: The download is not done in the first setup wizard, but in the later GOS administration menu as described in Chapter 7.2.4.1.4.1 (page 149), steps 1 – 4 and 9 – 13.

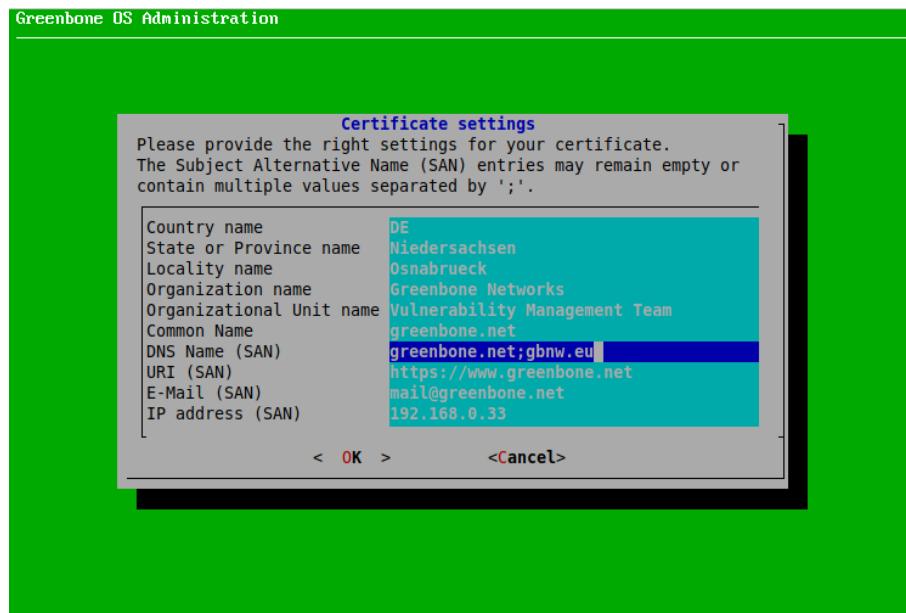


Fig. 5.20: Entering information for the certificate

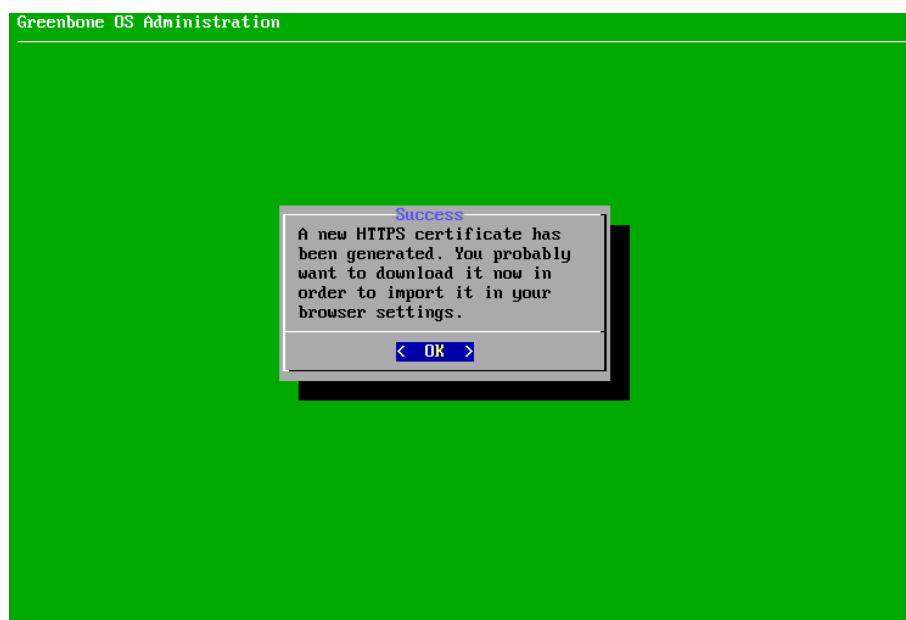


Fig. 5.21: Completing the HTTPS certificate



or

1. Select *CSR* and press *Enter*.
→ A message informs that a key pair and a certificate request are created.
2. Select *Continue* and press *Enter*.
3. Provide the settings for the certificate.

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

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

4. Select *OK* and press *Enter*.
5. Open the web browser and enter the displayed URL.
6. Download the PEM file.
→ The GOS administration menu displays a message to verify that the CSR has not been tampered with.
7. Verify the information by pressing *Enter*.

Note: When the certificate is signed it has to be uploaded to the GSM. The upload is not done in the first setup wizard, but in the later GOS administration menu as described in Chapter 7.2.4.1.4.2 (page 150), steps 1 – 4 and 11 – 14.



3. Creating a Web Administrator

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

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

The first web administrator (web user) that is created is automatically the Feed Import Owner (see Chapter 7.2.1.9 (page 130)).

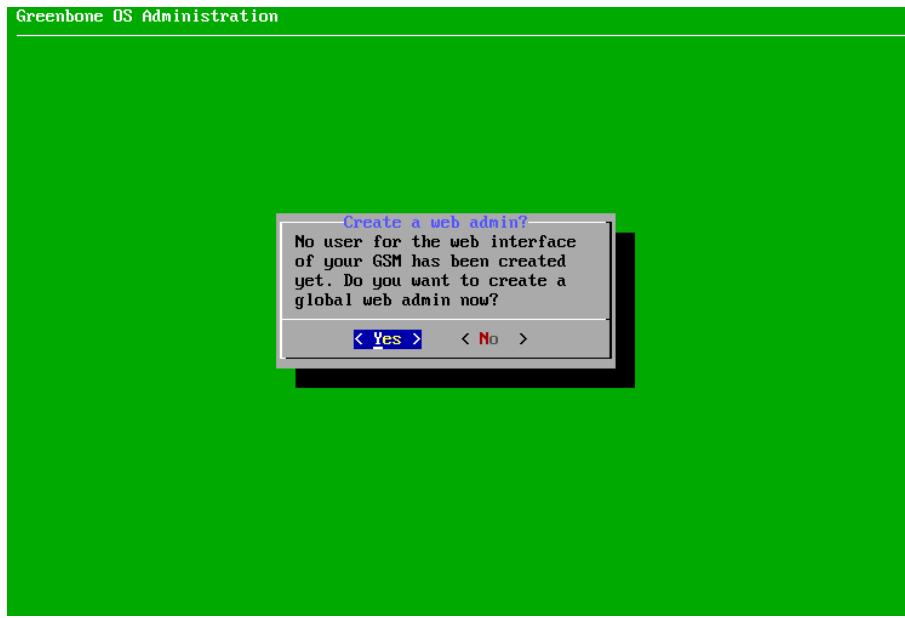


Fig. 5.22: Creating a web administrator

1. Select **Yes** and press **Enter**.
2. Enter the user name for the web administrator.
3. Enter the password for the web administrator twice.
4. Select **OK** and press **Enter**.
→ A message informs that the web administrator has been created.
5. Press **Enter** to close the message.



4. Entering or Uploading a Greenbone Security Feed (GSF) Subscription Key

If no valid GSF subscription key is stored on the appliance, the appliance only uses the public Greenbone Community Feed (GCF) and not the GSF. A GSF subscription key can be entered or uploaded as follows:

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

→ The editor is opened.



Fig. 5.23: Entering or uploading a GSF subscription key

2. Enter the subscription key.

3. Press **Ctrl + X**.

4. Press **Y** to save the changes.

5. Press **Enter**.

or

1. Select *HTTP Upload* and press **Enter**.

2. Open the web browser and enter the displayed URL.

3. Click *Browse...*, select the subscription key and click *Upload*.



5. Downloading the Feed

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

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

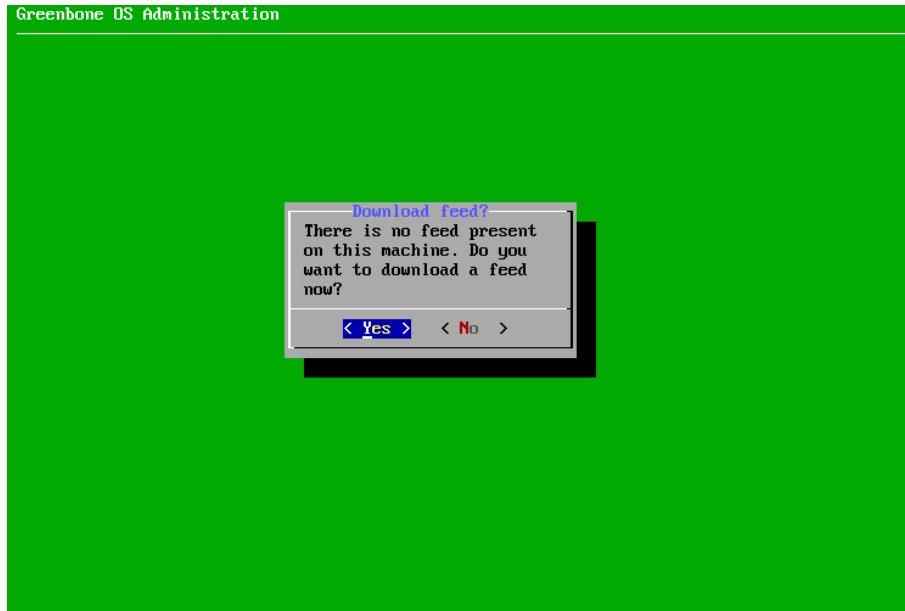


Fig. 5.24: Downloading the feed

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

2. Press Enter to close the message.

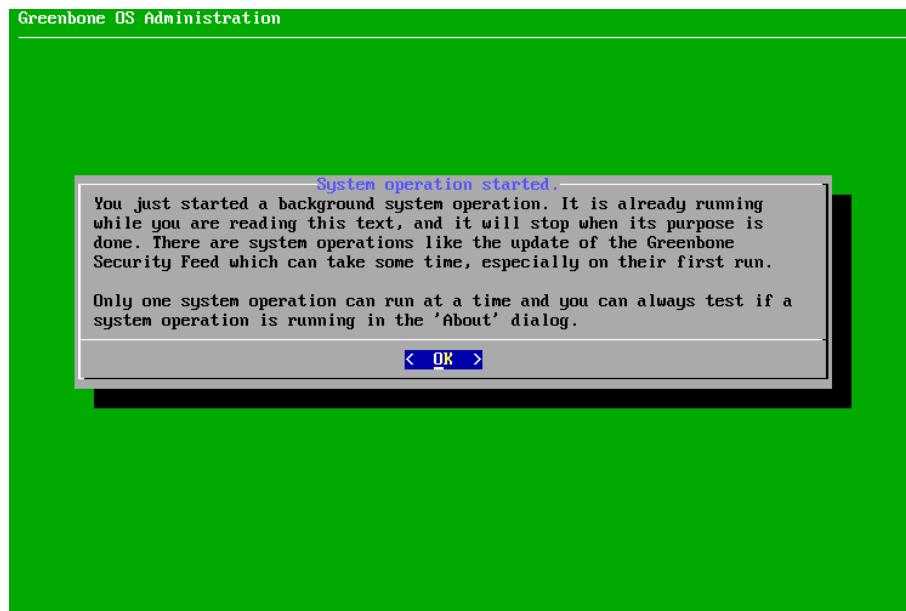


Fig. 5.25: Downloading the feed

6. Finishing the First Setup Wizard

Note: After the last step, a status check is performed. A message shows the result (see Fig. 5.26).

After closing the message by pressing **Enter** the GOS administration menu can be used as described in Chapter 7 (page 120).

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

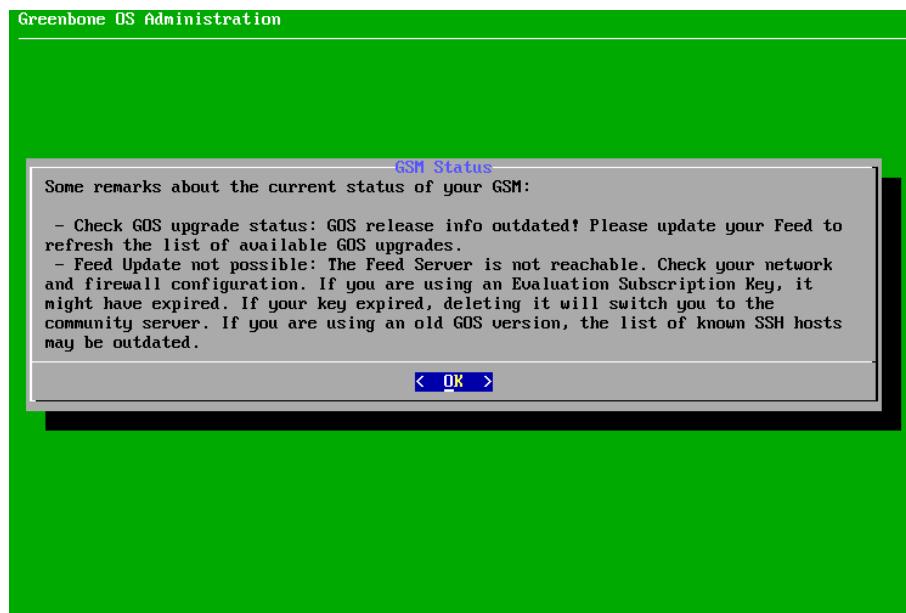


Fig. 5.26: Result of the status check



5.2.5 Logging into the Web Interface

The main interface of the GSM is the web interface, also called Greenbone Security Assistant (GSA). The web interface can be accessed as described in Chapter 8.1 (page 200).



5.3 GSM 150

This setup guide shows the steps required to put a GSM 150 appliance into operation.

The following checklist can be used to monitor the progress:

Step	Done
Power supply established (1 connector)	
Networking cables connected	
Console access established	
Keyboard layout selected	
IP address configured	
DNS server configured	
SSH service enabled (optional)	
SSL certificate created	
Web user account created	
GOS selfcheck run	

5.3.1 Installing the Appliance

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

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

For cabling the GSM 150 appliance has corresponding connectors at the front and back:

- **Front**

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

- **Back**

- 1 power supply

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

5.3.2 Utilizing the Serial Port

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

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

In Linux the command `screen` can be used in the command line to access the serial port by passing the device providing the serial port as parameter:

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



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

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

In Microsoft Windows the PuTTY⁶ application can be used. After starting it, the options as shown in Fig. 5.27 and the appropriate serial port have to be selected.

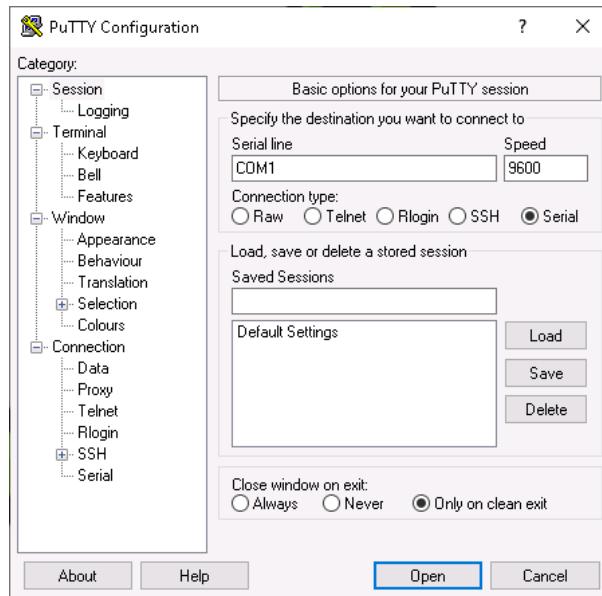


Fig. 5.27: Setting up the serial port in PuTTY

5.3.3 Starting the Appliance

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

The appliance will boot and after short time – depending on the exact model – the first messages will be displayed in the terminal application.

⁶ <https://www.chiark.greenend.org.uk/~sgtatham/putty/>



5.3.4 Performing a General System Setup

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

When the GSM is delivered by Greenbone Networks or after a factory reset, the GOS administration menu shows the first setup wizard after logging in to assist with the basic GOS configuration (see Fig. 5.28).

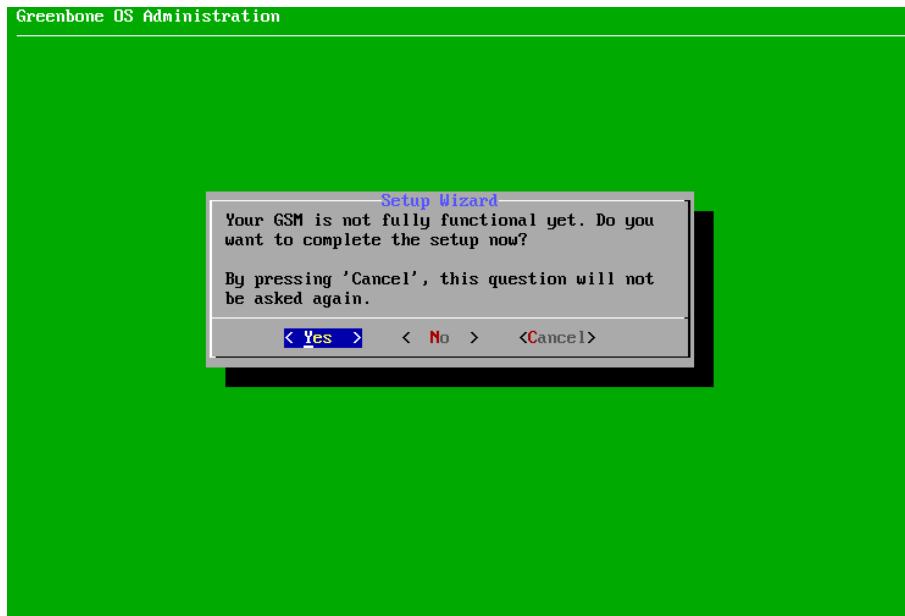


Fig. 5.28: Using the first setup wizard

By selecting *Yes* and pressing `Enter` the first setup wizard is opened and can be used as follows:

Note: By selecting *No* and pressing `Enter` the wizard can be closed. Steps which have not been completed yet are displayed when logging in again.

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

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

In case of a factory reset, all steps have to be carried out (see 20.8 (page 456)).

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

1. Configuring the Network

The network must be set up for the appliance to be fully functional. If there is no IP address configured, it is asked whether the network settings should be adjusted (see Fig. 5.29).

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

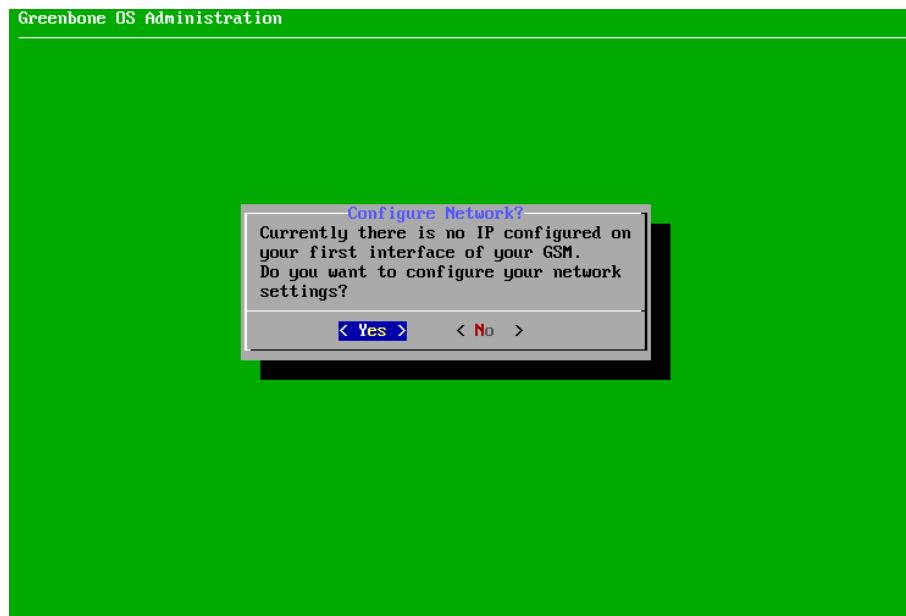


Fig. 5.29: Configuring the network settings

3. Select the desired interface and press Enter.

Note: Using interface eth0 is recommended.

If there is only one interface, the configuration of this interface is opened directly.

→ The interface can be configured (see Fig. 5.30).

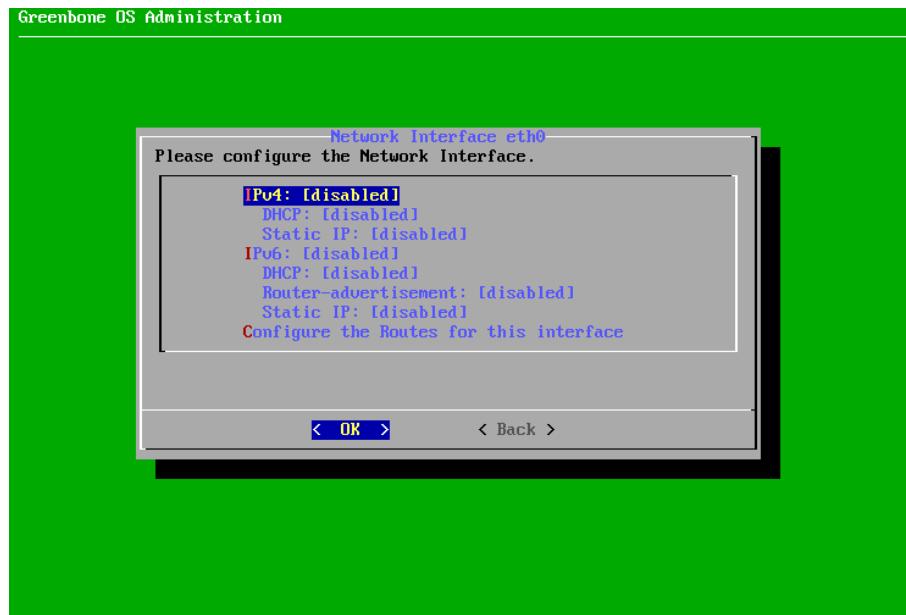


Fig. 5.30: Configuring the network interface

4. If DHCP should be used, select *DHCP* (for IPv4 or IPv6) and press Enter.
5. Select *Save* and press Enter.



6. Select *Back* and press *Enter*.
7. Select *Ready* and press *Enter*.
or
4. If a static IP address should be used, select *Static IP* (for IPv4 or IPv6) and press *Enter*.
5. Enter the IP address including the prefix length in the input box (see Fig. 5.31).

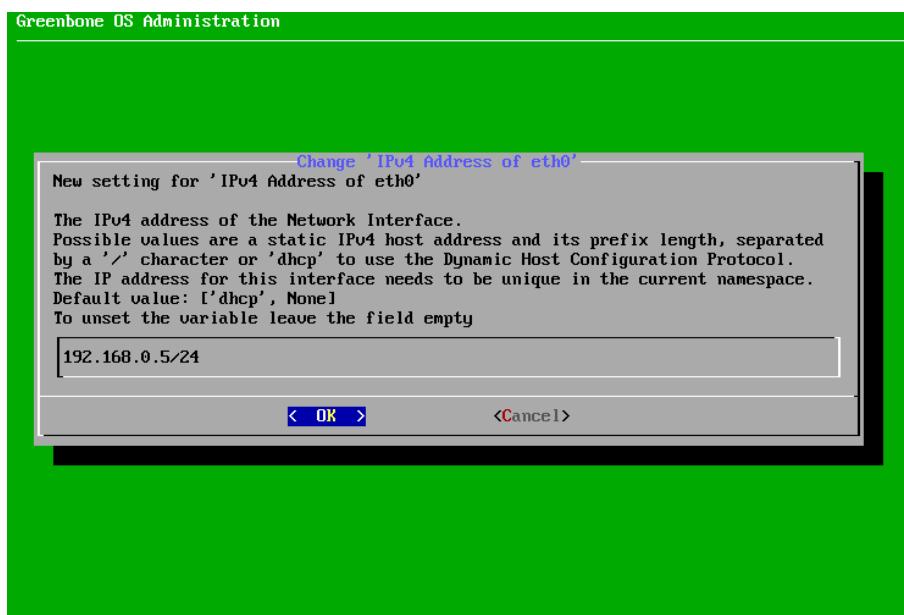


Fig. 5.31: Entering a static IP address

6. Press *Enter*.
→ A message informs that the changes have to be saved.
7. Press *Enter* to close the message.
8. Select *Save* and press *Enter*.
9. Select *Back* and press *Enter*.
10. Select *Ready* and press *Enter*.

2. Importing or Generating an HTTPS Certificate

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

1. Select *Import* and press *Enter* (see Fig. 5.32).
→ A message informs that a PKCS#12 file can be imported.
2. Select *Continue* and press *Enter*.
3. Open the web browser and enter the displayed URL.
4. Click *Browse...*, select the PKCS#12 file and click *Upload*.
→ When the certificate is retrieved by the GSM, the GOS administration menu displays the fingerprint of the certificate for verification.

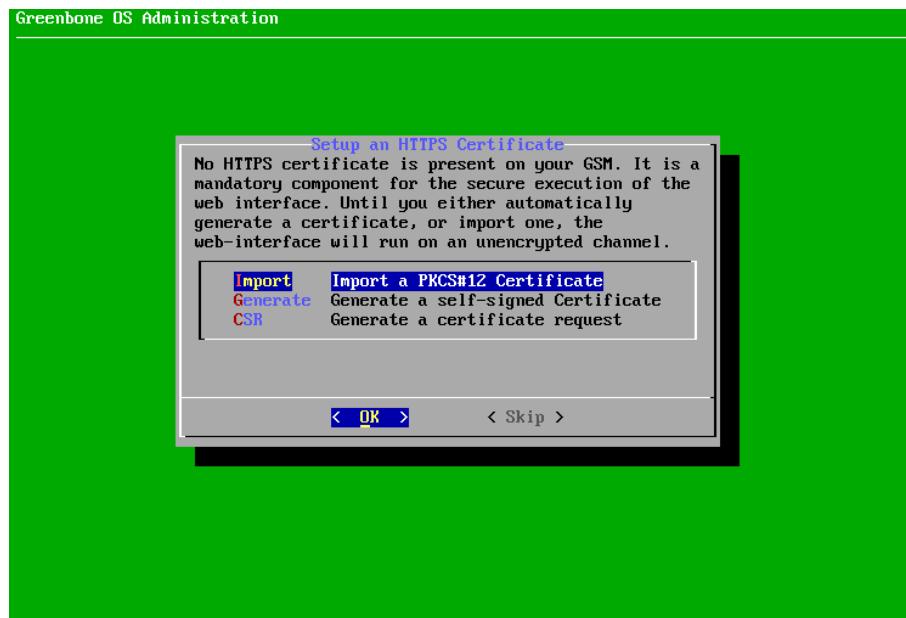


Fig. 5.32: Importing or generating an HTTPS certificate

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

or

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

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

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

3. Provide the settings for the certificate (see Fig. 5.33).

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

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

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

→ A message informs that the certificate is created and can be downloaded (see Fig. 5.34).

Note: The download is not done in the first setup wizard, but in the later GOS administration menu as described in Chapter 7.2.4.1.4.1 (page 149), steps 1 – 4 and 9 – 13.

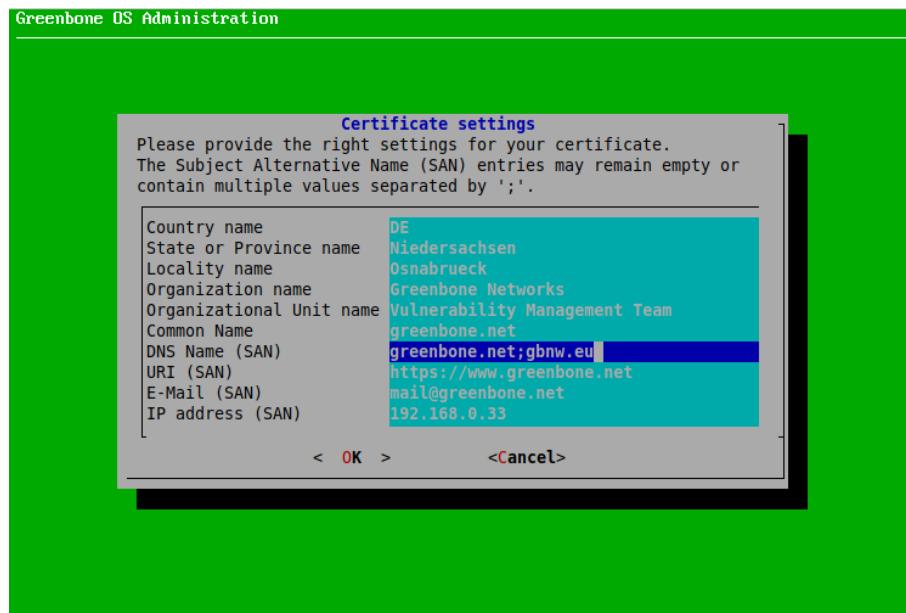


Fig. 5.33: Entering information for the certificate

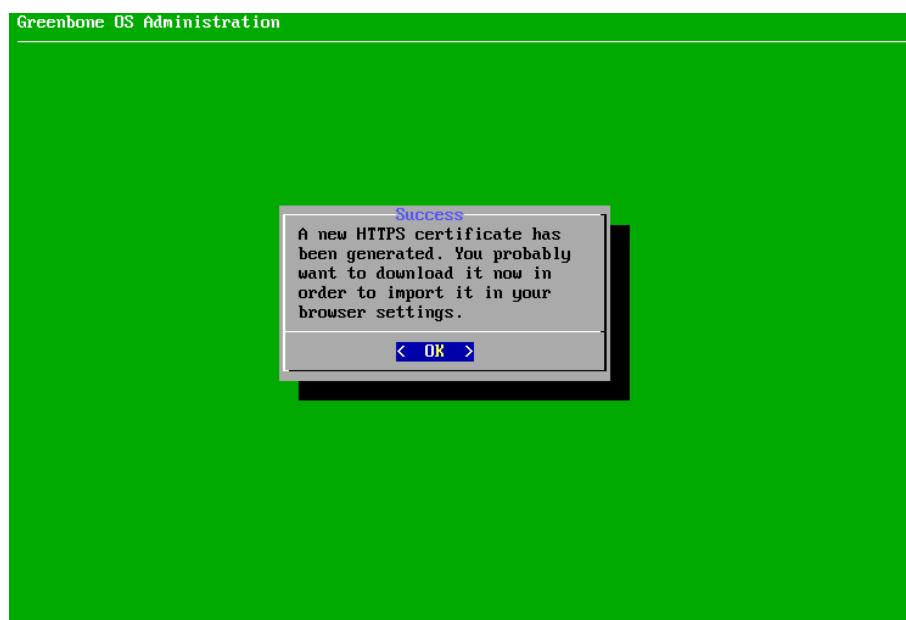


Fig. 5.34: Completing the HTTPS certificate



or

1. Select *CSR* and press *Enter*.
→ A message informs that a key pair and a certificate request are created.
2. Select *Continue* and press *Enter*.
3. Provide the settings for the certificate.

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

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

4. Select *OK* and press *Enter*.
5. Open the web browser and enter the displayed URL.
6. Download the PEM file.
→ The GOS administration menu displays a message to verify that the CSR has not been tampered with.
7. Verify the information by pressing *Enter*.

Note: When the certificate is signed it has to be uploaded to the GSM. The upload is not done in the first setup wizard, but in the later GOS administration menu as described in Chapter 7.2.4.1.4.2 (page 150), steps 1 – 4 and 11 – 14.



3. Creating a Web Administrator

If there is no web administrator, it is asked whether such an account should be created (see Fig. 5.35).

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

The first web administrator (web user) that is created is automatically the Feed Import Owner (see Chapter 7.2.1.9 (page 130)).

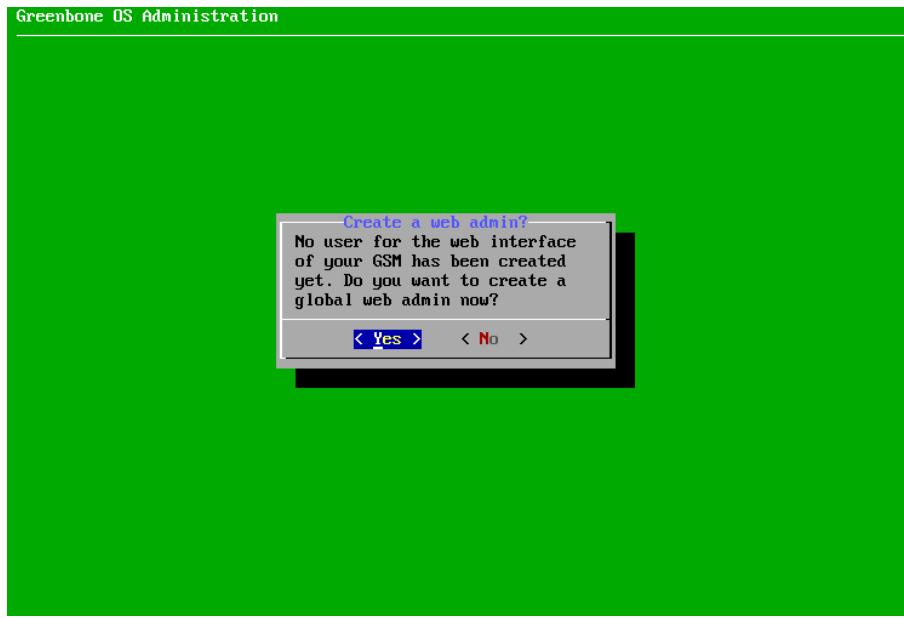


Fig. 5.35: Creating a web administrator

1. Select **Yes** and press **Enter**.
2. Enter the user name for the web administrator.
3. Enter the password for the web administrator twice.
4. Select **OK** and press **Enter**.
→ A message informs that the web administrator has been created.
5. Press **Enter** to close the message.



4. Entering or Uploading a Greenbone Security Feed (GSF) Subscription Key

If no valid GSF subscription key is stored on the appliance, the appliance only uses the public Greenbone Community Feed (GCF) and not the GSF. A GSF subscription key can be entered or uploaded as follows:

1. Select *Editor* and press **Enter** (see Fig. 5.36).

→ The editor is opened.



Fig. 5.36: Entering or uploading a GSF subscription key

2. Enter the subscription key.

3. Press **Ctrl + X**.

4. Press **Y** to save the changes.

5. Press **Enter**.

or

1. Select *HTTP Upload* and press **Enter**.

2. Open the web browser and enter the displayed URL.

3. Click *Browse...*, select the subscription key and click *Upload*.



5. Downloading the Feed

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

1. Select Yes and press Enter (see Fig. 5.37).

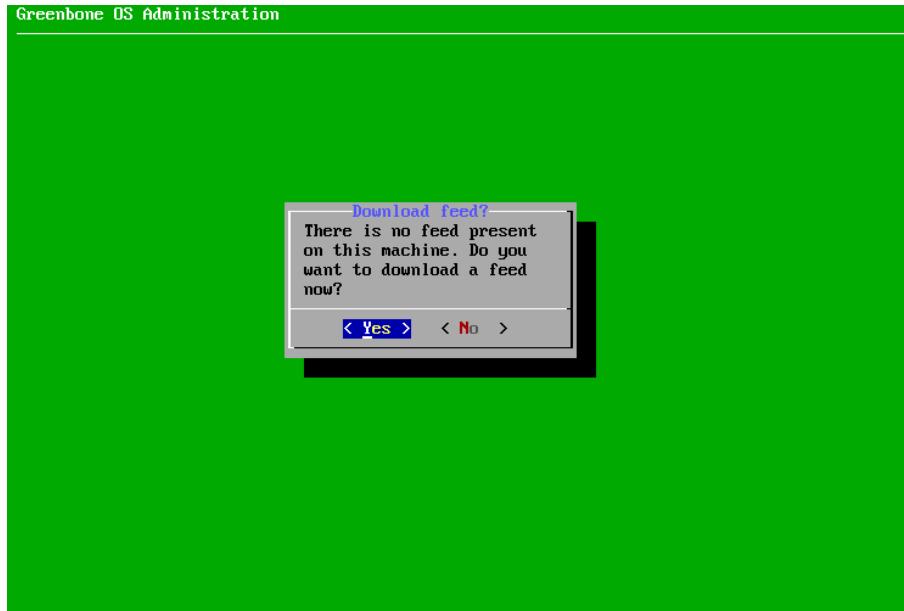


Fig. 5.37: Downloading the feed

→ A message informs that the feed update was started in the background (see Fig. 5.38).

2. Press Enter to close the message.

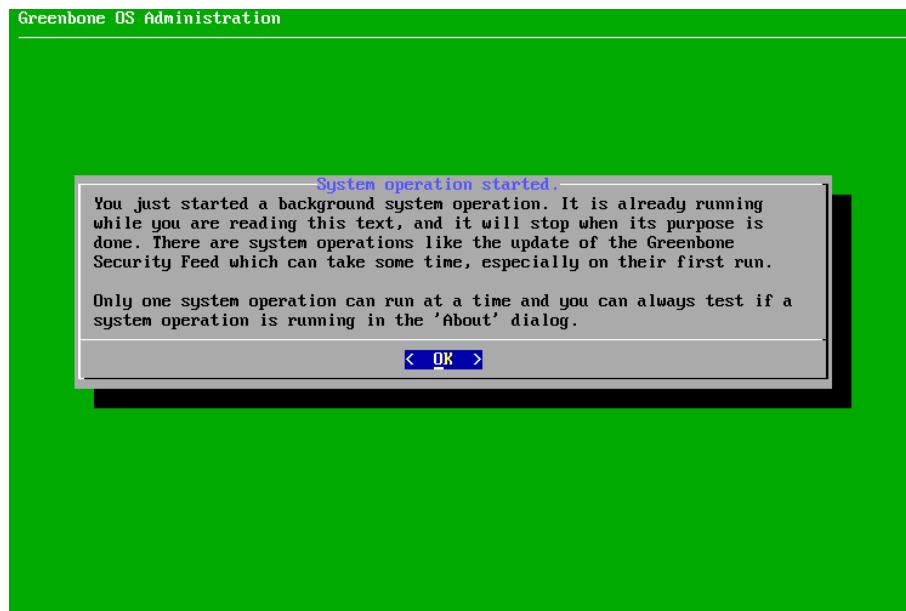


Fig. 5.38: Downloading the feed

6. Finishing the First Setup Wizard

Note: After the last step, a status check is performed. A message shows the result (see Fig. 5.39).

After closing the message by pressing **Enter** the GOS administration menu can be used as described in Chapter 7 (page 120).

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

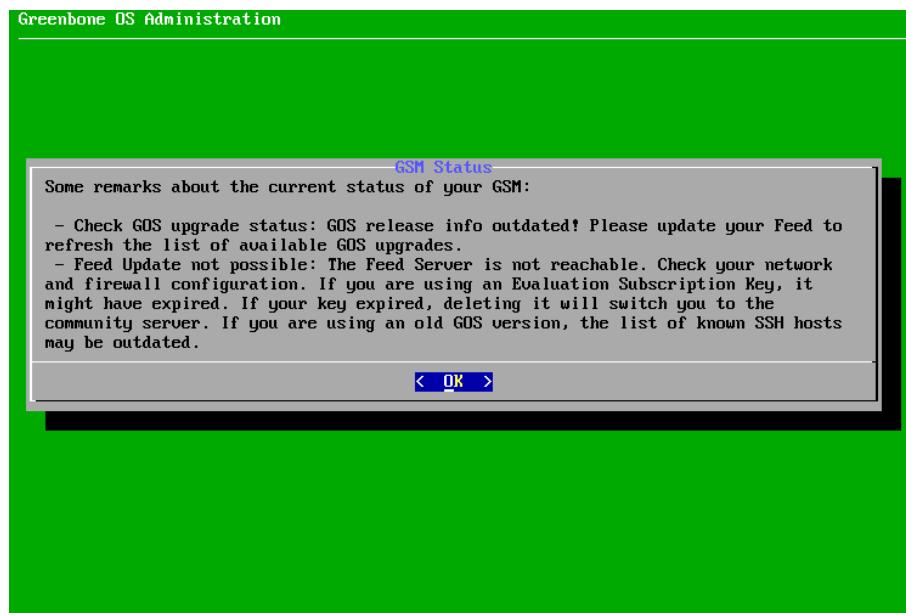


Fig. 5.39: Result of the status check



5.3.5 Logging into the Web Interface

The main interface of the GSM is the web interface, also called Greenbone Security Assistant (GSA). The web interface can be accessed as described in Chapter 8.1 (page 200).



5.4 GSM 35

This setup guide shows the steps required to put a GSM 35 sensor appliance into operation.

The following checklist can be used to monitor the progress:

Step	Done
Power supply established (1 connector)	
Networking cables connected	
Console access established	
Keyboard layout selected	
IP address configured	
DNS server configured	
SSH service enabled (optional)	
SSL certificate created	
GOS selfcheck run	

5.4.1 Installing the Appliance

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

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

For cabling the GSM 35 appliance has corresponding connectors at the front and back:

- **Front**

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

- **Back**

- 1 power supply

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

5.4.2 Utilizing the Serial Port

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

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

In Linux the command `screen` can be used in the command line to access the serial port by passing the device providing the serial port as parameter:

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



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

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

In Microsoft Windows the PuTTY⁷ application can be used. After starting it, the options as shown in Fig. 5.40 and the appropriate serial port have to be selected.

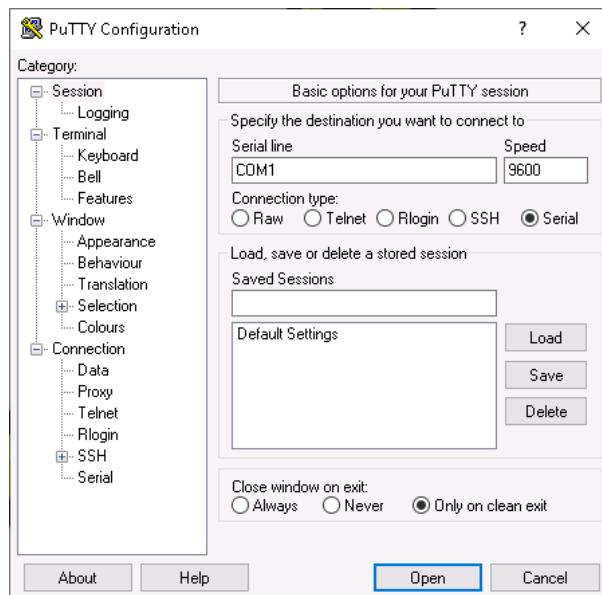


Fig. 5.40: Setting up the serial port in PuTTY

5.4.3 Starting the Appliance

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

The appliance will boot and after short time – depending on the exact model – the first messages will be displayed in the terminal application.

⁷ <https://www.chiark.greenend.org.uk/~sgtatham/putty/>



5.4.4 Performing a General System Setup

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

However, since the GSM 35 is a dedicated sensor, the master key has to be exchanged with the sensor.

When the GSM is delivered by Greenbone Networks or after a factory reset, the GOS administration menu shows the first setup wizard after logging in to assist with the basic GOS configuration (see Fig. 5.41).

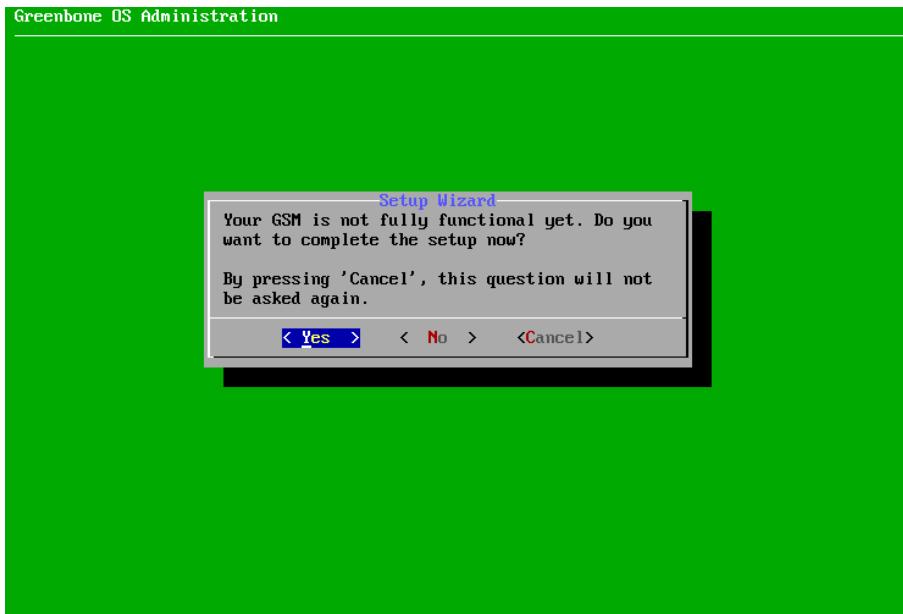


Fig. 5.41: Using the first setup wizard

By selecting *Yes* and pressing `Enter` the first setup wizard is opened and can be used as follows:

Note: By selecting *No* and pressing `Enter` the wizard can be closed. Steps which have not been completed yet are displayed when logging in again.

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

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

In case of a factory reset, all steps have to be carried out (see 20.8 (page 456)).

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

1. Configuring the Network

The network must be set up for the appliance to be fully functional. If there is no IP address configured, it is asked whether the network settings should be adjusted (see Fig. 5.42).

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

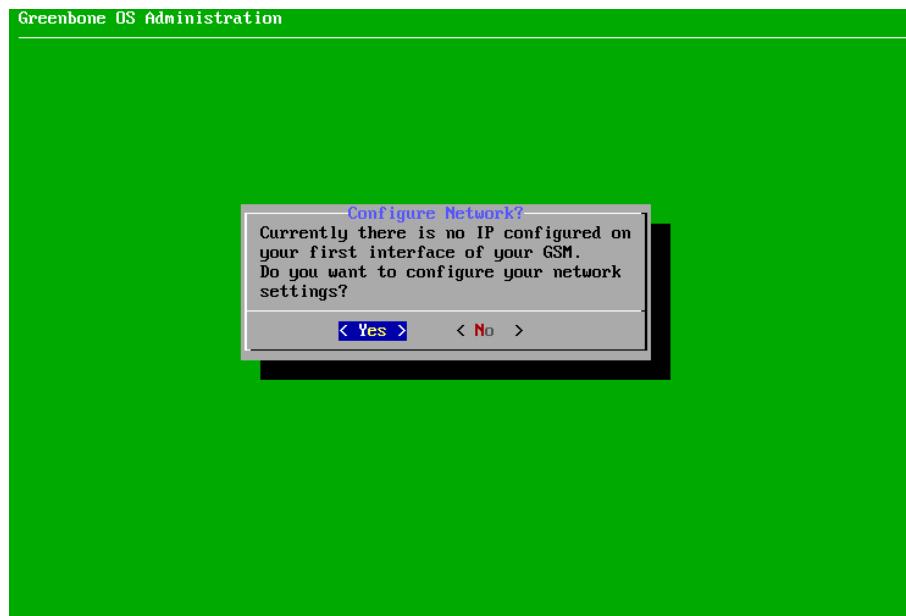


Fig. 5.42: Configuring the network settings

3. Select the desired interface and press Enter.

Note: Using interface eth0 is recommended.

If there is only one interface, the configuration of this interface is opened directly.

→ The interface can be configured (see Fig. 5.43).

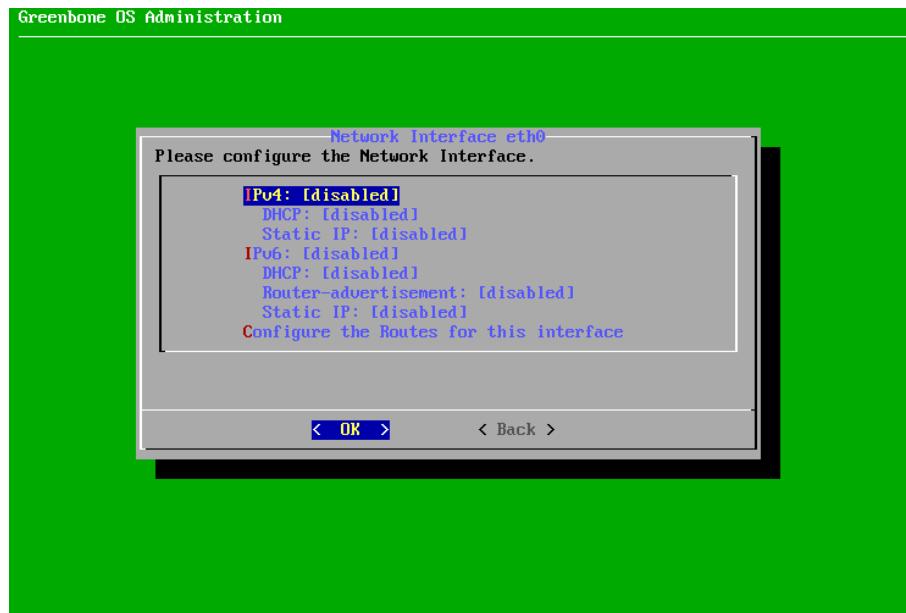


Fig. 5.43: Configuring the network interface

4. If DHCP should be used, select *DHCP* (for IPv4 or IPv6) and press Enter.
5. Select *Save* and press Enter.



6. Select *Back* and press **Enter**.
7. Select *Ready* and press **Enter**.
or
4. If a static IP address should be used, select *Static IP* (for IPv4 or IPv6) and press **Enter**.
5. Enter the IP address including the prefix length in the input box (see Fig. 5.44).

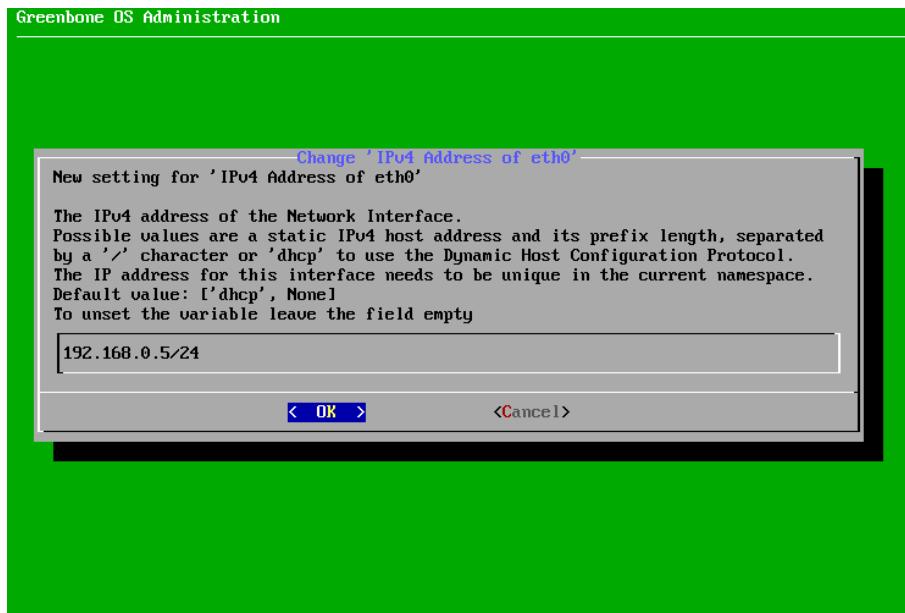


Fig. 5.44: Entering a static IP address

6. Press **Enter**.
→ A message informs that the changes have to be saved.
7. Press **Enter** to close the message.
8. Select *Save* and press **Enter**.
9. Select *Back* and press **Enter**.
10. Select *Ready* and press **Enter**.



2. Importing or Generating an HTTPS Certificate

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

1. Select *Import* and press *Enter* (see Fig. 5.45).
→ A message informs that a PKCS#12 file can be imported.

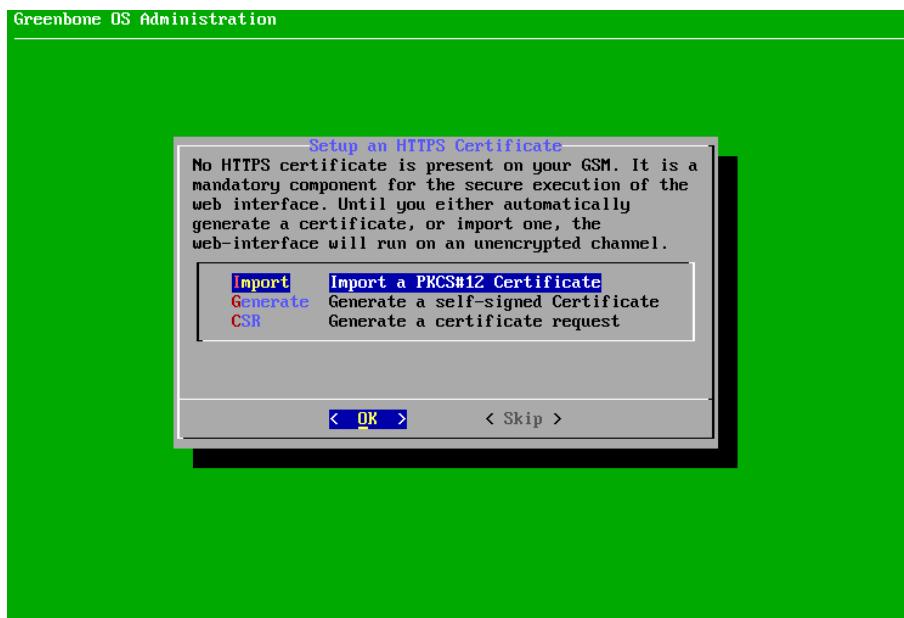


Fig. 5.45: Importing or generating an HTTPS certificate

2. Select *Continue* and press *Enter*.
3. Open the web browser and enter the displayed URL.
4. Click *Browse...*, select the PKCS#12 file and click *Upload*.
→ When the certificate is retrieved by the GSM, the GOS administration menu displays the fingerprint of the certificate for verification.
5. Check the fingerprint and confirm the certificate by pressing *Enter*.



or

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

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

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

3. Provide the settings for the certificate (see Fig. 5.46).

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

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

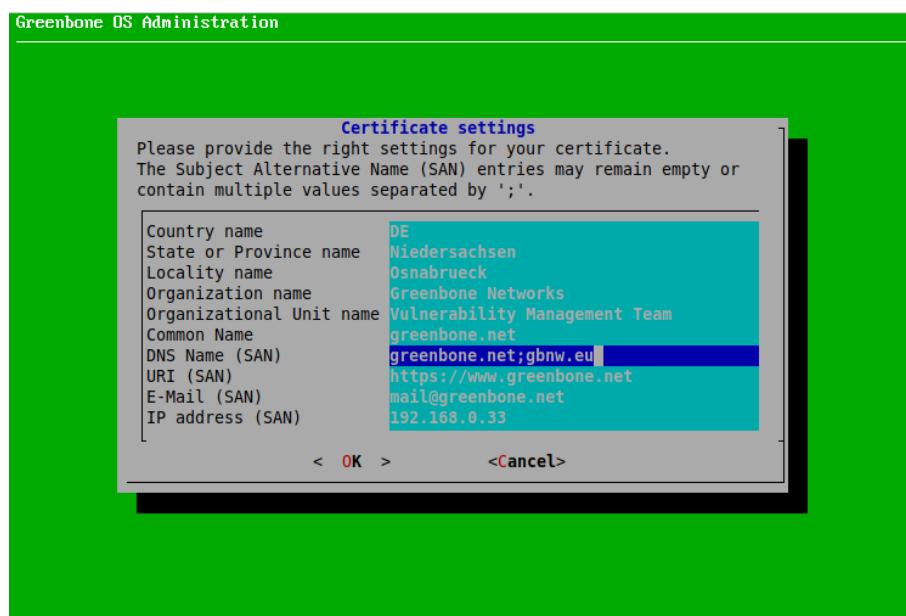


Fig. 5.46: Entering information for the certificate

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

→ A message informs that the certificate is created and can be downloaded (see Fig. 5.47).

Note: The download is not done in the first setup wizard, but in the later GOS administration menu as described in Chapter 7.2.4.1.4.1 (page 149), steps 1 – 4 and 9 – 13.



Fig. 5.47: Completing the HTTPS certificate

or

1. Select *CSR* and press *Enter*.
→ A message informs that a key pair and a certificate request are created.
2. Select *Continue* and press *Enter*.
3. Provide the settings for the certificate.

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

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

-
4. Select *OK* and press *Enter*.
 5. Open the web browser and enter the displayed URL.
 6. Download the PEM file.
→ The GOS administration menu displays a message to verify that the CSR has not been tampered with.
 7. Verify the information by pressing *Enter*.

Note: When the certificate is signed it has to be uploaded to the GSM. The upload is not done in the first setup wizard, but in the later GOS administration menu as described in Chapter 7.2.4.1.4.2 (page 150), steps 1 – 4 and 11 – 14.



3. Entering or Uploading a Greenbone Security Feed (GSF) Subscription Key

If no valid GSF subscription key is stored on the appliance, the appliance only uses the public Greenbone Community Feed (GCF) and not the GSF. A GSF subscription key can be entered or uploaded as follows:

1. Select *Editor* and press **Enter** (see Fig. 5.48).

→ The editor is opened.



Fig. 5.48: Entering or uploading a GSF subscription key

2. Enter the subscription key.

3. Press **Ctrl + X**.

4. Press **Y** to save the changes.

5. Press **Enter**.

or

1. Select *HTTP Upload* and press **Enter**.

2. Open the web browser and enter the displayed URL.

3. Click *Browse...*, select the subscription key and click *Upload*.



4. Downloading the Feed

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

1. Select Yes and press Enter (see Fig. 5.49).

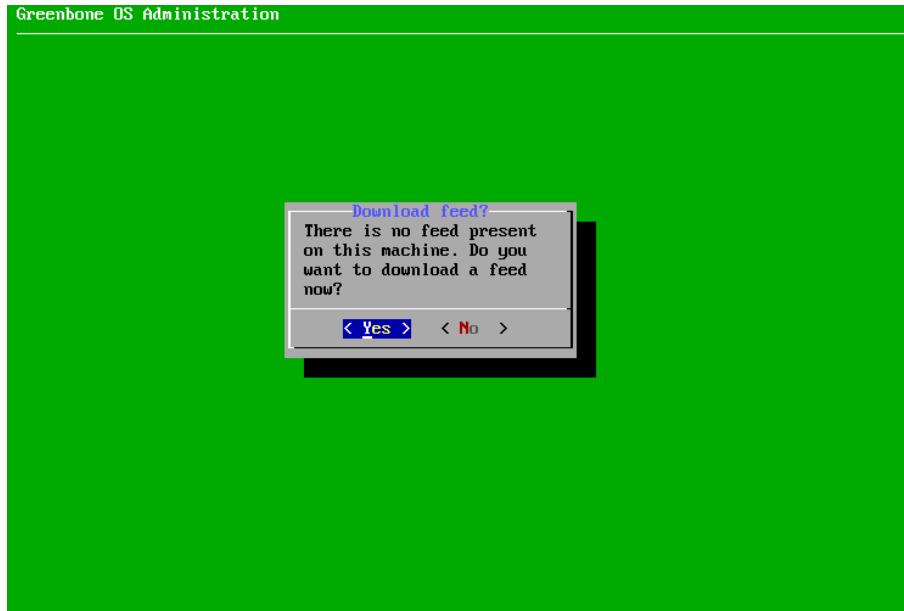


Fig. 5.49: Downloading the feed

→ A message informs that the feed update was started in the background (see Fig. 5.50).

2. Press Enter to close the message.

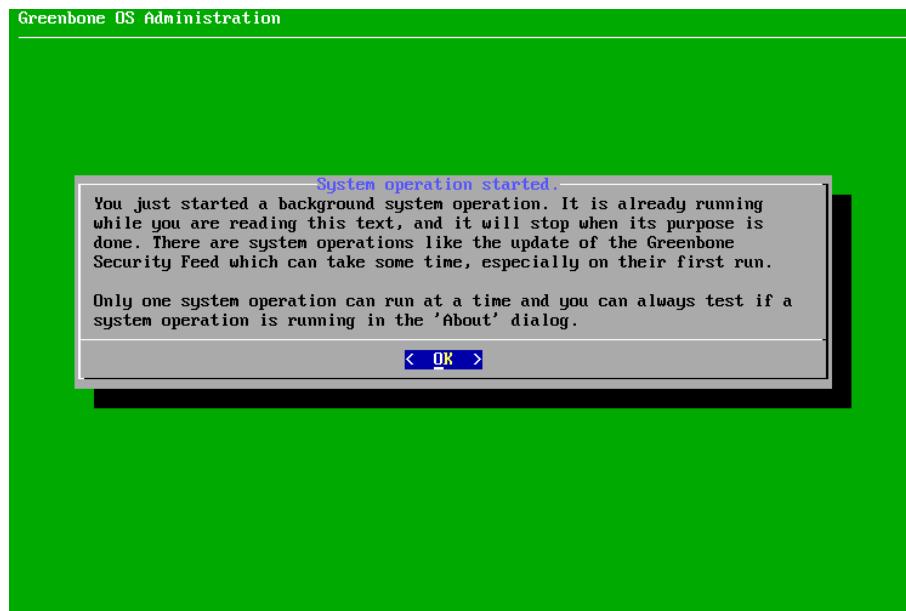


Fig. 5.50: Downloading the feed

5. Finishing the First Setup Wizard

Note: After the last step, a status check is performed. A message shows the result (see Fig. 5.51).

After closing the message by pressing **Enter** the GOS administration menu can be used as described in Chapter 7 (page 120).

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

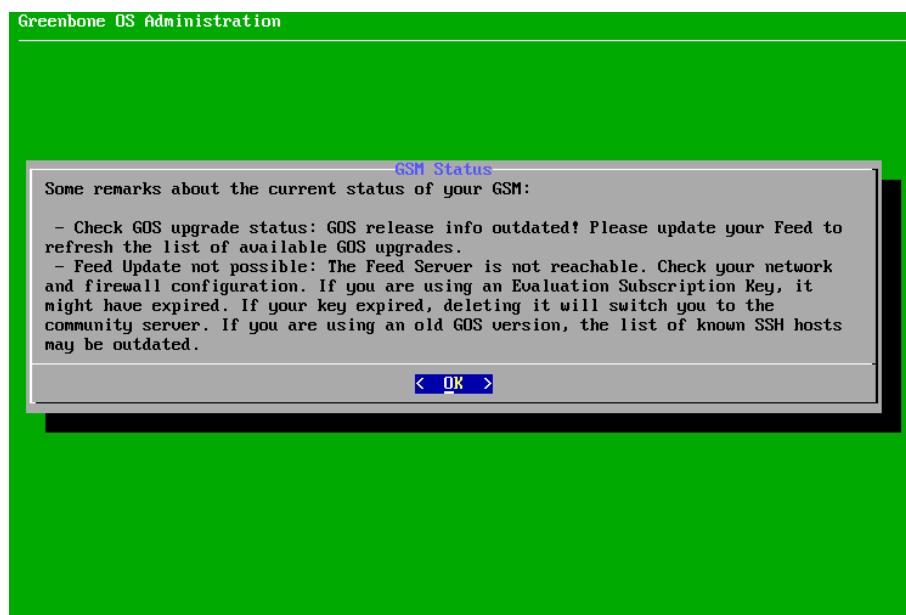


Fig. 5.51: Result of the status check



6. Exchanging the Master Key with the Sensor

Continue with Chapter 16 (page 409) to exchange the keys with the master.

Note: The GSM 35 does not offer any web interface. The sensor is solely managed by the master. Logging into the sensor is possible by using the console and SSH from the master.

If the communication between master and sensor fails, the rule set of any internal firewall governing the network connection may be adjusted.



5.5 GSM CENO/DECA/TERA/PETA/EXA

This setup guide shows the steps required to put a GSM CENO, GSM DECA, GSM TERA, GSM PETA or GSM EXA appliance into operation.

The following checklist can be used to monitor the progress:

Step	Done
Virtual environment installed	
Integrity verified (optional)	
OVA file imported	
Virtual machine settings checked	
Keyboard layout selected	
IP address configured	
DNS server configured	
SSH service enabled (optional)	
SSL certificate created	
Web user account created	
GOS selfcheck run	

5.5.1 Setup Requirements

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

5.5.1.1 Resources

The virtual appliances require at least the following resources:

GSM CENO

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

GSM DECA

- 4 virtual CPUs
- 8 GB RAM
- 140 GB hard disk

GSM TERA

- 6 virtual CPUs
- 8 GB RAM
- 140 GB hard disk

GSM PETA

- 8 virtual CPUs
- 16 GB RAM
- 140 GB hard disk



GSM EXA

- 12 virtual CPUs
- 24 GB RAM
- 140 GB hard disk

5.5.1.2 Supported Hypervisor

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

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

The following hypervisors are officially supported for running a GSM CENO:

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

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

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

5.5.1.3 Verification of Integrity

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

To request the checksum contact the Greenbone Networks Support via e-mail (support@greenbone.net) including the subscription number.

The integrity checksum can be provided via phone or via support portal at <https://support.greenbone.net>. Specify the preferred channel in the e-mail.

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

On Linux systems, the following command for calculating the checksum for the GSM CENO/DECA/TERA/PETA/EXA can be used:

```
sha256sum GSM-CENO-21.04.0-gsf20210430.ova
```

Note: The commands for the other GSM models differ according to the GSM model and the GSF subscription key.

On Microsoft Windows systems, the following command for calculating the checksum for the GSM CENO/DECA/TERA/PETA/EXA can be used in the Windows PowerShell:

```
Get-Filehash 'C:\<path>\GSM-CENO-21.04.0-gsf20210430.ova' -Algorithm SHA256
```

Note: The commands for the other GSM models differ according to the GSM model and the GSF subscription key.



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

5.5.2 Deploying the Appliance

The virtual appliance is provided by Greenbone Networks in the Open Virtualization Appliance (OVA) format. Each GSM CENO/DECA/TERA/PETA/EXA is activated using a unique subscription key.

Note: Cloning the GSM CENO/DECA/TERA/PETA/EXA and using several instances in parallel is not permitted and can result in inconsistencies and unwanted side effects.

To deploy a GSM CENO/DECA/TERA/PETA/EXA, it has to be imported into the hypervisor of choice as follows:

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

The figures show the installation of a GSM CENO. The installation of a GSM DECA/TERA/PETA/EXA is carried out equivalently. File names used in the example differ based on the GSM model and the GSF subscription key.

1. Install VMware ESXi for the current operating system.
2. Open the web interface of the VMware ESXi instance and log in.
3. Click *Virtual Machines* in the *Navigator* column on the left.
4. Click *Create / Register VM*.
5. Select *Deploy a virtual machine from an OVF or OVA file* and click *Next* (see Fig. 5.52).

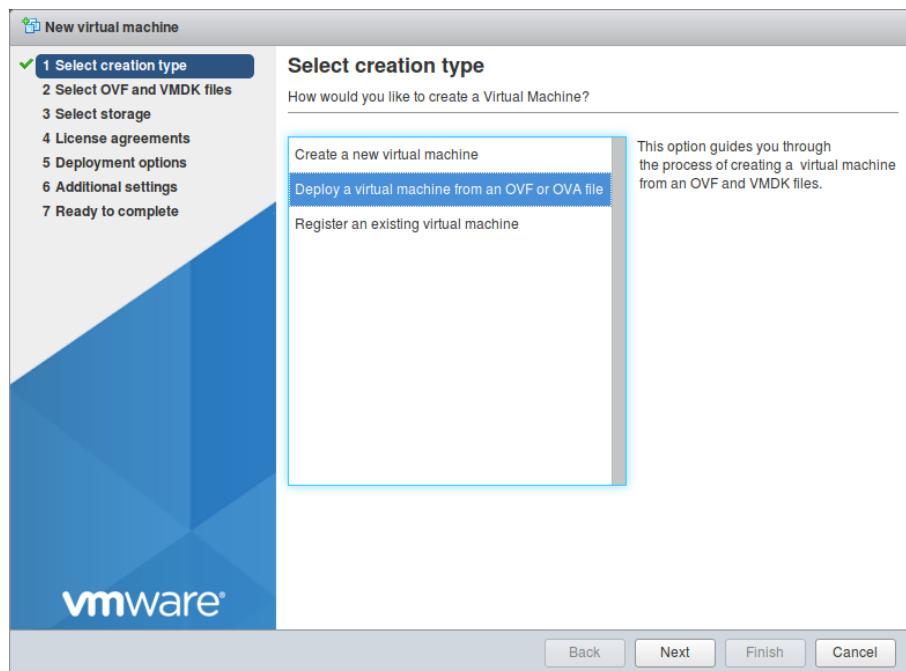


Fig. 5.52: Selecting the creation type

6. Enter a name for the virtual machine in the input box.
7. Click *Click to select files or drag/drop*, select the OVA file of the appliance and click *Next*.



8. Select the storage location in which to store the virtual machine files and click *Next*.
9. Adjust the deployment options as required and click *Next*.

Note: The default deployment settings may be used.

10. Check the configuration of the virtual machine (see Fig. 5.53).

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

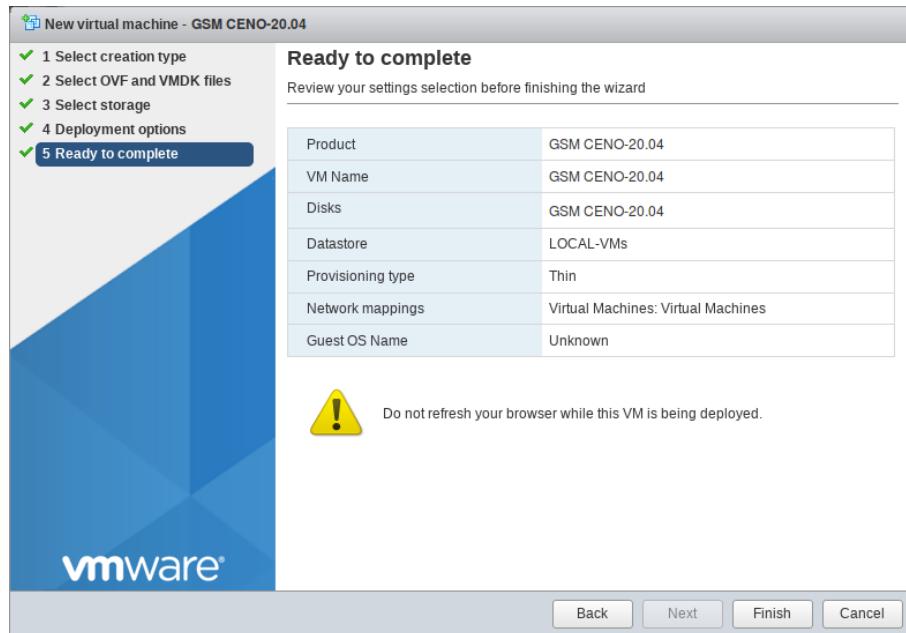


Fig. 5.53: Checking the configuration of the virtual machine

11. Click *Finish*.
→ The appliance is being imported. This can take up to 10 minutes.

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



12. When the appliance is imported, click *Virtual Machines* in the *Navigator* column on the left.
13. Select the appliance in the list and click *Power on* (see Fig. 5.54).

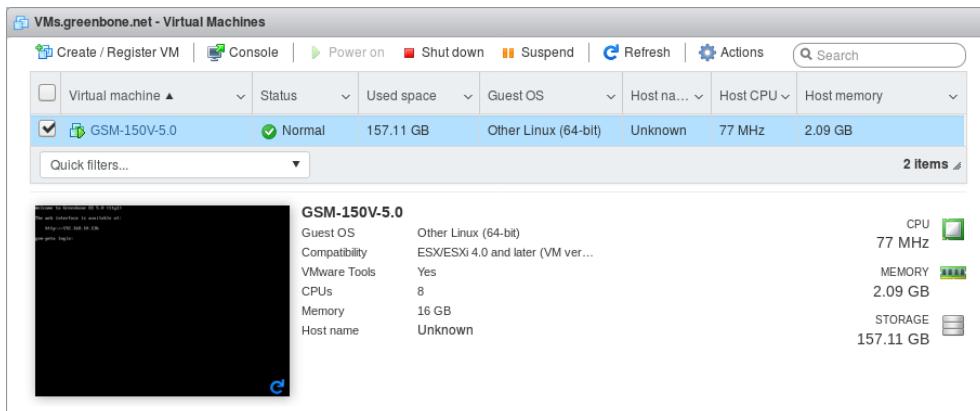


Fig. 5.54: Imported virtual machine

5.5.3 Performing a General System Setup

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

When the GSM is delivered by Greenbone Networks or after a factory reset, the GOS administration menu shows the first setup wizard after logging in to assist with the basic GOS configuration (see Fig. 5.55).

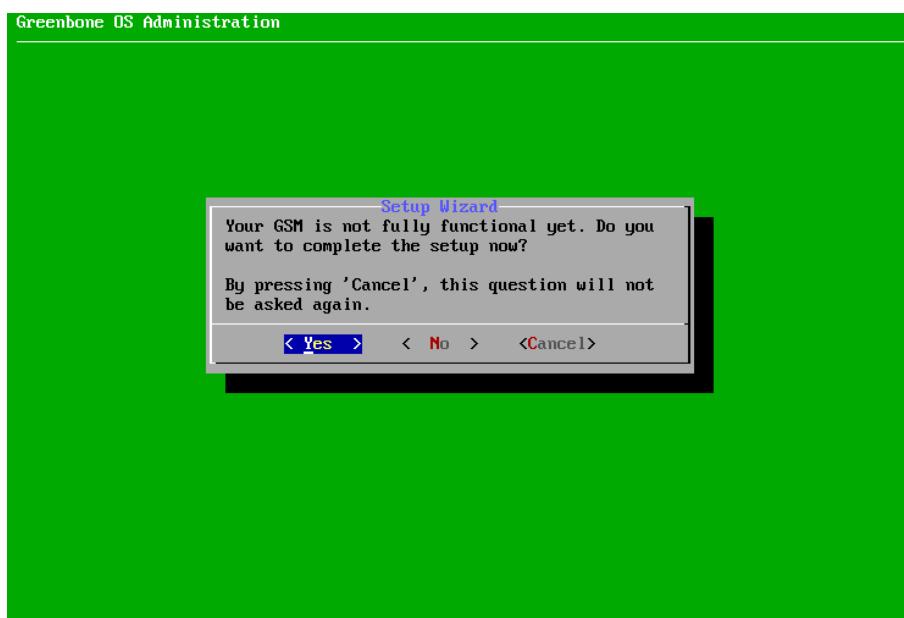


Fig. 5.55: Using the first setup wizard



By selecting *Yes* and pressing *Enter* the first setup wizard is opened and can be used as follows:

Note: By selecting *No* and pressing *Enter* the wizard can be closed. Steps which have not been completed yet are displayed when logging in again.

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

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

In case of a factory reset, all steps have to be carried out (see 20.8 (page 456)).

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

1. Importing or Generating an HTTPS Certificate

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

1. Select *Import* and press *Enter* (see Fig. 5.56).
→ A message informs that a PKCS#12 file can be imported.

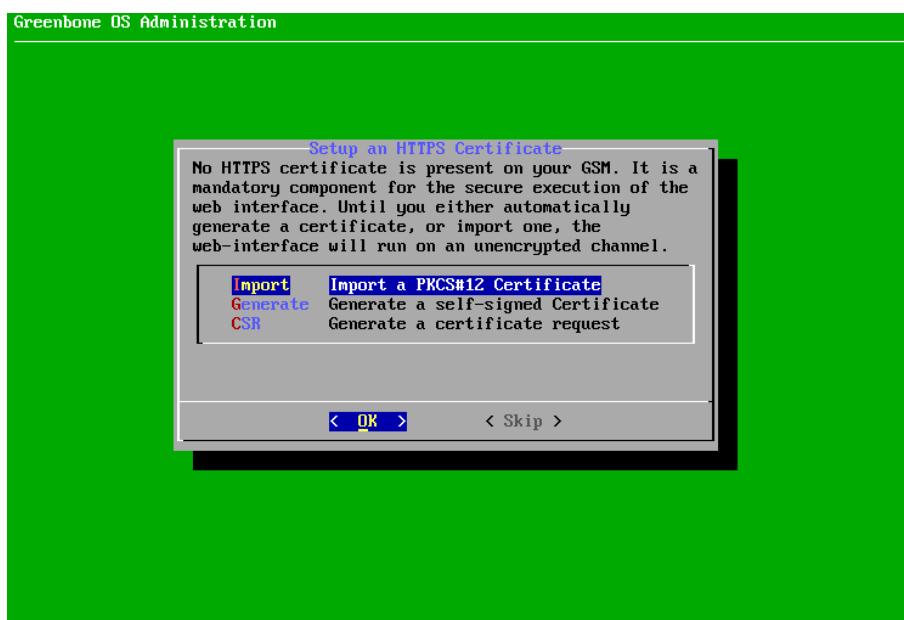


Fig. 5.56: Importing or generating an HTTPS certificate

2. Select *Continue* and press *Enter*.
3. Open the web browser and enter the displayed URL.
4. Click *Browse...*, select the PKCS#12 file and click *Upload*.
→ When the certificate is retrieved by the GSM, the GOS administration menu displays the fingerprint of the certificate for verification.
5. Check the fingerprint and confirm the certificate by pressing *Enter*.

or



1. Select *Generate* and press **Enter**.
→ A message informs that parameters have to be entered to generate the certificate.
2. Select *Continue* and press **Enter**.
3. Provide the settings for the certificate (see Fig. 5.57).

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

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

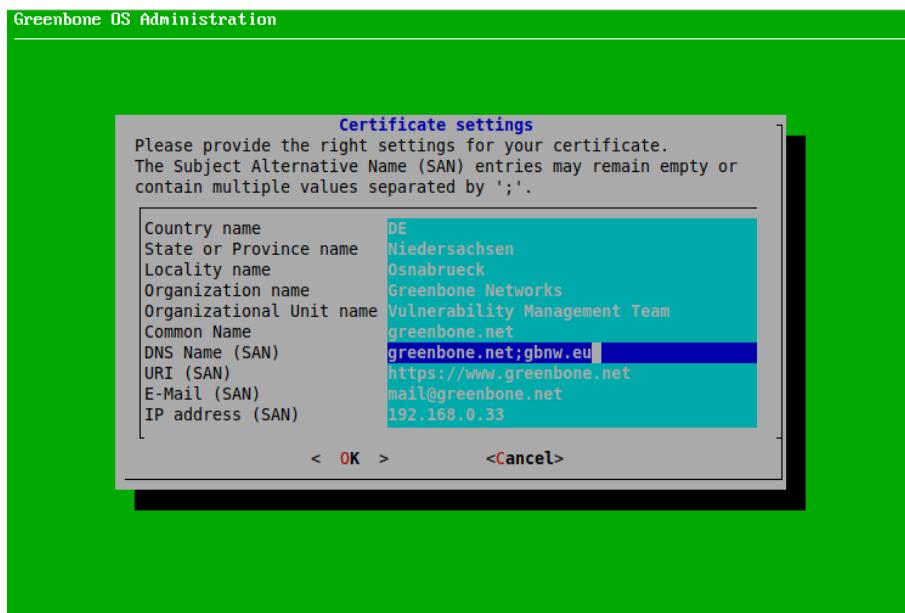


Fig. 5.57: Entering information for the certificate

4. Select *OK* and press **Enter**.
→ A message informs that the certificate is created and can be downloaded (see Fig. 5.58).

Note: The download is not done in the first setup wizard, but in the later GOS administration menu as described in Chapter 7.2.4.1.4.1 (page 149), steps 1 – 4 and 9 – 13.

or

1. Select *CSR* and press **Enter**.
→ A message informs that a key pair and a certificate request are created.
2. Select *Continue* and press **Enter**.
3. Provide the settings for the certificate.

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

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



Fig. 5.58: Completing the HTTPS certificate

4. Select **OK** and press **Enter**.
5. Open the web browser and enter the displayed URL.
6. Download the PEM file.
→ The GOS administration menu displays a message to verify that the CSR has not been tampered with.
7. Verify the information by pressing **Enter**.

Note: When the certificate is signed it has to be uploaded to the GSM. The upload is not done in the first setup wizard, but in the later GOS administration menu as described in Chapter 7.2.4.1.4.2 (page 150), steps 1 – 4 and 11 – 14.

2. Creating a Web Administrator

If there is no web administrator, it is asked whether such an account should be created (see Fig. 5.59).

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

The first web administrator (web user) that is created is automatically the Feed Import Owner (see Chapter 7.2.1.9 (page 130)).

1. Select **Yes** and press **Enter**.
2. Enter the user name for the web administrator.
3. Enter the password for the web administrator twice.
4. Select **OK** and press **Enter**.
→ A message informs that the web administrator has been created.
5. Press **Enter** to close the message.

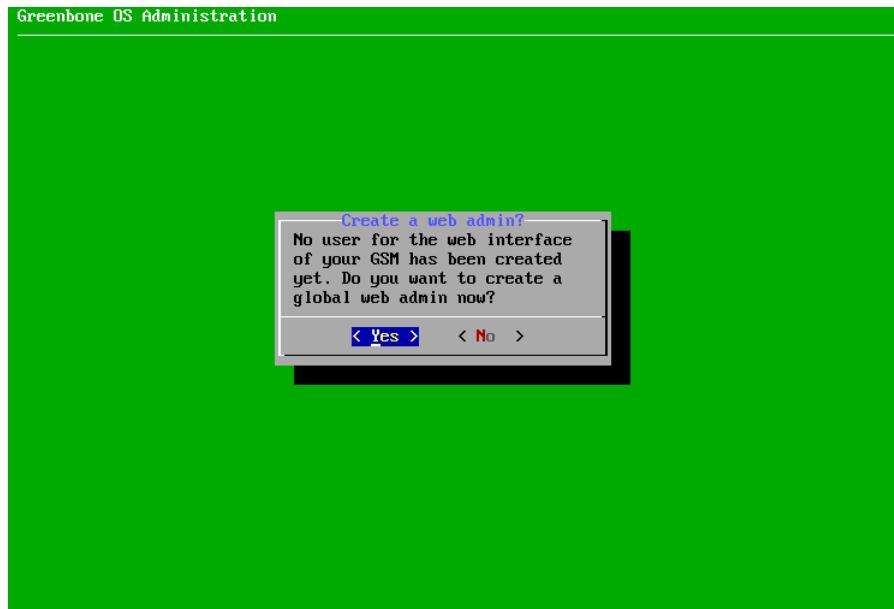


Fig. 5.59: Creating a web administrator

3. Entering or Uploading a Greenbone Security Feed (GSF) Subscription Key

If no valid GSF subscription key is stored on the appliance, the appliance only uses the public Greenbone Community Feed (GCF) and not the GSF. A GSF subscription key can be entered or uploaded as follows:

1. Select *Editor* and press **Enter** (see Fig. 5.60).
→ The editor is opened.
2. Enter the subscription key.
3. Press **Ctrl + X**.
4. Press **Y** to save the changes.
5. Press **Enter**.
or
1. Select *HTTP Upload* and press **Enter**.
2. Open the web browser and enter the displayed URL.
3. Click *Browse...*, select the subscription key and click *Upload*.



Fig. 5.60: Entering or uploading a GSF subscription key

4. Downloading the Feed

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

1. Select **Yes** and press **Enter** (see Fig. 5.61).
→ A message informs that the feed update was started in the background (see Fig. 5.62).
2. Press **Enter** to close the message.

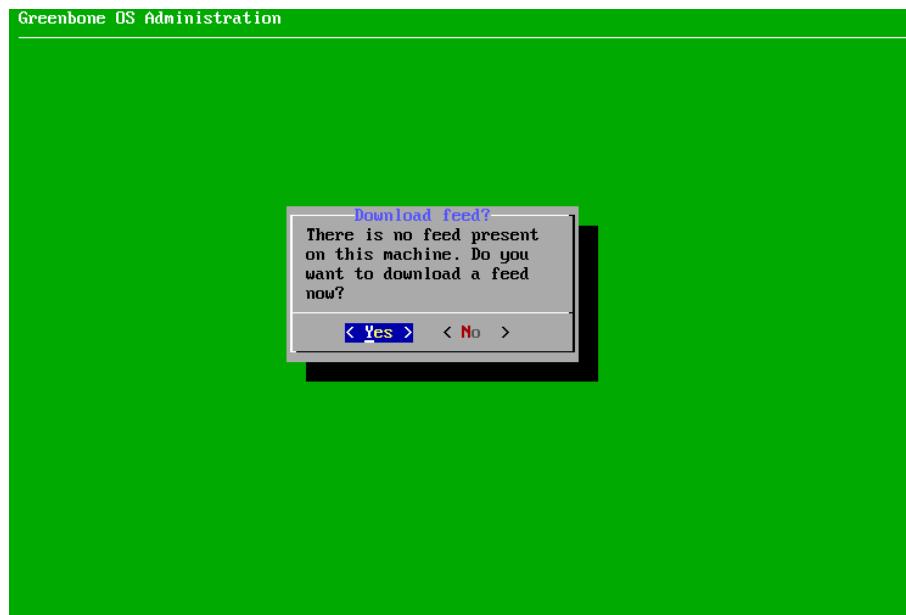


Fig. 5.61: Downloading the feed

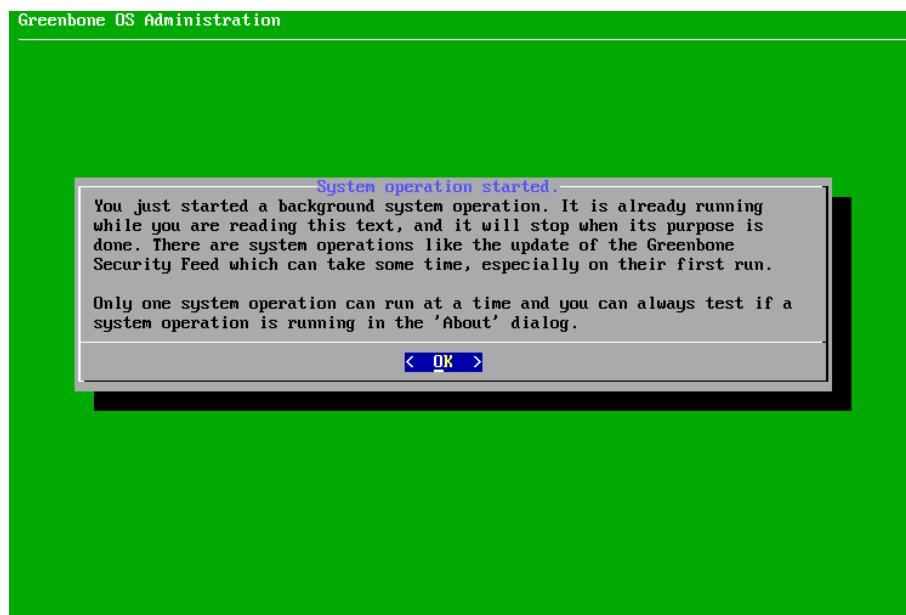


Fig. 5.62: Downloading the feed



5. Finishing the First Setup Wizard

Note: After the last step, a status check is performed. A message shows the result (see Fig. 5.63).

After closing the message by pressing `Enter` the GOS administration menu can be used as described in Chapter 7 (page 120).

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

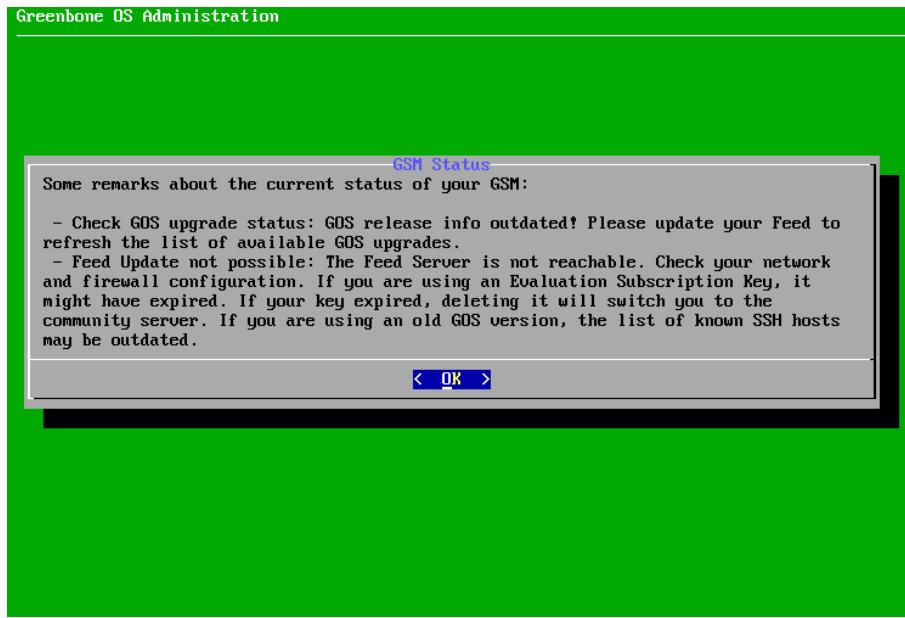


Fig. 5.63: Result of the status check

5.5.4 Logging into the Web Interface

The main interface of the GSM is the web interface, also called Greenbone Security Assistant (GSA). The web interface can be accessed as described in Chapter 8.1 (page 200).



5.6 GSM 25V

This setup guide shows the steps required to put a GSM 25V sensor appliance into operation.

The following checklist can be used to monitor the progress:

Step	Done
Virtual environment installed	
Integrity verified (optional)	
OVA file imported	
Virtual machine settings checked	
Keyboard layout selected	
IP address configured	
DNS server configured	
SSH service enabled (optional)	
SSL certificate created	
GOS selfcheck run	

5.6.1 Setup Requirements

This section lists the requirements for successfully deploying the GSM 25V appliance. All requirements have to be met.

5.6.1.1 Resources

The virtual appliance requires at least the following resources:

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

5.6.1.2 Supported Hypervisor

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

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

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

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



5.6.1.3 Verification of Integrity

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

To request the checksum contact the Greenbone Networks Support via e-mail (support@greenbone.net) including the subscription number.

The integrity checksum can be provided via phone or via support portal at <https://support.greenbone.net>. Specify the preferred channel in the e-mail.

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

On Linux systems the following command for calculating the checksum for the GSM 25V can be used:

```
sha256sum GSM-25V-21.04.0-gsf20210430.ova
```

On Microsoft Windows systems, the following command for calculating the checksum for the GSM 25V can be used in the Windows PowerShell:

```
Get-Filehash 'C:\<path>\GSM-25V-21.04.0-gsf20210430.ova' -Algorithm SHA256
```

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

5.6.2 Deploying the Appliance

The GSM 25V is provided by Greenbone Networks in the Open Virtualization Appliance (OVA) format.

Each GSM 25V is activated using a unique subscription key.

Note: Cloning the GSM 25V and using several instances in parallel is not permitted because and can result in inconsistencies and unwanted side effects.

To deploy the GSM 25V, it has to be imported into the hypervisor of choice as follows:

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

The figures show the installation of a GSM CENO. The installation of a GSM 25V is carried out equivalently. File names used in the example differ based on the GSM model and the GSF subscription key.

1. Install VMware ESXi for the current operating system.
2. Open the web interface of the VMware ESXi instance and log in.
3. Click *Virtual Machines* in the *Navigator* column on the left.
4. Click  *Create / Register VM*.
5. Select *Deploy a virtual machine from an OVF or OVA file* and click *Next* (see Fig. 5.64).
6. Enter a name for the virtual machine in the input box.
7. Click *Click to select files or drag/drop*, select the OVA file of the appliance and click *Next*.
8. Select the storage location in which to store the virtual machine files and click *Next*.

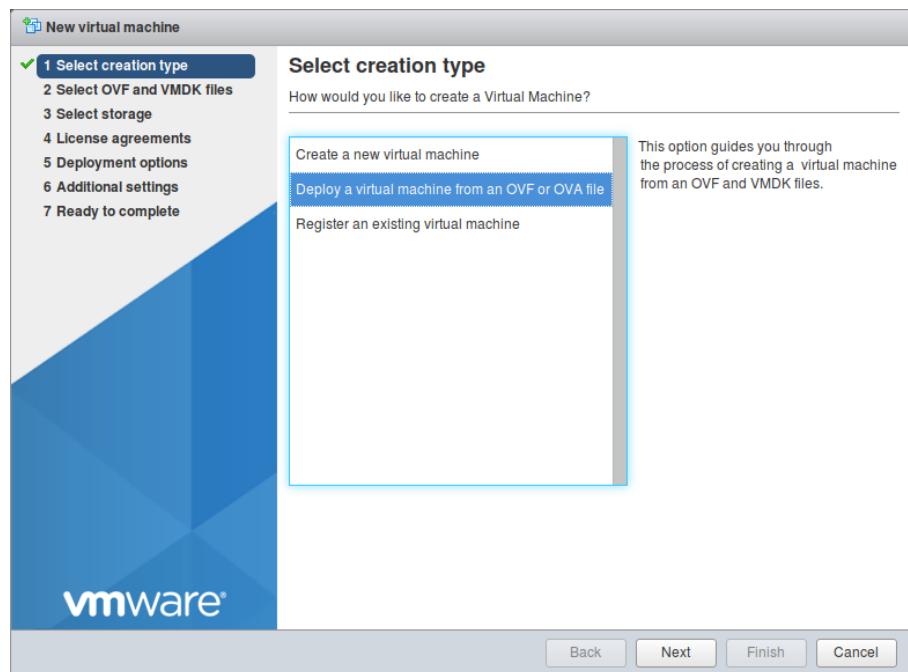


Fig. 5.64: Selecting the creation type

9. Adjust the deployment options as required and click *Next*.

Note: The default deployment settings may be used.

10. Check the configuration of the virtual machine (see Fig. 5.65).

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

11. Click *Finish*.

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

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

12. When the appliance is imported, click *Virtual Machines* in the *Navigator* column on the left.

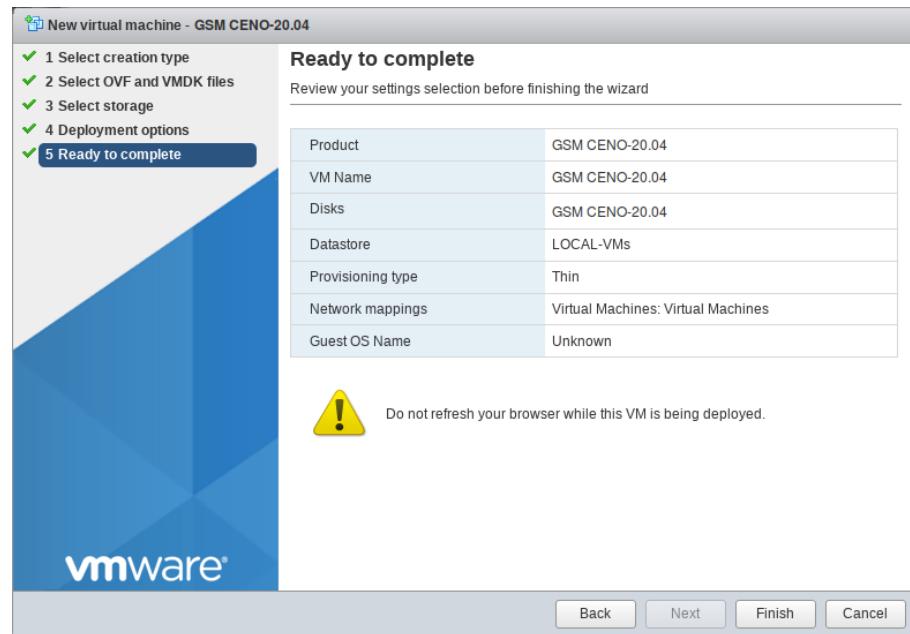


Fig. 5.65: Checking the configuration of the virtual machine

13. Select the appliance in the list and click *Power on* (see Fig. 5.66).

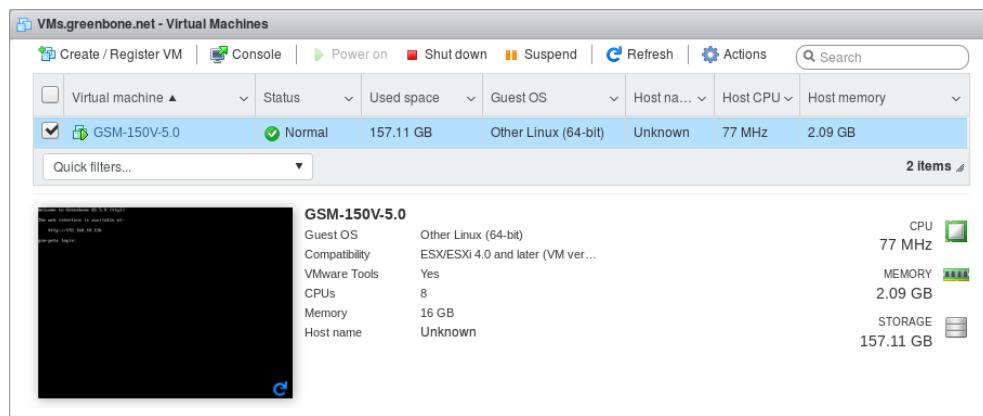


Fig. 5.66: Imported virtual machine

5.6.3 Performing a General System Setup

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

However, since the GSM 25V is a dedicated sensor, the master key has to be exchanged with the sensor.

When the GSM is delivered by Greenbone Networks or after a factory reset, the GOS administration menu shows the first setup wizard after logging in to assist with the basic GOS configuration (see Fig. 5.67).

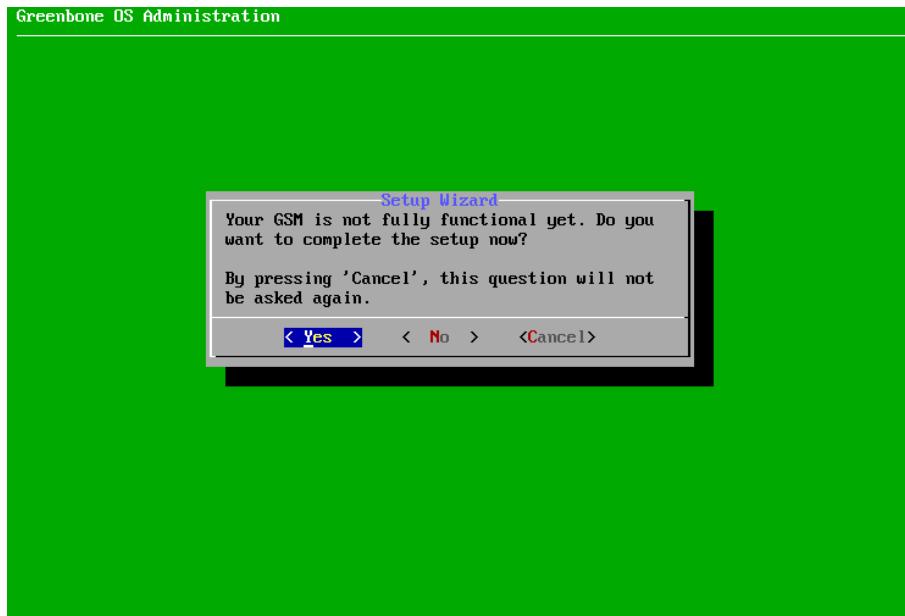


Fig. 5.67: Using the first setup wizard

By selecting *Yes* and pressing *Enter* the first setup wizard is opened and can be used as follows:

Note: By selecting *No* and pressing *Enter* the wizard can be closed. Steps which have not been completed yet are displayed when logging in again.

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

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

In case of a factory reset, all steps have to be carried out (see 20.8 (page 456)).

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

1. Importing or Generating an HTTPS Certificate

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

1. Select *Import* and press *Enter* (see Fig. 5.68).
→ A message informs that a PKCS#12 file can be imported.
2. Select *Continue* and press *Enter*.
3. Open the web browser and enter the displayed URL.
4. Click *Browse...*, select the PKCS#12 file and click *Upload*.
→ When the certificate is retrieved by the GSM, the GOS administration menu displays the fingerprint of the certificate for verification.

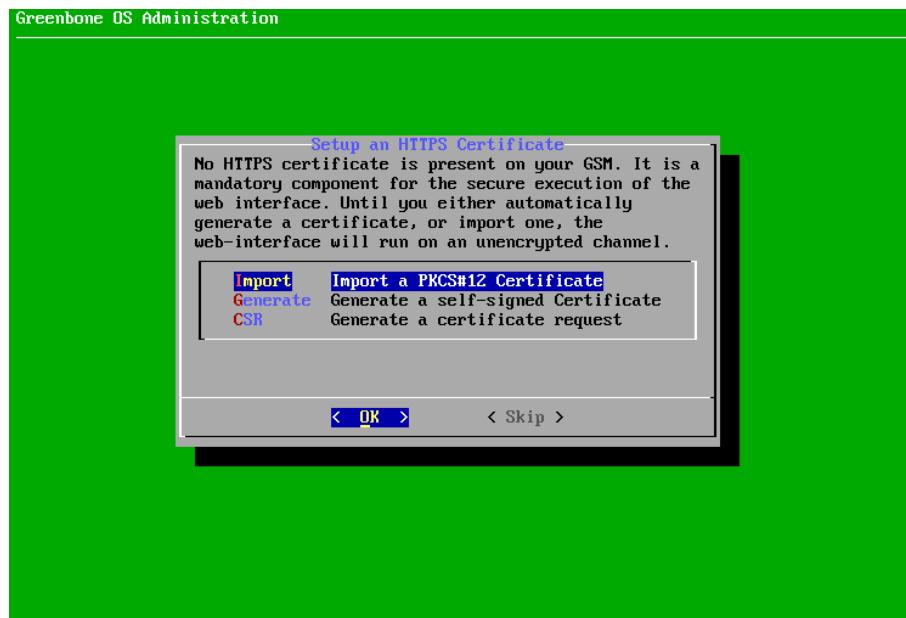


Fig. 5.68: Importing or generating an HTTPS certificate

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

or

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

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

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

3. Provide the settings for the certificate (see Fig. 5.69).

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

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

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

→ A message informs that the certificate is created and can be downloaded (see Fig. 5.70).

Note: The download is not done in the first setup wizard, but in the later GOS administration menu as described in Chapter 7.2.4.1.4.1 (page 149), steps 1 – 4 and 9 – 13.

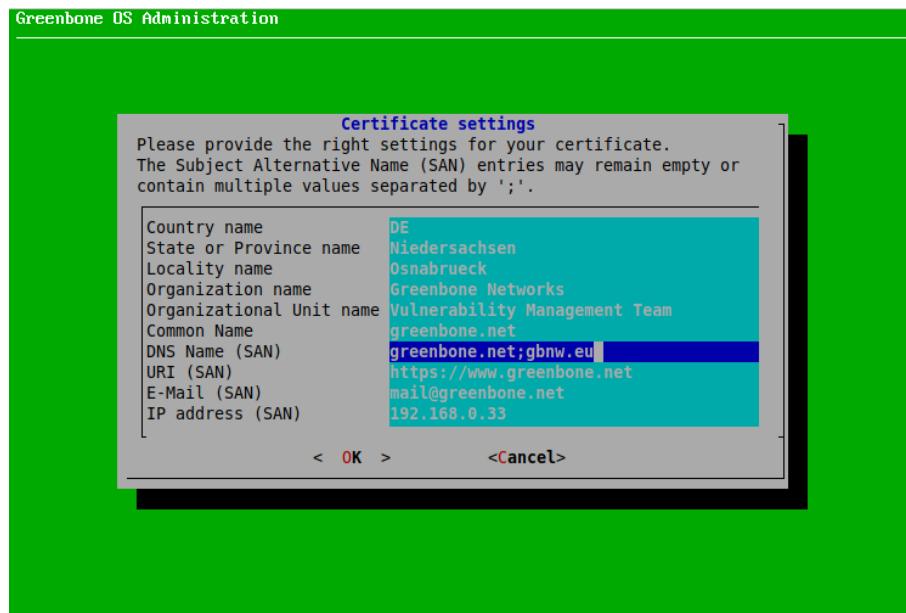


Fig. 5.69: Entering information for the certificate

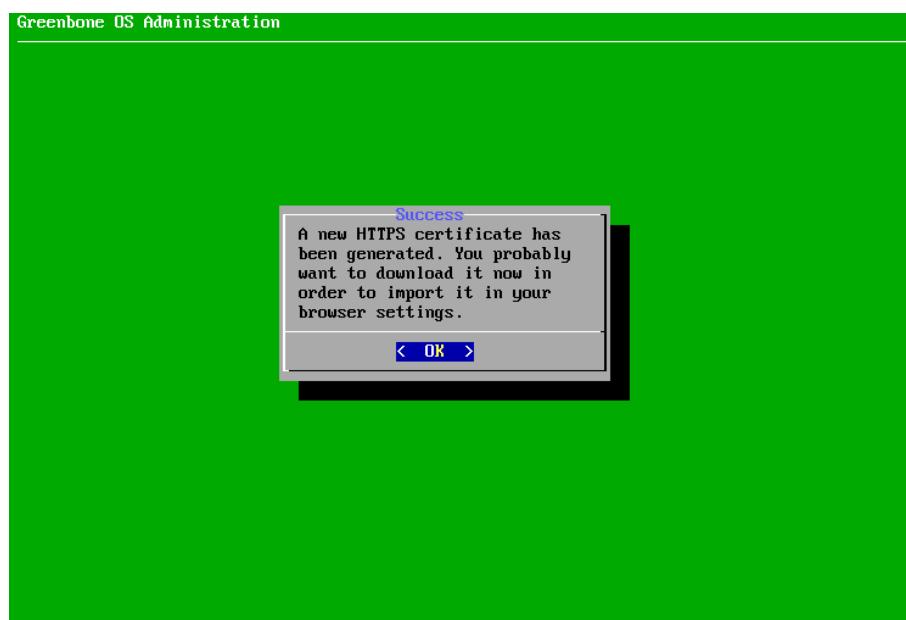


Fig. 5.70: Completing the HTTPS certificate



or

1. Select *CSR* and press *Enter*.
→ A message informs that a key pair and a certificate request are created.
2. Select *Continue* and press *Enter*.
3. Provide the settings for the certificate.

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

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

4. Select *OK* and press *Enter*.
5. Open the web browser and enter the displayed URL.
6. Download the PEM file.
→ The GOS administration menu displays a message to verify that the CSR has not been tampered with.
7. Verify the information by pressing *Enter*.

Note: When the certificate is signed it has to be uploaded to the GSM. The upload is not done in the first setup wizard, but in the later GOS administration menu as described in Chapter 7.2.4.1.4.2 (page 150), steps 1 – 4 and 11 – 14.

2. Entering or Uploading a Greenbone Security Feed (GSF) Subscription Key

If no valid GSF subscription key is stored on the appliance, the appliance only uses the public Greenbone Community Feed (GCF) and not the GSF. A GSF subscription key can be entered or uploaded as follows:

1. Select *Editor* and press *Enter* (see Fig. 5.71).
→ The editor is opened.



Fig. 5.71: Entering or uploading a GSF subscription key



2. Enter the subscription key.
3. Press **Ctrl + X**.
4. Press **Y** to save the changes.
5. Press **Enter**.
or
1. Select *HTTP Upload* and press **Enter**.
2. Open the web browser and enter the displayed URL.
3. Click *Browse...*, select the subscription key and click *Upload*.

3. Downloading the Feed

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

1. Select **Yes** and press **Enter** (see Fig. 5.72).

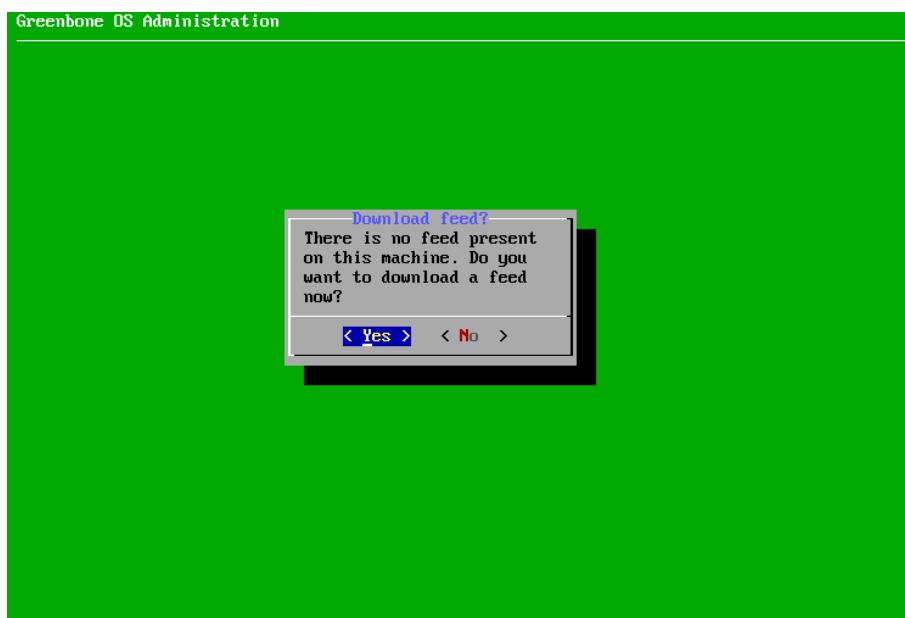


Fig. 5.72: Downloading the feed

→ A message informs that the feed update was started in the background (see Fig. 5.73).

2. Press **Enter** to close the message.

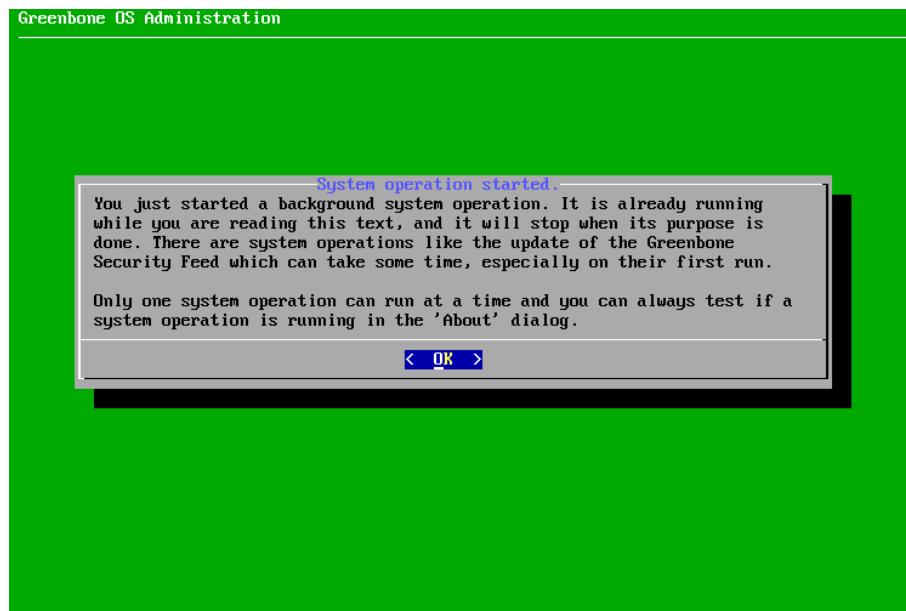


Fig. 5.73: Downloading the feed

4. Finishing the First Setup Wizard

Note: After the last step, a status check is performed. A message shows the result (see Fig. 5.74).

After closing the message by pressing **Enter** the GOS administration menu can be used as described in Chapter 7 (page 120).

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

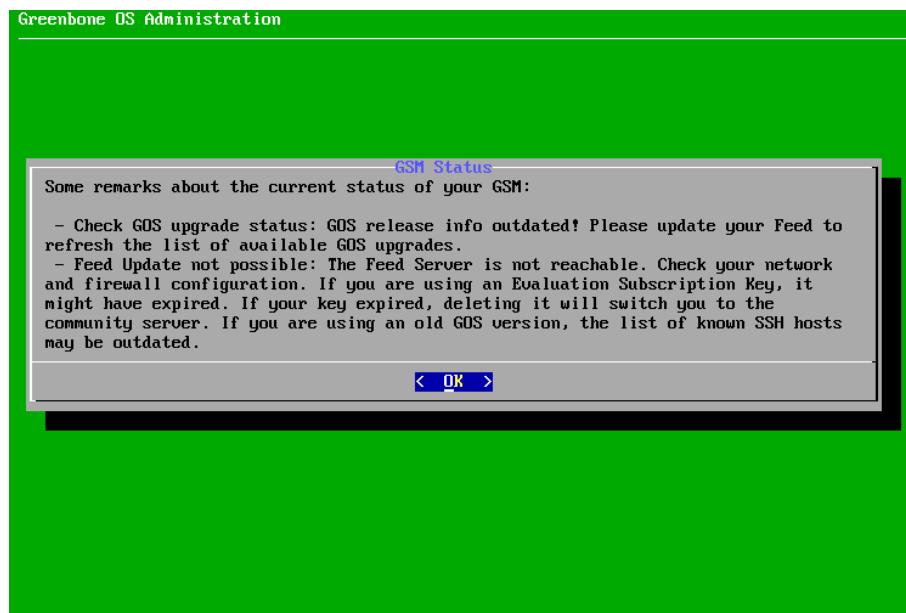


Fig. 5.74: Result of the status check



5. Exchanging the Master Key with the Sensor

Continue with Chapter 16 (page 409) to exchange the keys with the master.

Note: The GSM 25V does not offer any web interface. The sensor is solely managed by the master. Logging into the sensor is possible by using the console and SSH from the master.

If the communication between master and sensor fails, the rule set of any internal firewall governing the network connection may be adjusted.



5.7 GSM ONE

This setup guide shows the steps required to put a GSM ONE appliance into operation.

The following checklist can be used to monitor the progress:

Step	Done
Virtual environment installed	
Integrity verified (optional)	
OVA file imported	
Virtual machine settings checked	
Keyboard layout selected	
IP address configured	
DNS server configured	
SSH service enabled (optional)	
SSL certificate created	
Web user account created	
GOS selfcheck run	

5.7.1 Setup Requirements

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

5.7.1.1 Resources

The virtual appliance requires at least the following resources:

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

5.7.1.2 Supported Hypervisor

The following hypervisors are officially supported for running a GSM ONE:

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

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



5.7.1.3 Verification of Integrity

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

To request the checksum contact the Greenbone Networks Support via e-mail (support@greenbone.net) including the subscription number.

The integrity checksum can be provided via phone or via support portal at <https://support.greenbone.net>. Specify the preferred channel in the e-mail.

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

On Linux systems the following command for calculating the checksum for a GSM ONE can be used:

```
sha256sum GSM-ONE-21.04.0-gsf20210430.ova
```

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

```
Get-Filehash 'C:\<path>\GSM-ONE-21.04.0-gsf20210430.ova' -Algorithm SHA256
```

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

5.7.2 Deploying the Appliance

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

Each GSM ONE is activated using a unique subscription key.

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

To deploy a GSM ONE, it has to be imported into the hypervisor of choice as follows:

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

1. Install Oracle VirtualBox for the current operating system.

Note: VirtualBox is often included with Linux distributions.

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

2. Start VirtualBox.
3. Select *File > Import Appliance...* in the menu bar.
4. Click  and select the OVA file of the appliance (see Fig. 5.75).
5. Check the configuration of the virtual machine in the window *Appliance settings* (see Fig. 5.75). Values can be changed by double clicking into the input box of the respective value.

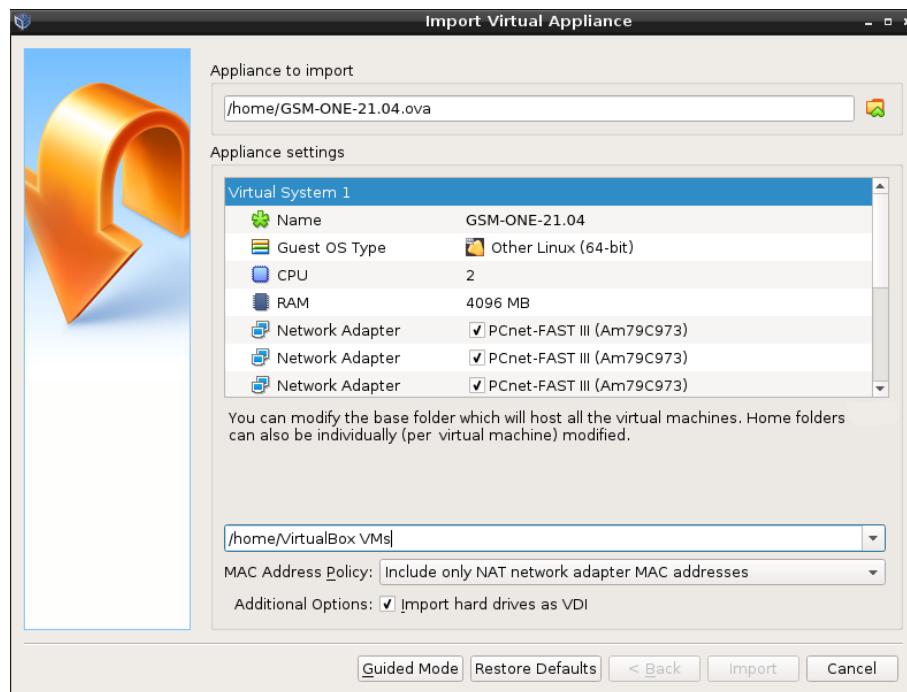


Fig. 5.75: Importing the OVA file of the appliance

Note: If possible, select 4096 MB RAM (memory) for optimal configuration of the virtual appliance.

6. Click *Import*.
 - The appliance is being imported. This can take up to 10 minutes.
 - When the appliance is imported, it is displayed in the left column in VirtualBox.
7. Select the appliance in the list and click *Start*.



5.7.3 Performing a General System Setup

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

When the GSM is delivered by Greenbone Networks or after a factory reset, the GOS administration menu shows the first setup wizard after logging in to assist with the basic GOS configuration (see Fig. 5.76).

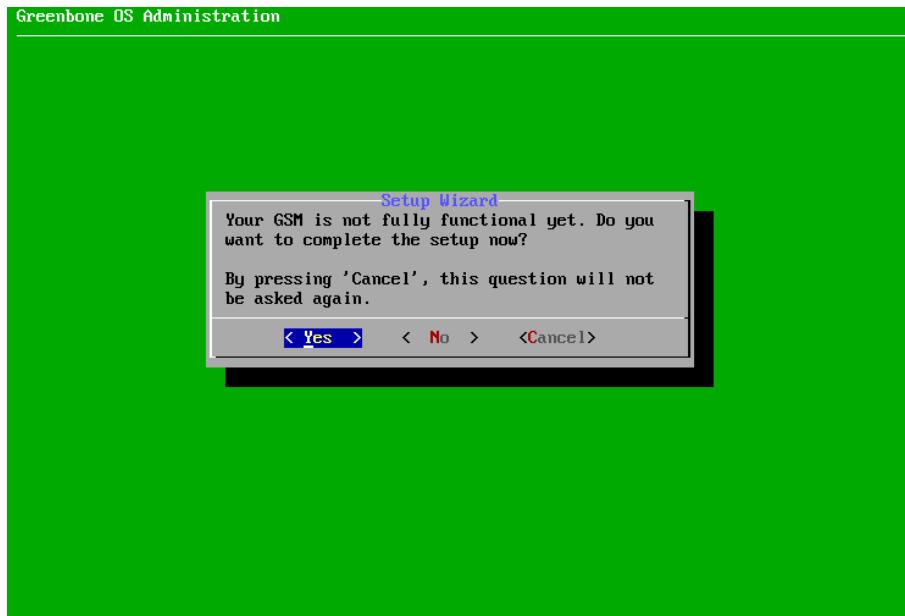


Fig. 5.76: Using the first setup wizard

By selecting *Yes* and pressing *Enter* the first setup wizard is opened and can be used as follows:

Note: By selecting *No* and pressing *Enter* the wizard can be closed. Steps which have not been completed yet are displayed when logging in again.

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

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

In case of a factory reset, all steps have to be carried out (see 20.8 (page 456)).

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

1. Importing or Generating an HTTPS Certificate

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

1. Select *Import* and press *Enter* (see Fig. 5.77).
→ A message informs that a PKCS#12 file can be imported.
2. Select *Continue* and press *Enter*.
3. Open the web browser and enter the displayed URL.
4. Click *Browse...*, select the PKCS#12 file and click *Upload*.

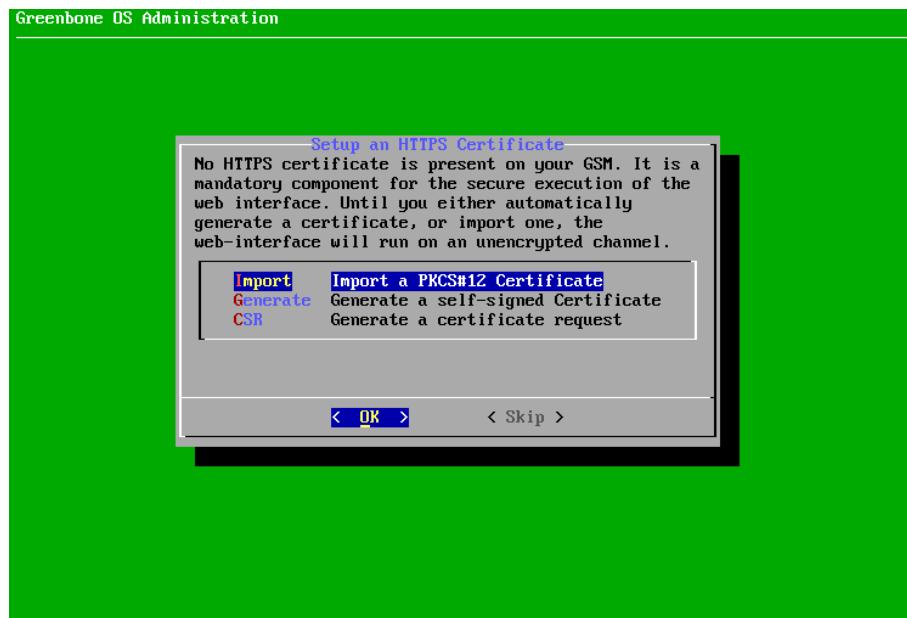


Fig. 5.77: Importing or generating an HTTPS certificate

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

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

or

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

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

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

3. Provide the settings for the certificate (see Fig. 5.78).

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

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

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

→ A message informs that the certificate is created and can be downloaded (see Fig. 5.79).

Note: The download is not done in the first setup wizard, but in the later GOS administration menu as described in Chapter 7.2.4.1.4.1 (page 149), steps 1 – 4 and 9 – 13.

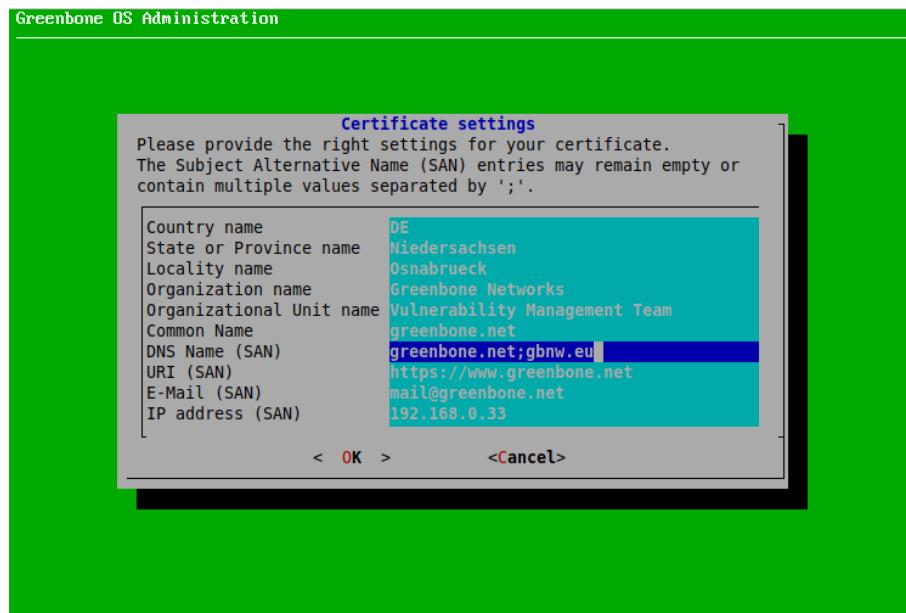


Fig. 5.78: Entering information for the certificate

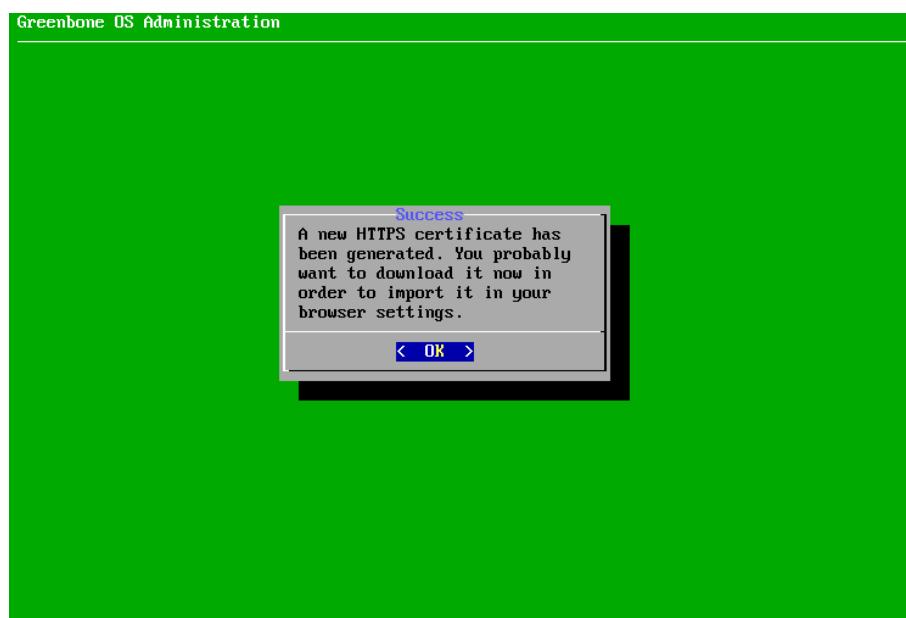


Fig. 5.79: Completing the HTTPS certificate



or

1. Select *CSR* and press *Enter*.
→ A message informs that a key pair and a certificate request are created.
2. Select *Continue* and press *Enter*.
3. Provide the settings for the certificate.

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

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

4. Select *OK* and press *Enter*.
5. Open the web browser and enter the displayed URL.
6. Download the PEM file.
→ The GOS administration menu displays a message to verify that the CSR has not been tampered with.
7. Verify the information by pressing *Enter*.

Note: When the certificate is signed it has to be uploaded to the GSM. The upload is not done in the first setup wizard, but in the later GOS administration menu as described in Chapter 7.2.4.1.4.2 (page 150), steps 1 – 4 and 11 – 14.



2. Creating a Web Administrator

If there is no web administrator, it is asked whether such an account should be created (see Fig. 5.80).

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

The first web administrator (web user) that is created is automatically the Feed Import Owner (see Chapter 7.2.1.9 (page 130)).

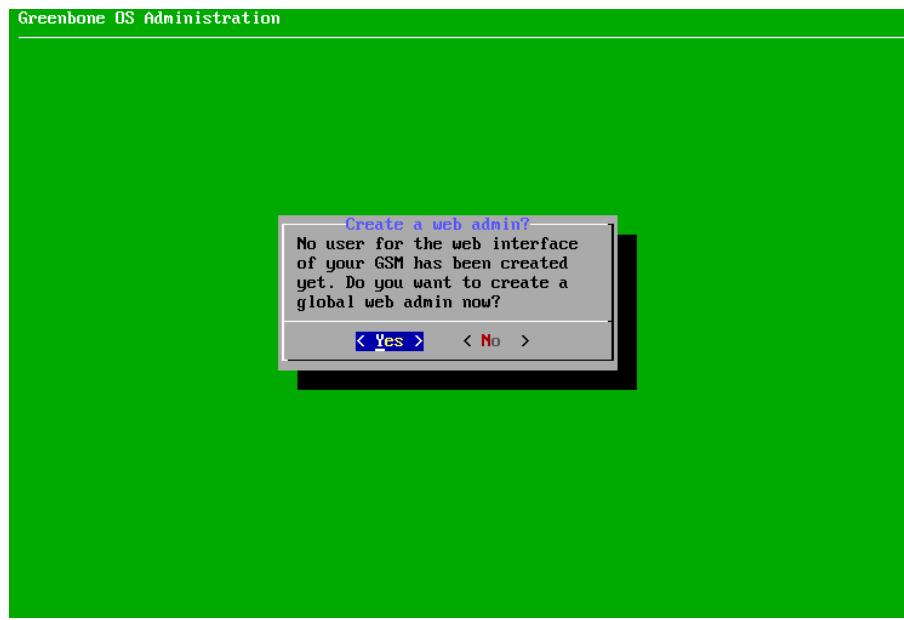


Fig. 5.80: Creating a web administrator

1. Select **Yes** and press **Enter**.
2. Enter the user name for the web administrator.
3. Enter the password for the web administrator twice.
4. Select **OK** and press **Enter**.
→ A message informs that the web administrator has been created.
5. Press **Enter** to close the message.



3. Entering or Uploading a Greenbone Security Feed (GSF) Subscription Key

If no valid GSF subscription key is stored on the appliance, the appliance only uses the public Greenbone Community Feed (GCF) and not the GSF. A GSF subscription key can be entered or uploaded as follows:

1. Select *Editor* and press **Enter** (see Fig. 5.81).

→ The editor is opened.



Fig. 5.81: Entering or uploading a GSF subscription key

2. Enter the subscription key.

3. Press **Ctrl + X**.

4. Press **Y** to save the changes.

5. Press **Enter**.

or

1. Select *HTTP Upload* and press **Enter**.

2. Open the web browser and enter the displayed URL.

3. Click *Browse...*, select the subscription key and click *Upload*.



4. Downloading the Feed

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

1. Select Yes and press Enter (see Fig. 5.82).

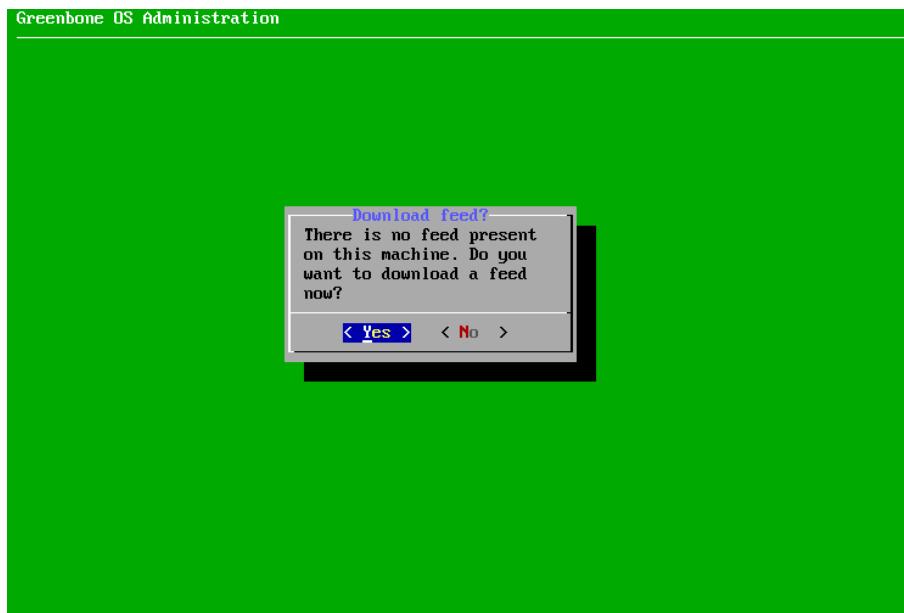


Fig. 5.82: Downloading the feed

→ A message informs that the feed update was started in the background (see Fig. 5.83).

2. Press Enter to close the message.

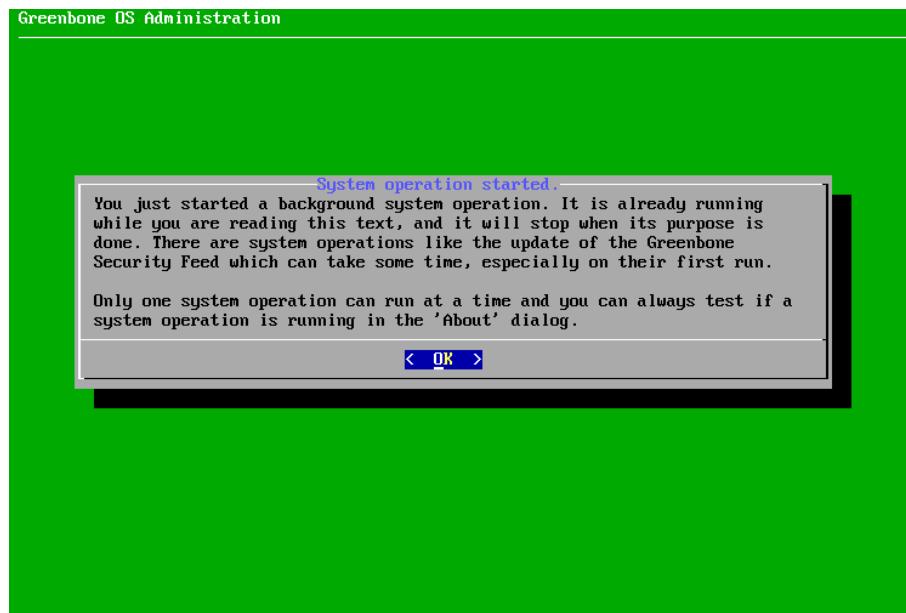


Fig. 5.83: Downloading the feed

5. Finishing the First Setup Wizard

Note: After the last step, a status check is performed. A message shows the result (see Fig. 5.84).

After closing the message by pressing **Enter** the GOS administration menu can be used as described in Chapter 7 (page 120).

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

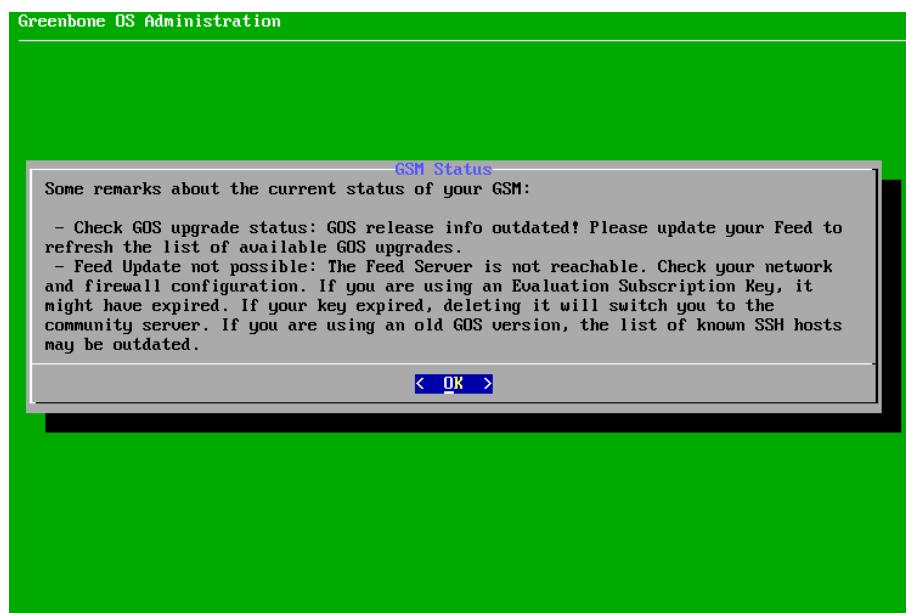


Fig. 5.84: Result of the status check



5.7.4 Logging into the Web Interface

The main interface of the GSM is the web interface, also called Greenbone Security Assistant (GSA). The web interface can be accessed as described in Chapter 8.1 (page 200).

CHAPTER 6

Upgrading from GOS 20.08 to GOS 21.04

Note: GOS 21.04 updates many vulnerability scanning and management components of the Greenbone Security Manager (GSM) to a major new version.

Only proceed with upgrading to GOS 21.04 after reading the release notes⁸ and performing a backup of the current data, either via the backup functionality of GOS or via a VM snapshot on the hypervisor. Further news and previews for GOS 21.04 can be found at <https://community.greenbone.net/c/news>.

Before upgrading to GOS 21.04, the latest version of GOS 20.08 must be installed on the GSM and the GSM must be rebooted.

If there are any questions, contact the Greenbone Networks Support via e-mail (support@greenbone.net).

6.1 Upgrading the Greenbone Security Manager

Note: Before upgrading to GOS 21.04, some requirements must be met in GOS 20.08:

- The sensor type of all configured sensors must be changed to OSP using the menu option *Migrate all sensors to OSP* as described here⁹.
 - A Feed Import Owner must be set as described here¹⁰.
 - The data objects must be installed. For this, a feed update is required after setting the Feed Import Owner.
-

⁸ <https://www.greenbone.net/en/roadmap-lifecycle/>

⁹ <https://docs.greenbone.net/GSM-Manual/gos-20.08/en/master-sensor-setup.html#managing-all-configured-sensors>

¹⁰ <https://docs.greenbone.net/GSM-Manual/gos-20.08/en/managing-gos.html#changing-the-feed-import-owner>

**Note:** For GSM 5300/6400:

Depending on how old these appliances are, they may run with SATA mode “IDE”. If this is the case, GOS 21.04 may not boot until the SATA mode is updated.

The SATA mode can be changed as described in Chapter 6.4.4.2 (page 117).

The upgrade to GOS 21.04 can be carried out as follows:

1. Select *Maintenance* and press *Enter*.
2. Select *Upgrade* and press *Enter*.
3. Select *Switch Release* and press *Enter*.

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

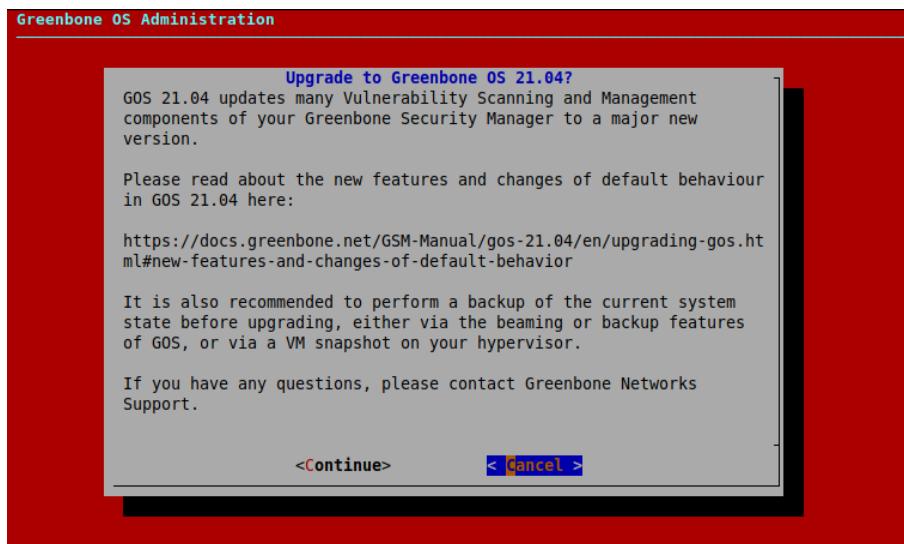


Fig. 6.1: Warning when upgrading to GOS 21.04

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

→ A warning informs that the GSM is locked during the upgrade to GOS 21.04 (see Fig. 6.2).

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

5. Select *Yes* and press *Enter*.

→ A message informs that the upgrade was started.

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

6. Select *Reboot* and press *Enter*.

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

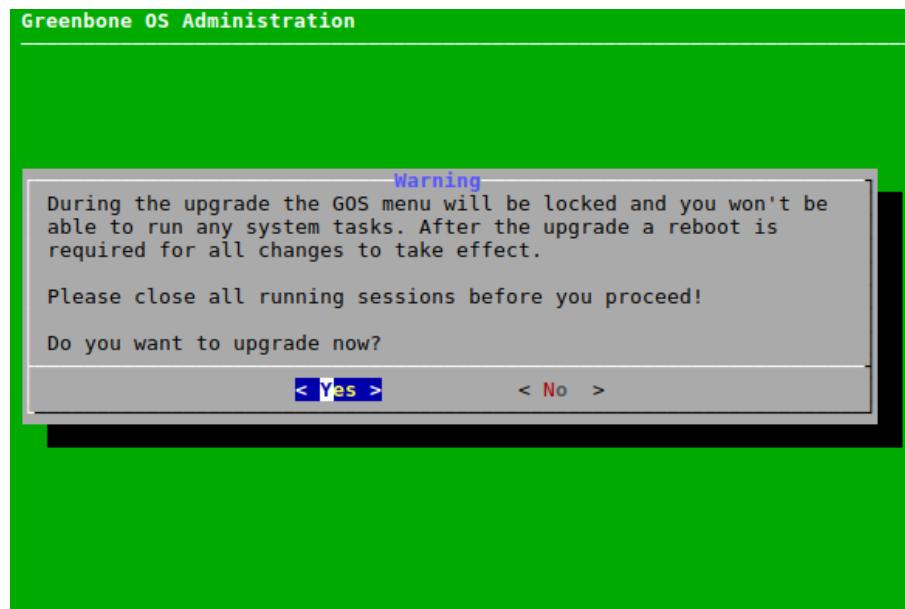


Fig. 6.2: Warning that system is locked during the upgrade

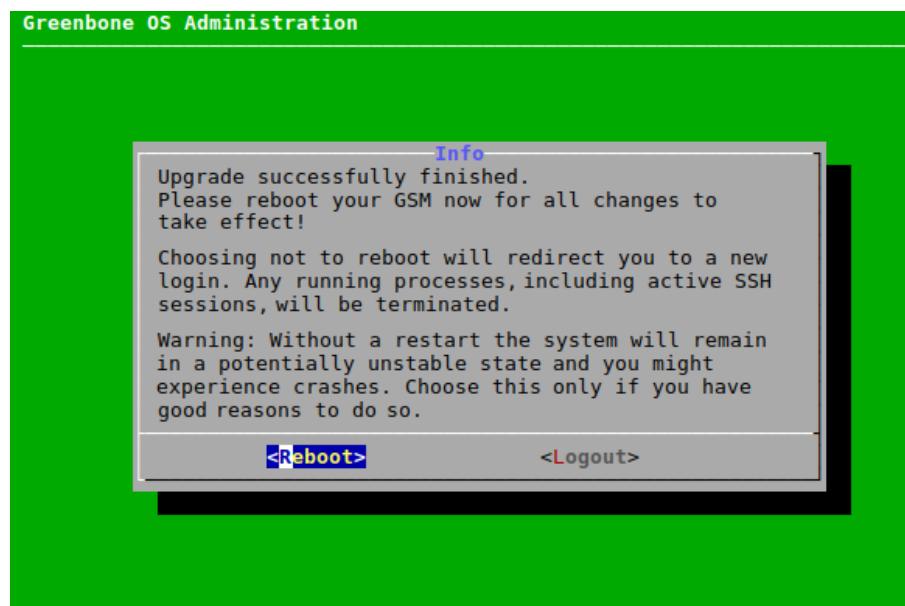


Fig. 6.3: Message after a successful upgrade



6.2 Upgrading the Flash Partition to the Latest Version

The internal flash partition of the GSM contains a backup copy of GOS and is used in case of a factory reset. Upgrading the GOS version stored on the flash partition is recommended (see Chapter 7.3.8 (page 190)).

6.3 Reloading the Web Interface After an Upgrade

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

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

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

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

6.4 New Features and Changes of Default Behavior

The following list displays the changes of default behavior from GOS 20.08 to GOS 21.04. Depending on the current features used, these changes may apply to the currently deployed setup.

Note: Check the following list to decide whether changes to the currently deployed setup are required. The Greenbone Networks Support (support@greenbone.net) may help during this process.

6.4.1 Reports

With GOS 21.04, two new report formats are introduced: Vulnerability Report PDF and Vulnerability Report HTML.

The new report formats are modern and clear in appearance and structure. They contain information about all vulnerabilities found.

Note: The new report formats are distributed via the Greenbone Security Feed (GSF).

To obtain the latest version of the report formats, a feed update may be required before or after upgrading to GOS 21.04 (see Chapter 7.3.6 (page 189)).

6.4.2 CVSS

With GOS 21.04, CVSS v3.0/v3.1 is supported. The extent of the CVSS v3.0/v3.1 support depends on the Greenbone Security Feed.

However, NVTs and CVEs may contain CVSS v2 and/or CVSS v3.0/v3.1 data. If an NVT/CVE contains both CVSS v2 data and CVSS v3.0/v3.1 data, the CVSS v3.0/v3.1 data is always used and shown.

The page *CVSS Calculator* now contains both a calculator for CVSS v2 and a calculator for CVSS v3.0/v3.1.

The *CVSS Base Vector* shown in the details preview and on the details page of an NVT can now be v2, v3.0 or v3.1.



The table on the page *CVEs* now contains the entries *Name*, *Description*, *Published*, *CVSS Base Vector* and *Severity*. The *CVSS Base Vector* can be v2, v3.0 or v3.1. Clicking on the CVSS base vector opens the page *CVSS Calculator*. The input boxes of the corresponding calculator are already pre-filled.

6.4.3 Boreas Alive Scanner

The Boreas alive scanner is a host alive scanner that identifies the active hosts in a target network. It was introduced with GOS 20.08, but was still optional. With GOS 21.04, the Boreas alive scanner is made default.

In comparison to the port scanner *Nmap* that was traditionally used, the Boreas alive scanner is not limited regarding the maximum number of concurrently performed alive status scans and thus, faster. It is especially suitable for large network ranges with only a small number of active hosts.

6.4.4 Hardware Appliances

6.4.4.1 New Hardware Models for Midrange Class

With GOS 21.04, a new generation of Midrange hardware appliances is introduced.

The new hardware now uses SSD-type hard drives instead of HDDs, which are 10 times faster and also quieter and lighter. There is also more hard drive space available. The RAM type is now DDR4 instead of DDR3, which makes the RAM much faster due to a higher clock rate (3200 MHz). There is also twice to four times as much RAM available. Additionally, a new, faster CPU of the latest generation has been installed.

Additionally, the ports of the appliances changed from 6 ports GbE-Base-TX and 2 ports 1 GbE SFP to 8 ports GbE-Base-TX and 2 ports 10 GbE SFP+.

The product names remain as they are.

6.4.4.2 Preparation for Upgrading a GSM 5300/6400

When upgrading a GSM 5300 or GSM 6400 to GOS 21.04, an additional preparation may be necessary.

Depending on how old these appliances are, they may run with SATA mode “IDE”. If this is the case, GOS 21.04 may not boot. The SATA mode has to be changed to “AHCI”.

The SATA mode can be changed in the BIOS. To enter the BIOS, press `Delete` repeatedly while rebooting or powering on the GSM. In the tab *Advanced*, select *SATA Configuration* and change the *SATA mode* to *AHCI Mode*.

6.4.5 Virtual Appliances

The officially supported hypervisors for the virtual appliances are changed with GOS 21.04.

The GSM EXA/PETA/TERA/DECA and 25V can be used with Microsoft Hyper-V, VMware vSphere Hypervisor (ESXi) and Huawei FusionCompute.

The GSM CENO can be used with Microsoft Hyper-V and VMware vSphere Hypervisor (ESXi).

The GSM ONE can be used with Oracle VirtualBox, VMware Workstation Pro and VMware Workstation Player.

Additionally, GOS 21.04 supports the ARM instruction set on Huawei FusionCompute.



6.4.6 Scanning Through a VPN

With GOS 21.04, OpenVPN is integrated in GOS to enable scanning through a Virtual Private Network (VPN). This feature is only available on virtual appliances of the Midrange Class. The VPN feature allows for targets that are reachable via the VPN tunnel to be scanned, but has no effect on other targets, network settings, or master-sensor connections.

The VPN connection is configured and established via the GOS administration menu using the IP address of the VPN and a PKCS#12 file containing the necessary certificate authority, certificate, and private key files.

6.4.7 HTTPS

With GOS 21.04, the nginx web server is used in addition to the Greenbone Security Assistant Daemon (gsad). nginx uses OpenSSL instead of GnuTLS for defining the available ciphers and protocols of the server.

Operating the web interface is only possible with TLS versions 1.2 or 1.3. For the configuration of the TLS version, the GOS administration menu contains a new menu under *Setup > Services > HTTPS > Protocols*. There the selection of TLSv1.2, TLSv1.3 or both at the same time is possible. By default, both options are selected. In this case, the web browser selects the version according to its configuration.

The menu under *Setup > Services > HTTPS > Ciphers* is only displayed if TLS version 1.2 is selected (either alone or in combination with version 1.3). The ciphers are now configured with a different string and the TLS version can no longer be configured using the string.

If only TLS version 1.3 is selected, the cipher suites cannot be configured and the default value of OpenSSL is used instead.

If non-default HTTPS ciphers were configured in GOS 20.08, the ciphers can be reconfigured directly after upgrading to GOS 21.04. In this case, the same dialogs as in *Setup > Services > HTTPS > Protocols* and *Setup > Services > HTTPS > Ciphers* are displayed one after the other. If only TLSv1.3 is chosen in the *Protocols* dialog, the *Ciphers* dialog is not shown.

If the ciphers are not reconfigured, the default protocol and cipher settings of GOS 21.04 are used.

Additionally, the menus under *Setup > Services > HTTPS > Certificate > Generate* and *Setup > Services > HTTPS > Certificate > CSR* allow the configuration of a Subject Alternative Name (SAN).

6.4.8 Sensors

With GOS 21.04, the Greenbone Management Protocol (GMP) is no longer used to control a sensor GSM via a master GSM. All sensors now use the Open Scanner Protocol (OSP) as the controlling protocol.

In GOS, the sensor type *GMP Sensor* is retired. On the web interface, the scanner type *GMP Scanner* is retired.

This leads to the sensors being light-weighted and avoids the need for additional credentials on the sensor.

6.4.9 Network Backend

With GOS 21.04, the network configuration backend in GOS is improved. This prevents loss of connectivity in specific network setups as well as connection issues with SSH sessions.

The GSM no longer needs to be restarted after specific network settings have been changed.

The networking mode can be updated to the new mode *gnm* directly after upgrading to GOS 21.04. If the networking mode is not updated directly after upgrading, it can be changed in the new menu under *Setup > Network > Switch Networking Mode*.



6.4.10 Web Interface

6.4.10.1 Auto False Positives

With GOS 21.04, the *Auto-FP* function is retired.

Old filters with `autofp=` will remain untouched during migration but have no effect anymore.

6.4.10.2 Severity Class Scheme

With GOS 21.04, the selection of alternative severity class schemes (*BSI Vulnerability Traffic Light* and *PCI-DSS*) is removed from the user settings. There is now only the *NVD Vulnerability Severity Ratings* scheme to determine severity classes based on the severity.

During migration, any selection other than the default will fall back to the default.

6.4.10.3 Simultaneous Scanning via Multiple IP Addresses

Some devices – especially IoT devices – may crash when scanned via several IP addresses at the same time. For example, this can happen if the device is connected via IPv4 and IPv6.

With GOS 21.04, it is possible to avoid scanning via several IP addresses at the same time using the new setting *Allow simultaneous scanning via multiple IPs* when creating a target.

The default of this setting is *Yes* and reflects the behavior of previous GOS releases.

6.4.11 Greenbone Management Protocol (GMP)

The Greenbone Management Protocol (GMP) has been updated to version 21.04 and the API has been adjusted slightly. The usage of some commands has changed and several commands, elements and attributes have been deprecated. The complete reference guide and the list of changes are available here¹¹.

¹¹ <https://docs.greenbone.net/API/GMP/gmp-21.04.html>

CHAPTER 7

Managing the Greenbone Operating System

Note: This chapter documents all possible menu options.

However, not all GSM models support all of these menu options. Check the tables in Chapter 3 (page 18) to see whether a specific feature is available for the used GSM model.

7.1 General Information

7.1.1 Greenbone Security Feed (GSF) Subscription Key

When purchasing a Greenbone Security Manager (GSM), a unique Greenbone Security Feed (GSF) subscription key is pre-installed to grant the GSM access to the Greenbone Update Service, also called the Greenbone Feed Service. The subscription key is used for authorization purposes only, not for billing or encryption.

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

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

A factory reset will delete the subscription key from the GSM and the subscription key has to be re-installed. If a factory reset is planned, contact the Greenbone Networks Support via e-mail (support@greenbone.net) to receive a copy of the subscription key.

7.1.2 Authorization Concept

The GSM offers two different levels of access:

- **Web Interface/GMP – User Level** The user level is available via the web interface or the Greenbone Management Protocol (GMP).
- **GOS Administration Menu – System Level** The system level is only available via console or secure shell protocol (SSH).



7.1.2.1 User Level Access

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

Accessing the user level is possible either via the web interface, also called Greenbone Security Assistant (GSA), or via Greenbone Management Protocol (GMP).

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

When the GSM is delivered by Greenbone Networks or after a factory reset, no user level account is configured on the GSM. It is necessary to create at least one such account via the system level.

Note: For more information about the web interface see Chapters 8 (page 200) and 9 (page 221).

For more information about GMP see Chapter 15 (page 399).

7.1.2.2 System Level Access

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

GOS is managed using a menu-based graphical interface (GOS administration menu). The system administrator is not required to use the command line (shell) for configuration or maintenance tasks. Shell access is provided for support and troubleshooting purposes only.

Accessing the system level requires either console access (serial, hypervisor or monitor/keyboard) or a connection via SSH. To use SSH, a network connection is required and the SSH service has to be enabled (see Chapter 7.2.4.4 (page 154)).

When the GSM is delivered by Greenbone Networks or after a factory reset, a default system administrator account and password is pre-configured. During the initial setup the system administrator password should be changed (see Chapter 7.2.1.1 (page 124)).

Accessing the GOS Administration Menu Using the Console

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

```
Welcome to Greenbone OS 20.08 (tty1)
The web interface is available at:
http://192.168.178.67
gsm login: _
```

Fig. 7.1: Login prompt of the appliance



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

- user: admin
- password: admin

Note: During the first setup this password should be changed (see Chapter 7.2.1.1 (page 124)).

When the GSM is delivered by Greenbone Networks or after a factory reset, a setup wizard is shown after the login to assist with the basic configuration of GOS. By selecting *Yes* and pressing *Enter* all mandatory settings can be configured. By selecting *No* or *Cancel* and pressing *Enter* the setup wizard is closed.

Accessing the GOS Administration Menu Using SSH

Note: When the GSM is delivered by Greenbone Networks or after a factory reset, SSH access may be deactivated and has to be enabled first using the console (see Chapter 7.2.4.4 (page 154)). A network connection is required for SSH as well (see Chapter 7.2.2.4 (page 134)).

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

```
$ ssh admin@<gsm>
```

Replace `<gsm>` with the IP address or domain name of the GSM appliance.

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

1. Start the GOS administration menu.
 2. Select *Setup* and press *Enter*.
 3. Select *Services* and press *Enter*.
 4. Select *SSH* and press *Enter*.
 5. Select *Fingerprint* and press *Enter*.
- The fingerprint is displayed on the GOS administration menu.

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

7.1.3 Using the GOS Administration Menu



The steps for using the GOS administration menu which are described in the following chapters are briefly explained in a video based on GOS 5.0¹² (German only).

¹² <https://youtu.be/3uzuxJv8Oak>



The GOS administration menu can be navigated using a keyboard. The arrow keys of the keyboard can be used to move the current menu selection. Pressing `Enter` is used to confirm the current menu selection and to continue. Pressing `Space` is used to toggle on/off switches. The current menu can be exited by pressing `Esc`.

Configuration changes made in the GOS administration menu are not activated immediately. Instead, the menu option `Save` is added below the other options (see Fig. 7.2). The changes take effect by selecting `Save` and pressing `Enter`.

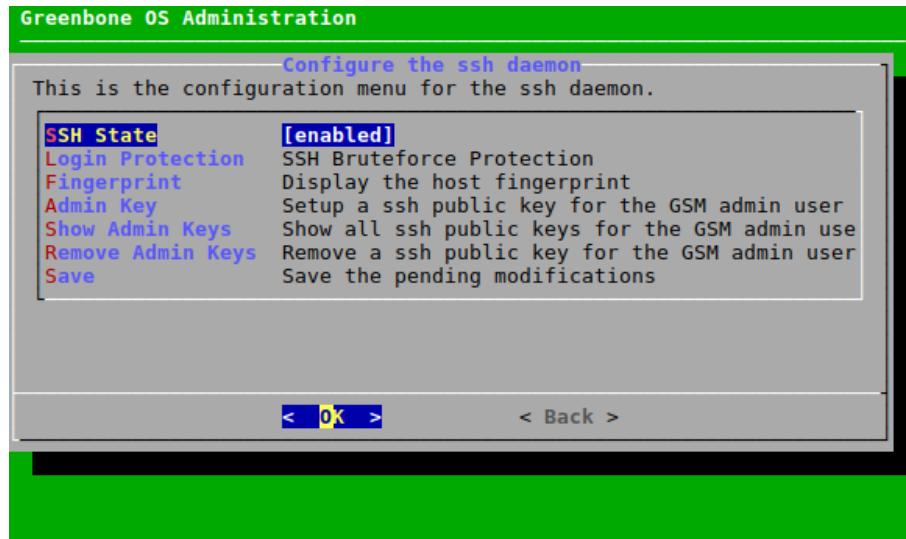


Fig. 7.2: New menu option for saving outstanding changes

If a menu is exited without saving the outstanding changes, a warning is displayed (see Fig. 7.3). The changes can be saved by selecting `Yes` and pressing `Enter`. If `No` is selected, the changes are discarded.

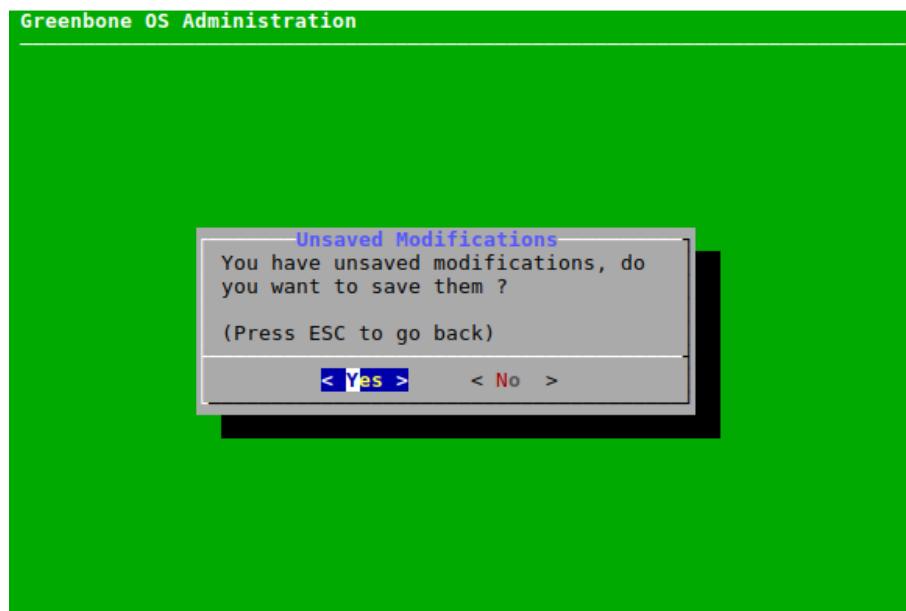


Fig. 7.3: Saving outstanding changes



7.2 Setup Menu

7.2.1 Managing Users

The GOS administration menu offers the possibility to manage web users. Web users are the users of the web interface of the GSM.

7.2.1.1 Changing the System Administrator Password

The password of the system administrator can be changed. This is especially important during the first base configuration. The factory setting is not suitable for a production environment. The password can be changed as follows:

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

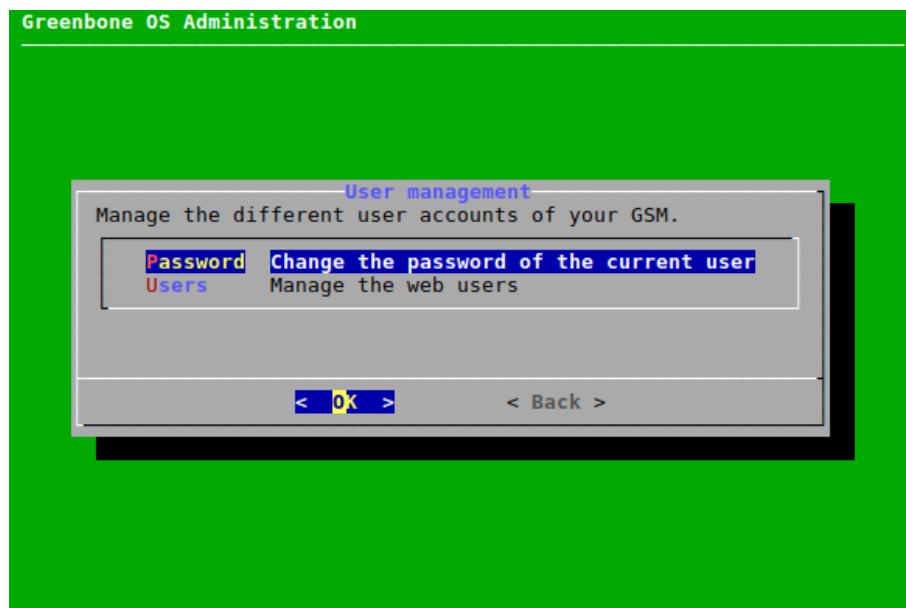


Fig. 7.4: Accessing the user management

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



Fig. 7.5: Changing the system administrator password

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

Note: Trivial passwords are rejected. This includes the default password `admin` as well.



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

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

7.2.1.2 Managing Web Users

Note: There are no web users for the GSM models GSM 35 and GSM 25V.

For these GSM models, this chapter is not relevant.

To be able to use the GSM appliance a web administrator must be set up. This user is being referred to as scan administrator in some documentation and by some applications.

The set-up of the first web administrator is only possible using the GOS administration menu as follows:

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

→ Several new options are displayed (see Fig. 7.6).



Fig. 7.6: Managing the web users

4. Select **List Users** and press **Enter** to display a list of all configured web users.

Note: More than one user with administrative rights can be set up.

To edit the existing users, or add users with fewer permissions, the web interface has to be used.



7.2.1.3 Creating a Web Administrator

A web administrator can be created as follows:

1. Select *Setup* and press *Enter*.
2. Select *User* and press *Enter*.
3. Select *Users* and press *Enter*.
4. Select *Admin User* and press *Enter*.
5. Determine the user name and the password of the web administrator and press *Tab* (see Fig. 7.7).
6. Press *Enter*.

→ The web administrator is created and can be edited in the web interface.

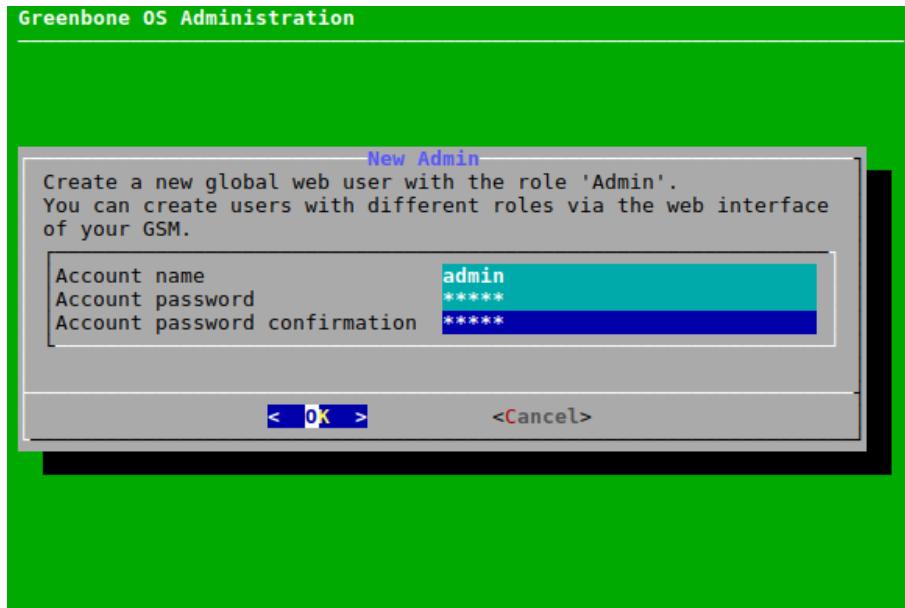


Fig. 7.7: Creating a new web administrator

7.2.1.4 Enabling a Guest User

To allow a guest to log in without needing a password, this feature has to be activated as follows:

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

→ The guest user is enabled and can log in to the web interface without needing the password (see Fig. 7.8).

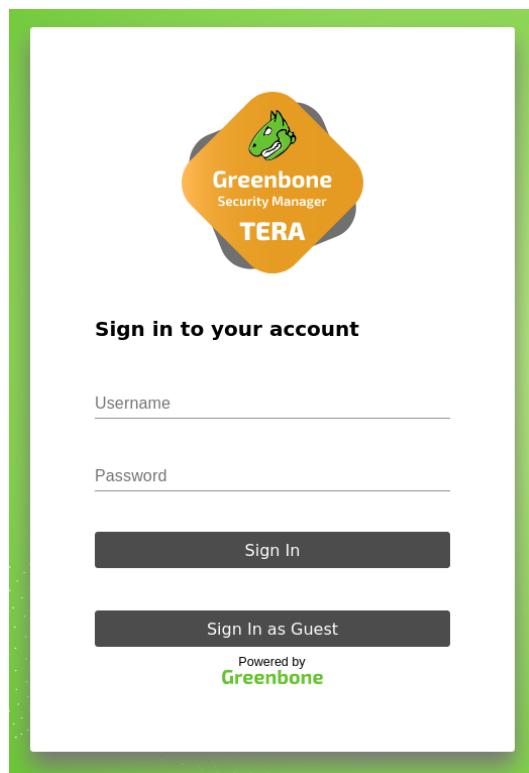


Fig. 7.8: Logging in as a guest user without password

7.2.1.5 Creating a Super Administrator

A super administrator can be created as follows:

1. Select *Setup* and press **Enter**.
2. Select *User* and press **Enter**.
3. Select *Users* and press **Enter**.
4. Select *Super Admin* and press **Enter**.
→ A warning asks to confirm the process (see Fig. 7.9).
5. Select *Yes* and press **Enter**.
6. Determine the user name and the password of the super administrator and press **Tab**.
7. Press **Enter**.
→ The super administrator is created and can be edited in the web interface.

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

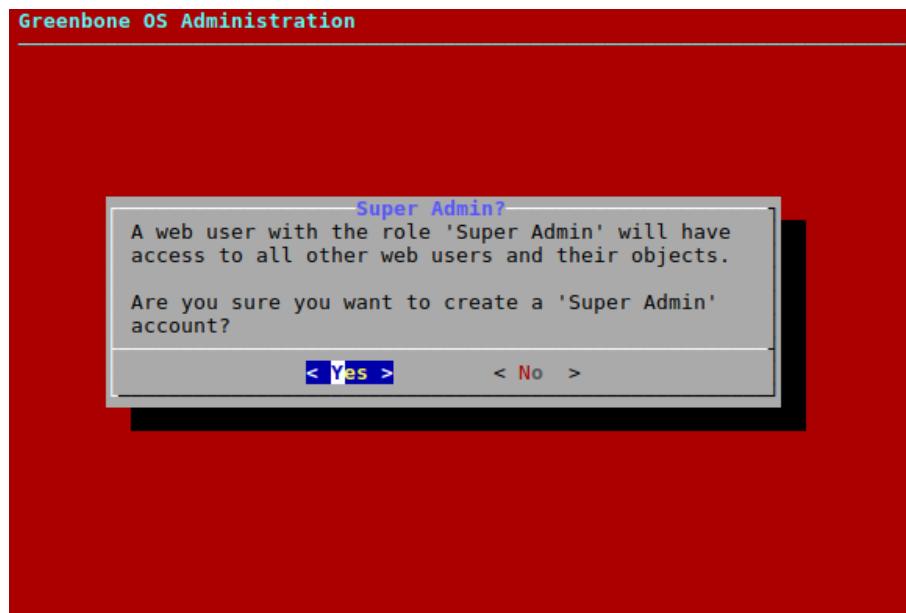


Fig. 7.9: Warning when creating a new super administrator

7.2.1.6 Deleting a User Account

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

A web user can be deleted as follows:

1. Select *Setup* and press *Enter*.
2. Select *User* and press *Enter*.
3. Select *Users* and press *Enter*.
4. Select *Delete Account* and press *Enter*.
5. Select the web user that should be deleted and press *Enter*.
→ A message asks whether an inheritor should be chosen.
6. If an inheritor should be selected, select *Yes* and press *Enter*.
7. Select the web user that should be the inheritor and press *Enter*.

Note: The web user is deleted immediately.

Note: The user who is Feed Import Owner cannot be deleted. Another Feed Import Owner has to be set or the setting has to be unset first (see Chapter 7.2.1.9.1 (page 130))

8. Press *Enter* to return to the previous menu.



7.2.1.7 Changing a User Password

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

1. Select *Setup* and press *Enter*.
2. Select *User* and press *Enter*.
3. Select *Users* and press *Enter*.
4. Select *Change Password* and press *Enter*.
5. Select the web user of which the password should be changed and press *Enter*.
6. Enter the new password twice and press *Tab* (see Fig. 7.10).

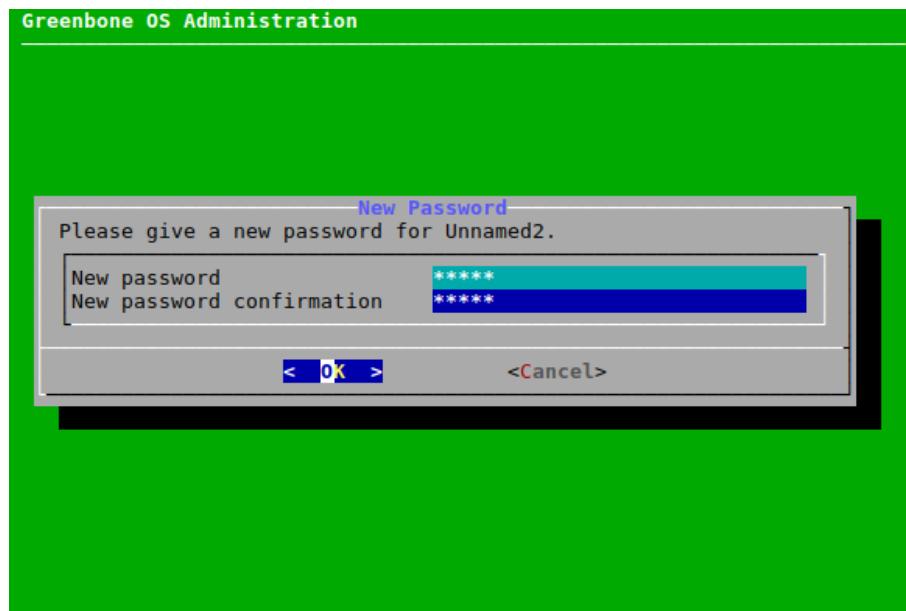


Fig. 7.10: Changing a user password

7. Press *Enter*.

7.2.1.8 Changing the Password Policy

The requirements for passwords can be changed as follows:

1. Select *Setup* and press *Enter*.
2. Select *User* and press *Enter*.
3. Select *Users* and press *Enter*.
4. Select *Password Policy* and press *Enter*.
5. Select *Length* and press *Enter* to set the minimal length a password must have.
Select *Username* and press *Enter* to determine whether user name and password can be the same.
Select *Complex* and press *Enter* to determine whether a password has to contain at least one letter, one number and one symbol.

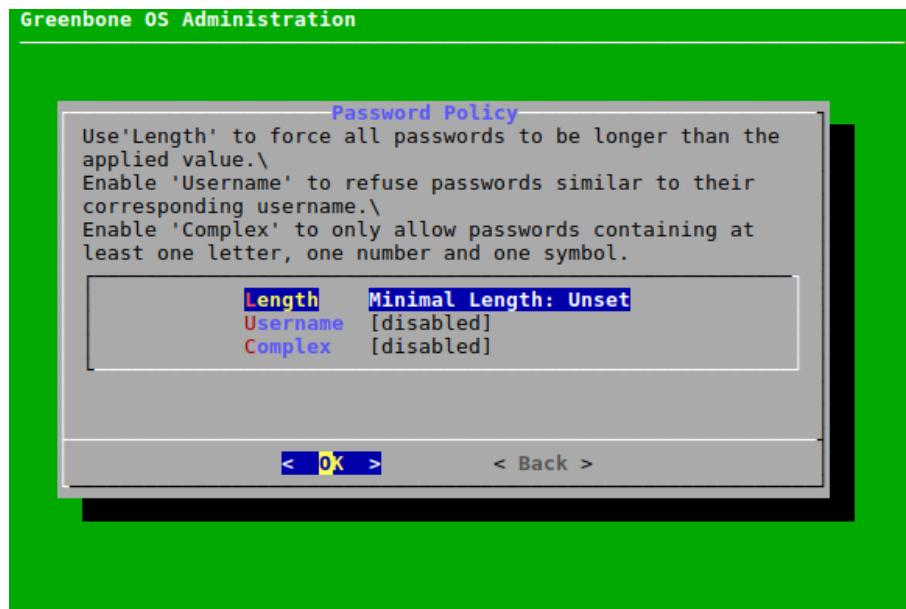


Fig. 7.11: Changing the password policy

7.2.1.9 Configuring the Settings for Data Objects

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

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

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

Note: If the objects remain in the trashcan, they do not count as deleted yet and are not downloaded anew during the next feed update.

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

The Feed Import Owner, a super administrator (default role) and an administrator (default role) who currently has permissions for the objects may also grant additional permissions for the objects to other users (see Chapter 9.4.1.1 (page 231) or 9.4.1.2 (page 232)). Normally, this only applies to the default roles. Custom roles have to be granted permissions manually first.

Changing the Feed Import Owner

The Feed Import Owner is set during the first setup of the GSM (see Chapters 6 (page 113) and 5 (page 26)). However, the Feed Import Owner can be changed at a later time.

Note: If the Feed Import Owner is changed, the next time the objects are imported from the feed, they will be owned by the new Feed Import Owner, as well as the associated permissions for the configured roles. The previous Feed Import Owner will still own the objects until then.

If the previous Feed Import Owner removes the objects, they will be imported during the feed update, and ownership will be given to the new Feed Import Owner.



The Feed Import Owner can be changed as follows:

1. Select *Setup* and press *Enter*.
2. Select *User* and press *Enter*.
3. Select *Users* and press *Enter*.
4. Select *Distributed Data* and press *Enter* (see Fig. 7.12).

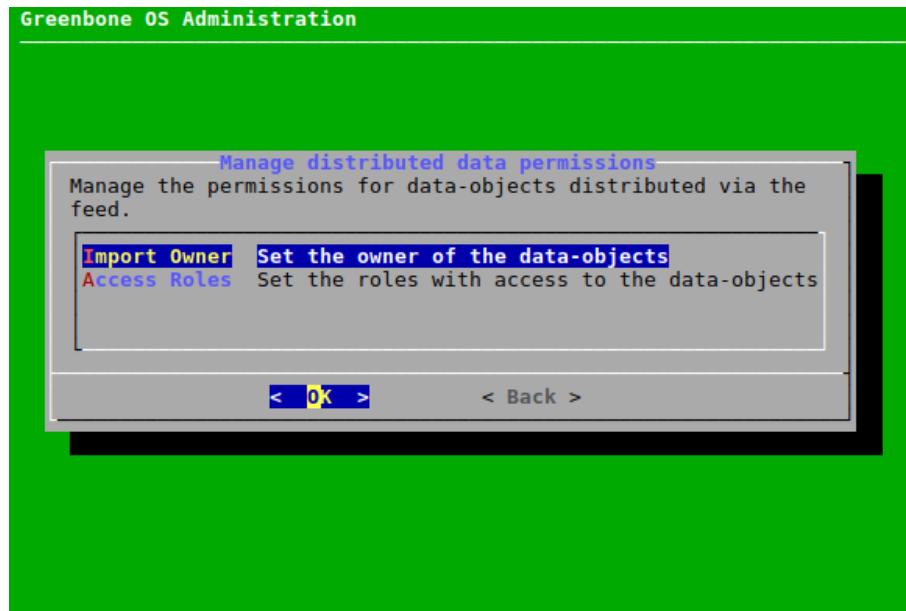


Fig. 7.12: Configuring the settings for the data objects

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

Note: The user who is Feed Import Owner cannot be deleted (see Chapter 7.2.1.6 (page 128)). Another Feed Import Owner or (*Unset*) has to be selected.

Setting the Access Roles

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

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

1. Select *Setup* and press *Enter*.
2. Select *User* and press *Enter*.
3. Select *Users* and press *Enter*.
4. Select *Distributed Data* and press *Enter*.
5. Select *Access Roles* and press *Enter*.
6. Select the roles that should be able to see and use the data objects and press *Space* (see Fig. 7.13).
7. Press *Enter*.

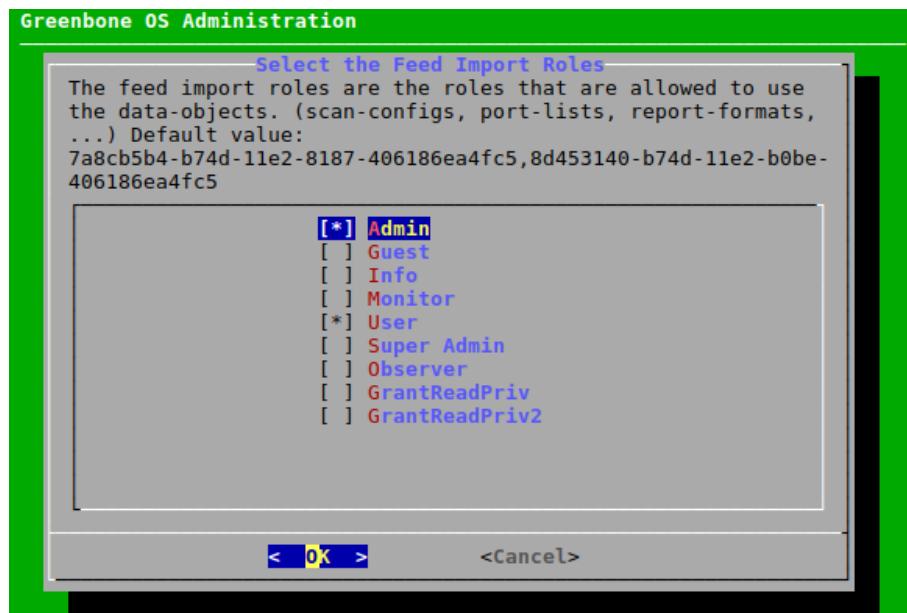


Fig. 7.13: Selecting the roles that can use data objects

7.2.2 Configuring the Network Settings

7.2.2.1 Updating the Networking Mode to *gnm*

After upgrading from GOS 20.08 to GOS 21.04 (see Chapter 6 (page 113)), a message is displayed, offering to switch to the new network mode *gnm*.

If the networking mode is not updated directly after upgrading to GOS 21.04, it can be changed as follows:

1. Select *Setup* and press *Enter*.
2. Select *Network* and press *Enter*.
3. Select *Switch Networking Mode* and press *Enter*.
→ A message asks to confirm the change.
4. Press *Enter*.
→ A message informs that the networking mode has been updated.
5. Press *Enter* to close the message.

Note: After the networking mode is updated, the menu option *Switch Networking Mode* is no longer available.

7.2.2.2 General Information About Namespaces

Some GSM models (GSM 5400/6500 and GSM 400/450/600/650) have two different namespaces:

- **Namespace: Management** This namespace includes all interfaces required for management activities.
- **Namespace: Scan1** This namespace includes all interfaces required for scanning purposes.



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

Only interfaces in the management namespace can handle management traffic. This includes accessing the GOS administration menu, the web interface, the Greenbone Feed Server and configuring the master-sensor communication.

Interfaces in the scan namespace only handle scan traffic.

The namespaces are separated to connect only the interfaces in the scan namespace to networks accessible from the internet. In that way, attacks from the internet cannot reach the management interfaces of the GSM.

Tip: Separating the namespaces is recommended.

7.2.2.3 Switching an Interface to Another Namespace

Interfaces that should be moved to another namespace can be selected as follows:

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

Note: Interfaces in the scan namespace are marked with * (see Fig. 7.14).

Interfaces in the management namespace are labeled accordingly.

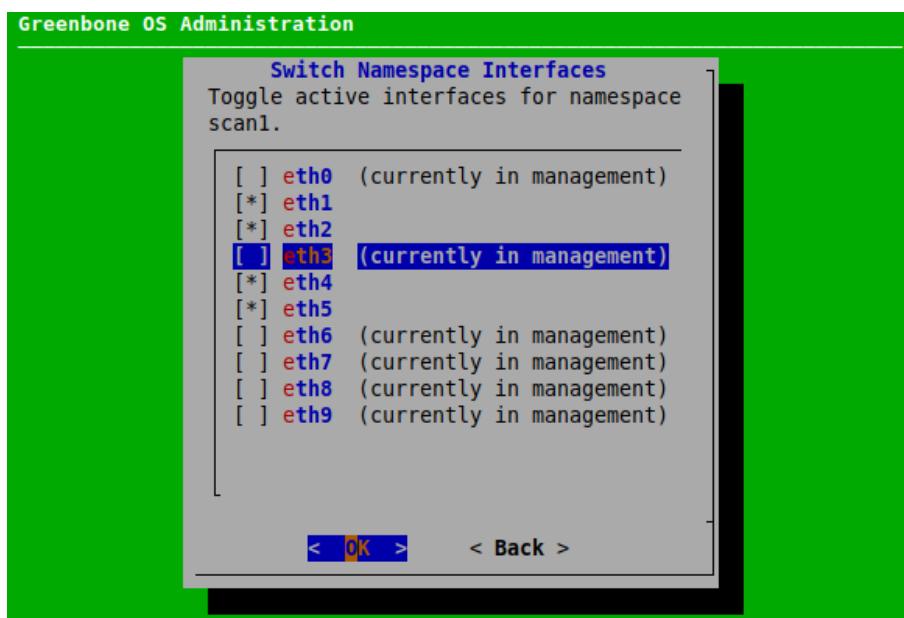


Fig. 7.14: Switching interfaces to another namespace

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



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

6. Press Enter.

7.2.2.4 Configuring Network Interfaces

Note: At least one network interface must be configured to access the GSM using the network. Usually the first network adapter *eth0* is used for this. The administrator has to configure this network interface and to attach the appliance to the network.

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

Network interfaces can be configured as follows:

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

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

→ The interface can be configured (see Fig. 7.15).

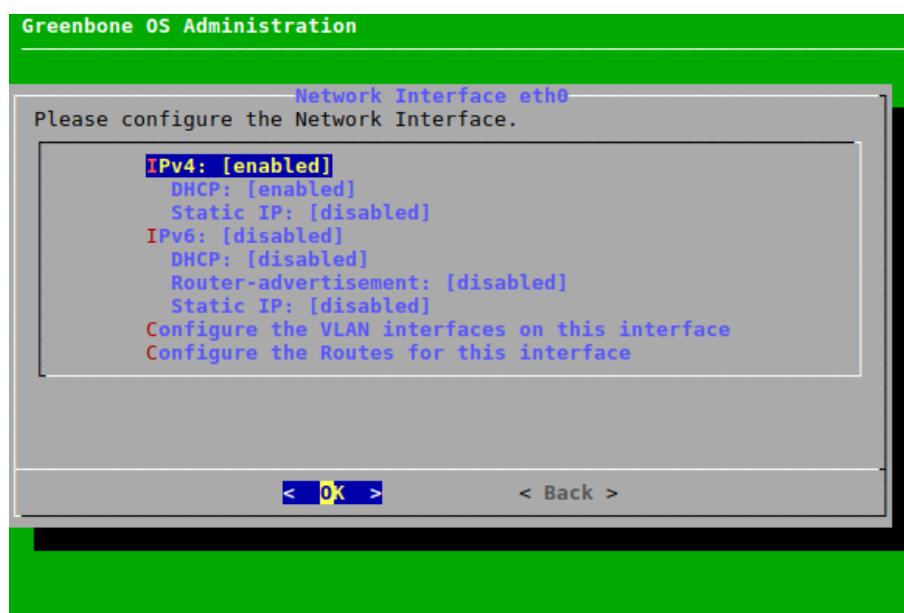


Fig. 7.15: Configuring the network interface



Setting up a Static IP Address

1. Select the desired interface (see Chapter 7.2.2.4 (page 134)).
2. Select *Static IP* (for IPv4 or IPv6) and press **Enter**.
3. Delete `dhcp` from the input box and replace it with the correct IP address including the prefix length (see Fig. 7.16).

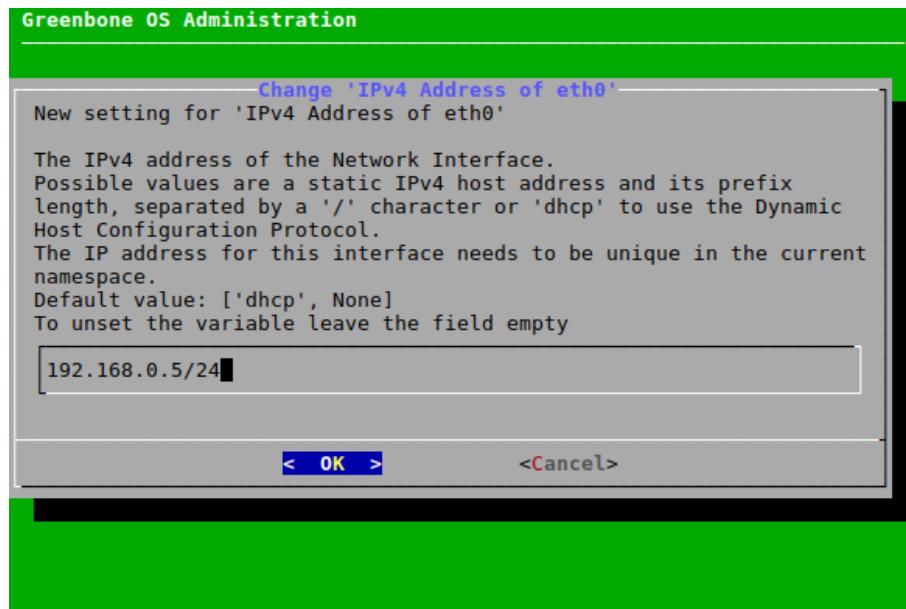


Fig. 7.16: Entering a static IP address

4. Press **Enter**.
→ A message informs that the changes have to be saved (see Chapter 7.1.3 (page 122)).
5. Press **Enter** to close the message.

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

Configuring a Network Interface to Use DHCP

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

1. Select the desired interface (see Chapter 7.2.2.4 (page 134)).
2. Select *DHCP* (for IPv4 or IPv6) and press **Enter**.



Configuring the Maximum Transmission Unit (MTU)

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

1. Select the desired interface (see Chapter 7.2.2.4 (page 134)).
2. Select *MTU* (for IPv4 or IPv6) and press **Enter**.
3. Enter the MTU in the input box.
4. Press **Enter**.
→ A message informs that the changes have to be saved (see Chapter 7.1.3 (page 122)).
5. Press **Enter** to close the message.

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

Using the Router Advertisement for IPv6

If the configuration of IP addresses and the routing for IPv6 should be performed automatically, router advertisement can be enabled as follows:

1. Select the desired interface (see Chapter 7.2.2.4 (page 134)).
2. Select *Router-advertisement* and press **Enter**.



Configuring VLANs

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

A new VLAN subinterface can be created as follows:

1. Select the desired interface (see Chapter 7.2.2.4 (page 134)).
2. Select *Configure the VLAN interfaces on this interface* and press **Enter**.
3. Select *Configure a new VLAN interface* and press **Enter**.
4. Enter the VLAN ID in the input box and press **Enter** (see Fig. 7.17).
→ A message informs that the changes have to be saved (see Chapter 7.1.3 (page 122)).

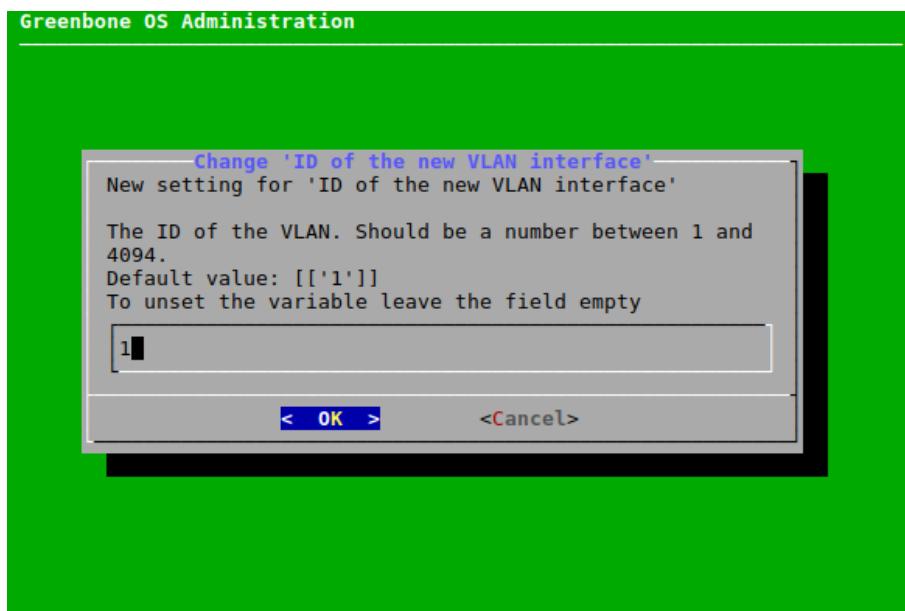


Fig. 7.17: Creating a new VLAN subinterface

5. Press **Enter** to close the message.

→ The new interface can be configured using IPv4 and IPv6 (see Fig. 7.18).

All created subinterfaces can be configured as follows:

1. Select the desired interface (see Chapter 7.2.2.4 (page 134)).
2. Select *Configure the VLAN interfaces on this interface* and press **Enter**.
3. Select *Configure the VLAN interface ...* for the desired subinterface.
4. Configure the subinterface as described in Chapter 7.2.2.4 (page 134).

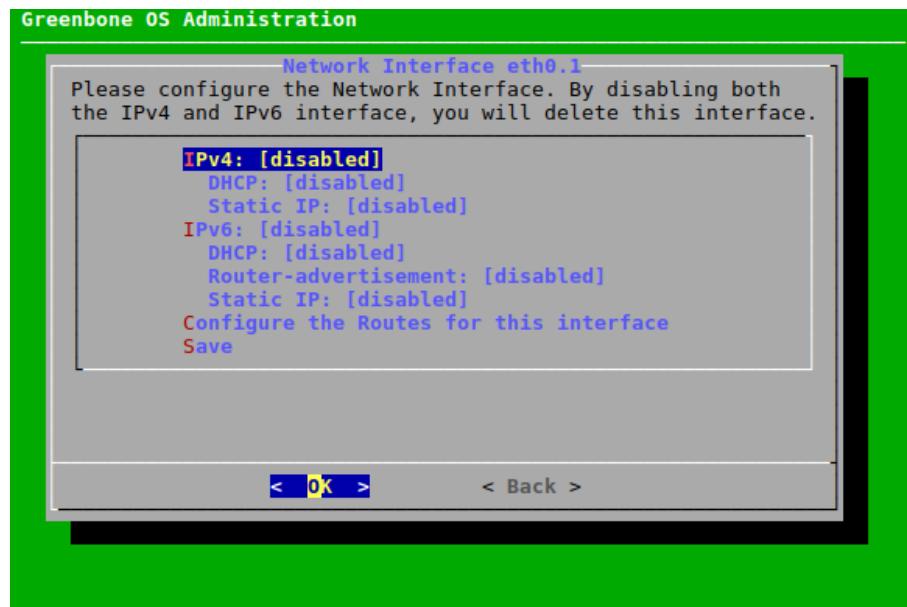


Fig. 7.18: Configuring the VLAN subinterface

Configuring the Routes for an Interface

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

1. Select the desired interface (see Chapter 7.2.2.4 (page 134)).
2. Select *Configure the Routes for this interface* and press **Enter**.
3. Select *Configure IPv4 Routes* or *Configure IPv6 Routes* and press **Enter** (see Fig. 7.19).

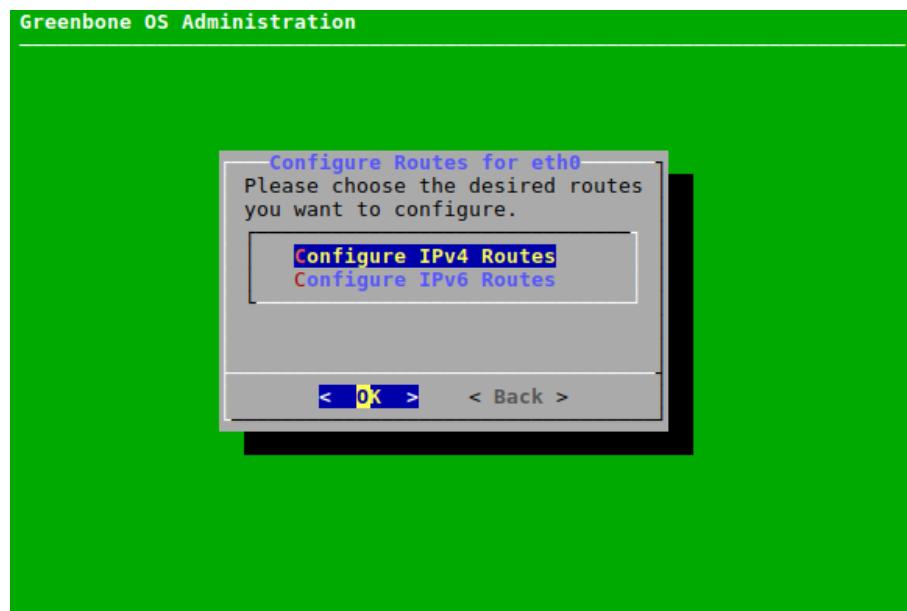


Fig. 7.19: Configuring routes for an interface

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



All created routes can be configured as follows:

1. Select the desired interface (see Chapter 7.2.2.4 (page 134)).
2. Select *Configure the Routes for this interface* and press **Enter**.
3. Select *Configure IPv4 Routes* or *Configure IPv6 Routes* and press **Enter**.
4. Select the desired route and press **Enter**.
5. Edit the route, select *OK* and press **Enter**.

7.2.2.5 Configuring the DNS Server

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

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

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

The DNS server can be configured as follows:

1. Select *Setup* and press **Enter**.
2. Select *Network* and press **Enter**.
3. Select *Namespace: Management* and press **Enter**.
4. Select *DNS* and press **Enter**.
5. Select the desired DNS server and press **Enter**.
6. Enter the IP address used as the DNS server in the input box and press **Enter** (see Fig. 7.20).

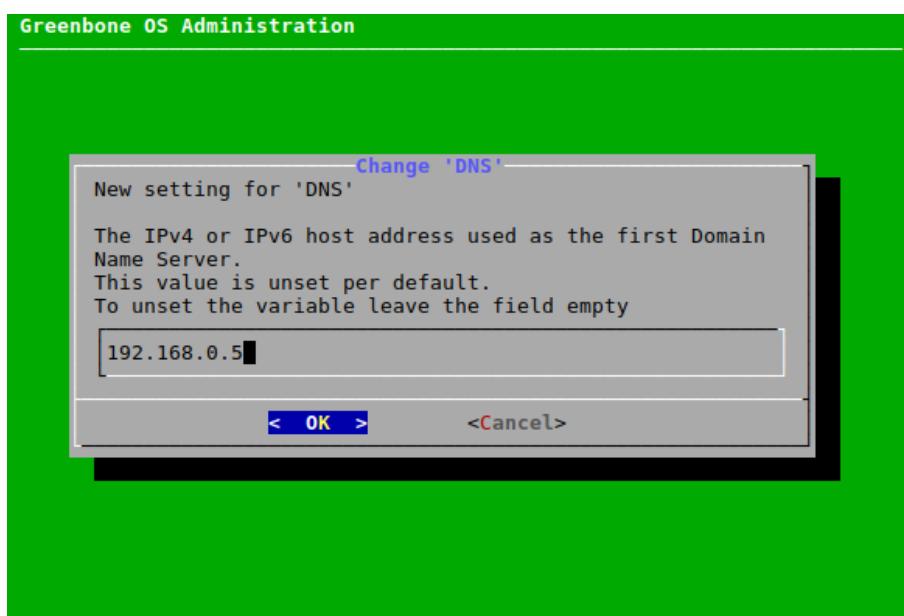


Fig. 7.20: Configuring the DNS server

→ A message informs that the changes have to be saved (see Chapter 7.1.3 (page 122)).

7. Press **Enter** to close the message.



Note: Whether the DNS server can be reached and is functional can be determined by performing a self-check (see Chapter 7.3.1 (page 178)).

7.2.2.6 Configuring the Global Gateway

The global gateway may be obtained automatically using DHCP or router advertisements. The global gateway is often called the default gateway as well.

Note: If the GSM is configured to use static IP addresses, the global gateway has to be configured manually. Separate options are available for IPv4 and IPv6.

If using DHCP to assign IP addresses, the global gateway will be set via DHCP unless the global gateway has been set explicitly.

The global gateway can be configured as follows:

1. Select *Setup* and press *Enter*.
2. Select *Network* and press *Enter*.
3. Select the namespace for which the global gateway should be configured and press *Enter*.
4. Select *Global Gateway* for IPv4 or *Global Gateway (IPv6)* for IPv6 and press *Enter*.
5. Select the desired interface and press *Enter* (see Fig. 7.21).

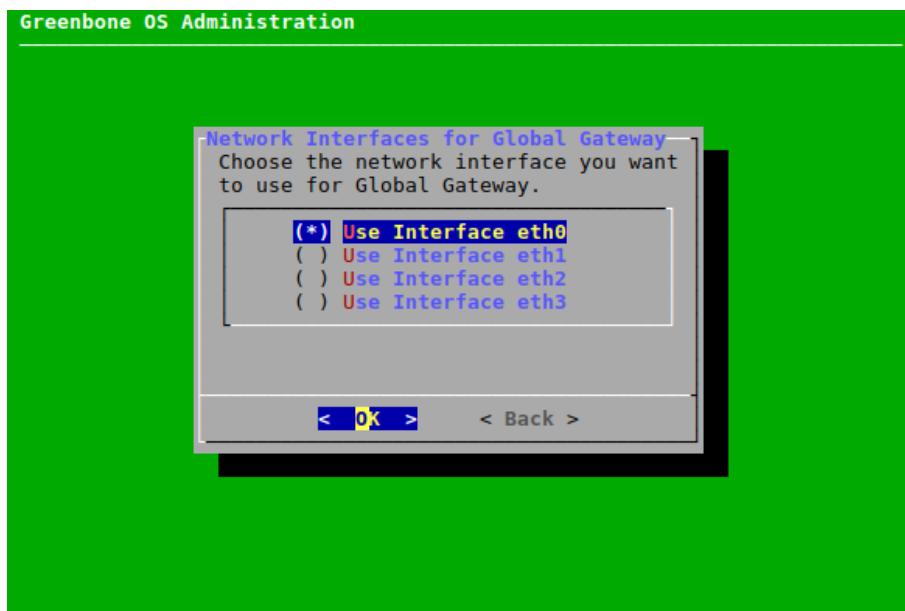


Fig. 7.21: Configuring the global gateway

6. Enter the IP address used as the global gateway in the input box and press *Enter*.
→ A message informs that the changes have to be saved (see Chapter 7.1.3 (page 122)).
7. Press *Enter* to close the message.



7.2.2.7 Setting the Host Name and the Domain Name

While the GSM does not require a special host name, the host name is an important item when creating certificates and sending e-mails.

The host name is used to configure the short host name and the domain name option is used for the domain suffix. The factory default values are:

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

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

1. Select *Setup* and press *Enter*.
2. Select *Network* and press *Enter*.
3. Select *Namespace: Management* and press *Enter*.
4. Select *Hostname* or *Domainname* and press *Enter*.
5. Enter the host name or the domain name in the input box and press *Enter* (see Fig. 7.22).

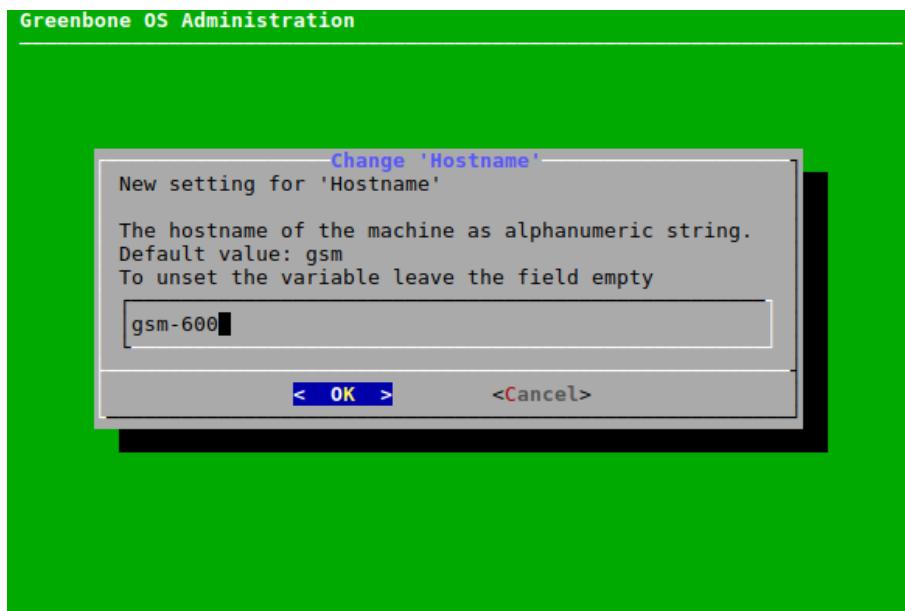


Fig. 7.22: Setting the host name/domain name

→ A message informs that the changes have to be saved (see Chapter 7.1.3 (page 122)).

6. Press *Enter* to close the message.

7.2.2.8 Restricting the Management Access

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

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

Note: This feature overlaps with the separation of namespaces (see Chapter 7.2.2 (page 132)). Separating the namespaces is recommended.



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

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

1. Select *Setup* and press *Enter*.
2. Select *Network* and press *Enter*.
3. Select *Namespace: Management* and press *Enter*.
4. Select *Management IP (v4)* or *Management IP (v6)* and press *Enter*.
5. Enter the IP address for the management interface in the input box and press *Enter* (see Fig. 7.23).

Note: The IP address has to be the IP address of one of the interfaces in the management namespace. If another IP address is set, the management interface will not be available.

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

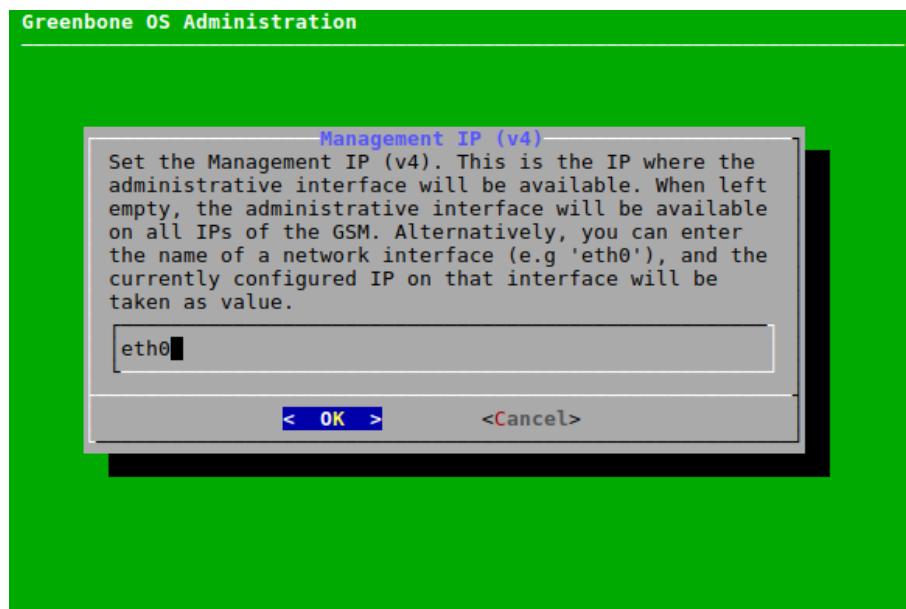


Fig. 7.23: Restricting the management access

7.2.2.9 Displaying the MAC and IP Addresses and the Network Routes

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

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

The MAC and IP addresses of the interfaces or network routes can be displayed as follows:

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



3. Select the namespace for which the IP addresses, MAC addresses or network routes should be displayed and press **Enter**.
4. Select **MAC**, **IP** or **Routes** and press **Enter**.
→ The MAC/IP addresses or the network routes of the selected namespace are displayed (see Fig. 7.24).

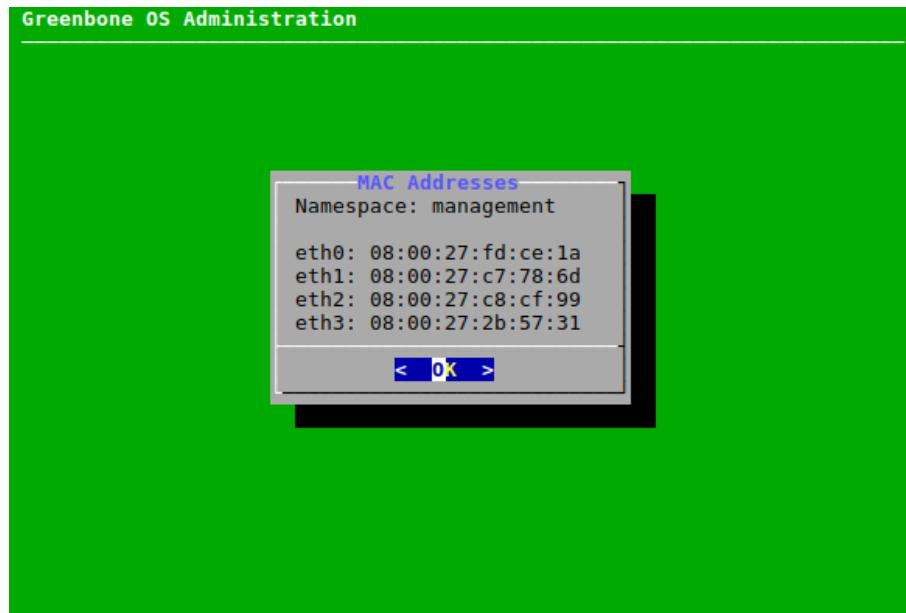


Fig. 7.24: Displaying the MAC/IP addresses or network routes

7.2.3 Configuring a Virtual Private Network (VPN) Connection

OpenVPN is integrated in GOS. To run scans through a VPN tunnel, a VPN connection has to be set up.

Note: Scanning through a VPN tunnel is only available for virtual appliances of the Midrange Class (see Chapter 3 (page 18)).

The VPN feature allows for targets that are reachable via the VPN tunnel to be scanned, but has no effect on other targets, network settings, or master-sensor connections.

The VPN tunnel is always initiated from the appliance side.

For the authentication of the GSM in the VPN, a PKCS#12 file with the following requirements is needed:

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



7.2.3.1 Setting up a VPN Connection

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

A new VPN connection can be set up as follows:

1. Select **Setup** and press **Enter**.
2. Select **VPN** and press **Enter**.
3. Select **Add a new VPN** and press **Enter** (see Fig. 7.25).

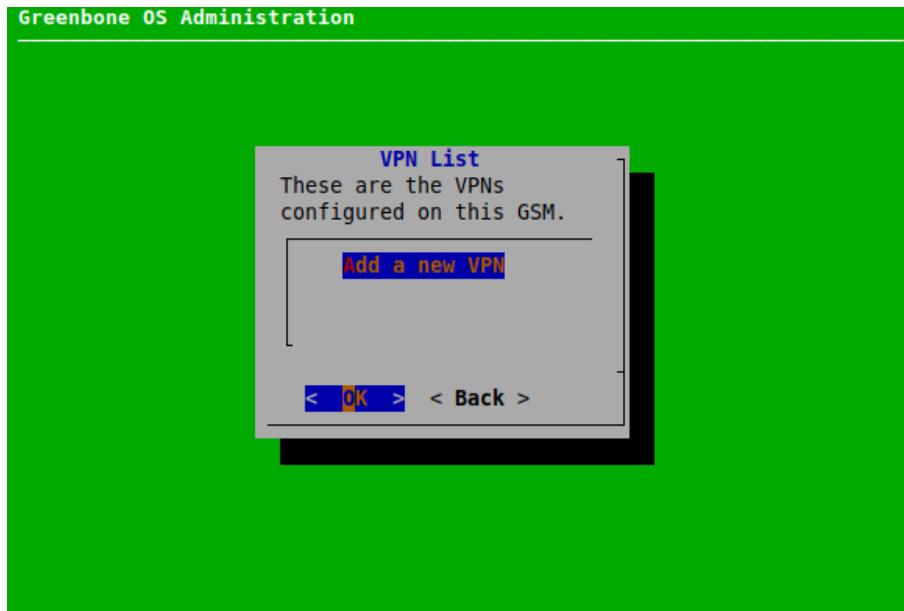


Fig. 7.25: Adding a VPN connection

4. Enter the IP address of the VPN in the input box and press **Enter**.
5. Open the web browser and enter the displayed URL.
6. Click *Browse...*, select the PKCS#12 container and click *Upload*.
7. If an export password was used to protect the PKCS#12 container, enter the password and press **Enter**.
→ A message informs that the PKCS#12 file was successfully extracted.
8. Press **Enter**.

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

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

9. Select *Certificate Authority* and press **Enter**.
10. Open the web browser and enter the displayed URL.
11. Click *Browse...*, select the CA file and click *Upload*.
→ A message informs that the CA file was imported successfully.
12. Press **Enter**.



→ The VPN connection is established and targets reachable via the VPN can be scanned (see Chapter 10.2 (page 248)).

7.2.3.2 Editing or Deleting a VPN Connection

The VPN connection can be edited as follows:

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

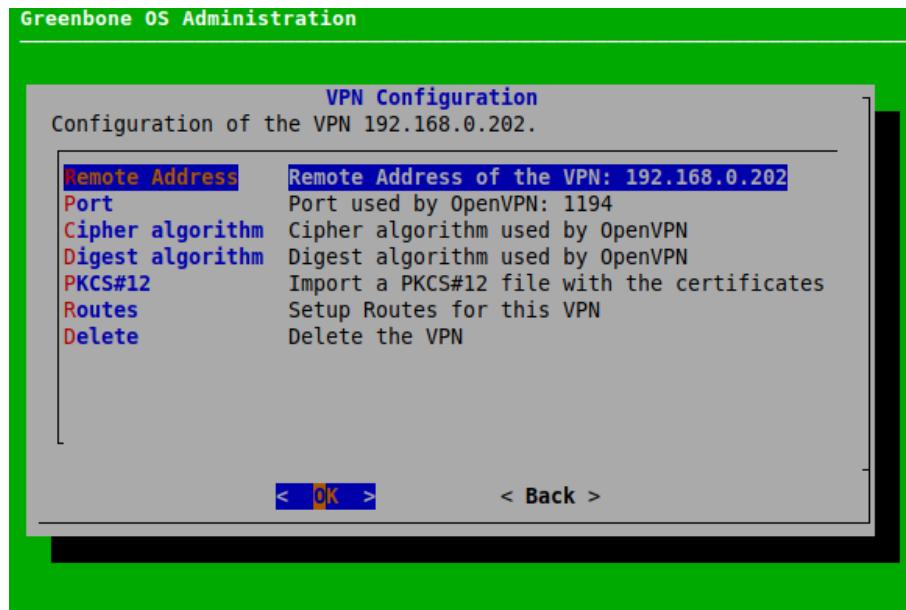


Fig. 7.26: Editing or deleting a VPN connection

The following actions are available:

Remote Address Define the IP address of the VPN.

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

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

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

PKCS#12 Replace the PKCS#12 file.

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

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

Delete Delete the VPN connection.

7.2.4 Configuring Services

To access the GSM appliance remotely, many interfaces are available:

HTTPS The web interface is the usual option for the creation, execution and analysis of vulnerability scans. It is activated by default and cannot be deactivated.



GMP (Greenbone Management Protocol) GMP allows for the communication with other Greenbone Networks products (e.g., an additional GSM). It is required for the master-sensor communication (see Chapter 16 (page 409)).

It can also be used for the communication of in-house software with the appliance (see Chapter 15 (page 399)).

SSH SSH allows to access the GOS administration menu of the GSM. This access is deactivated by default and must be activated first, e.g., by using the serial console. Additionally, SSH is required for feed updates from the Greenbone Feed Server and for the master-sensor communication (see Chapter 16 (page 409)).

SNMP SNMP read access of the GSM is possible via SNMPv3 (see Chapter 7.2.4.5 (page 157)).

7.2.4.1 Configuring HTTPS

Configuring the Timeout of the Web Interface

The timeout value of the web interface can be set as follows:

1. Select *Setup* and press *Enter*.
2. Select *Services* and press *Enter*.
3. Select *HTTPS* and press *Enter*.
4. Select *Timeout* and press *Enter*.
5. Enter the desired value for the timeout in the input box and press *Enter*.

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

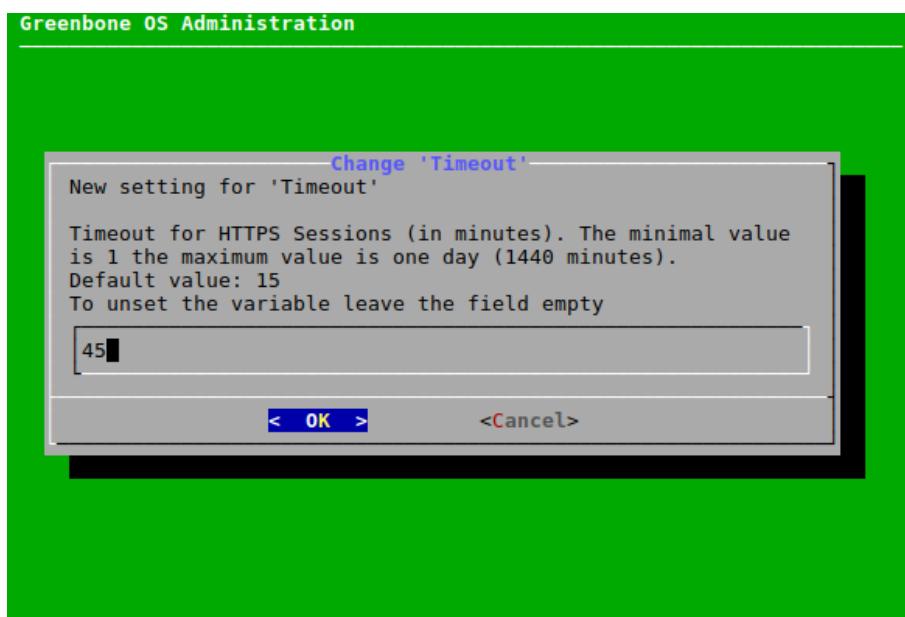


Fig. 7.27: Setting the timeout

→ A message informs that the changes have to be saved (see Chapter 7.1.3 (page 122)).

6. Press *Enter* to close the message.



Configuring the Protocols

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

1. Select *Setup* and press *Enter*.
2. Select *Services* and press *Enter*.
3. Select *HTTPS* and press *Enter*.
4. Select *Protocols* and press *Enter*.
5. Select the desired protocol version and press *Space* (see Fig. 7.28).

Note: By default, both versions are selected.

If *TLSv1.2* is selected (either alone or in combination with version 1.3), the ciphers for the HTTPS connection can be configured (see Chapter 7.2.4.1.3 (page 147)).

If only *TLSv1.3* is selected, the default value for *-ciphersuites* val of OpenSSL¹³ for the cipher suites is used. In this case, the menu option for configuring the ciphers (see Chapter 7.2.4.1.3 (page 147)) is not available.

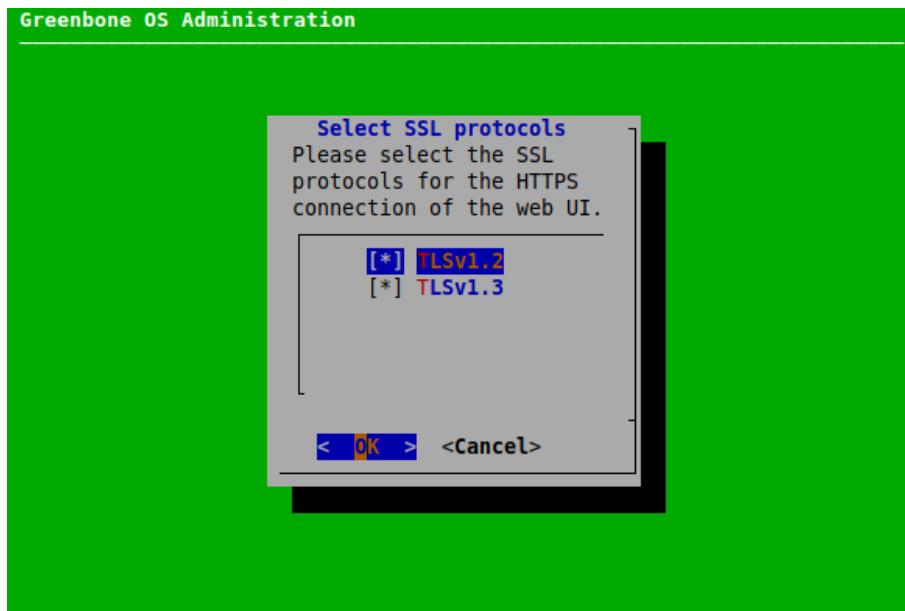


Fig. 7.28: Configuring the protocols for the HTTPS connection

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

Configuring the Ciphers

If TLS version 1.2 is used for the HTTPS connection of the web interface (either alone or in combination with version 1.3, see Chapter 7.2.4.1.2 (page 147)), the HTTPS ciphers can be configured. The current setting allows only secure ciphers using at least 128 bit key length, explicitly disallowing the cipher suites used by SSLv3 and TLSv1.0. Note that for TLSv1.1 no ciphers exist.

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

¹³ <https://www.openssl.org/docs/man1.1.1/man1/ciphers.html>



2. Select *Services* and press **Enter**.
3. Select *HTTPS* and press **Enter**.
4. Select *Ciphers* and press **Enter**.
5. Enter the desired value in the input box and press **Enter** (see Fig. 7.29).

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

More information about the syntax can be found here¹⁴.

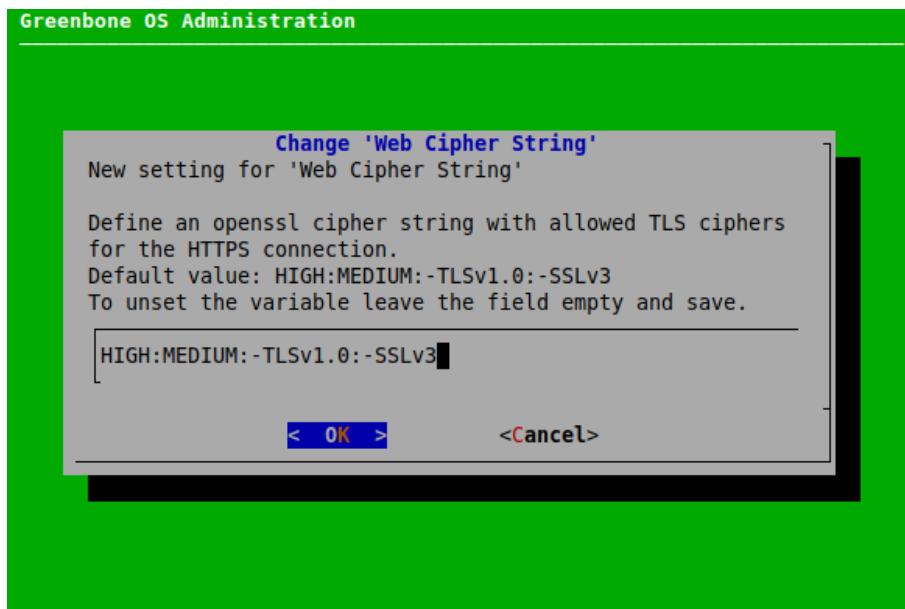


Fig. 7.29: Configuring the ciphers

→ A message informs that the changes have to be saved (see Chapter 7.1.3 (page 122)).

6. Press **Enter** to close the message.

Managing Certificates

The GSM appliance basically uses two types of certificates:

- Self-signed certificates
- Certificates issued by an external CA

All modern operating systems support the creation and management of their own CA. Under Microsoft Windows Server the Active Directory Certificate Services support the administrator in the creation of a root CA¹⁵. For Linux systems various options are available. One option is described in the IPSec-Howto¹⁶.

When creating and exchanging certificates it needs to be considered that the administrator verifies how the systems are accessed later before creating the certificate. The IP address or the DNS name is stored when creating the certificate. Additionally, after creating the certificate a reboot is required so that all services can use the new certificate. This needs to be taken into consideration when changing certificates.

¹⁴ <https://www.openssl.org/docs/man1.1.1/man1/ciphers.html>

¹⁵ [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc731183\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc731183(v=ws.11))

¹⁶ <http://www.ipsec-howto.org/x600.html>



The current certificate can be displayed as follows:

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

→ The certificate is displayed.

Self-Signed Certificates

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

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

To support a quick setup, the GSM supports self-signed certificates. For most GSM models, such a certificate is not installed by default and must be created by the administrator. The GSM ONE, however, already comes with a pre-installed certificate.

Self-signed certificates can be easily created as follows:

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

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

6. Confirm the message by selecting *Yes* and pressing *Enter*.
7. Provide the settings for the certificate (see Fig. 7.30), select *OK* and press *Enter*.

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

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

→ When the process is finished, a message informs that the certificate can be downloaded.

8. Press *Enter* to close the message.
9. Select *Download* and press *Enter*.
10. Open the web browser and enter the displayed URL.
11. Download the PEM file.

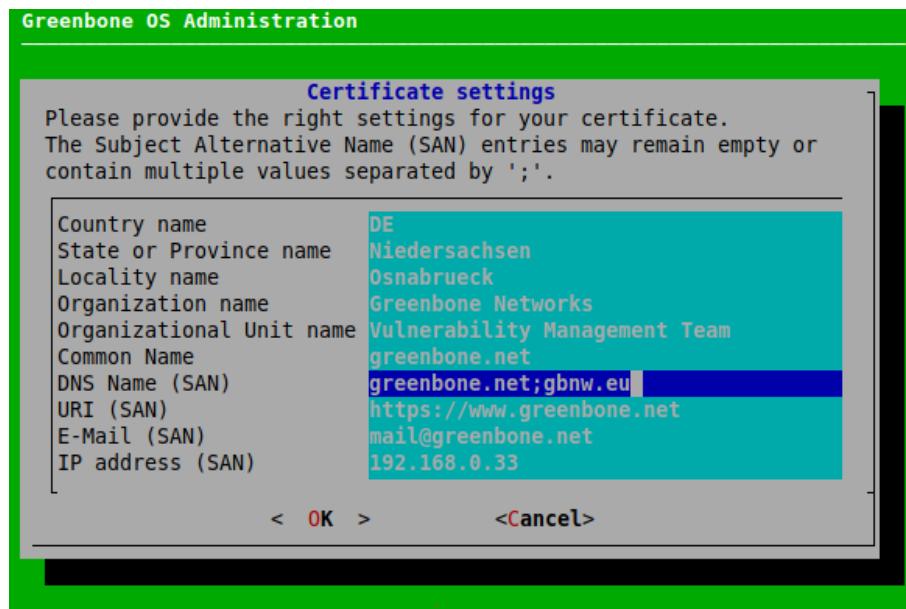


Fig. 7.30: Providing settings for the certificate

12. In the GOS administration menu press **Enter**.
 - When the certificate is retrieved by the GSM, the GOS administration menu displays the fingerprint of the certificate for verification.
13. Check the fingerprint and confirm the certificate by pressing **Enter**.
 - To enable the new certificate a *Reboot* of the GSM is required (see Chapter 7.3.9.1 (page 191)).

Certificate by an External Certificate Authority (CA)

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

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

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

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

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

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



4. Select *Certificate* and press **Enter**.
5. Select *CSR* and press **Enter**.
→ A message informs that the current certificate and private key will be overwritten.
6. Confirm the message by selecting *Yes* and pressing **Enter**.
7. Provide the settings for the certificate (see Fig. 7.31), select *OK* and press **Enter**.

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

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

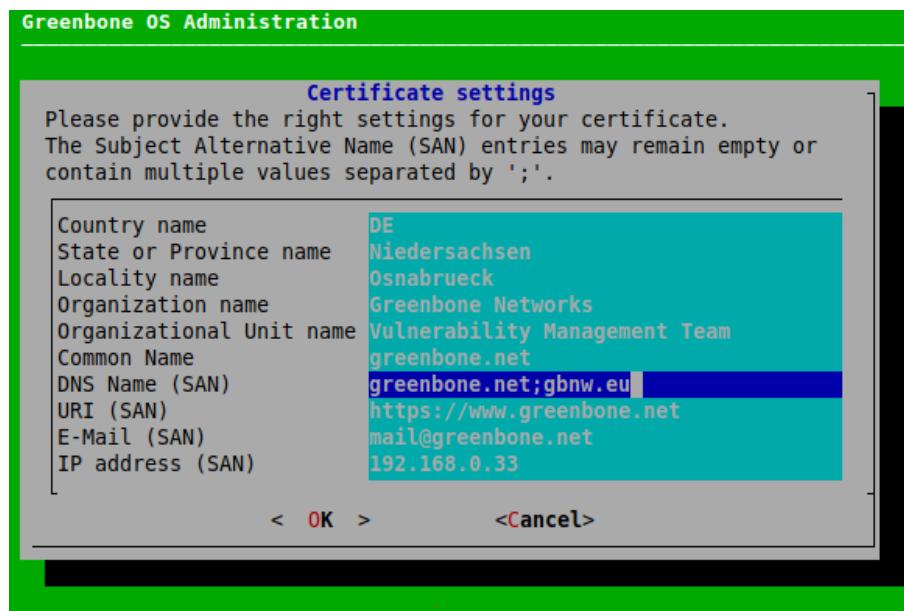


Fig. 7.31: Providing settings for the certificate

8. Open the web browser and enter the displayed URL.
9. Download the PEM file.
→ The GOS administration menu displays a message to verify that the CSR has not been tampered with.
10. Verify the information by pressing **Enter**.
11. When the certificate is signed, select *Certificate* and press **Enter**.
12. Open the web browser and enter the displayed URL.
13. Click *Browse...*, select the signed certificate and click *Upload*.
→ When the certificate is retrieved by the GSM, the GOS administration menu displays the fingerprint of the certificate for verification.
14. Check the fingerprint and confirm the certificate by pressing **Enter**.
→ To enable the new certificate a *Reboot* of the GSM is required (see Chapter 7.3.9.1 (page 191)).

If a private key and a signed certificate which should be used for the GSM are already available, they can be imported. The private key and the certificate need to be formatted as a PKCS#12 file. The file can be protected using an export password.



The PKCS#12 file can be imported as follows:

1. Select *Setup* and press *Enter*.
2. Select *Services* and press *Enter*.
3. Select *HTTPS* and press *Enter*.
4. Select *Certificate* and press *Enter*.
5. Select *PKCS#12* and press *Enter*.
→ A message informs that the current certificate and private key will be overwritten.
6. Confirm the message by selecting *Yes* and pressing *Enter*.
7. Open the web browser and enter the displayed URL.
8. Click *Browse...*, select the PKCS#12 container and click *Upload*.

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

- When the certificate is retrieved by the GSM, the GOS administration menu displays the fingerprint of the certificate for verification.
9. Check the fingerprint and confirm the certificate by pressing *Enter*.
→ To enable the new certificate a *Reboot* of the GSM is required (see Chapter 7.3.9.1 (page 191)).

Displaying Fingerprints

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

1. Select *Setup* and press *Enter*.
2. Select *Services* and press *Enter*.
3. Select *HTTPS* and press *Enter*.
4. Select *Fingerprints* and press *Enter*.
→ The following fingerprints of the currently active certificate are displayed:
 - SHA1
 - SHA256
 - BB



```

Greenbone OS Administration

Certificate Fingerprints

SHA1
Fingerprint=3E:99:30:DE:4B:07:01:00:BE:9B:BF:F7:83:ED:B5:20:6F:DF:A
4:40

SHA256
Fingerprint=74:38:6E:D3:D1:10:F8:DE:2E:1E:C6:36:A7:8E:2D:57:66:DB:A
0:03:24:FF:8E:FD:AC:4A:A1:12:6B:5A:4F:65

BB
Fingerprint=xomec-rocus-bibav-tukes-menylv-sutiv-heruc-gebuz-zoxax

< OK >

```

Fig. 7.32: Displaying the fingerprints

7.2.4.2 Configuring the Greenbone Management Protocol (GMP)

The Greenbone Management Protocol (GMP) can be activated using the GOS administration menu as follows:

Note: The SSH service has to be enabled before GMP can be enabled (see Chapter 7.2.4.4 (page 154)).

1. Select *Setup* and press *Enter*.
2. Select *Services* and press *Enter*.
3. Select *GMP* and press *Enter*.
4. Press *Enter* to enable or disable GMP (see Fig. 7.33).
→ A message informs that the changes have to be saved (see Chapter 7.1.3 (page 122)).
5. Press *Enter* to close the message.

7.2.4.3 Configuring the Open Scanner Protocol (OSP)

The Open Scanner Protocol (OSP) can be activated using the GOS administration menu as follows:

Note: The SSH service has to be enabled before OSP can be enabled (see Chapter 7.2.4.4 (page 154)).

1. Select *Setup* and press *Enter*.
2. Select *Services* and press *Enter*.
3. Select *OSP* and press *Enter*.
4. Press *Enter* to enable or disable OSP.
→ A message informs that the changes have to be saved (see Chapter 7.1.3 (page 122)).
5. Press *Enter* to close the message.

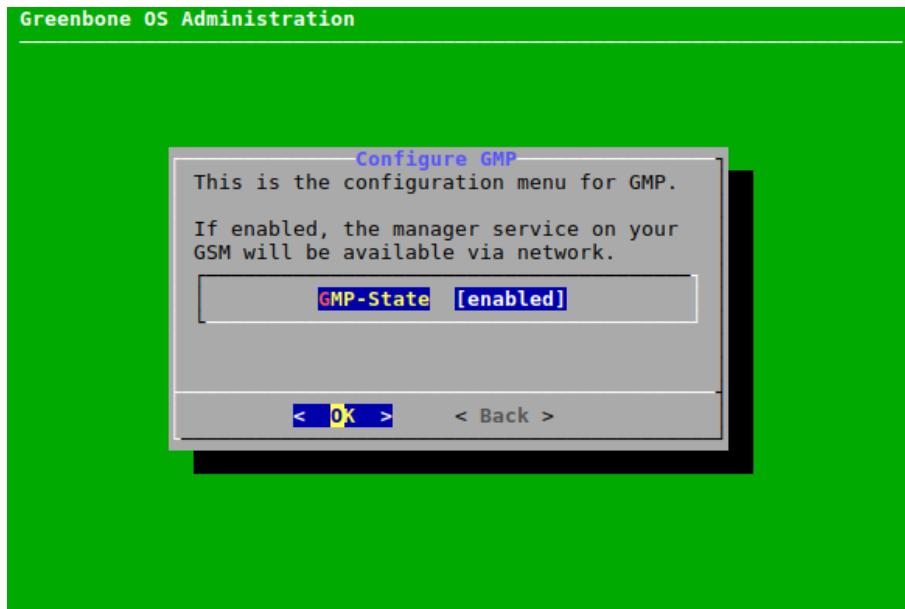


Fig. 7.33: Enabling GMP

7.2.4.4 Configuring SSH

Enabling the SSH State

The SSH server embedded in the GSM can be enabled in the GOS administration menu as follows:

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

Enabling and Managing a Login Protection

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

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

Note: The login protection does not block logging in via SSH admin key if such a key is set up (see Chapter 7.2.4.4.3 (page 155)).

The login protection can be enabled and managed as follows:

1. Select **Setup** and press **Enter**.
2. Select **Services** and press **Enter**.
3. Select **SSH** and press **Enter**.
4. Select **Login Protection** and press **Enter**.

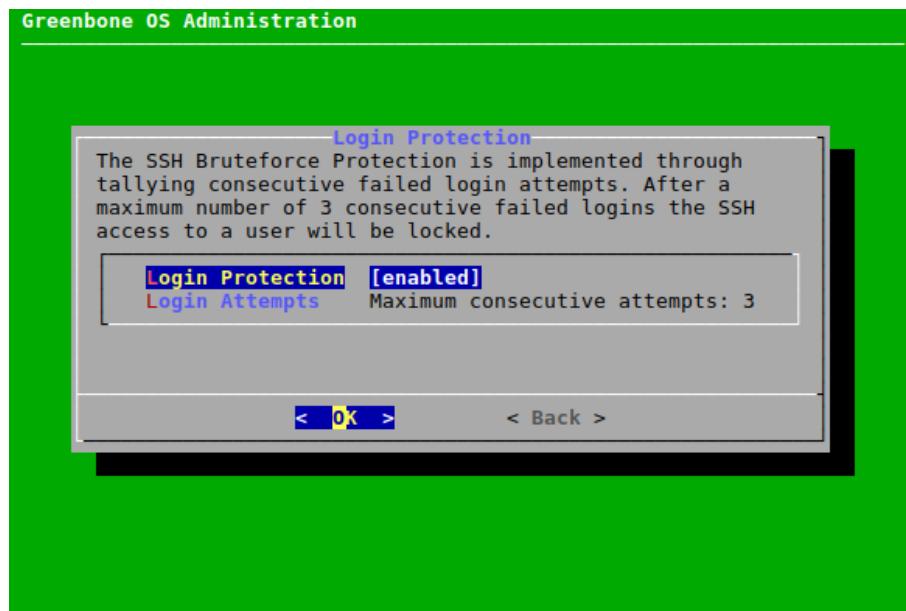


Fig. 7.34: Setting a login protection

5. Select *Login Protection* and press `Enter` (see Fig. 7.34).
→ A message informs that the login protection can lead to a locked SSH access.
6. Select *Continue* and press `Enter` to enable the login protection.
7. Select *Login Attempts* and press `Enter`.
8. Enter the desired value and press `Enter`.
→ A message informs that the changes have to be saved (see Chapter 7.1.3 (page 122)).
9. Press `Enter` to close the message.

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

1. Select *Setup* and press `Enter`.
2. Select *User* and press `Enter`.
3. Select *Unlock SSH* and press `Enter`.
→ The login attempt counter is reset.
4. Press `Enter` to close the message.

Adding an SSH Admin Key

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

Note: SSH keys can be generated with OpenSSH by using the command `ssh-keygen` on Linux or `puttygen.exe` if using PuTTY on Microsoft Windows. The formats Ed25519 or RSA are supported. All SSH keys must correspond to RFC 4716¹⁷.

¹⁷ <https://tools.ietf.org/html/rfc4716>



An SSH admin key can be uploaded as follows:

1. Select **Setup** and press **Enter**.
2. Select **Services** and press **Enter**.
3. Select **SSH** and press **Enter**.
4. Select **Admin Key** and press **Enter**.
5. Open the web browser and enter the displayed URL (see Fig. 7.35).

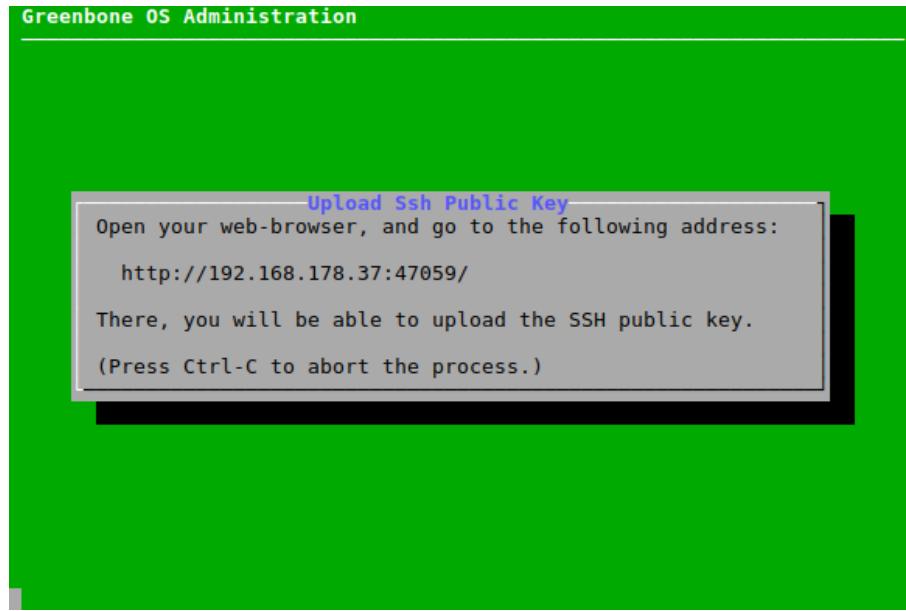


Fig. 7.35: Uploading an SSH public key

6. Click **Browse...**, select the SSH public key and click **Upload**.
→ When the upload is completed, a message informs that the login via SSH is possible.

Displaying Fingerprints

The GSM provides different host keys for its own authentication. The client decides which public key to use. In the GOS administration menu the fingerprint of the public keys used by the SSH server of the appliance can be displayed as follows:

1. Select **Setup** and press **Enter**.
2. Select **Services** and press **Enter**.
3. Select **SSH** and press **Enter**.
4. Select **Fingerprint** and press **Enter**.
→ The SHA256 fingerprints of the following keys are displayed:
 - ED25519
 - RSA



7.2.4.5 Configuring SNMP

The GSM appliance supports SNMP. The SNMP support can be used for sending traps through alerts and monitoring of vital parameters of the appliance.

The supported parameters are specified in a Management Information Base (MIB) file. The current MIB is available from the Greenbone Tech-Doc-Portal¹⁸.

The GSM supports SNMPv3 for read access and SNMPv1 for traps.

The SNMPv3 can be configured as follows:

1. Select *Setup* and press *Enter*.
2. Select *Services* and press *Enter*.
3. Select *SNMP* and press *Enter*.
4. Select *SNMP* and press *Enter* to enable SNMP.
→ Several new options are displayed (see Fig. 7.36).

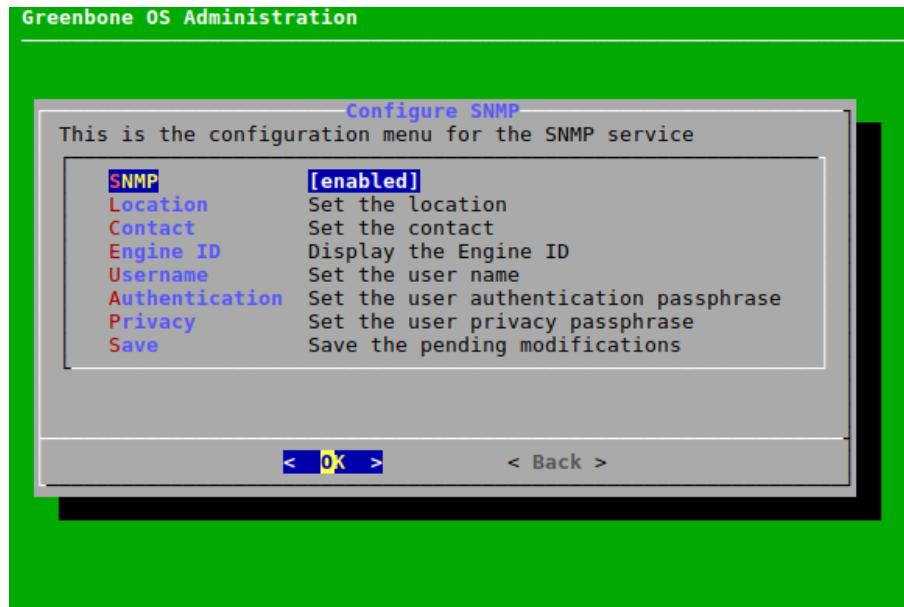


Fig. 7.36: Configuring SNMPv3

5. Select *Location* and press *Enter*.
6. Enter the location of the SNMP service in the input box and press *Enter*.
7. Select *Contact* and press *Enter*.
8. Enter the contact of the SNMP service in the input box and press *Enter*.
9. Select *Username* and press *Enter*.
10. Enter the SNMP user name in the input box and press *Enter*.

Note: When configuring the authentication and privacy passphrase be aware of the fact that the GSM uses SHA-1 and AES128 respectively.

11. Select *Authentication* and press *Enter*.

¹⁸ <https://docs.greenbone.net/API/SNMP/snmp-gos-20.08-21.04.en.html>



12. Enter the SNMP user authentication passphrase in the input box and press **Enter**.
13. Select *Privacy* and press **Enter**.
14. Enter the SNMP user privacy passphrase in the input box and press **Enter**.

Note: After a user has been configured, the engine ID of the GSM can be displayed by selecting *Engine ID* and pressing **Enter**.

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

```
$ snmpwalk -v 3 -l authPriv -u user -a sha -A password -x aes -X key 192.168.222.115
iso .3.6.1.2.1.1.0 = STRING: "Greenbone Security Manager"
iso .3.6.1.2.1.1.5.0 = STRING: "gsm"
...
```

The following information can be gathered:

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

7.2.4.6 Configuring a Port for the Temporary HTTP Server

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

A permanent port can be configured as follows:

1. Select *Setup* and press **Enter**.
2. Select *Services* and press **Enter**.
3. Select *Temporary HTTP* and press **Enter**.
4. Select *Port* and press **Enter**.
5. Enter the port in the input box and press **Enter**.
→ A message informs that the changes have to be saved (see Chapter 7.1.3 (page 122)).
6. Press **Enter** to close the message.

7.2.5 Configuring Periodic Backups

The GSM supports automatic daily backups. These backups are stored locally or remote using the following scheme:

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

Backups older than one year will be deleted automatically. In factory state backups are disabled.



Periodic Backups can be enabled as follows:

1. Select *Setup* and press *Enter*.
2. Select *Backup* and press *Enter*.
3. Select *Periodic Backup* and press *Enter* (see Fig. 7.37).
→ Periodic backups are enabled.

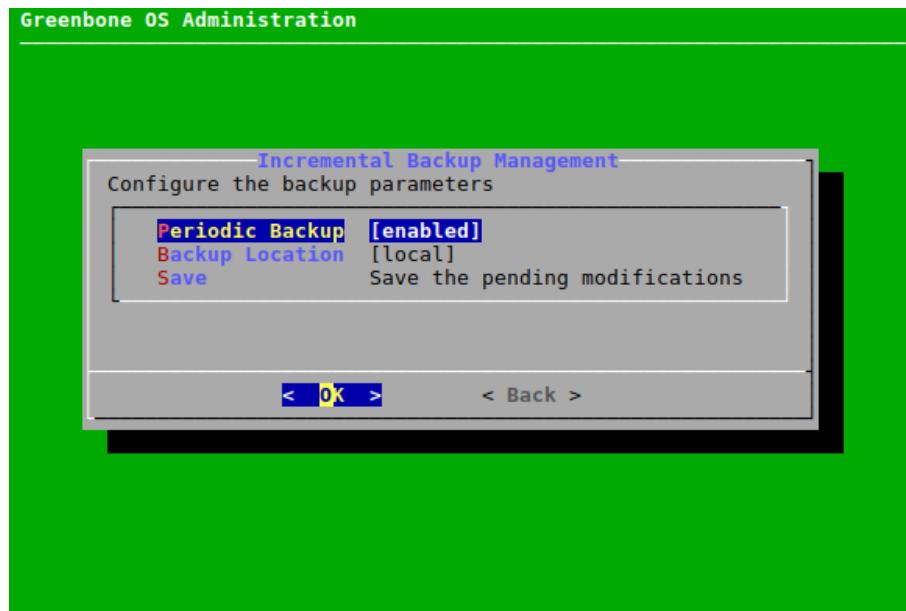


Fig. 7.37: Configuring periodic backups

By default, backups are stored locally. To store them on a remote server the server has to be set up appropriately. The GSM uses the Secure File Transfer Protocol (SFTP) supported by SSH to transfer the backups.

Set up a remote server as follows:

1. Select *Setup* and press *Enter*.
2. Select *Backup* and press *Enter*.
3. Select *Backup Location* and press *Enter*.
→ More options for the backup location are added (see Fig. 7.38).
4. Select *Server* and press *Enter*.
5. Enter the remote server address in the following format:
`username@hostname[:port]/directory`

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

6. Select *OK* and press *Enter*.
→ A message informs that the changes have to be saved (see Chapter 7.1.3 (page 122)).
7. Press *Enter* to close the message.

Note: The GSM uses a public key to identify the remote server before logging in.

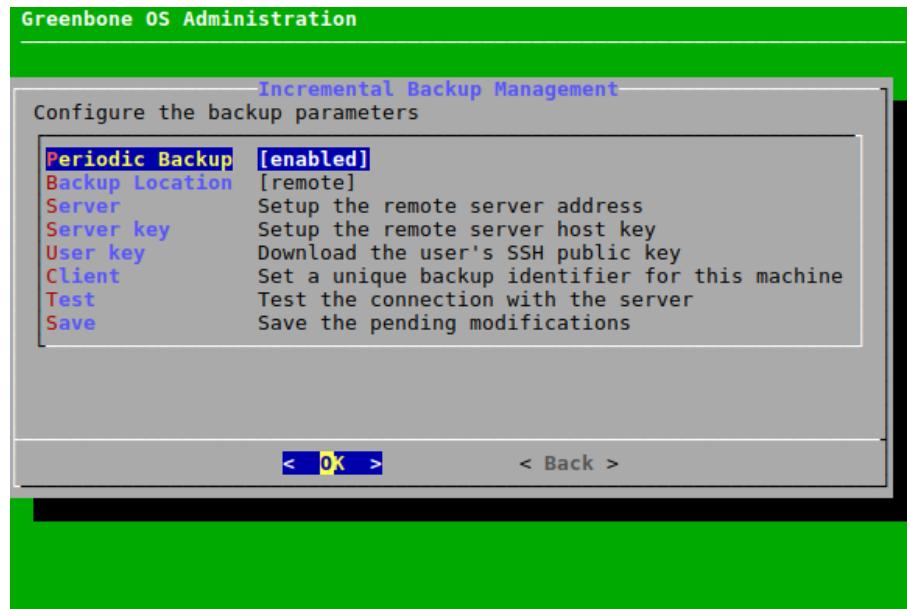


Fig. 7.38: Setting up the remote server

8. Select *Server key* and press Enter.
9. Open the web browser and enter the displayed URL (see Fig. 7.39).

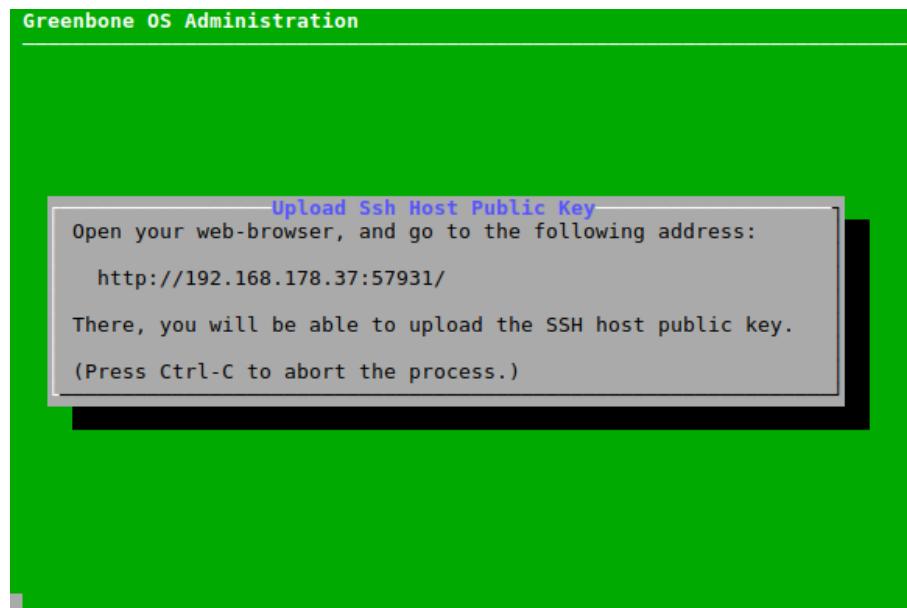


Fig. 7.39: Setting up the server key

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

Tip: The SSH host public key has to be looked up on the remote backup server. On Linux and most Unix-like systems it can be found under /etc/ssh/ssh_host_*_key.pub.



Note: The GSM uses an SSH private key to log in on the remote server. To enable this login process the public key of the GSM must be enabled in the `authorized_keys` file on the remote server. The GSM generates such a private/public key pair.

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

Note: If several GSM appliances upload their backups to the same remote server, the files must be distinguishable. For this a unique backup identifier has to be defined. If this identifier is not set, the hostname will be used. If the hostname was modified from the default and is unique, the backup files will be distinguishable as well.

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

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

16. Select *Test* and press **Enter**.
→ The login to the remote system is tested.

7.2.6 Configuring the Feed Synchronization

The Greenbone Security Feed (GSF) provides updates to the Network Vulnerability Tests (NVT), the SCAP data (CVE and CPE) and the advisories from the CERT-Bund and DFN-CERT. Additionally, the GSF provides updates for GOS.

A GSF subscription key is required to use the GSF (see Chapter 7.1.1 (page 120)). This key allows the GSM to download the GSF provided by Greenbone Networks.

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



The steps for configuring the feed synchronization which are described in the following chapters are briefly explained in a video based on GOS 5.0¹⁹ (German only).

¹⁹ <https://youtu.be/4AYd4uzweY0>



7.2.6.1 Adding a Greenbone Security Feed (GSF) Subscription Key

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

For information about the GSF subscription key see Chapter 7.1.1 (page 120).

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

The key can be added using HTTP as follows:

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

→ A message informs that the current subscription key will be overwritten (see Fig. 7.40).

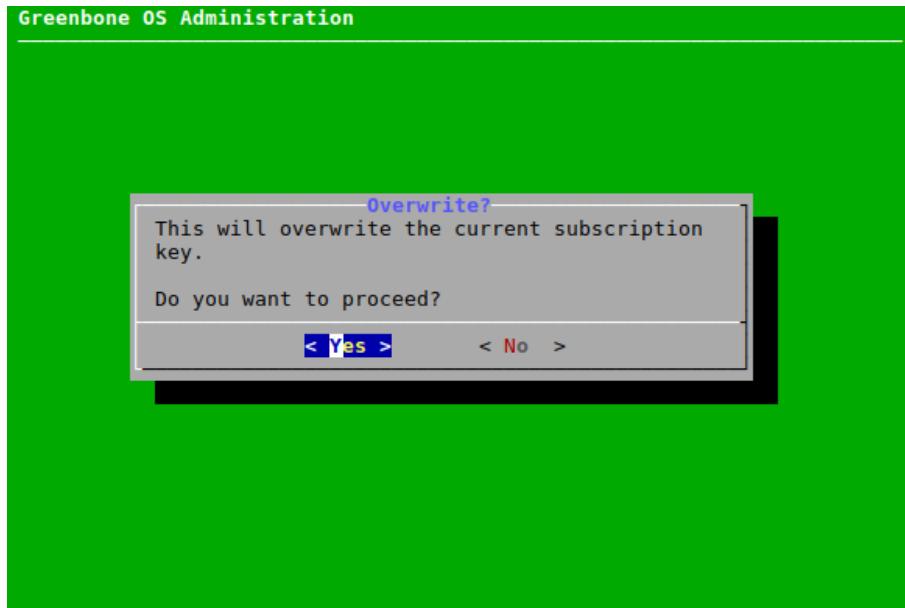


Fig. 7.40: Overwriting the current subscription key

4. Select *Yes* and press *Enter*.
5. Open the web browser and enter the displayed URL.
6. Click *Browse...*, select the subscription key and click *Upload*.

The key can be added using the editor as follows:

1. Select *Setup* and press *Enter*.
 2. Select *Feed* and press *Enter*.
 3. Select *Key(Editor)* and press *Enter*.
- A message informs that the current subscription key will be overwritten (see Fig. 7.40).
4. Select *Yes* and press *Enter*.
 - The editor is opened.
 5. Enter the subscription key.



6. Press **Ctrl + X**.
7. Press **Y** to save the changes.
8. Press **Enter**.

7.2.6.2 Enabling or Disabling Synchronization

The automatic synchronization of the GSF can be disabled if the GSM does not have any internet access and should not try to access the Greenbone Networks services on the internet. The synchronization can be enabled again.

The synchronization can be enabled or disabled as follows:

1. Select **Setup** and press **Enter**.
2. Select **Feed** and press **Enter**.
3. Select **Synchronisation** and press **Enter**.
→ The synchronization is enabled.
4. The synchronization can be disabled by selecting **Synchronisation** and pressing **Enter** again.

Note: The time of the automatic feed synchronization can be set by changing the maintenance time (see Chapter 7.2.12 (page 177)).

7.2.6.3 Configuring the Synchronization Port

The GSF is provided by Greenbone Networks on two different ports:

- 24/tcp
- 443/tcp

While port 24/tcp is the default port, many firewall setups do not allow traffic to pass to this port on the internet. So the modification of the port to 443/tcp is possible. This port is most often allowed.

The port can be configured as follows:

1. Select **Setup** and press **Enter**.
2. Select **Feed** and press **Enter**.
3. Select **Greenbone Server** and press **Enter**.
4. Select **Sync port** and press **Enter**.
5. Select the desired port and press **Enter** (see Fig. 7.41).

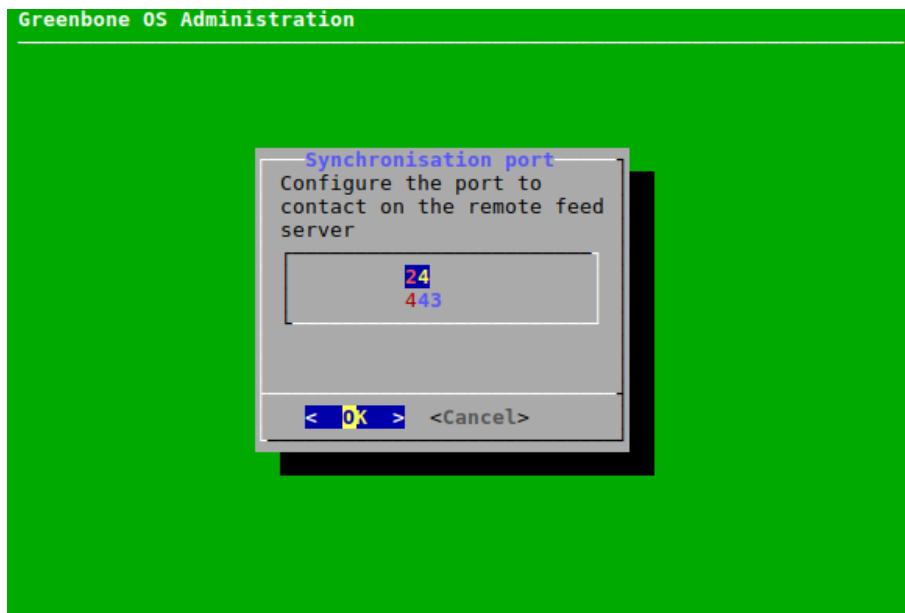


Fig. 7.41: Configuring the synchronization port

Note: The port 443/tcp is usually used by HTTPS traffic. While the GSM uses this port, the actual traffic is not HTTPS but SSH. The GSM uses rsync embedded in SSH to retrieve the feed. Firewalls supporting deep inspection and application awareness may still reject the traffic if these features are enabled.

7.2.6.4 Setting the Synchronization Proxy

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

The proxy can be set as follows:

1. Select *Setup* and press *Enter*.
2. Select *Feed* and press *Enter*.
3. Select *Greenbone Server* and press *Enter*.
4. Select *Sync proxy* and press *Enter*.
5. Enter the URL of the proxy in the input box (see Fig. 7.42).

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

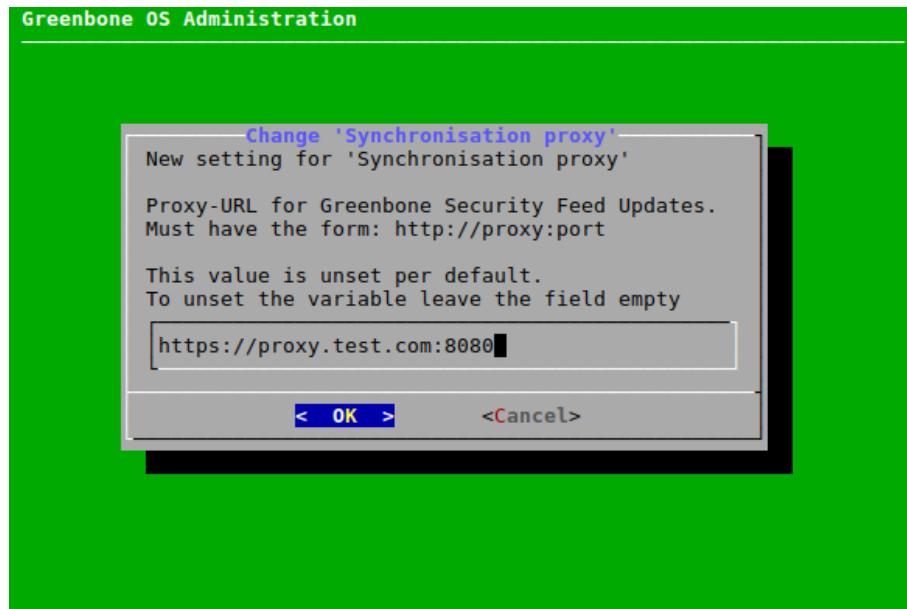


Fig. 7.42: Setting the synchronization proxy

7.2.6.5 Deleting the Greenbone Security Feed (GSF) Subscription Key

The GSF subscription key can be removed. This is useful if an appliance is at the end of life and is not used anymore. The cleanup ensures that no licenses are left on the appliance. Without the GSF subscription key the GSM will only retrieve the Greenbone Community Feed.

There is a warning when choosing this option.

The cleanup can be done as follows:

1. Select *Setup* and press **Enter**.
2. Select *Feed* and press **Enter**.
3. Select *Cleanup* and press **Enter**.
→ A warning informs that the synchronization with the GSF is no longer possible after the cleanup (see Fig. 7.43).
4. Select *Yes* and press **Enter**.
→ A message informs that the GSF subscription key has been deleted.
5. Press **Enter** to close the message.

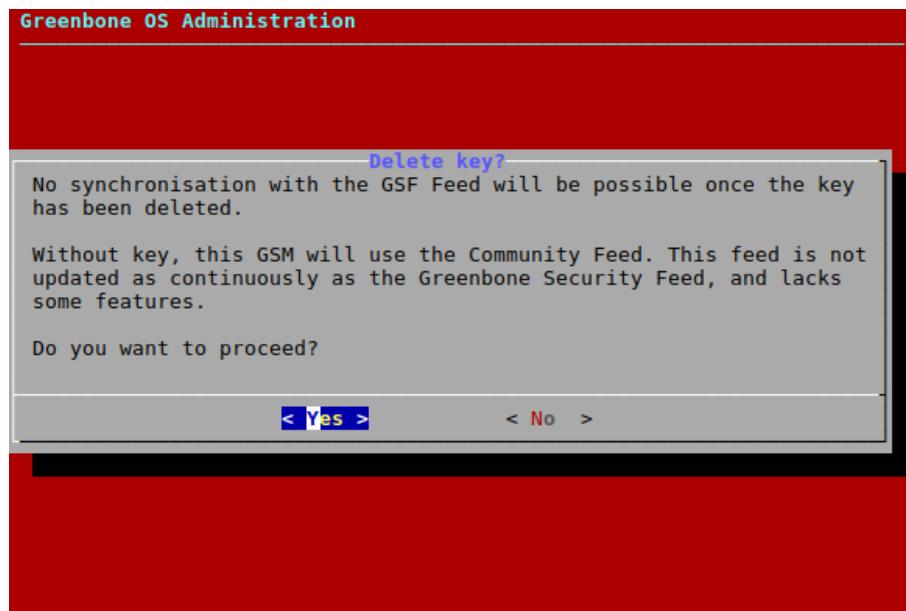


Fig. 7.43: Removing the GSF subscription key

7.2.7 Configuring the GSM as an Airgap Master/Sensor

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

Two GSMS are required:

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

All GSM models from GSM 400 or higher can be configured as an Airgap master/sensor.

Two options are available for the Airgap function:

- Greenbone Airgap USB stick
- Airgap FTP server

7.2.7.1 Using the Airgap USB Stick

The updates and upgrades are loaded from a GSM that is connected to the internet and copied to a USB stick. The USB stick can then be used to update the second GSM.

Note: The USB stick has to be a specific Greenbone Airgap USB stick provided by Greenbone Networks. Contact the Greenbone Networks support via e-mail (support@greenbone.net) providing the customer number to request a respective Airgap USB stick.

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

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

1. In the GOS administration menu of the Airgap master select *Setup* and press *Enter*.



2. Select *Feed* and press **Enter**.
3. Select *Airgap Master* and press **Enter**.
4. Select *USB Master* and press **Enter** (see Fig. 7.44).

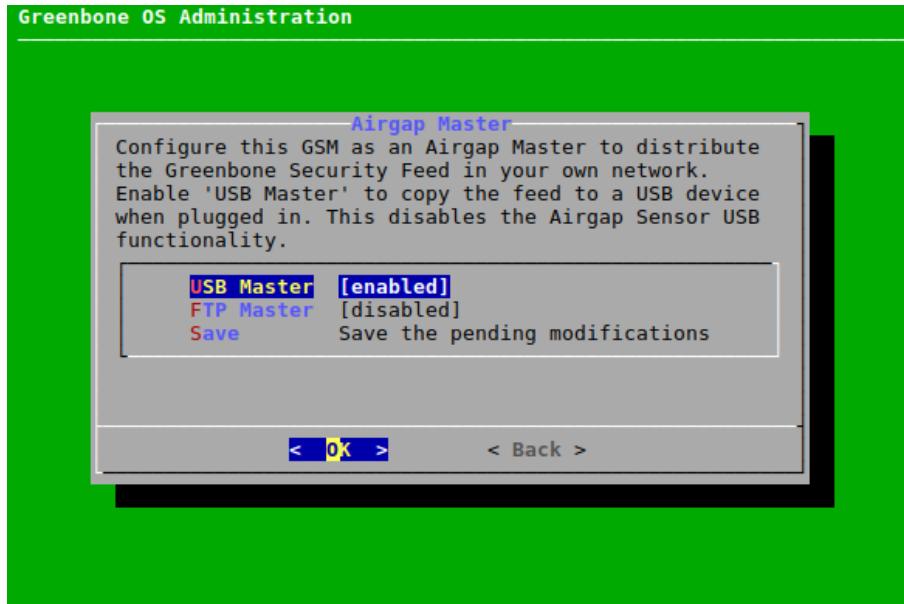


Fig. 7.44: Configuring the Airgap USB master

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

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

6. Connect the Airgap USB stick to the Airgap master.
→ The data transfer starts automatically.
7. When the data transfer is finished, connect the Airgap USB stick to the Airgap sensor.
→ The data transfer starts automatically.

7.2.7.2 Using the Airgap FTP Server

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

The FTP server takes on the function of the Airgap USB stick (see Chapter 7.2.7.1 (page 166)).

- The Airgap master picks up the updates/upgrades from the Greenbone server and writes it to the FTP server at its maintenance time.
- The Airgap sensor downloads the updates/upgrades from the FTP server at its maintenance time.

Note: Ensure that the maintenance time of the Airgap sensor is at least three hours behind the maintenance time of the Airgap master (see Chapter 7.2.8 (page 169)).



The data transfer using the Airgap FTP server is performed as follows:

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

→ Additional menu options for the configuration of the FTP server are shown (see Fig. 7.45).

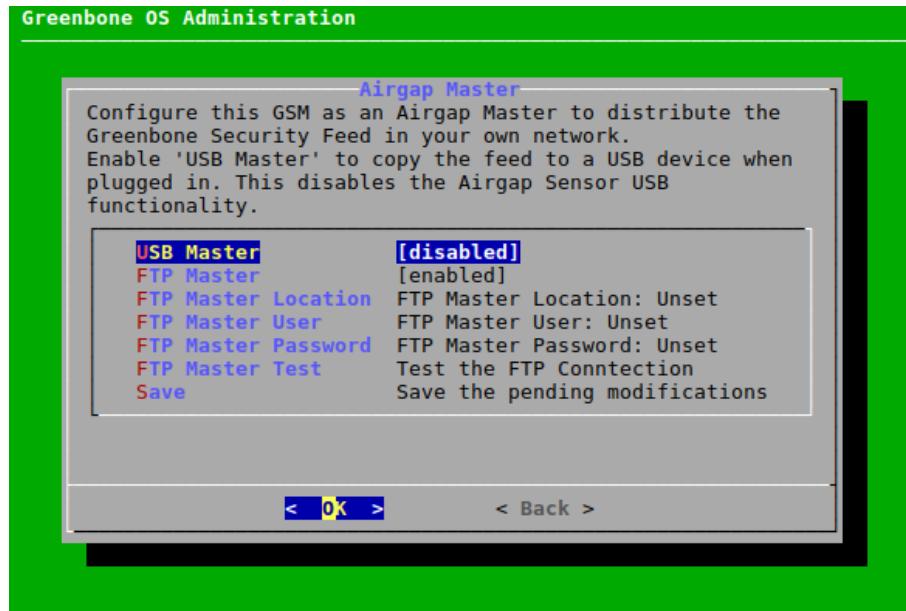


Fig. 7.45: Configuring the FTP server for the Airgap master

5. Select *FTP Master Location* and press *Enter*.
6. Enter the path of the FTP server in the input box and press *Enter*.
7. Select *FTP Master User* and press *Enter*.
8. Enter the user used for logging into the FTP server in the input box and press *Enter*.
9. Select *FTP Master Password* and press *Enter*.
10. Enter the password used for logging into the FTP server in the input box and press *Enter*.
11. Select *FTP Master Test* and press *Enter*.
→ It is tested whether a login with the entered information is working.
12. Select *Save* and press *Enter*.
13. In the GOS administration menu of the Airgap sensor select *Setup* and press *Enter*.
14. Select *Feed* and press *Enter*.
15. Select *Airgap Sensor* and press *Enter*.
16. Execute steps 5 to 12 in the GOS administration menu of the Airgap sensor using the same input as for the Airgap master.

Note: The menu options have slightly different names compared to the GOS administration menu of the Airgap master (see Fig. 7.46).



→ The data transfer starts automatically.

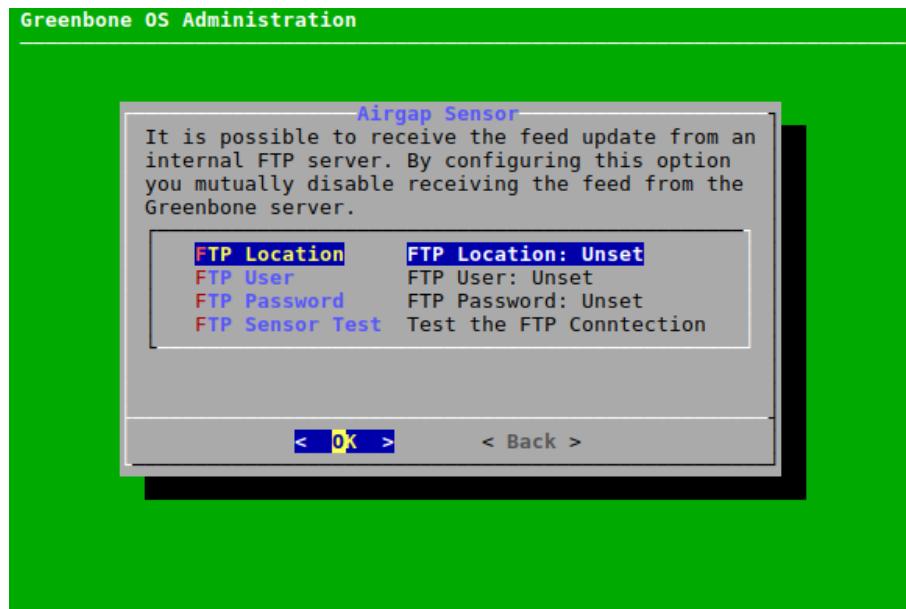


Fig. 7.46: Configuring the FTP server for the Airgap sensor

7.2.8 Configuring the Time Synchronization

To synchronize the appliance with central time servers, the GSM supports the Network Time Protocol (NTP). Up to four different NTP servers can be configured. The appliance will choose the most suitable server. During an outage of one server, another server will be used automatically.

Both IP addresses and DNS names are supported.

The NTP settings can be configured as follows:

1. Select *Setup* and press *Enter*.
2. Select *Timesync* and press *Enter*.
3. Select *Time synchronisation* and press *Enter*.
→ The time synchronization is enabled.
4. Select the desired time server and press *Enter* (see Fig. 7.47).
5. Enter the time server in the input box and press *Enter*.
→ A message informs that the changes have to be saved (see Chapter 7.1.3 (page 122)).
6. Press *Enter* to close the message.

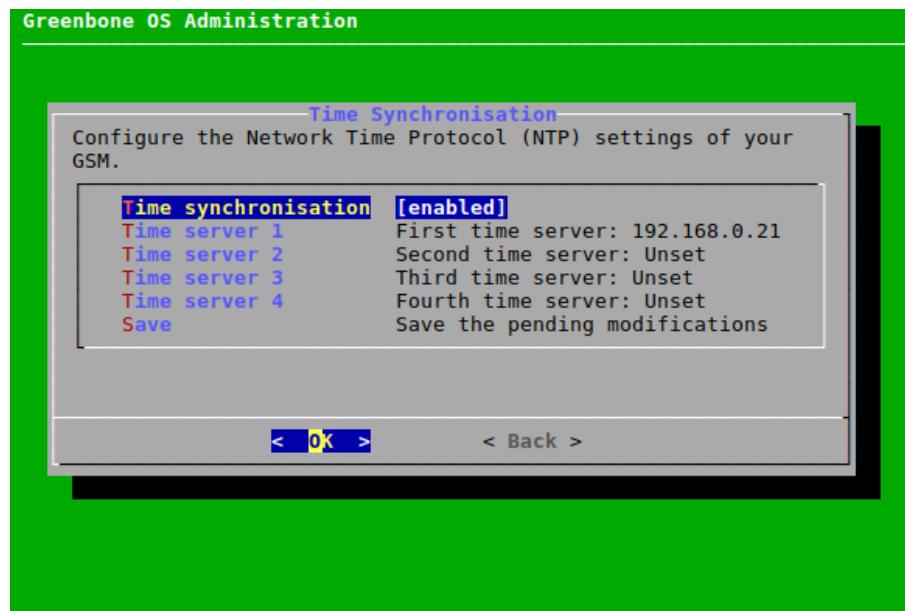


Fig. 7.47: Configuring the NTP settings

7.2.9 Selecting the Keyboard Layout

The keyboard layout of the appliance can be modified as follows:

1. Select *Setup* and press *Enter*.
2. Select *Keyboard* and press *Enter*.
→ All available keyboard layouts are displayed. The current layout has the annotation (*selected*) (see Fig. 7.48).

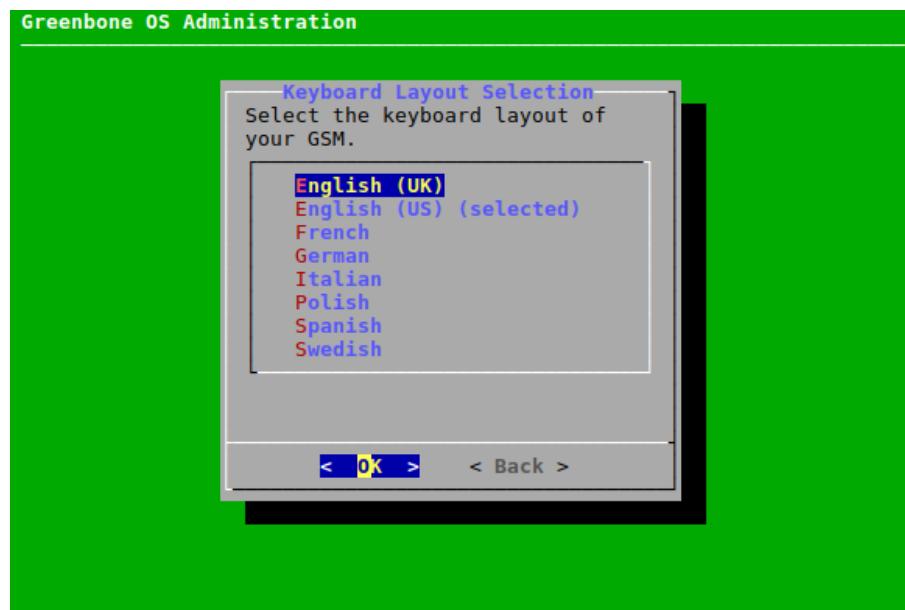


Fig. 7.48: Selecting the keyboard layout

3. Select the desired keyboard layout and press *Enter*.



- A message asks to confirm the change.
- 4. Select **Yes** and press **Enter**.
- A message informs that the layout has been changed.

7.2.10 Configuring Automatic E-Mails

If reports should automatically be sent via e-mail after the completion of a scan, the appliance needs to be configured with a mail server. This server is called a mailhub or smart host. The appliance itself does not come with a mail server.

Note: The appliance does not store e-mails in case of delivery failure. There will be no second delivery attempt.

Possible spam protection on the mail server such as grey listing must be deactivated for the appliance.

Authentication using a user name and password is not supported by the appliance. The authentication must be done IP based.

7.2.10.1 Configuring the Mail Server

Note: Make sure that the mail server is set up correctly and securely to prevent a misuse for spam purposes.

The mail server can be configured as follows:

1. Select **Setup** and press **Enter**.
2. Select **Mail** and press **Enter**.
3. Select **Mail** and press **Enter**.
4. Enter the URL of the mailhub in the input box (see Fig. 7.49).



Fig. 7.49: Configuring the mailhub



5. Select *OK* and press *Enter*.

→ A message informs that the changes have to be saved (see Chapter 7.1.3 (page 122)).

6. Press *Enter* to close the message.

Note: A port that is used for the mailhub can be configured if desired.

7. Select *Mailhub Port* and press *Enter*.

8. Enter the port in the input field and press *Enter*.

→ A message informs that the changes have to be saved (see Chapter 7.1.3 (page 122)).

9. Press *Enter* to close the message.

7.2.10.2 Configuring SMTP Authentication for the Mail Server

Optionally, SMTP authentication can be configured for the used mail server as follows:

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

2. Select *Mail* and press *Enter*.

3. Select *SMTP Authentication Requirements* and press *Enter* to enable SMTP authentication (see Fig. 7.50).

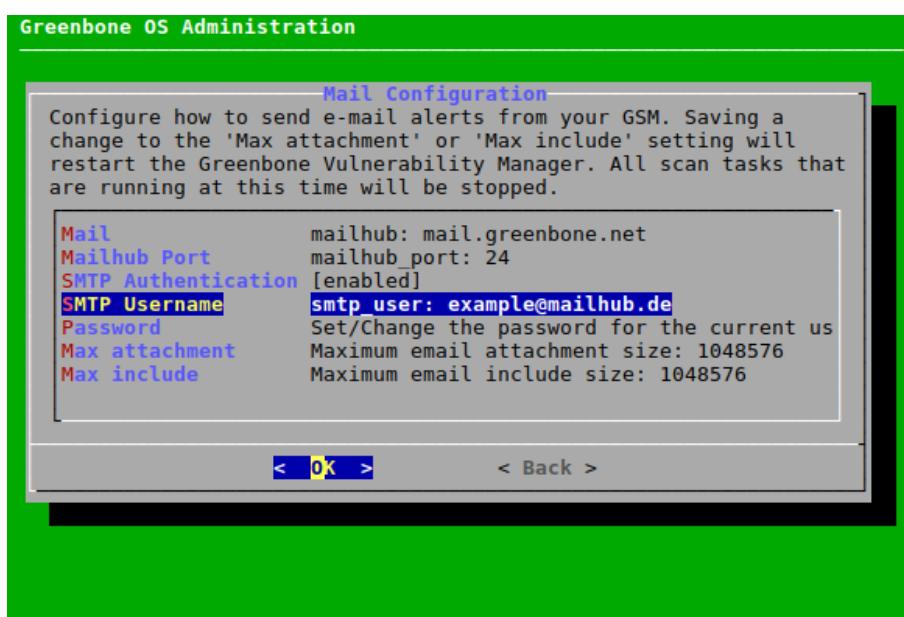


Fig. 7.50: Configuring SMTP authentication

4. Select *SMTP Username* and press *Enter*.

5. Enter the user name of the account used for authentication in the input field and press *Enter*.

→ A message informs that the changes have to be saved (see Chapter 7.1.3 (page 122)).

6. Press *Enter* to close the message.

7. Select *Password* and press *Enter*.



8. Enter the password of the account used for authentication twice and press **Tab**.

Note: Passwords must not be longer than 128 characters.

9. Press **Enter**.

7.2.10.3 Configuring the Size of Included or Attached Reports

The maximum size (in bytes) of reports included in or attached to an e-mail (see Chapter 10.12 (page 305)) can be limited as follows:

1. Select **Setup** and press **Enter**.
2. Select **Mail** and press **Enter**.
3. Select **Max attachment** or **Max include** and press **Enter**.

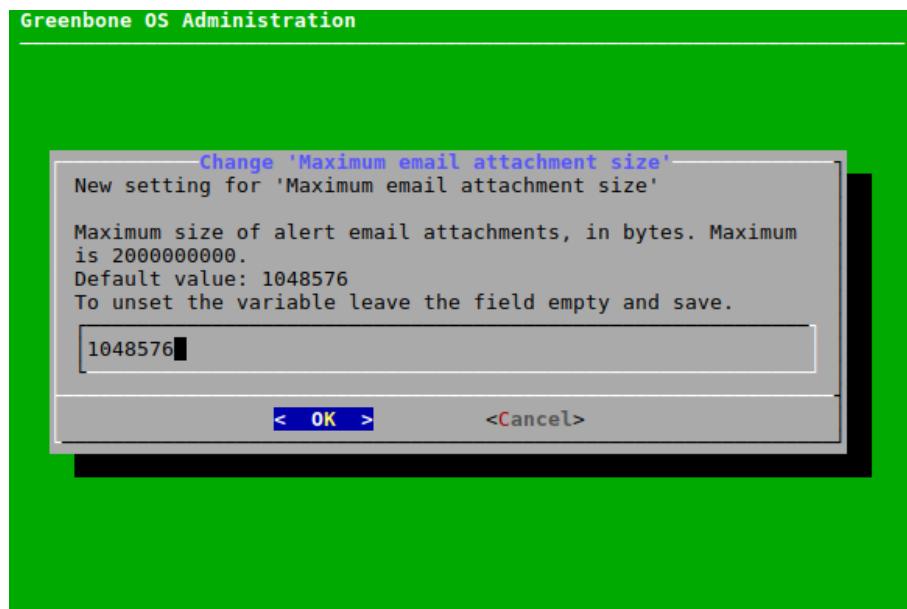


Fig. 7.51: Setting the maximum size of included or attached reports

4. Enter the maximum size (in bytes) in the input box (see Fig. 7.51).
5. Select **OK** and press **Enter**.
→ A message informs that the changes have to be saved (see Chapter 7.1.3 (page 122)).
6. Press **Enter** to close the message.

7.2.11 Configuring the Collection of Logs

The GSM supports the configuration of a central logging server for the collection of logs. Either only the security relevant logs or all system logs can be sent to a remote logging server. The security relevant logs contain:

- User authentication
- User authorization



The GSM uses the syslog protocol. Central collection of the logs allows for central analysis, management and monitoring of logs. Additionally, the logs are always stored locally as well.

One logging server can be configured for each kind of log (security relevant logs or all system logs).

As transport layer UDP (default), TLS and TCP can be used. TCP ensures the delivery of the logs even if a packet loss occurs. If a packet loss occurs during a transmission via UDP, the logs will be lost. TLS enables an optional authentication of the sender via TLS. This process is not RFC 5425 compliant.

7.2.11.1 Configuring the Logging Server

The logging server can be set up as follows:

1. Select *Setup* and press *Enter*.
2. Select *Remote Syslog* and press *Enter*.
3. Select *Security Syslog* and press *Enter* to enable security relevant logs (see Fig. 7.52).
or
3. Select *Full Syslog* and press *Enter* to enable all system logs (see Fig. 7.52).

Note: Both logs can be enabled.

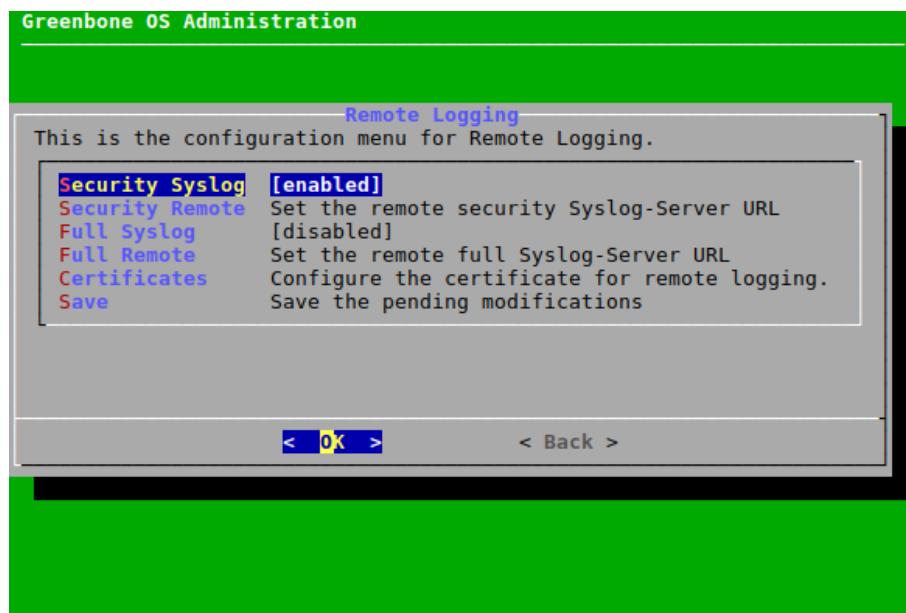


Fig. 7.52: Configuring the logs

4. Select *Security Remote* and press *Enter* to set the logging server URL for security relevant logs.
or
4. Select *Full Remote* and press *Enter* to set the logging server URL for all system logs.
5. Enter the logging server URL in the input box (see Fig. 7.53).

Note: If no port is specified, the default port 514 will be used.

If the protocol is not specified, UDP will be used.



→ A message informs that the changes have to be saved (see Chapter 7.1.3 (page 122)).

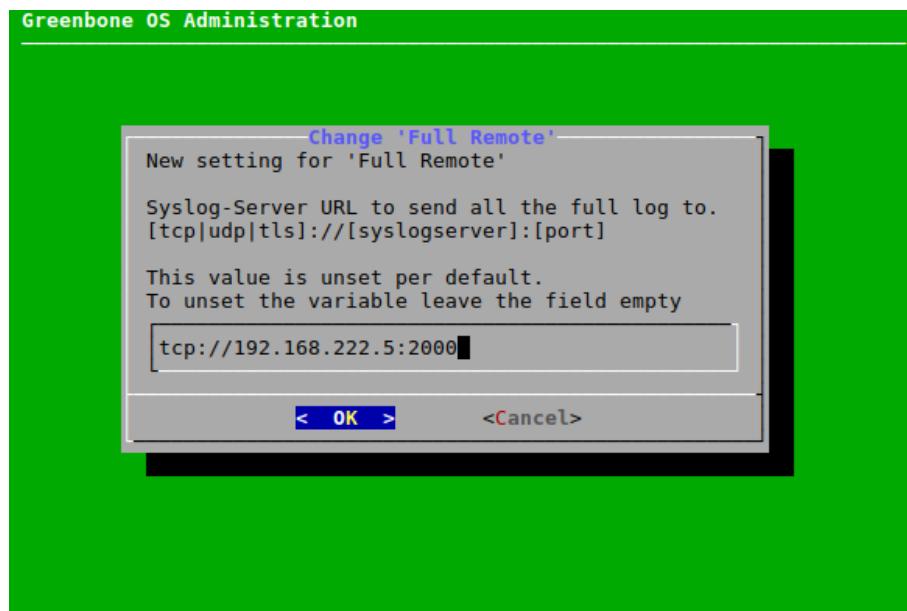


Fig. 7.53: Configuring the logging server

6. Press `Enter` to close the message.

7.2.11.2 Managing HTTPS Certificates for Logging

HTTPS certificates for logging can be managed as follows:

1. Select *Setup* and press `Enter`.
2. Select *Remote Syslog* and press `Enter`.
3. Select *Certificates* and press `Enter`.
4. Select *Generate* and press `Enter` to generate a certificate.
→ A message informs that the current certificate and private key will be overwritten.
5. Confirm the message by selecting *Yes* and pressing `Enter`.
6. Provide the settings for the certificate (see Fig. 7.54), select *OK* and press `Enter`.

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

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

→ When the process is finished, a message informs that the certificate can be downloaded.

7. Press `Enter` to close the message.
8. Select *Certificates* and press `Enter`.
9. Select *Download* and press `Enter`.
10. Open the web browser and enter the displayed URL.
11. Download the file.

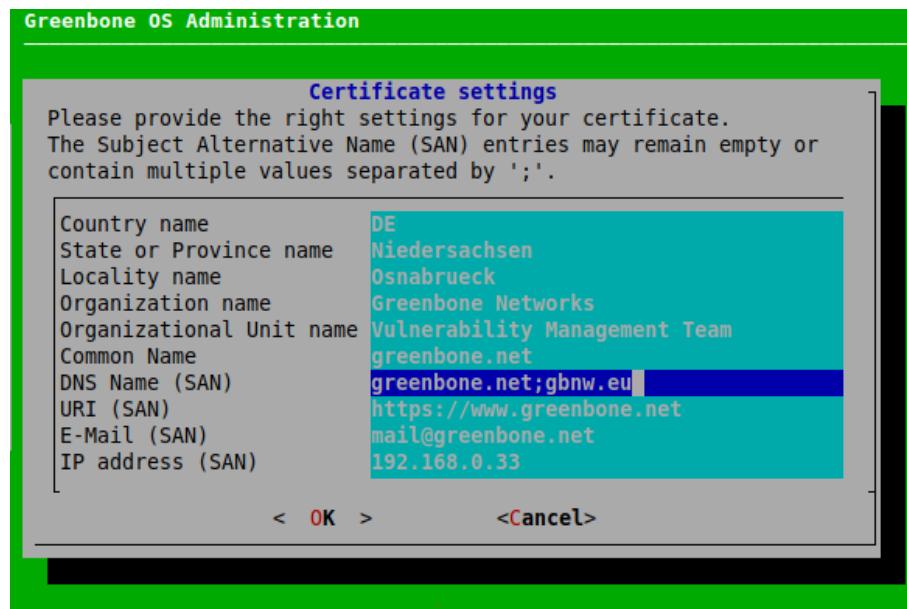


Fig. 7.54: Providing settings for the certificate

12. In the GOS administration menu press **Enter**.

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

13. Check the fingerprint and confirm the certificate by pressing **Enter**.

→ To enable the new certificate a *Reboot* of the GSM is required (see Chapter 7.3.9.1 (page 191)).

The certificate and the according fingerprint can be displayed as follows:

1. Select *Setup* and press **Enter**.
2. Select *Remote Syslog* and press **Enter**.
3. Select *Certificates* and press **Enter**.
4. Select *Show* and press **Enter** to display the certificate.

Select *Fingerprints* and press **Enter** to display the fingerprint.

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

- SHA1
- SHA256



7.2.12 Setting the Maintenance Time

During maintenance the daily feed synchronization takes place. Any time during the day can be chosen except for 10:00 a.m. to 1:00 p.m. UTC. During this period Greenbone Networks itself updates the feed and disables the synchronization services.

The default maintenance time is a random time between 3:00 a.m. and 5:00 a.m. UTC.

The maintenance time can be set as follows:

1. Select **Setup** and press **Enter**.
2. Select **Time** and press **Enter**.
3. Enter the desired maintenance time in the input box and press **Enter** (see Fig. 7.55).

Note: The time has to be converted to UTC before entering it.

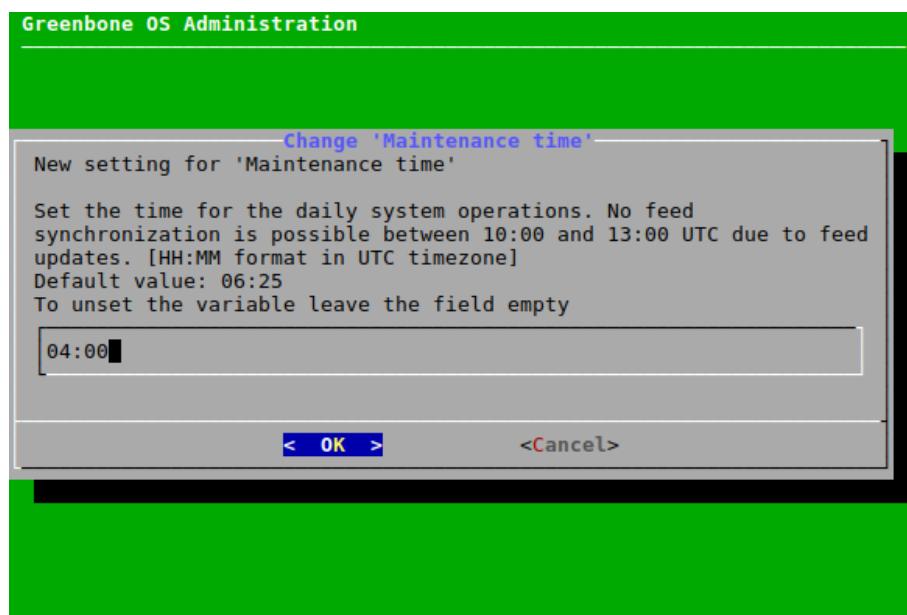


Fig. 7.55: Configuring the maintenance time

- A message informs that the changes have to be saved (see Chapter 7.1.3 (page 122)).
4. Press **Enter** to close the message.



7.3 Maintenance Menu

7.3.1 Performing a Self-Check

The self-check option checks the setup of the appliance. It displays wrong or missing configuration details which might prevent the correct function of the appliance. The following items are checked:

- Network connection
- DNS resolution
- Feed reachability
- Available updates
- User configuration

The self-check is performed as follows:

1. Select *Maintenance* and press **Enter**.
2. Select *Selfcheck* and press **Enter**.

→ The self-check is performed and any found problems are listed on the result page (see Fig. 7.56).

```
Greenbone OS Administration

Selfcheck failed! Please use the following information to correct
the problem.
If you need help, please contact the Greenbone Support

Check GOS upgrade status failed!
  Severity: High
  Solution: GOS release info outdated! Please update your Feed to
refresh the list of available GOS upgrades.
Check if Feed is up to date failed!
  Severity: Normal
  Solution: The Greenbone Feed is older than 10 day. You should
download the newest Feed in the Feed menu.
Check Sensor Connections failed!
  Severity: Normal
  Solution: Currently it is not possible to connect to one or more
of the configured GSM Sensors. To check the configuration and test
the single connection go to Setup -> Master -> Sensors.

< OK >
```

Fig. 7.56: Performing a self-check



7.3.2 Performing and Restoring a Backup

Scheduled local and remote backups are configured in the menu *Setup* (see Chapter 7.2.5 (page 158)).

Backups can also be performed manually. Depending on the backup location configured within Chapter 7.2.5 (page 158), the manually triggered backups are stored remotely or locally. These backups can be transferred to a USB stick for offsite storage.

The backup includes user data (e.g., tasks, reports, results) and system settings, i.e., the GOS configuration.

7.3.2.1 Performing a Backup Manually

A backup can be performed manually as follows:

1. Select *Maintenance* and press *Enter*.
2. Select *Backup* and press *Enter*.
3. Select *Incremental Backup* and press *Enter* (see Fig. 7.57).

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

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

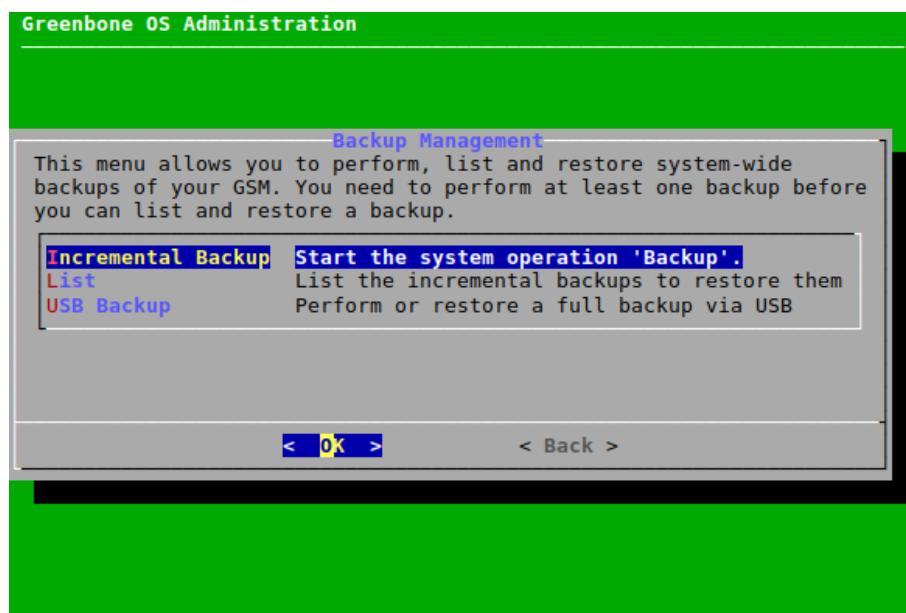


Fig. 7.57: Triggering a backup manually



7.3.2.2 Restoring a Backup Manually

Note: Only backups created with the currently used GOS version or the previous GOS version can be restored. For GOS 21.04, only backups from GOS 20.08 or GOS 21.04 can be imported. If an older backup should be imported, e.g., from GOS 5 or GOS 6, an appliance with a matching GOS version has to be used.

Backups from GOS versions newer than the currently used GOS version are not supported as well. If a newer backup should be imported, an appliance with a matching GOS version has to be used.

Furthermore, only backups created with the same GSM model (see Chapter 3 (page 18)) can be restored.

Additionally, it is checked whether the GSF subscription keys of the backup and of the GSM on which the backup should be restored are identical. If the keys do not match, a warning is displayed and the user has to confirm that the key on the GSM should be overwritten.

If there are any questions, contact the Greenbone Networks Support via e-mail (support@greenbone.net).

A backup can be restored as follows:

1. Select *Maintenance* and press **Enter**.
2. Select *Backup* and press **Enter**.
3. Select *List* and press **Enter**.
4. Select the desired backup and press **Enter**.
5. Select *Yes* and press **Enter** if both user data and system settings should be uploaded.
or
5. Select *No* and press **Enter** if only user data should be uploaded.

Note: The system settings include all GOS configurations, e.g., the network settings. The data includes all vulnerability scanning and vulnerability management information.

→ A warning informs that all local settings are lost if the backup is restored (see Fig. 7.58).

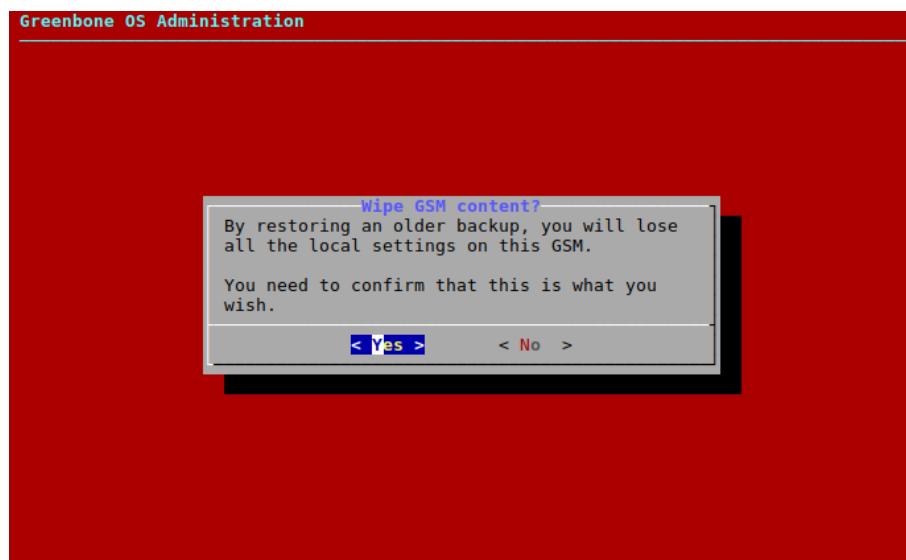


Fig. 7.58: Restoring a backup



6. Confirm the message by selecting **Yes** and pressing **Enter**.
→ A message informs that the restoration was started in the background.

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

7.3.2.3 Performing a Backup Using a USB Stick

Backups can be transferred to a USB stick as follows:

1. Connect a USB stick to the GSM.
- Note:** A FAT-formatted USB stick has to be used. In case of problems, another USB stick or another USB port on the GSM should be tried.
2. Select *Maintenance* and press **Enter**.
3. Select *Backup* and press **Enter**.
4. Select *USB Backup* and press **Enter**.
5. Select *Backup* and press **Enter** (see Fig. 7.59).

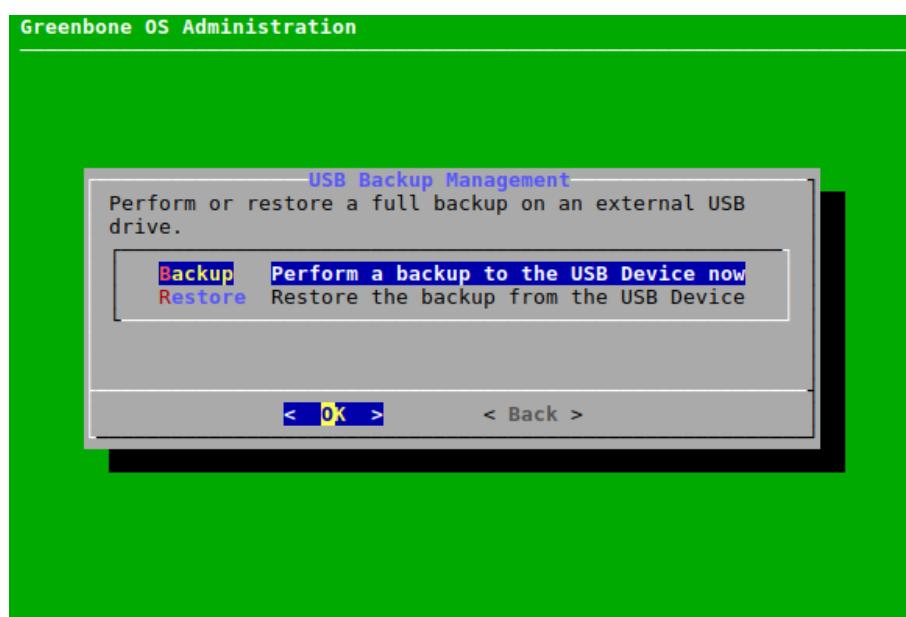


Fig. 7.59: Performing a backup using a USB stick

- A message asks to confirm the backup.
6. Select **Yes** and press **Enter**.
→ A message informs that the backup was started in the background.

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



7.3.2.4 Restoring a Backup Using a USB Stick

Note: Only backups created with the currently used GOS version or the previous GOS version can be restored. For GOS 21.04, only backups from GOS 20.08 or GOS 21.04 can be imported. If an older backup should be imported, e.g., from GOS 5 or GOS 6, an appliance with a matching GOS version has to be used.

Backups from GOS versions newer than the currently used GOS version are not supported as well. If a newer backup should be imported, an appliance with a matching GOS version has to be used.

Furthermore, only backups created with the same GSM model (see Chapter 3 (page 18)) can be restored.

Additionally, it is checked whether the GSF subscription keys of the backup and of the GSM on which the backup should be restored are identical. If the keys do not match, a warning is displayed and the user has to confirm that the key on the GSM should be overwritten.

If there are any questions, contact the Greenbone Networks Support via e-mail (support@greenbone.net).

Backups can be restored from a USB stick as follows:

1. Connect a USB stick to the GSM.

Note: A FAT-formatted USB stick has to be used. In case of problems, another USB stick or another USB port on the GSM should be tried.

2. Select *Maintenance* and press *Enter*.
3. Select *Backup* and press *Enter*.
4. Select *USB Backup* and press *Enter*.
5. Select *Restore* and press *Enter* (see Fig. 7.59).
6. Select *Yes* and press *Enter* if both user data and system settings should be uploaded.
or
6. Select *No* and press *Enter* if only user data should be uploaded.

Note: The system settings include all GOS configurations, e.g., the network settings. The data includes all vulnerability scanning and vulnerability management information.

→ A warning informs that all local settings are lost if the backup is restored (see Fig. 7.60).

7. Confirm the message by selecting *Yes* and pressing *Enter*.
→ A message informs that the restoration was started in the background.

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

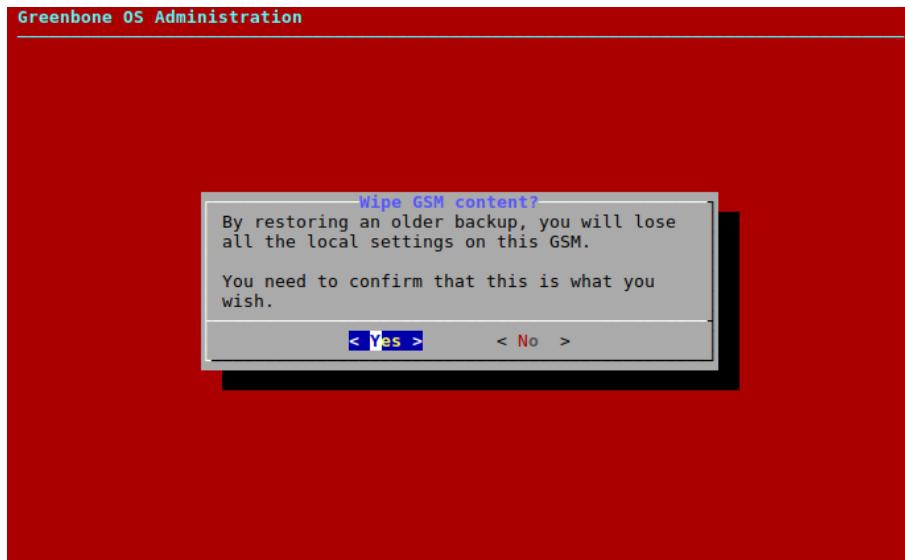


Fig. 7.60: Restoring a backup

7.3.3 Copying Data and Settings to Another GSM with Beaming

The current state of a GSM can be copied to another GSM. This includes user data (e.g., tasks, reports, results) and system settings, i.e., the GOS configuration.

On the receiving GSM, the user can decide whether to import only the user data, or both the user data and the system settings.

Note: Beaming is only allowed to a GSM of the same or of a higher GSM model.

Beaming to a GSM TRIAL is not supported.

7.3.3.1 Beaming Directly from Another GSM

The beaming image can be created and copied directly as follows:

Note:

- GSM A = Sending GSM
 - GSM B = Receiving GSM
-

1. In the GOS administration menu of GSM A, select *Maintenance* and press *Enter*.

2. Select *Beaming* and press *Enter*.

3. Select *Download* and press *Enter* (see Fig. 7.61).

→ A message informs that the beaming image creation was started in the background.

When the creation is finished, a message informs that a password that has to be noted will be shown.

4. Press *Enter*.

5. Note the password. It is needed in step 13.

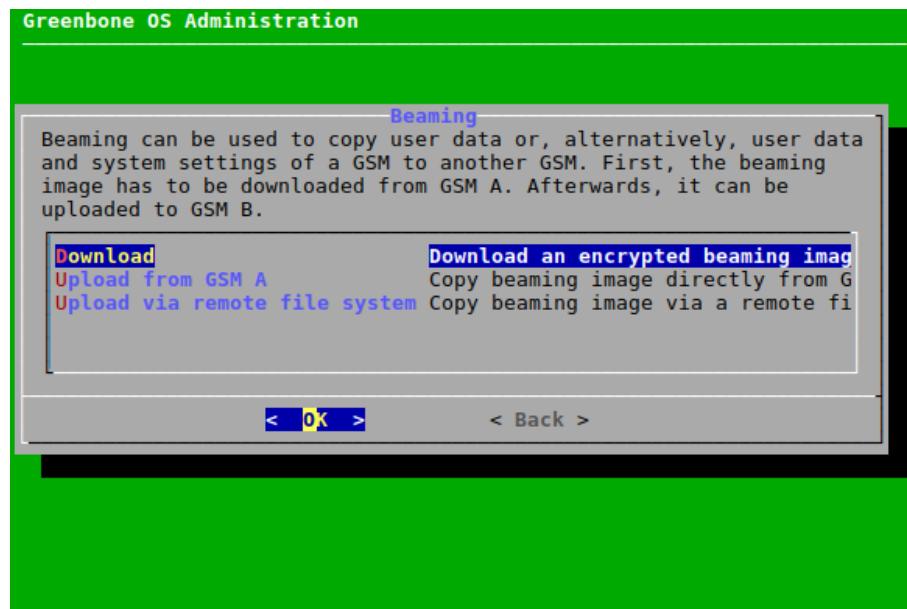


Fig. 7.61: Downloading a beaming image

6. Press `q` to close the editor.

Important: Do not close the message displaying the URL.

7. In the GOS administration menu of GSM B, select *Maintenance* and press `Enter`.
8. Select *Beaming* and press `Enter`.
9. Select *Upload from GSM A* and press `Enter`.
10. Enter the URL displayed in the GOS administration menu of GSM A in the input box and press `Enter`.

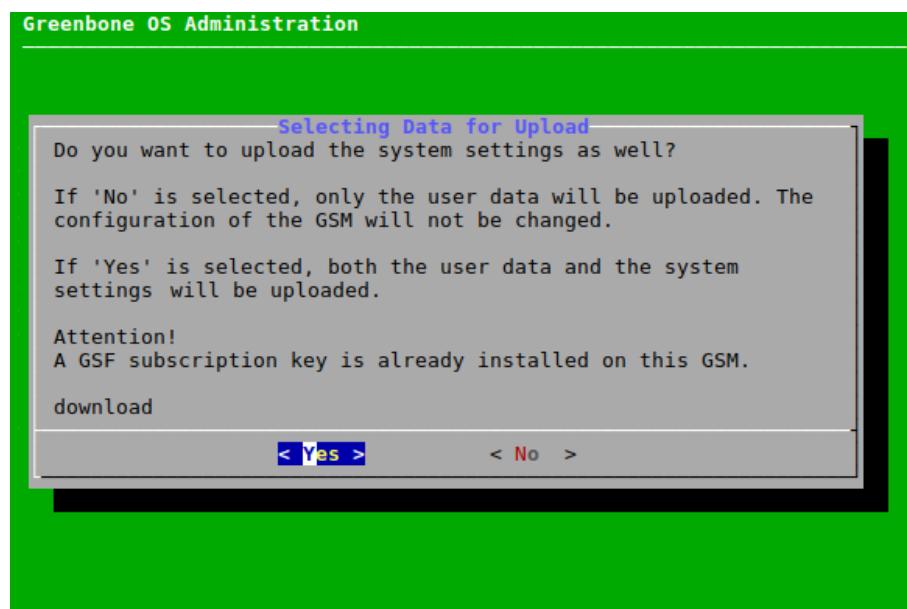


Fig. 7.62: Selecting the data and settings for uploading



11. Select **Yes** and press **Enter** if both user data and system settings should be uploaded.
or
11. Select **No** and press **Enter** if only user data should be uploaded.
→ A warning asks to confirm the process.
12. Select **Yes** and press **Enter**.
13. Enter the password from step 5 in the input box and press **Enter** (see Fig. 7.63).

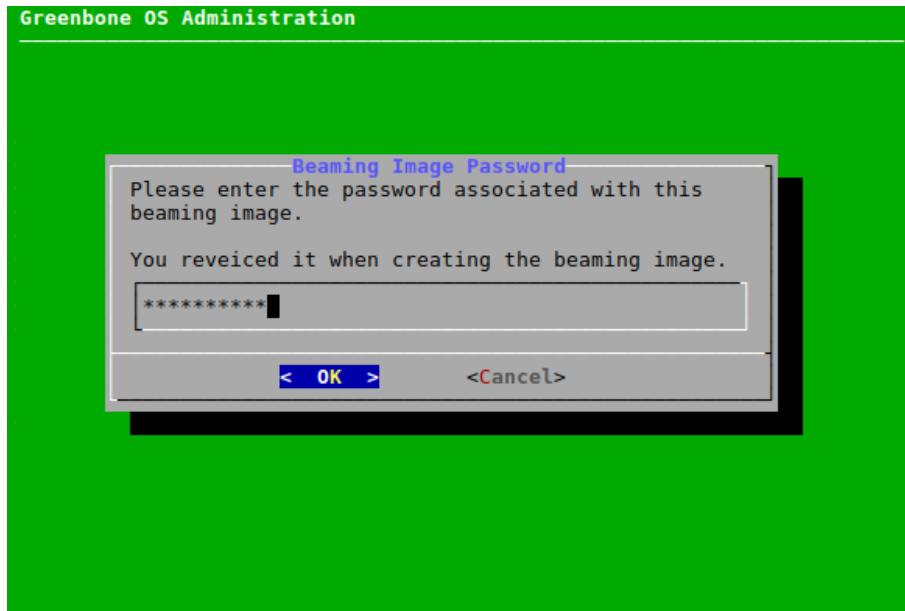


Fig. 7.63: Entering the password for the beaming image

- A message informs that the beaming image upload was started in the background.
When the upload is finished, a message is displayed.
14. Press **Enter**.



7.3.3.2 Beaming via Remote File System

A beaming image can be created, downloaded, stored, and imported later via a remote file system as follows:

Note:

- GSM A = Sending GSM
 - GSM B = Receiving GSM
-

1. In the GOS administration menu of GSM A, select *Maintenance* and press **Enter**.
2. Select *Beaming* and press **Enter**.
3. Select *Download* and press **Enter** (see Fig. 7.64).

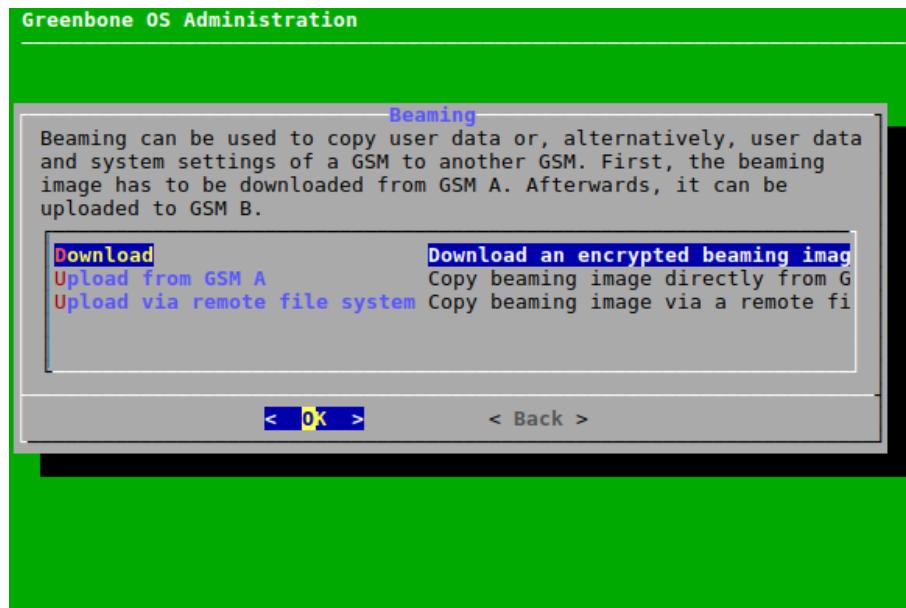


Fig. 7.64: Downloading a beaming image

→ A message informs that the beaming image creation was started in the background.

When the creation is finished, a message informs that a password that has to be noted will be shown.

4. Press **Enter**.
5. Note the password. It is needed in step 16.
6. Press **q** to close the editor.
7. Open the web browser and enter the displayed URL.
8. Download the GSMB file.
9. In the GOS administration menu of GSM B, select *Maintenance* and press **Enter**.
10. Select *Beaming* and press **Enter**.
11. Select *Upload via remote file system* and press **Enter**.
12. Open the web browser and enter the displayed URL.
13. Click *Browse...*, select the GSMB file and click *Upload*.

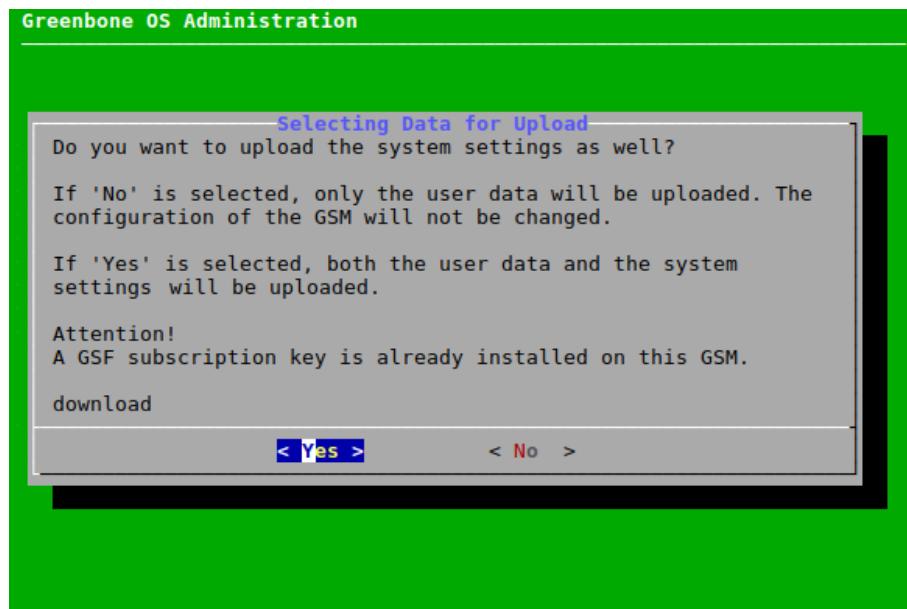


Fig. 7.65: Selecting the data and settings for uploading

14. Select **Yes** and press **Enter** if both user data and system settings should be uploaded.
or
14. Select **No** and press **Enter** if only user data should be uploaded.
→ A warning asks to confirm the process.
15. Select **Yes** and press **Enter**.
16. Enter the password from step 5 in the input box and press **Enter** (see Fig. 7.66).

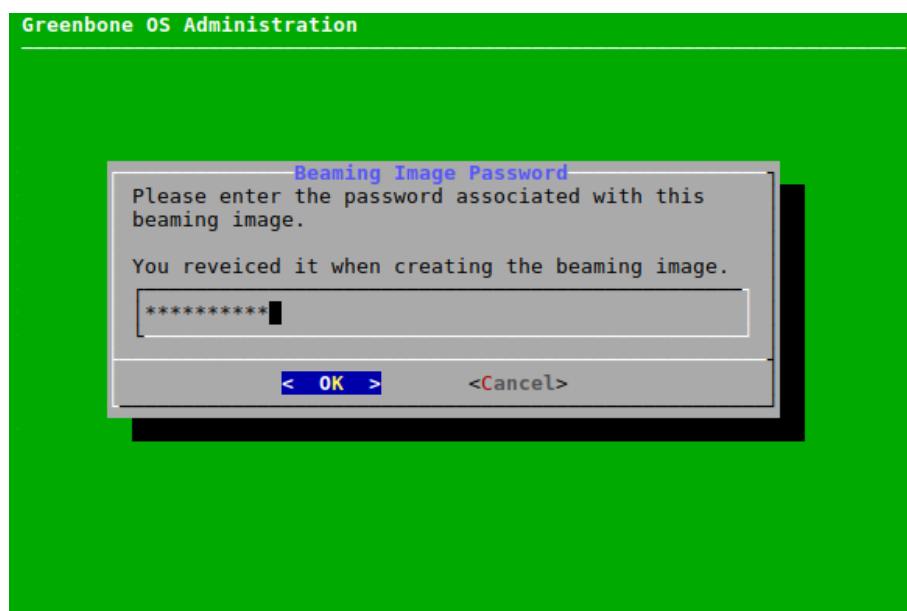


Fig. 7.66: Entering the password for the beaming image

- A message informs that the beaming image upload was started in the background.
- When the upload is finished, a message is displayed.



17. Press **Enter**.

7.3.4 Performing a GOS Upgrade

During the daily feed update the appliance will also download new GOS upgrades if available. While the upgrades are automatically downloaded, they are not automatically installed.

Note: Since the upgrades might interrupt current scan tasks, they need to be scheduled carefully.

Upgrades can be installed manually as follows:

1. Select *Maintenance* and press **Enter**.
2. Select *Upgrade* and press **Enter**.
3. Select *Upgrade* and press **Enter** to install an upgrade.
or
3. Select *Switch Release* and press **Enter** to switch to a new release.
→ A message informs that the upgrade was started in the background.

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

Note: If errors occur when using the web interface after a GOS upgrade, the browser or page cache has to be emptied (see Chapter 6.3 (page 116)).

Occasionally, a reboot of the appliance is required as well (see Chapter 7.3.9.1 (page 191)). The self-check shows an according note if this is the case (see Chapter 7.3.1 (page 178)).

Note: By default, a successful GOS upgrade on the master starts a GOS upgrade on connected sensors as well. Nonetheless, an upgrade can manually be installed on sensors (see Chapter 7.3.5 (page 188)).

7.3.5 Performing a GOS Upgrade on Sensors

A GOS upgrade on a sensor can be installed as follows:

1. Select *Maintenance* and press **Enter**.
2. Select *Upgrade* and press **Enter**.
3. Select *Sensors* and press **Enter**.
4. Select the desired sensor and press **Space**.
→ The sensor is marked with *. Multiple sensors can be selected at the same time.
Sensors that are not ready for an upgrade are labelled accordingly.
5. Press **Enter**.
→ A message informs that the upgrade was started in the background.



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

7.3.6 Performing a Feed Update

By default, the appliance will try to download new feeds and GOS upgrades daily.

The feed synchronization can be triggered manually as follows:

1. Select *Maintenance* and press **Enter**.
2. Select *Feed* and press **Enter**.
3. Select *Update* and press **Enter** (see Fig. 7.67).
→ A message informs that the feed update was started in the background.

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

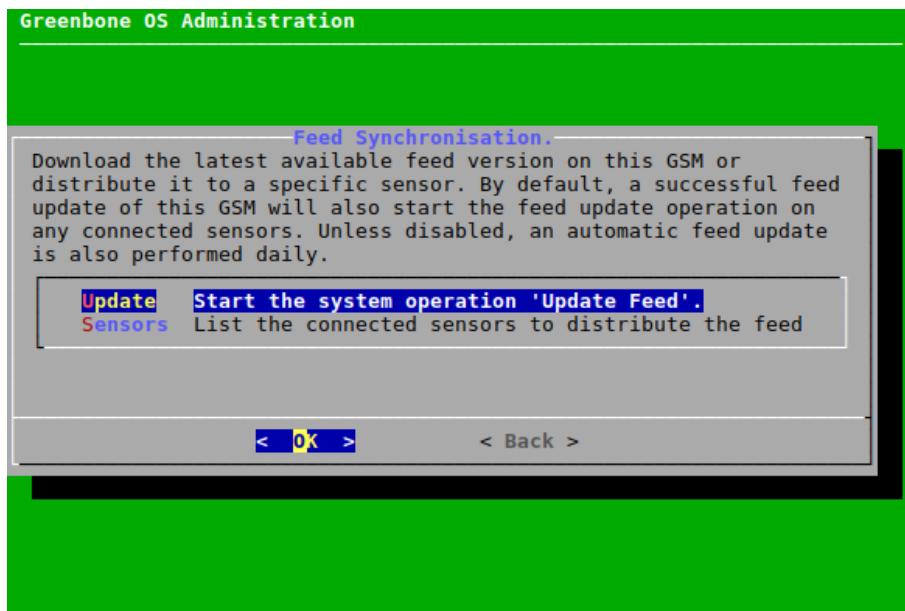


Fig. 7.67: Triggering a feed update manually

Note: By default, a successful feed update on the master starts a feed update on connected sensors as well. Nonetheless, a feed update can manually be pushed to sensors (see Chapter 7.3.7 (page 189)).

7.3.7 Performing a Feed Update on Sensors

A feed update can be pushed to a sensor as follows:

1. Select *Maintenance* and press **Enter**.
2. Select *Feed* and press **Enter**.



3. Select *Sensors* and press *Enter*.
4. Select the desired sensor and press *Enter* (see Fig. 7.68).
→ A message informs that the feed update was started in the background.

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

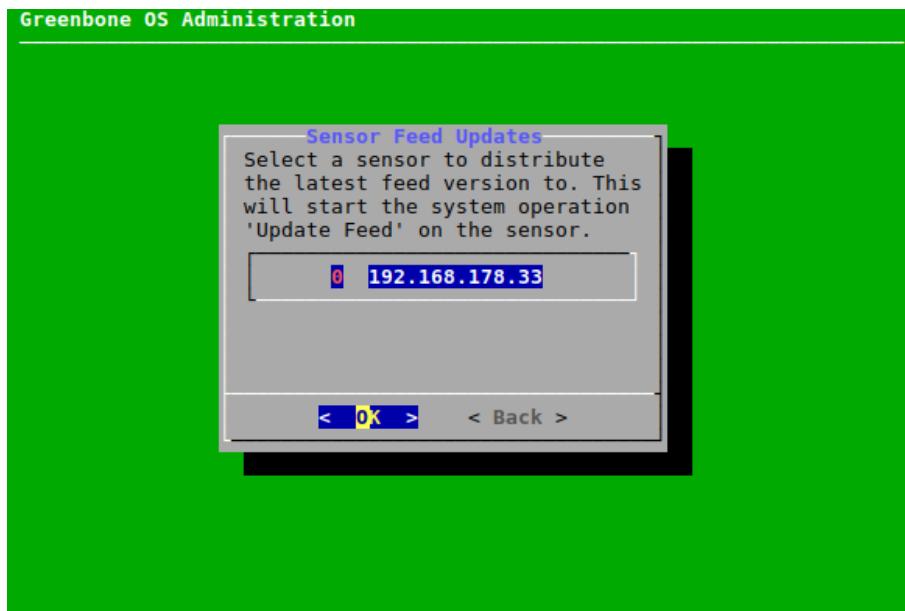


Fig. 7.68: Selecting the sensor

7.3.8 Upgrading the Flash Partition

The flash partition is used to perform factory resets of the GSM. To make factory resets easier, it should be upgraded to the latest GOS version.

Note: Make sure the GSM itself is able to establish a connection to the Greenbone Feed Server.

It is not possible to upgrade the flash partition of sensors via the master.

The flash partition can be upgraded as follows:

1. Upgrade the GSM to the latest GOS version (see Chapter 7.3.4 (page 188)).
2. Select *Maintenance* and press *Enter*.
3. Select *Flash* and press *Enter*.
4. Select *Download* and press *Enter* (see Fig. 7.69).
→ The latest flash image is downloaded.

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



5. When the download is finished, select *Write* and press *Enter* (see Fig. 7.69).
→ The image is written to the flash partition. The process may take up to 20 minutes.

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

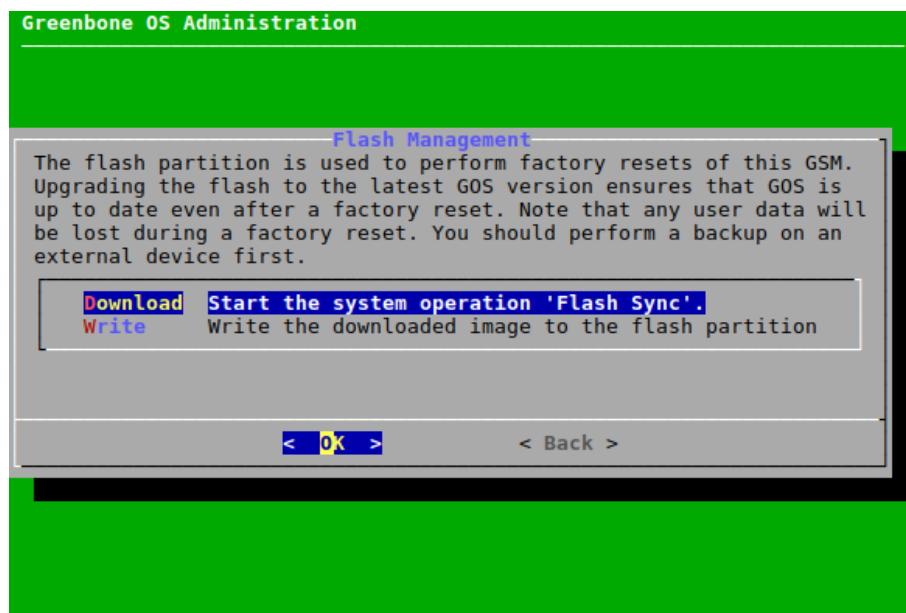


Fig. 7.69: Upgrading the flash partition

7.3.9 Shutting down and Rebooting the Appliance

Important: The GSM should not be turned off using the power switch.

The appliance should be shut down and rebooted using the GOS administration menu instead. This ensures that mandatory cleanup processes are run during the shutdown and reboot.

7.3.9.1 Rebooting the Appliance

The appliance is rebooted as follows:

1. Select *Maintenance* and press *Enter*.
2. Select *Power* and press *Enter*.
3. Select *Reboot* and press *Enter*.
→ A message asks to confirm the reboot (see Fig. 7.70).
4. Select *Yes* and press *Enter*.
→ The appliance will reboot. The reboot process may take up to several minutes.

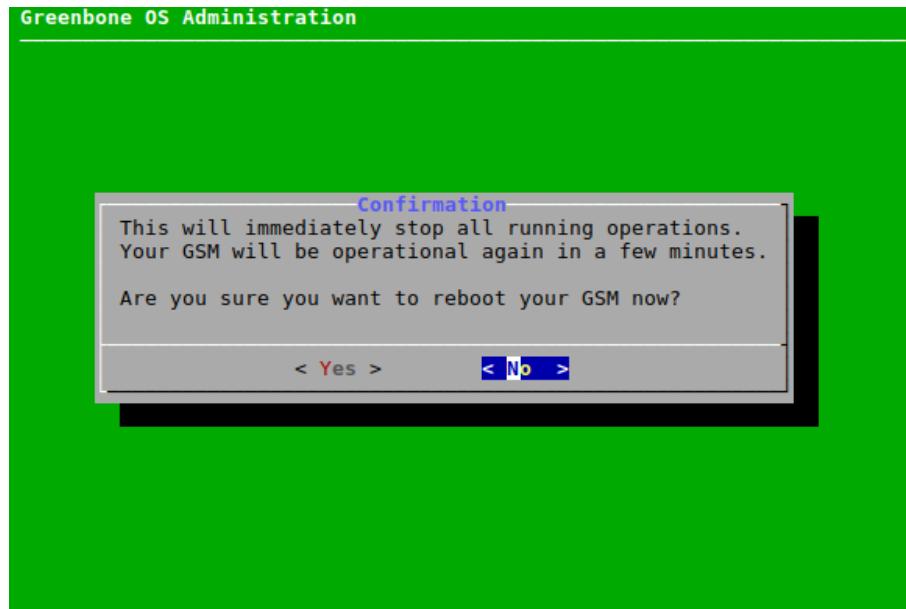


Fig. 7.70: Rebooting the appliance

7.3.9.2 Shutting down the Appliance

The appliance is shut down as follows:

1. Select *Maintenance* and press *Enter*.
2. Select *Power* and press *Enter*.
3. Select *Shutdown* and press *Enter*.
→ A message asks to confirm the shutdown (see Fig. 7.71).



Fig. 7.71: Shutting down the appliance

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



→ The appliance will shutdown. The shutdown process may take up to several minutes.

7.4 Advanced Menu

7.4.1 Displaying Log Files of the GSM

The log files of the GSM can be displayed as follows:

1. Select *Advanced* and press *Enter*.
2. Select *Logs* and press *Enter*.
3. Select the desired logs and press *Enter* (see Fig. 7.72).
→ The log file is displayed in a viewer.
4. Press *q* to quit the viewer.

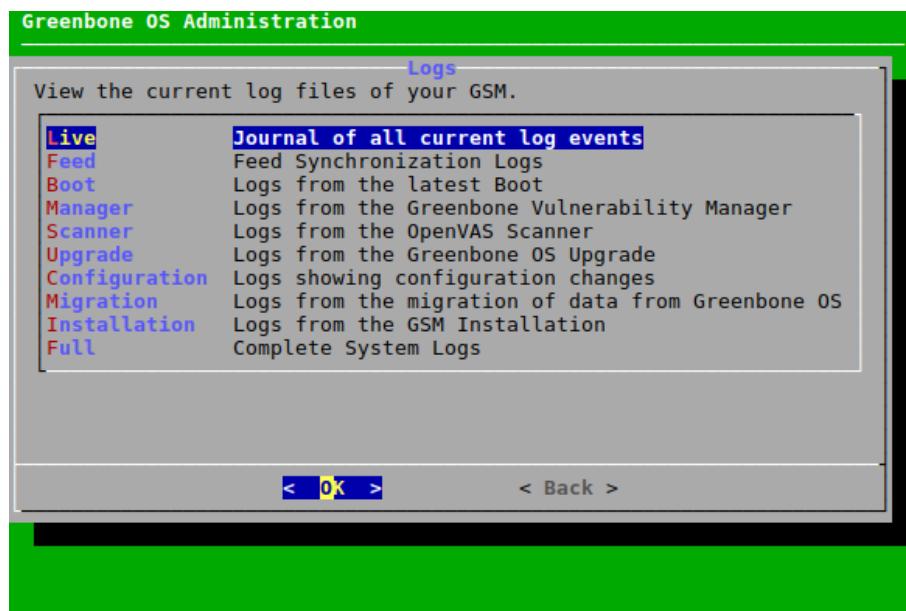


Fig. 7.72: Selecting the log files

7.4.2 Performing Advanced Administrative Work

7.4.2.1 Managing the Superuser Account

When the shell is accessed, a Linux command line as the unprivileged user *admin* is displayed (see Chapter 7.4.2.3 (page 197)). Any Linux command can be executed.

Note: The privileged account *root* (superuser) should only be used in consultation with the Greenbone Networks Support (support@greenbone.net).

If any modifications are done without consultation, the entitlement to receive assistance by the Greenbone Networks Support expires.



To obtain root privileges on the GSM, the command `su` has to be entered in the shell. Using `su` to switch from the *admin* user to the *root* user is disabled by default.

The superuser has to be enabled and provided with a password as follows:

1. Select *Advanced* and press `Enter`.
2. Select *Support* and press `Enter`.
3. Select *Superuser* and press `Enter`.
4. Select *Superuser State* and press `Enter` (see Fig. 7.73).

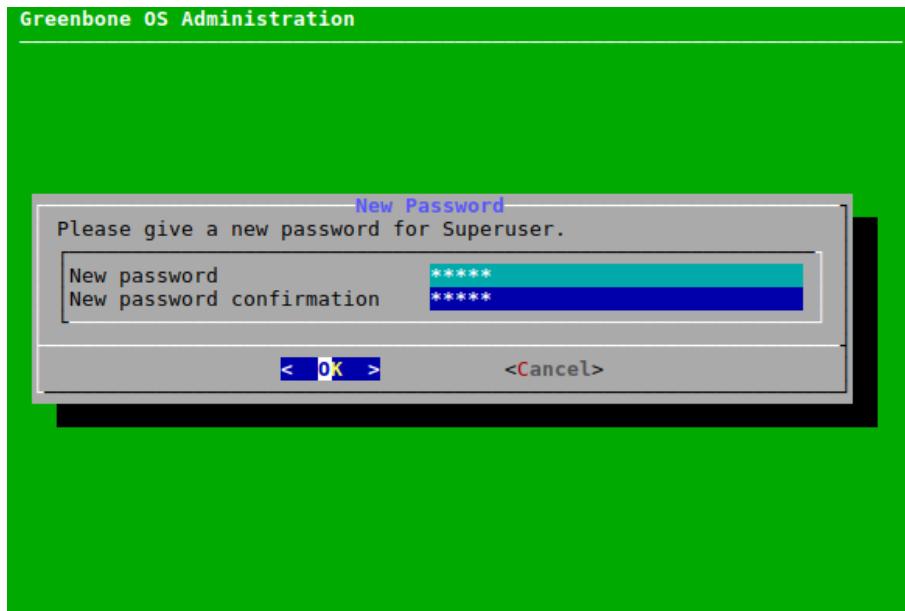


Fig. 7.73: Enabling the superuser

→ A warning informs that root privileges should only be obtained by exception and while consulting the Greenbone Networks Support (support@greenbone.net).

5. Select *Yes* and press `Enter`.
→ A message informs that the changes have to be saved (see Chapter 7.1.3 (page 122)).
6. Press `Enter` to close the message.
7. Select *Password* and press `Enter` (see Fig. 7.73).
8. Enter the password twice, select *OK* and press `Enter` (see Fig. 7.74).

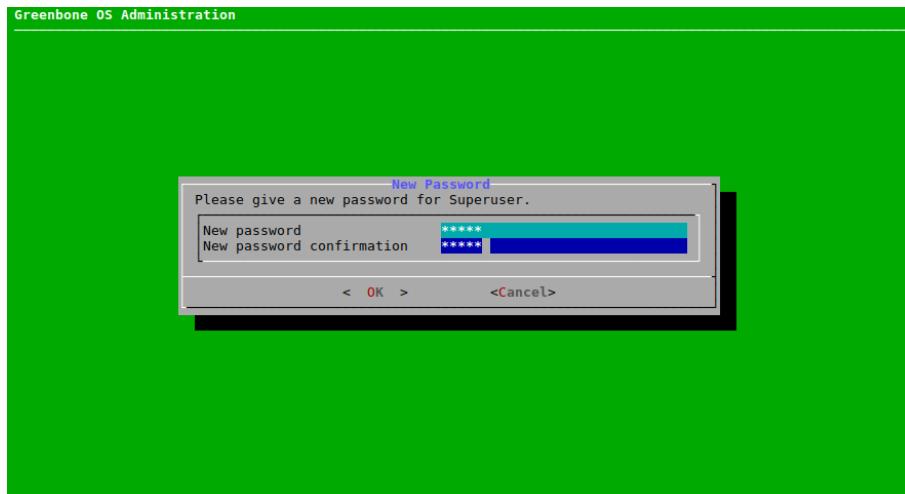


Fig. 7.74: Defining the superuser password

7.4.2.2 Generating and Downloading a Support Package

Sometimes the Greenbone Networks Support requires additional information to troubleshoot and support customers. The required data is collected as an (encrypted) support package including all configuration data of the GSM appliance.

The package can be encrypted using the GPG public key of the Greenbone Networks Support. The support package is stored on the appliance.

A support package can be created as follows:

1. Select *Advanced* and press *Enter*.
2. Select *Support* and press *Enter*.
3. Select *Support Package* and press *Enter*.
→ A message asks to confirm the generation of the support package.
4. Select *Yes* and press *Enter*.
→ A message asks whether the support package should be encrypted (see Fig. 7.75).
5. Select *Yes* and press *Enter* to encrypt the support package.
or
5. Select *No* and press *Enter* to not encrypt the support package.
6. If an encrypted support package was chosen, open the web browser, enter the displayed URL and download the GPG file (encrypted ZIP folder).
or

Note: If the support package is not encrypted, the download needs to be done using the Secure Copy Protocol (SCP). For this, SSH has to be enabled first (see Chapter 7.2.4.4 (page 154)).

6. If an unencrypted support package was chosen, enter the displayed command using SCP (see Fig. 7.76) and download the support package (ZIP folder).

Note: The “.” at the end can be replaced with a path. If the “.” is maintained, the current folder is chosen.

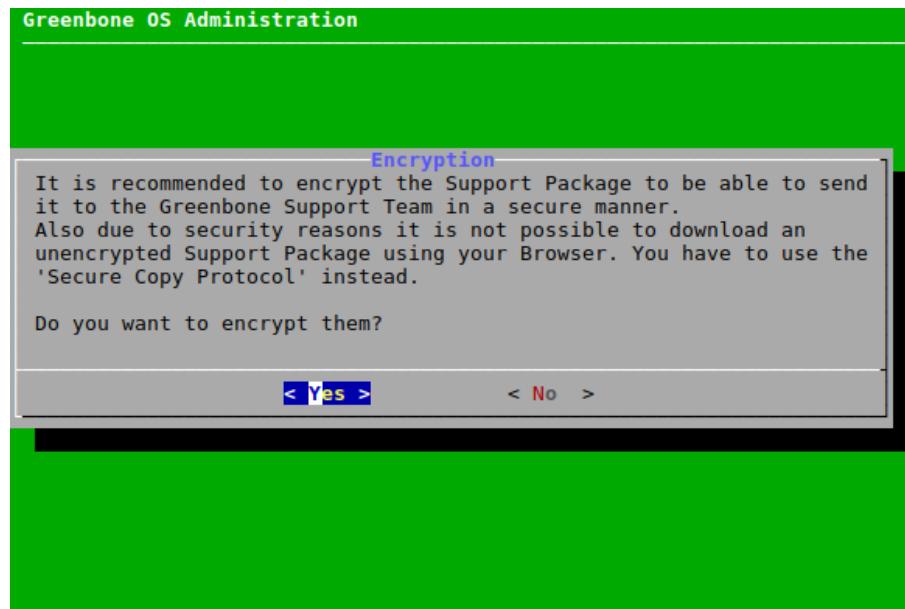


Fig. 7.75: Downloading a support package

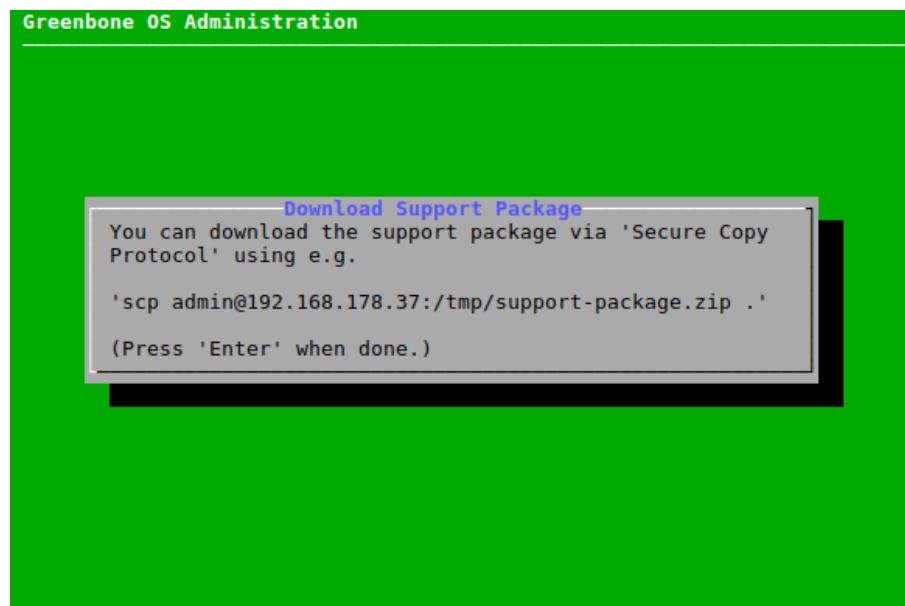


Fig. 7.76: Downloading an unencrypted support package



7. Send the ZIP folder via e-mail to the Greenbone Networks Support (support@greenbone.net).

On Microsoft Windows systems the support package can be downloaded using either `pscp`, a command line tool included in PuTTY, or smarTTY, a graphical tool implementing SCP.

7.4.2.3 Accessing the Shell

Shell access is not required for any administrative work, but may be requested by Greenbone Networks Support for diagnostics and support.

The shell can be accessed as follows:

1. Select *Advanced* and press `Enter`.
2. Select *Support* and press `Enter`.
3. Select *Shell* and press `Enter`.

→ A warning informs that the shell level is undocumented and should not be used for administrative settings (see Fig. 7.77).

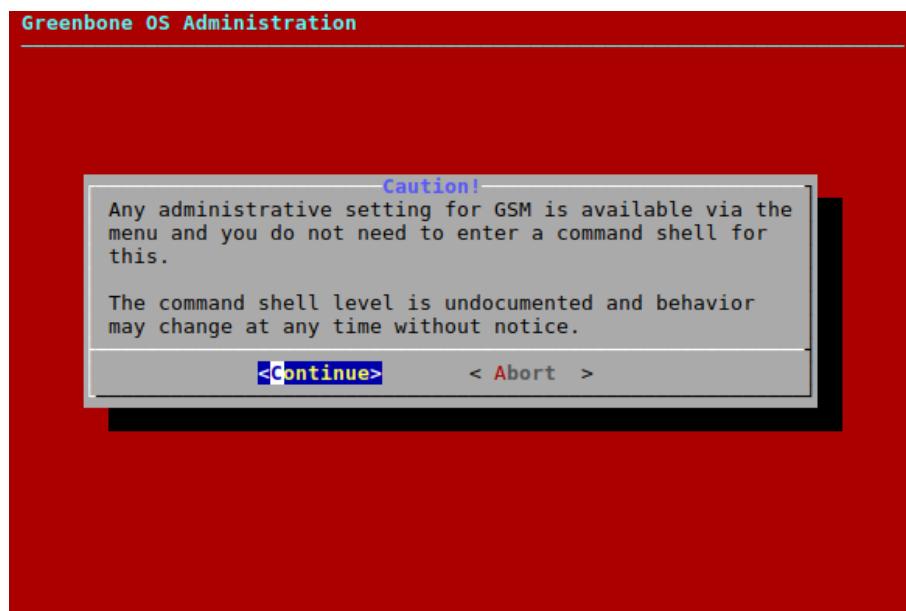


Fig. 7.77: Warning when accessing the shell

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

→ A Linux shell is opened using the unprivileged user *admin* (see Fig. 7.78).

```
Welcome to Greenbone OS command line administration.
Type ^D (Ctrl-D), or 'exit' to return to the Greenbone OS Administration menu.

admin@gos50-gsm400:~$
```

Fig. 7.78: Accessing the local shell



Note: Accessing as *root* requires the enabling of the superuser and the determination of a password (see Chapter 7.4.2.1 (page 193)). Afterwards, switching to *root* using the command `su` is possible.

5. Enter `exit` or press `Ctrl + D` to quit the shell.

7.4.3 Displaying the Greenbone Security Feed (GSF) Subscription Key

The GSF subscription key (see Chapter 7.2.6.1 (page 162)) can be displayed as follows:

1. Select *Advanced* and press `Enter`.
2. Select *Subscription* and press `Enter` (see Fig. 7.79).
→ The subscription key is displayed in a viewer.
3. Press `q` to quit the viewer.

7.4.4 Displaying the Copyright File

The copyright file can be displayed as follows:

1. Select *Advanced* and press `Enter`.
2. Select *Copyright* and press `Enter` (see Fig. 7.79).
→ The copyright file is displayed in a viewer.
3. Press `q` to quit the viewer.

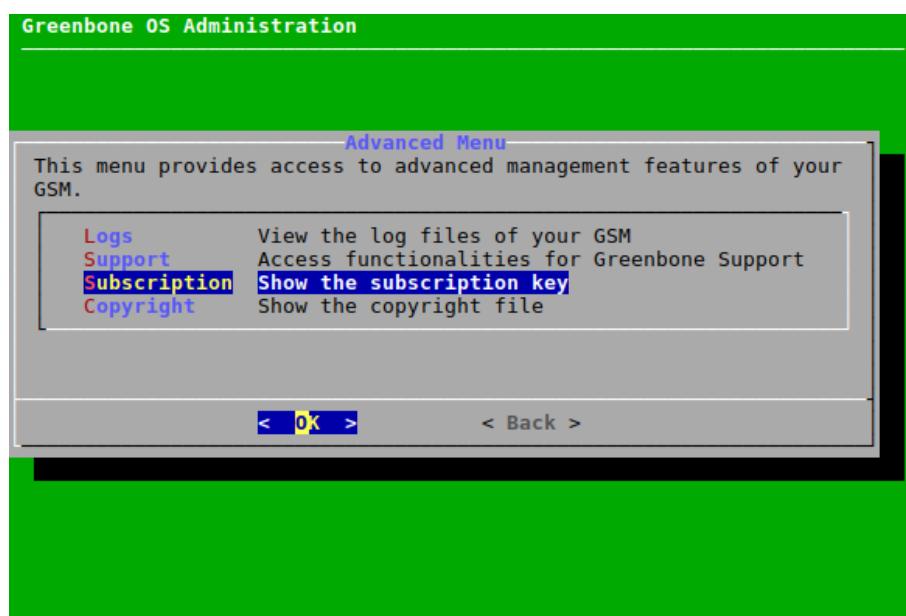


Fig. 7.79: Displaying the GSF subscription key or the copyright file



7.5 Displaying Information about the Appliance

Information about the GSM can be displayed by selecting *About* and pressing **Enter**.

The following information is displayed:

- GSM model
- GOS version
- Feed version
- Name of the GSF subscription key
- IP address of the web interface
- Configured sensors
- Currently running system operations

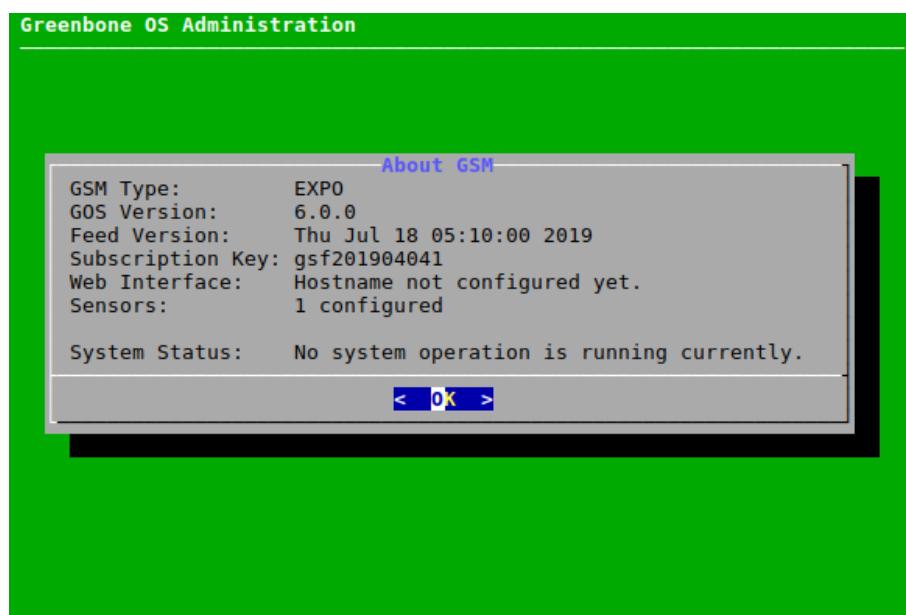


Fig. 7.80: Displaying information about the GSM

CHAPTER 8

Getting to Know the Web Interface

8.1 Logging into the Web Interface

The main interface of the GSM is the web interface, also called Greenbone Security Assistant (GSA). The web interface can be accessed as follows:

1. Open the web browser.
2. Enter the IP address of the web interface of the GSM.

Tip: The IP address of the GSM is displayed on the login prompt of the console or in the GOS administration menu after selecting *About* and pressing *Enter*.

3. Log in using the web administrator created during the setup (see Chapter 5 (page 26)).

8.2 List Pages and Details Pages

Basically, there are two different types of pages on the web interface: list pages and details pages.

List page List pages are opened by selecting the desired page in the menu bar (see Fig. 8.1/2), e.g., selecting *Scans > Tasks* in the menu bar opens the list page *Tasks*.

List pages give a overview of all objects of one kind (see Fig. 8.1/6), e.g., the list page *Tasks* shows all existing tasks. Additionally, actions for single objects are provided. General actions for the selected object type are available in the upper left corner (see Fig. 8.1/7).

Dashboards (see Fig. 8.1/5) display various information concerning the selected object type in graphic or tabular form.

The filter bar in the upper right corner (see Fig. 8.1/3) can be used to display a desired selection of the objects.



Fig. 8.1: List page with dashboards and tabular overview

- 1 – User settings and logout (see Chapter 8.8 (page 218))
- 2 – Menu bar
- 3 – Filter bar (see Chapter 8.4 (page 207))
- 4 – Actions for dashboards (not available on all pages, see Chapter 8.3 (page 203))
- 5 – Dashboard with dashboard displays (not available on all pages, see Chapter 8.3 (page 203))
- 6 – List of all objects of the selected object type (see Fig. 8.2)
- 7 – Actions for object type, depending on page content

The list of objects (see Fig. 8.2) provides information such as name, status, type or possible actions for single objects (see Fig. 8.2/2). The information shown in the table depends on the object type.

Some actions (e.g., tagging, exporting, deleting) can be applied to multiple objects (see Fig. 8.2/3).

The table lists various objects with columns for Name, Status, Reports, Last Report, Severity, Trend, and Actions. The 'Actions' column contains icons for copy, delete, etc.

Numbered callouts point to specific elements:

- 1: Page navigation buttons at the top right.
- 2: Actions for single objects (copy, delete, etc.) shown in a context menu over a table row.
- 3: Actions for multiple/all objects (copy, delete, etc.) shown in a context menu over the entire table.
- 4: Applied filter information at the bottom left.
- 5: Unfolding all details preview for all objects button at the bottom right.

Fig. 8.2: List of all objects

- 1 – Switching between pages
- 2 – Actions for single objects, depending on page content
- 3 – Actions for multiple/all objects, depending on page content
- 4 – Applied filter (see Chapter 8.4 (page 207))
- 5 – Unfolding all details preview for all objects



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.

By clicking on an object in the column *Name* a preview of the details is opened (see Fig. 8.3).

The screenshot shows a details preview for a 'DMZ Mail Scan' object. The page header includes a search icon, a table with columns: Status (Done), Reports (1), Last Report (Thu, Jan 9, 2020 9:16 AM UTC), Severity (2.6 (Low)), Trend, and Actions. The main content area is labeled 'Target' and contains sections for 'Scanner' (Name: OpenVAS Default, Type: OpenVAS Scanner, Scan Config: Full and fast, Order for target hosts: sequential), 'Assets' (Add to Assets: Yes, Apply Overrides: Yes, Min QoD: 70 %), and 'Scan' (Duration of last Scan: 9 minutes, Auto delete Reports: Do not automatically delete reports). A note at the bottom states '(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)'. The footer includes an 'Apply to page contents' button and navigation links for 1 - 10 of 10.

Fig. 8.3: Details preview

- 1 – Switching between pages
- 2 – Actions for single objects, depending on page content
- 3 – Actions for multiple/all objects, depending on page content
- 4 – Applied filter (see Chapter 8.4 (page 207))
- 5 – Details preview of the selected object
- 6 – Opening the details page of the selected object (see below)
- 7 – Unfolding all details preview for all objects

Details page The details page of a specific object is opened by clicking on the name of the object in the column *Name* on the list page and clicking (see Fig. 8.3/6).

The details page provides further information and actions (see Fig. 8.4).

The details are divided into categories which can be selected using the registers (see Fig. 8.4/4). For most objects, user tags (see Chapter 8.5 (page 214)) and permissions (see Chapter 9.4 (page 231)) can be added on the details page.

General actions for the selected object type as well as actions for the single object are available in the upper left corner (see Fig. 8.4/5). The following actions are always present:

- Open the corresponding chapter of the user manual.
- Open the list page of the corresponding object type.



1 – User settings and logout (see Chapter 8.8 (page 218))
 2 – Menu bar
 3 – Details of the selected object
 4 – Registers for different subcategories
 5 – Actions for object type, depending on page content

Fig. 8.4: Details page

- 1 – User settings and logout (see Chapter 8.8 (page 218))
- 2 – Menu bar
- 3 – Details of the selected object
- 4 – Registers for different subcategories
- 5 – Actions for object type, depending on page content

8.3 Dashboards and Dashboard Displays

Many pages of the web interface show dashboard displays on the top of the page depending on the page content.

There are two types of dashboard displays: charts and tables.

For each page there is a default setting of displays. The default setting can be restored by clicking ⌂ on the right side above the displays.

8.3.1 Adding and Deleting Dashboard Displays

A new display can be added as follows:

1. Click ⌂ on the right side above the displays.
2. Select the desired display in the drop-down list (see Fig. 8.5).

Tip: The input box above the selectable options can be used to filter the options.

3. Click **Add**.

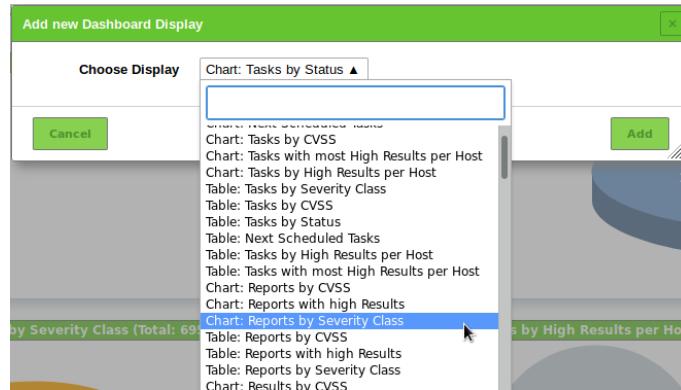


Fig. 8.5: Adding a display

A display can be deleted by clicking in the upper right corner of the display (see Fig. 8.6).

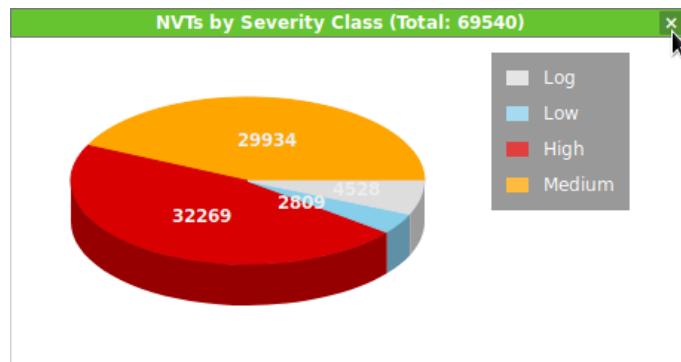


Fig. 8.6: Deleting a display

8.3.2 Editing a Dashboard Display

Depending on the display there are several options which can be selected by moving the mouse to the right edge of a display (see Fig. 8.7):

- Apply a filter to the display. The filter has to be configured for the object type shown in the display.
- Download the chart as an SVG file (only for charts).
- Download the table as a CSV file (only for tables).
- Hide or show a legend (only for charts).
- Switch between 2D and 3D presentation (only for charts).

8.3.3 Organizing Displays in Dashboards

Dashboard displays can be summarized to dashboards. They can be individual compilations of displays but there are predefined dashboards which can be chosen as well.

There can be up to 10 dashboards.

By default, there is only the overview dashboard giving a short overview of tasks, CVEs and VTs (see Fig. 8.8).

The dashboards are displayed by selecting *Dashboards* in the menu bar.

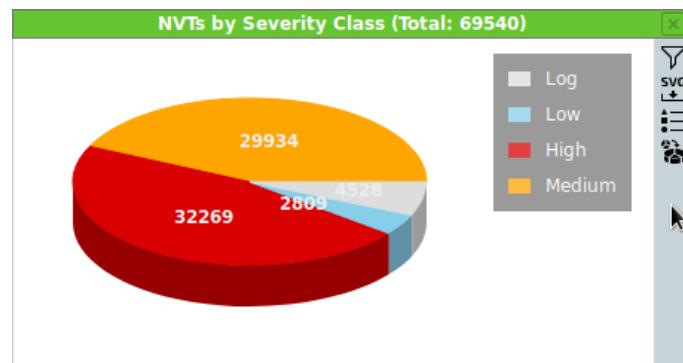


Fig. 8.7: Choosing further options for a display

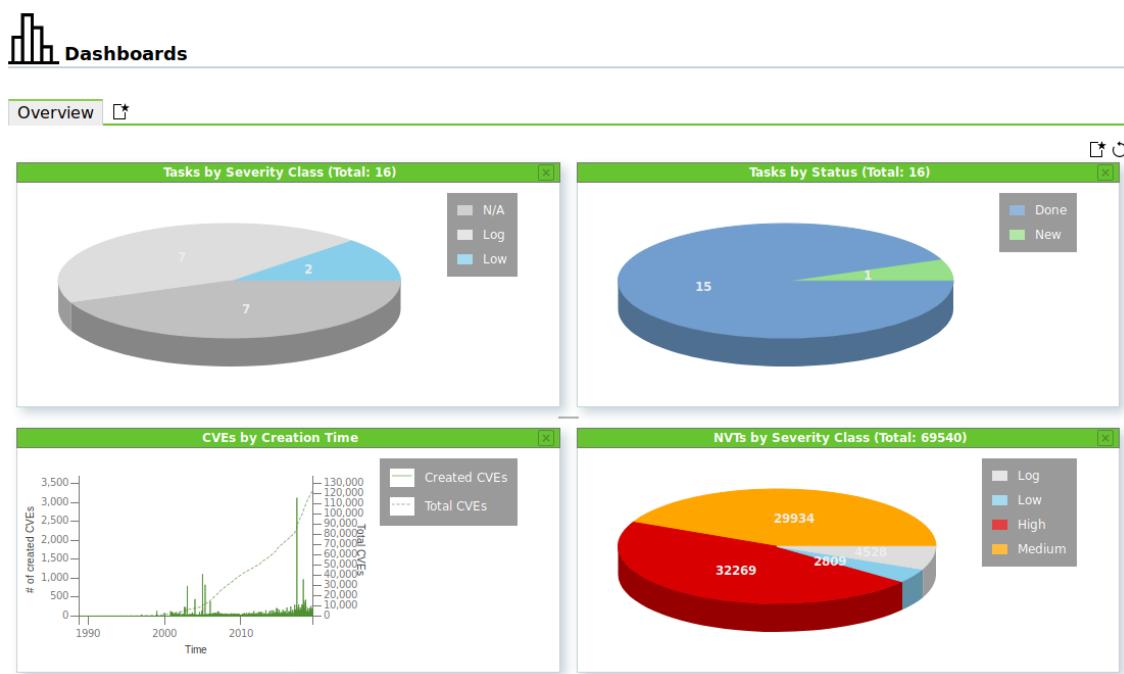


Fig. 8.8: Overview dashboard



8.3.3.1 Adding a New Dashboard

A new dashboard can be created as follows:

1. Click  in the register bar above the dashboard (see Fig. 8.9).

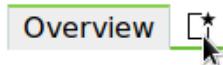


Fig. 8.9: Adding a new dashboard

2. Enter the name of the dashboard in the input box *Dashboard Title*.
3. Select the displays that should be shown by default in the drop-down list *Initial Displays* (see Fig. 8.10).

The following default settings for the shown displays are possible:

- Default: the dashboard contains the same displays as the overview dashboard.
- Scan Displays: the dashboard contains displays concerning tasks, results and reports.
- Asset Displays: the dashboard contains displays concerning hosts and operating systems.
- SecInfo Displays: the dashboard contains displays concerning VTs, CVEs, and CERT-Bund Advisories.
- Empty: the dashboard contains no displays.

Additionally, already existing dashboards can be chosen.

Tip: The displays can later be edited as well (see Chapters 8.3.1 (page 203) and 8.3.2 (page 204)).

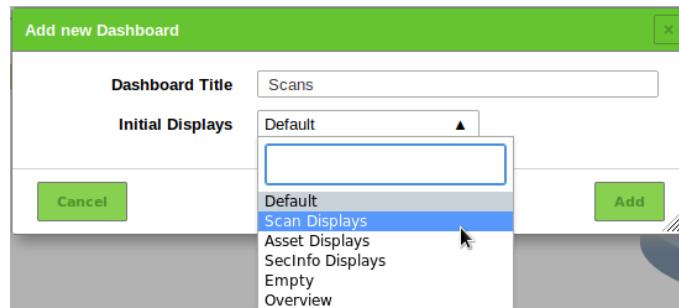


Fig. 8.10: Adding a new dashboard

4. Click *Add*.

→ The dashboard is added and shown in the register bar (see Fig. 8.11).

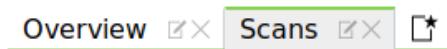


Fig. 8.11: Registers of available dashboards



8.3.3.2 Editing a Dashboard

Displays can be added to or deleted from a dashboard as described in Chapter 8.3.1 (page 203).

The displays in a dashboard can be edited as described in Chapter 8.3.2 (page 204).

A dashboard can be renamed as follows:

1. Click in the register of the dashboard in the register bar (see Fig. 8.12).



Fig. 8.12: Renaming or deleting a dashboard

2. Change the name in the input box *Dashboard Title*.
3. Click **Save**.

8.3.3.3 Deleting a Dashboard

A dashboard can be deleted by clicking in the register of the dashboard in the register bar (see Fig. 8.12).

8.4 Filtering the Page Content

Almost every page in the web interface offers the possibility to filter the displayed content.

8.4.1 Adjusting the Filter Parameters



Fig. 8.13: Filter bar at the top of the page

Multiple filter parameters are combined to form the Powerfilter.

Note: The filter is context aware which means that the filter parameters depend on the currently opened page.

The filter parameters can be entered in the input box in the filter bar (see Fig. 8.13) using the specific syntax of the filter (see Chapter 8.4.2 (page 209)) or be modified as follows:

1. Click in the filter bar (see Fig. 8.13).
2. Select and modify the filter parameters (see Fig. 8.14).

Keywords which should be searched for can be entered in the input box *Filter*.

Note: The Powerfilter is not case-sensitive. All uppercase letters are transformed to lowercase letters before applying the filter.

3. Activate the checkbox *Store filter* as if the filter should be stored for reuse.
4. Enter the name for the filter in the input box *Store filter as*.



The screenshot shows the 'Update Filter' dialog box. It includes fields for filtering by severity (High selected), solution type (All selected), QoD (70%), and sorting (Severity, Descending). A 'Store filter as:' dropdown contains 'filter1'. Buttons for 'Cancel' and 'Update' are at the bottom.

Fig. 8.14: Adjusting the filter

5. Click *Update*.

→ The filter parameters are applied.

Next to the input box in the filter bar the following actions are available:

- Remove the currently applied filter.
- Update the filter with the current input.
- Reset the filter parameters to the default settings.
- A saved Powerfilter can be applied by selecting it in the drop-down list (see Fig. 8.15).

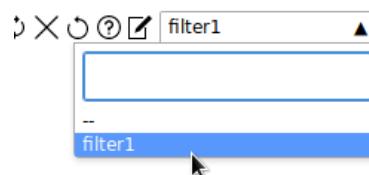


Fig. 8.15: Selecting a saved Powerfilter

Tip: If a specific filter should always be activated on a page, it can be set as the default filter in the user settings (see Chapter 8.8 (page 218)).

Powerfilters can also be created using the page *Filters* as follows:

1. Select *Configuration > Filters* in the menu bar.
2. Create a new filter by clicking



3. Define the name of the filter.
4. Define the filter criteria in the input box *Term* (see Chapter 8.4.2 (page 209)).
5. Select the object type for which the filter should be applied in the drop-down list *Type* (see Fig. 8.16).

The screenshot shows a 'New Filter' dialog box with the following fields:

- Name:** Filter1
- Comment:** (empty)
- Term:** apply_overrides=1 min_qod=70 rows=100 first=1 sort=name
- Type:** Result

At the bottom are 'Cancel' and 'Save' buttons.

Fig. 8.16: Creating a new filter

6. Click *Save*.
- The filter can be used for the object type for which it was created.

8.4.2 Syntax of the Powerfilter

When applied, the filter parameters are shown in the lower left corner of the page (see Fig. 8.17).

(Applied filter: apply_overrides=1 min_qod=70 rows=100 first=1 sort=name levels=mhlgl)

Fig. 8.17: Applied filter parameters

The filter uses a specific syntax which has to be considered when entering the filter keywords directly in the input box in the filter bar.

8.4.2.1 Global Keywords

In general, the specification of the following keywords is always possible:

Note: These keywords apply to the whole filter request and should only be mentioned once.

Example: filter requests like `name~test` and `rows=20` or `name~def` and `rows=30` are not allowed. In this case, only `rows=30` would be applied.

- **rows:** Number of rows that are displayed per page. Per default the value is `rows=10`. Entering a value of `-1` will display all results. Entering a value of `-2` will use the value that was pre-set in *My Settings* under *Rows Per Page* (see Chapter 8.8 (page 218)).

Note: Using `rows=-1` may cause performance issues if large amounts of data have to be processed.

If long page loading times are encountered, another filter for the rows should be used.

- **first:** Determination of the first object displayed. Example: if the filter returns 50 results, `rows=10 first=11` displays the results 11 to 20.



- **sort:** Determination of the column used for sorting the results. The results are sorted ascending. Example: `sort=name` sorts the results by name. The sorting can also be done by clicking the title of the column. After applying the filter, upper cases of the column names are changed to lower cases and spaces are changed to underscores. Typical column names are:

- `name`
- `severity`
- `host`
- `location`
- `qod` (Quality of detection)
- `comment`
- `modified`
- `created`

Note: `sort` is not applicable for report details pages (see Chapter 11.2.1 (page 320)).

- **sort-reverse:** Determination of the column used for sorting the results (see above). The results are sorted descending.

Note: `sort-reverse` is not applicable for report details pages (see Chapter 11.2.1 (page 320)).

- **tag:** Selection of results with a specific tag (see Chapter 8.5 (page 214)). It can be filtered by a specific tag value (`tag="server=mail"`) or only by the tag (`tag="server"`). Regular expressions are also allowed.

Note: By filtering using tags custom categories can be created and used in the filters. This allows for versatile and granular filter functionality.

- **tag_id:** Selection of results with a specific tag (see Chapter 8.5 (page 214)). It is filtered by the UUID of the tag. The UUID of a tag can be found on the tag's details page (see Chapter 8.5.4 (page 215)). The filter stays valid, even if the name of the tag is changed.

8.4.2.2 Operators

When specifying the components the following operators are used:

- = equals, e.g., `rows=10`
- ~ contains, e.g., `name~admin`
- < less than, e.g., `created<-1w` → older than a week
- > greater than, e.g., `created>-1w` → younger than a week
- `regexp` regular expression, e.g., `regexp 192.168.[0-9]+.[0-9]`

The following operators are **not** supported:

- `<=`
- `>=`
- `()`



There are a couple of special features:

- If no value follows `=`, all results without this filter parameter are displayed. This example shows all results without a comment:

```
comment=
```

- If a keyword should be found but it is not defined which column to scan, all columns will be scanned. This example searches whether at least one column contains the stated value:

```
=192.168.15.5
```

- The data is usually or-combined. This can be specified with the keyword `or`. To achieve an and-combination the keyword `and` needs to be specified:

```
modified>2019-01-01 and name=services
```

- `and` is resolved before `or`, i. e., `x and y or a and b` → `(x and y) or (a and b)`
Expressions like `x and (a or b)` have to be written as `x and a or x and b`.
- Using `not` negates the filter. This example shows all results that do not contain “192.168.81.129”:

```
not ~192.168.81.129
```

8.4.2.3 Text Phrases

In general, text phrases that are being searched for can be specified.

The following examples show the differences:

overflow Finds all results that contain the word *overflow*. This applies to *Overflow* as well as to *Bufferoverflow*. Also, `192.168.0.1` will find `192.168.0.1` as well as `192.168.0.100`.

remote exploit Finds all results containing *remote* or *exploit*. Of course, results that contain both words will be displayed as well.

remote and exploit Finds all results containing both *remote* and *exploit*. The results do not have to be found in the same column.

"remote exploit" The exact string is being searched for and not the individual words.

regexp 192.168.[0-9]+.[0-9] The regular expression is being searched for.

8.4.2.4 Time Specifications

Time specifications in the Powerfilter can be absolute or relative.

Absolute time specification An absolute time specification has the following format:

```
2014-05-26T13h50
```

If the time is left out, a time of 12:00 am will be assumed automatically. The time specification can be used in the search filter, e.g., `created>2014-05-26`.

Relative time specification Relative time specifications are always calculated in relation to the current time.

Time specification in the past are defined with a preceding minus (-). Time specification without a preceding character are interpreted as being in the future. For time periods the following letters can be used:

- `s` second



- *m* minute
- *h* hour
- *d* day
- *w* week
- *m* month (30 days)
- *y* year (365 days)

For example, entering *created>-5d* shows the results that were created within the past 5 days. A combination such as *5d1h* is not permitted but has to be replaced with *121h*.

To limit the time period, e.g., month for which information should be displayed, the following expression can be used:

```
modified>2019-01-01 and modified<2019-01-31
```

8.4.3 Examples for Powerfilters

Here are some examples for powerfilter:

- `127.0.0.1` shows any object that has “127.0.0.1” anywhere in the text of any column.
- `127.0.0.1 iana` shows any object that has “127.0.0.1” or “iana” anywhere in the text of any column.
- `127.0.0.1 and iana` shows any object that has “127.0.0.1” and “iana” anywhere in the text of any column.
- `regexp 192.168.[0-9]+.[0-9]` shows any object that has an IP style string starting with “192.168” anywhere in the text of any column.
- `name=localhost` shows any object with the exact name “localhost”.
- `name~local` shows any object with “local” anywhere in the name.
- `name:^local` shows any object with a name starting with “local”.
- `port_list~tcp` shows any object that has “tcp” anywhere in the port list name.
- `modified>2019-02-03 and modified<2019-02-05` shows any object that was modified between `2019-02-03 0:00` and `2019-02-05 0:00`.
- `created>2019-02-03T13h00` shows any object that was created after 13:00 on 2019-02-03.
- `rows=20 first=1 sort=name` shows the first twenty objects sorted by the column *Name*.
- `created>-7d` shows any object that was created within the past 7 days.
- `=127.0.0.1` shows any object that has “127.0.0.1” as the exact name in any column.
- `tag="geo:long=52.2788` shows any object that has a tag named “geo:long” with the value “52.2788”.
- `tag~geo` shows any object that has a tag with a name containing “geo”.

8.4.4 Managing Powerfilters

List Page

All existing Powerfilters can be displayed by selecting *Configuration > Filters* in the menu bar (see Fig. 8.18).

For all Powerfilters the following information is displayed:

Name Name of the filter.



Term Filter terms that form the Powerfilter (see Chapter 8.4.2 (page 209)).

Type Object type for which the Powerfilter can be applied.

For all Powerfilters the following actions are available:

- Move the Powerfilter to the trashcan.
- Edit the Powerfilter.
- Clone the Powerfilter.
- Export the Powerfilter as an XML file.

Name	Term	Type	Actions
filter1	apply_overrides=0 min_qod=70 rows=100 first=1 sort=name levels=ml	Result	
Filter_Alert	first=1 rows=-1 sort=name	Alert	
Filter_SecInfo	first=10 rows=5 sort=date	Info	

(Applied filter: rows=30 first=1 sort=name)

Apply to page contents ▾

1 - 3 of 3

Fig. 8.18: Managing Powerfilters

Note: By clicking or below the list of filters more than one filter can be moved to the trashcan or exported at a time. The drop-down list is used to select which filters are moved to the trashcan or exported.

Details Page

Click on the name of a filter to display the details of the filter. Click to open the details page of the filter.

The following registers are available:

Information General Information about the Powerfilter.

User Tags Assigned tag (see Chapter 8.5 (page 214)).

Permissions Assigned permissions (see Chapter 9.4 (page 231)).

The following actions are available in the upper left corner:

- Open the corresponding chapter of the user manual.
- Show the list page of all Powerfilters.
- Create a new Powerfilter (see Chapter 8.4.1 (page 207)).
- Clone the Powerfilter.
- Edit the Powerfilter.
- Move the Powerfilter to the trashcan.
- Export the Powerfilter as an XML file.



8.5 Using Tags

Tags are information that can be linked to any object. Tags are created directly with the objects and can only be linked to the object type they are created for.

Tags can be used to filter objects (see Chapter 8.4 (page 207)).

Example: when filtering for `tag=target` the specific tag must be set. Otherwise, the desired result would not be found. With `tag="target=mailserver"` the exact tag with the respective value must be set (see Fig. 8.19).

The screenshot shows a 'New Tag' dialog box. The 'Name' field contains 'target'. The 'Comment' field contains 'Server type'. The 'Value' field contains 'mailserver'. The 'Resource Type' dropdown is set to 'Target'. Below it, there's a dropdown menu and an input field for 'Resources' containing 'b95789c4-18e6-419e-42c2-0e7fbfe0a7e'. The 'Active' section has two radio buttons: 'Yes' (selected) and 'No'. At the bottom are 'Cancel' and 'Save' buttons.

Fig. 8.19: Tag for the object type *Target*

8.5.1 Linking a Tag to a Single Object

A tag for a single object can be created as follows:

1. Open the details page of the object (see Chapter 8.2 (page 200)).
2. Click on the register *User Tags*.
3. Click in the opened section *User Tags*.
4. Define the tag (see Fig. 8.19).
5. Click *Save*.

8.5.2 Linking a Tag to Multiple Objects

A tag can be added to multiple objects of the same type (e.g., tasks, targets, scanners) as follows:

1. Open the list page of an object type.
2. Filter the list so that only the objects that should have the tag are displayed.
3. In the drop-down list below the list of objects select to which objects the tag should be added (see Fig. 8.20).

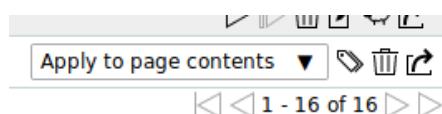


Fig. 8.20: Selecting the objects



Note: *Apply to page contents* links the tag to all objects which are visible on the current page.

Apply to all filtered links the tag to all objects which are affected by the filter even if they are not visible on the current page.

or

2. In the drop-down list below the list of objects select *Apply to selection*.
3. Activate the checkboxes of the objects that should have the tag in the column *Actions*.
4. Click below the list of objects.
5. Select the tag in the drop-down list *Choose Tag* (see Fig. 8.21).

Note: Only tags which are created for the chosen object type can be selected.

Additionally, a new tag can be created by clicking .

The screenshot shows a modal dialog titled "Add Tag to Page Contents". Inside, there's a dropdown menu labeled "Choose Tag" with "target:server" selected. Below it, there are fields for "Value" (set to "mail") and "Comment" (set to "Server type"). At the bottom left is a green "Cancel" button, and at the bottom right is a green "Add Tag" button.

Fig. 8.21: Selecting a tag for multiple objects

6. Click *Add Tag*.

8.5.3 Creating a Tag

In addition to linking tags directly to an object, tags can be created on the page *Tags* and assigned afterwards.

1. Select *Configuration > Tags* in the menu bar.
2. Create a new tag by clicking .
3. Define the tag. Select the object type for which the tag can be assigned in the drop-down list *Resource Type*.
4. Click *Save*.

8.5.4 Managing Tags

List Page

All existing tags can be displayed by selecting *Configuration > Tags* in the menu bar.

For all tags the following actions are available:

- Disable the tag if it is enabled.
- Enable the tag if it is disabled.



- ✖ Move the tag to the trashcan.
- ✎ Edit the tag.
- ⌚ Clone the tag.
- ↗ Export the tag as an XML file.

Note: By clicking ✖ or ↗ below the list of tags more than one tag can be moved to the trashcan or exported at a time. The drop-down list is used to select which tags are moved to the trashcan or exported.

Details Page

Click on the name of a tag to display the details of the tag. Click ⓘ to open the details page of the tag.

The following registers are available:

Information General information about the tag.

Assigned Items Objects to which the tag is assigned. The objects are only displayed if the tag is enabled.

Permissions Assigned permissions (see Chapter 9.4 (page 231)).

The following actions are available in the upper left corner:

- ⓘ Open the corresponding chapter of the user manual.
- ⌂ Show the list page of all tags.
- ⚡ Create a new tag (see Chapter 8.5.3 (page 215)).
- ⌚ Clone the tag.
- ✎ Edit the tag.
- ✖ Move the tag to the trashcan.
- ↗ Export the tag as an XML file.
- ⓘ Disable the tag if it is enabled.
- ⓘ Enable the tag if it is disabled.

8.6 Using the Trashcan

The page *Trashcan* is opened by selecting *Administration > Trashcan* in the menubar. The page lists all objects that are currently in the trashcan, grouped by object type.

Note: Objects in the trashcan do not count as deleted yet. They are only finally deleted when manually deleting them from the trashcan, or when emptying the whole trashcan.

The summary table *Content* shows all possible types of deleted objects with object counts. By clicking on an object name the corresponding section is shown (see Fig. 8.22).

The trashcan can be emptied by clicking *Empty Trash*.

In the section of the respective object type the single objects can be managed (see Fig. 8.23):

- Clicking ⌂ moves the object out of the trashcan and back to its regular page. The object cannot be restored if it depends on another object in the trashcan.



Type	Items
Alerts	0
Configs	1
Credentials	0
Filters	0
Groups	0
Notes	0
Overrides	0
Permissions	0
Port Lists	0
Report Formats	0
Roles	0
Scanners	0
Schedules	0
Tags	1
Targets	2
Tasks	23
Tickets	0

Fig. 8.22: Contents of the trashcan

- Clicking removes the object entirely from the system. The object cannot be deleted if another object in the trashcan depends on it.

File Content Violation	File Content	Any	10.0 (High)	yes		
Error on File System	File Content: Errors	Any	5.0 (Medium)	yes		
File Content Violation	File Content: Violations	Any	5.0 (Medium)	yes		
OS End of Life Detection	OS End Of Life Detection	Any	2.0 (Low)	no		
TCP Timestamps	TCP timestamps	Any	5.0 (Medium)	yes		

Fig. 8.23: Restoring or deleting a trashcan object



8.7 Displaying the Feed Status

The synchronization status of all SecInfo can be displayed by selecting *Administration > Feed Status* in the menu bar.

The following information is displayed (see Fig. 8.24):

Type Feed type (NVT, SCAP, CERT or GVMD_DATA).

Content Type of information provided by the feed.

Origin Name of the feed service that is used to synchronize the SecInfo.

Version Version number of the feed data.

Status Status information of the feed, e.g., time since the last update.

If a feed update is currently being performed, *Update in progress...* is displayed. This status is displayed for all feeds, even if only one feed is currently being updated.

Type	Content	Origin	Version	Status
NVT	NVTs	Greenbone Security Feed	20200810T0503	Current
SCAP	CVES CPEs OVAL Definitions	Greenbone SCAP Feed	20200810T0130	Current
CERT	CERT-Bund Advisories DFN-CERT Advisories	Greenbone CERT Feed	20200810T0030	Current
GVMD_DATA	Compliance Policies Port Lists Report Formats Scan Configs	Greenbone GVMd data Feed	20200803T1409	7 days old

Fig. 8.24: Displaying the feed status

8.8 Changing the User Settings

Every user of the GSM appliance can manage their own settings for the web interface. These settings can be accessed by moving the mouse over in the upper right corner and clicking *My settings* (see Fig. 8.25).

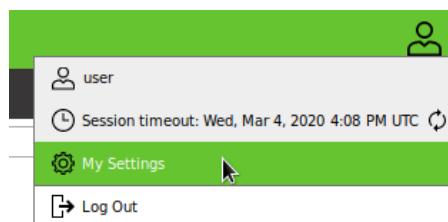


Fig. 8.25: Accessing the user settings



The settings can be modified by clicking .

Fig. 8.26: Managing user settings

Important settings are:

Timezone The GSM saves all information in the UTC time zone internally. In order to display the data in the time zone of the user the respective selection is required.

Change Password The user password can be changed here.

User Interface Language The language can be defined here. The browser setting are used per default.

Rows Per Page This defines the default number of objects shown per list page on the web interface. A high number of rows per page increases loading times. Custom user filters may override this setting (see Chapter 8.4 (page 207)).

Details Export File Name This defines the default name of the file for exported object details. For the file name the following placeholders can be used:

- %C: the creation date in the format YYYYMMDD. Changed to the current date if a creation date is not available.
- %c: the creation time in the format HHMMSS. Changed to the current time if a creation time is not available.
- %D: the current date in the format YYYYMMDD.
- %F: the name of the used report format (XML for lists and types other than reports).
- %M: the modification date in the format YYYYMMDD. Changed to the creation date or to the current date if a modification date is not available.
- %m: the modification time in the format HHMMSS. Changed to the creation time or to the current time if a modification time is not available.
- %N: the name for the object or the associated task for reports. Lists and types without a name will use the type (see %T).



- %T: the object type, e.g., “task”, “port_list”. Pluralized for list pages.
- %t: the current time in the format HHMMSS.
- %U: the unique ID of the object or “list” for lists of multiple objects.
- %u: the name of the currently logged in user.
- %%: the percent sign (%).

List Export File Name This defines the default name of the file for exported object lists (see above).

Report Export File Name This defines the default name of the file for exported reports (see above).

Auto Cache Rebuild The automatic cache rebuild can be enabled or disabled here. If many actions are performed in a row (e.g., deleting of multiple objects) with enabled automatic cache rebuild, each action triggers the cache rebuild leading to a slowed down process. For such cases, the automatic cache rebuild can be disabled temporarily.

Dynamic Severity This defines whether the severity of an existing result is changed if the severity of the underlying VT changes. Otherwise, the new severity only affects future scans.

Default Severity The default severity can be specified here. In case no severity is assigned to a VT, the default severity is used.

Defaults Settings The default selections or entries for various settings can be specified here.

Filter Settings Specific default filters for each page can be specified here. The filters are then activated automatically when the page is loaded.

8.9 Opening the User Manual

The user manual can be opened by selecting *Help > User Manual* in the menu bar.

Additionally, the user manual can be opened on any page by clicking ⓘ in the upper left corner. The chapter related to the page content is opened.

8.10 Logging Out of the Web Interface

Logging out of the web interface can be done by moving the mouse over ⓘ in the upper right corner and clicking *Log Out* (see Fig. 8.27).

If no action is performed for a defined period of time, the user is logged out automatically (see Chapter 7.2.4.1.1 (page 146)). The default timeout is 15 minutes.

The remaining time until the user is automatically logged out can be displayed by moving the mouse over ⓘ. By clicking ⏪ the timeout can be reset.

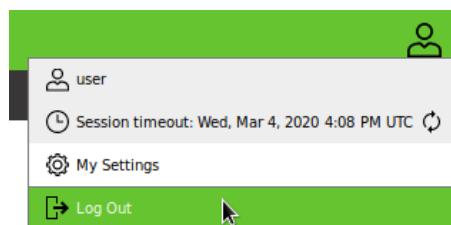


Fig. 8.27: Logging out of the web interface

CHAPTER 9

Managing the Web Interface Access

Note: This chapter documents all possible menu options.

However, not all GSM models support all of these menu options. Check the tables in Chapter 3 (page 18) to see whether a specific feature is available for the used GSM model.

9.1 Users

The Greenbone Security Manager (GSM) allows for the definition and management of multiple users with different roles and permissions. When initializing the GSM, the first user – the web/scan administrator – is already created in the GOS administration menu. With this user, additional users can be created and managed.

Roles The GSM user management supports a role based permission concept when accessing the web interface. Various roles are already set up by default. Additional roles can be created and used by an administrator. The role defines which options of the web interface can be viewed and modified by the user. The role enforcement is not implemented in the web interface but rather in the underlying Greenbone Management Protocol (GMP) and so affects all GMP clients. Read and write access can be assigned to roles separately.

Groups In addition to roles the GSM user management supports groups as well. This serves mainly for logical grouping.

Groups and roles may be used to assign permissions to several users at once.

Each user is assigned an IP address range containing the allowed or denied targets. The GSM appliance will refuse to scan any other IP addresses than the ones specified. Similarly, the access to specific interfaces of the GSM appliance can be allowed or denied.

The user management is completely done with the GSM. External sources for the user management are not supported. However, to support central authentication and to allow password synchronization the GSM can be integrated with a central LDAP or RADIUS server (see Chapter 9.5 (page 240)). The server will only be used to verify the password during the login process of the user. All other settings are performed in the user management of the GSM.



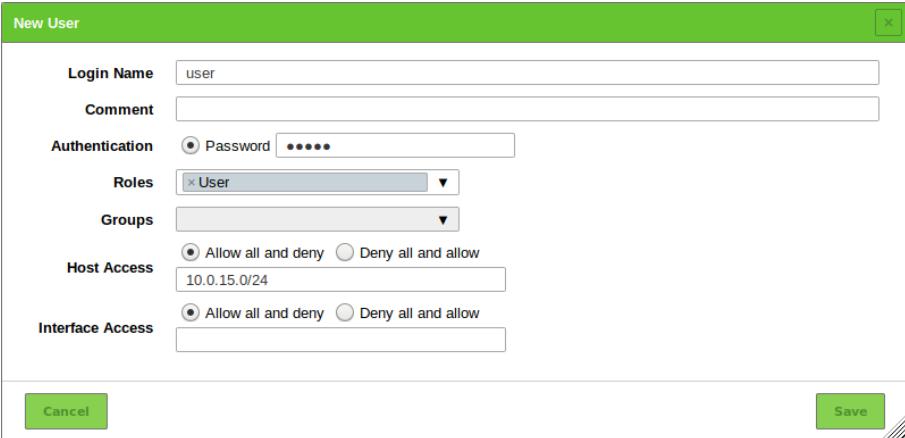
9.1.1 Creating and Managing Users

9.1.1.1 Creating a User

Users can be created as follows:

Note: Only administrators are allowed to create and manage additional users.

1. Log in as an administrator.
2. Select *Administration > Users* in the menu bar.
3. Create a new user by clicking .
4. Define the user (see Fig. 9.1).



The screenshot shows the 'New User' dialog box. The 'Login Name' field contains 'user'. The 'Comment' field is empty. Under 'Authentication', 'Password' is selected with a masked password. In the 'Roles' dropdown, 'User' is chosen. The 'Groups' dropdown is empty. Under 'Host Access', the 'Allow all and deny' radio button is selected, and the IP range '10.0.15.0/24' is listed. Under 'Interface Access', the 'Allow all and deny' radio button is selected. At the bottom left is a 'Cancel' button, and at the bottom right is a 'Save' button.

Fig. 9.1: Creating a new user

5. Click *Create*.

→ The user is created and displayed on the page *Users*.

The following details of the user can be defined:

Login Name This is the name used for logging in. When an LDAP or a RADIUS server is used for central password management, the user needs to be created with the identical name (rDN) as used by the server (see Chapter 9.5 (page 240)). The name can contain letters and numbers and can be at most 80 characters long.

Authentication This is the password used for logging in. The password can contain any type of character and can be at most 40 characters long.

Note: When using special characters, note that they have to be available on all used keyboards and operating systems.

Note: When a central user management is used, more options are available (see Chapter 9.5 (page 240)).

Roles Each user can have multiple roles. The roles define the permissions of a user when using GMP. The roles *Admin*, *User*, *Info*, *Observer*, *Guest* and *Monitor* are available. Additionally, it is possible to add and configure custom roles (see Chapter 9.2.2 (page 227)).



If a user with a custom role should be able to use the web interface, at least the following permissions are necessary for that role:

- *authenticate*
- *get_settings*
- *help*

For further details see Chapter 9.2 (page 225).

Groups Each user can be a member of multiple groups. Permissions management can be performed using groups as well (see Chapter 9.4 (page 231)).

Host Access Hosts on which the user is allowed to run scans. The restrictions also apply to administrators but they are allowed to remove them themselves. Normal users (*User*) and roles without access to the user management cannot circumvent the restrictions. Basically either a whitelist (deny all and allow) or a blacklist (allow all and deny) is possible.

- **Whitelist** The scanning of all systems is denied in general. Only explicitly listed systems are allowed to be scanned.
- **Blacklist** The scanning of all systems is allowed in general. Only explicitly listed systems are not allowed to be scanned.

Tip: In general the whitelist methodology should be used. This ensures that users do not scan systems lying beyond their responsibility, located somewhere on the Internet or reacting to malfunctioning scans by accident.

System names as well as IPv4 and IPv6 addresses can be entered. Individual IP addresses as well as address ranges and network segments can be specified. The following listing shows some examples:

- 192.168.15.5 (IPv4 address)
- 192.168.15.5-192.168.15.27 (IPv4 range long form)
- 192.168.15.5-27 (IPv4 range short form)
- 192.168.15.128/25 (CIDR notation)
- 2001:db8::1 (IPv6 address)
- 2001:db8::1-2001:db8::15 (IPv6 range long form)
- 2001:db8::1-15 (IPv6 range short form)
- 2001:db8::/120 (CIDR notation)

All options can be mixed and matched and entered as a comma-separated list. The netmask in the CIDR notation is restricted to a maximum of 20 IP addresses for IPv4 and 116 IP addresses for IPv6. In both cases the result is a maximum of 4096 IP addresses.

Interface Access This refers to the input box *Network Source Interface* when creating a new task (see Chapter 10.2.2 (page 251)). If a task is bound to a certain network interface by its configuration and a user has no access to this network interface, the user is restricted from running the task successfully. A comma-separated list of network adapters can be entered. Similar to *Host Access* a whitelist or a blacklist methodology is possible (see above).

9.1.1.2 Managing Users

List Page

All existing users can be displayed by selecting *Administration > Users* in the menu bar when logged in as an administrator.



For all users the following information is displayed:

Name Name of the user. Global users are users who are created in the GOS administration menu (see Chapter 7.2.1 (page 124)) and are marked with

Roles Role of the user (see Chapter 9.2 (page 225)).

Groups Groups to which the user belongs (see Chapter 9.3 (page 229)).

Host Access Hosts on which the user is allowed to run scans.

Authentication Type Type of authentication: *Local* if a password is used, *RADIUS* or *LDAP* if a central user management is used (see Chapter 9.5 (page 240)).

For all users the following actions are available:

- Delete the user. Only users which are currently not logged in and which are not super administrator can be deleted.
- Edit the user.
- Clone the user.
- Export the user as an XML file.

Note: By clicking or below the list of users more than one user can be deleted or exported at a time. The drop-down list is used to select which users are deleted or exported.

Details Page

Click on the name of a user to display the details of the user. Click to open the details page of the user (see Fig. 9.2).

The following registers are available:

Information General information about the user.

User Tags Assigned tags (see Chapter 8.5 (page 214)).

Permissions Permissions of the user or of other users/roles/groups to the resources of the user (see Chapter 9.4 (page 231)).

The following actions are available in the upper left corner:

- Open the corresponding chapter of the user manual.
- Show the list page of all users.
- Create a new user (see Chapter 9.1.1.1 (page 222)).
- Clone the user.
- Edit the user.
- Delete the user. Only users which are currently not logged in and which are not super administrator can be deleted.
- Export the user as an XML file.



User: user ID: b18d0e89-235d-4d1e-b47f-d2b7e96edb1 Created: Mon, Jun 17, 2019 11:36 AM UTC Modified: Mon, Jun 17, 2019 11:36 AM UTC

Information	User Tags (0)	Permissions (1)
Comment		
Roles	User	
Groups		
Host Access	Allow all	
Interface Access	Allow all	
Authentication Type	Local	

Fig. 9.2: Details of a user

9.1.2 Simultaneous Login

It is possible that two users are logged in at the same time.

If the same user wants to log in more than once at the same time, the login must be performed from a different PC or with a different browser. Another login in the same browser invalidates the first login.

9.1.3 Creating a Guest Login

The guest user is only allowed restricted access to the web interface.

To allow the guest access, a user can be created and assigned the role *Guest* (see Chapter 9.1.1 (page 222)).

Having knowledge of the password the guest user can now log in and is presented with the page *Dashboards*.

To allow a guest to log in without needing a password, this feature has to be activated in the GOS administration menu (see Chapter 7.2.1.4 (page 126)).

9.2 Roles

The web interface supports the creation and configuration of own user roles.

The following roles are available by default:

- **Admin** This role has all permissions by default. It is especially allowed to create and manage other users, roles and groups.
- **User** This role has all permissions by default except for user, role and group management. This role is not allowed to synchronize and manage the feeds. In the web interface there is no access to the page *Administration*.
- **Info** This role (Information Browser) has only read access to the NVTs and SCAP information. All other information is not accessible. The role can modify personal setting, e.g., change the password.
- **Guest** This role corresponds with the role *Info* but is not allowed to change the user settings.
- **Monitor** This role has access to system reports of the GSM (see Chapter 17.1 (page 417)).
- **Observer** This role has read access to the system but is not allowed to start or create new scans. It has only read access to the scans for which it has been set as an observer.
- **Super Admin** This role has access to all objects of all users. It has no relation to the super user (*su/root*) in the GOS administration menu. This role cannot be configured in the web interface and users with



this role cannot be deleted using the web interface. Users with this role should be managed using the GOS administration menu (see Chapter 9.2.5 (page 229)).

Note: Only administrators are allowed to create and manage additional roles.

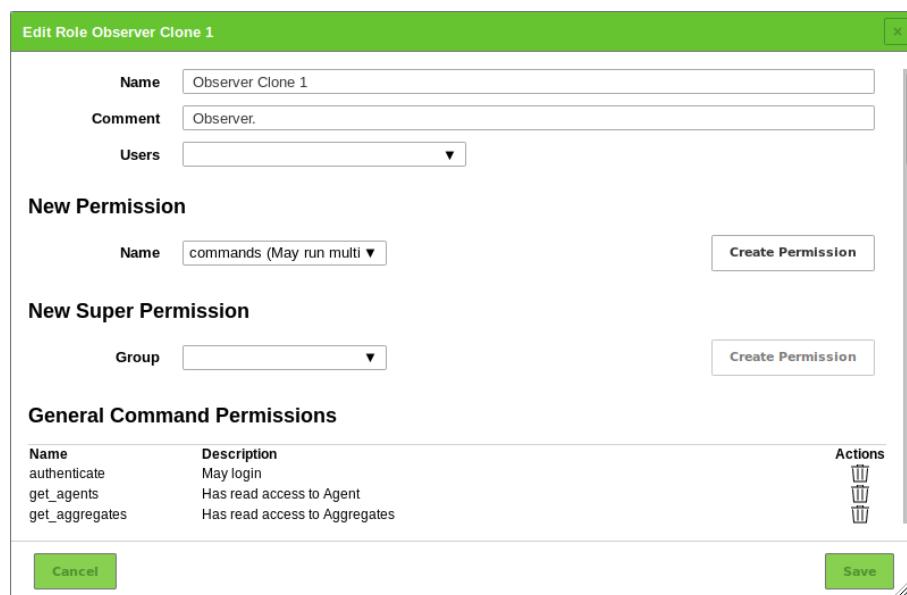
Note: Modifying the default roles is not possible but they can be copied (cloned) and subsequently modified. This ensures consistent behaviour when updating the software.

9.2.1 Cloning an Existing Role

When an existing role closely reflects the demands, a new role can be created by cloning the existing role:

1. Log in as an administrator.
2. Select *Administration > Roles* in the menu bar.
3. In the row of an existing role click .
4. In the row of the clone click .
5. Enter the name of the role in the input box *Name* (see Fig. 9.3).
6. Select the users that should have the role in the drop-down list *Users*.
7. Add a permission by selecting it in the drop-down list *Name* and clicking *Create Permission*.
8. Add a super permission by selecting the respective group in the drop-down list *Group* and clicking *Create Permission*.

Delete a permission by clicking  in the list *General Command Permissions*.



Name	Description	Actions
authenticate	May login	
get_agents	Has read access to Agent	
get_aggregates	Has read access to Aggregates	

Fig. 9.3: Editing a cloned role

9. Click *Save*.



9.2.2 Creating a Role

When a role with only limited functionality should be created, it can be started with a new, empty role:

1. Log in as an administrator.
2. Select *Administration > Roles* in the menu bar.
3. Create a new role by clicking .
4. Define the role.

The following details of the role can be defined:

Name The name of the role can contain letters and numbers and can be at most 80 characters long.

Comment (optional) A comment describes the role in more detail.

Users The users with this role can be selected in the drop-down list *Users*. Alternatively, roles can be managed in the user profile (see Chapter 9.1.1 (page 222)).

5. Click *Save*.
- The role is created and displayed on the page *Roles*.
6. In the row of the newly created role click .
7. Add a permission by selecting it in the drop-down list *Name* and clicking *Create Permission*.

Note: If users with the role should be able to use the web interface, at least the following permissions are necessary:

- *authenticate*
- *get_settings*
- *help*

The permission *write_settings* allows users to change their own password, time zone and other personal settings.

8. Add a super permission by selecting the respective group in the drop-down list *Group* and clicking *Create Permission*.
- Delete a permission by clicking  in the list *General Command Permissions*.
9. Click *Save*.

9.2.3 Managing Roles

List Page

All existing roles can be displayed by selecting *Administration > Roles* in the menu bar.

For all roles the following information is displayed:

Name Name of the role. All default roles are global roles and are marked with .

For all roles the following actions are available:

-  Move the role to the trashcan. Only self-created roles can be moved to the trashcan.
-  Edit the role. Only self-created roles can be edited.
-  Clone the role.



- Export the role as an XML file.

Note: By clicking or below the list of roles more than one role can be moved to the trashcan or exported at a time. The drop-down list is used to select which roles are moved to the trashcan or exported.

Details Page

Click on the name of a role to display the details of the role. Click to open the details page of the role.

The following registers are available:

Information General information about the role.

General Command Permissions GMP commands that can be executed by this role.

User Tags Assigned tags (see Chapter 8.5 (page 214)).

Permissions Permissions of the role or of other users/roles/groups to the role's resources (see Chapter 9.4 (page 231)).

The following actions are available in the upper left corner:

- Open the corresponding chapter of the user manual.
- Show the list page of all roles.
- Create a new role (see Chapter 9.2.2 (page 227)).
- Clone the role.
- Edit the role. Only self-created roles can be edited.
- Move the role to the trashcan. Only self-created roles can be moved to the trashcan.
- Export the role as an XML file.

9.2.4 Assigning Roles to a User

A user can have more than one role to group permissions.

The roles are assigned when creating a new user (see Fig. 9.4, see Chapter 9.1.1 (page 222)). If more than one role is assigned to a user, the permissions of the roles will be added.

The screenshot shows the 'New User' dialog box. In the 'Roles' section, 'Guest' and 'Observer' are selected. Under 'Host Access' and 'Interface Access', both 'Allow all and deny' and 'Deny all and allow' options are available for selection.

Fig. 9.4: Creating a new user with multiple roles



9.2.5 Creating a Super Administrator

The role *Super Admin* is the highest level of access.

The role *Admin* is allowed to create, modify and delete users. Additionally, it can view, modify and delete permissions but is subordinated to those permissions as well. If any user creates a private scan configuration but does not share it, the administrator cannot access it.

The role *Super Admin* is more suited for diagnostic purposes. The super administrator is excluded from permission restrictions and allowed to view and edit any configuration settings of any user.

The super administrator has to be created in the GOS administration menu (see Chapter 7.2.1.5 (page 127))

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

9.3 Groups

Groups are used to logically assemble users. An unlimited number of groups can be created.

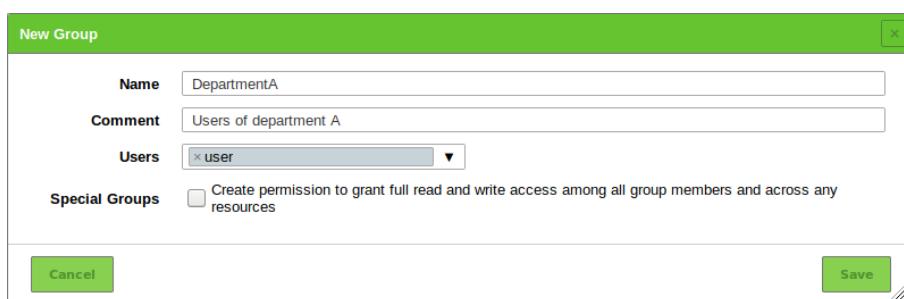
Permissions can be assigned for the groups (see Chapter 9.4 (page 231)). By default, no groups are set up.

9.3.1 Creating a Group

A group can be created as follows:

Note: Only administrators are allowed to create and manage groups.

1. Log in as an administrator.
2. Select *Administration > Groups* in the menu bar.
3. Create a new group by clicking .
4. Define the group (see Fig. 9.5).



The screenshot shows the 'New Group' dialog box. At the top, it says 'New Group'. Below that, there are four input fields: 'Name' with the value 'DepartmentA', 'Comment' with the value 'Users of department A', 'Users' with a dropdown menu showing 'x user', and 'Special Groups' with a checkbox labeled 'Create permission to grant full read and write access among all group members and across any resources'. At the bottom, there are two buttons: 'Cancel' on the left and 'Save' on the right.

Fig. 9.5: Creating a new group

5. Click *Save*.
→ The group is created and displayed on the page *Groups*.

The following details of the group can be defined:

Name The name of the group can contain letters and numbers and can be at most 80 characters long.

Comment (optional) A comment describes the group in more detail.



Users The members of the group can be selected in the drop-down list *Users*. Alternatively, group memberships can be managed in the user profile (see Chapter 9.1.1 (page 222)).

Special Groups Activate the checkbox if all group members should have read and write access to all resources of the group.

9.3.2 Managing Groups

List Page

All existing groups can be displayed by selecting *Administration > Groups* in the menu bar.

For all groups the following information is displayed:

Name Name of the group.

For all groups the following actions are available:

- Move the group to the trashcan.
- Edit the group.
- Clone the group.
- Export the group as an XML file.

Note: By clicking or below the list of groups more than one group can be moved to the trashcan or exported at a time. The drop-down list is used to select which groups are moved to the trashcan or exported.

Details Page

Click on the name of a group to display the details of the group. Click to open the details page of the group.

The following registers are available:

Information General information about the group.

User Tags Assigned tags (see Chapter 8.5 (page 214)).

Permissions Permissions of the group or of other users/roles/groups to the resources of the group (see Chapter 9.4 (page 231)).

The following actions are available in the upper left corner:

- Open the corresponding chapter of the user manual.
- Show the list page of all groups.
- Create a new group (see Chapter 9.3.1 (page 229)).
- Clone the group.
- Edit the group.
- Move the group to the trashcan.
- Export the group as an XML file.



9.4 Permissions

Select *Administration > Permissions* to display all permissions assigned on the system. If multiple roles are created, there can easily be hundreds of permissions.

Each permission relates to exactly one subject. A permission enables a subject to perform an associated action.

Subjects can be of the following types:

- Users
- Roles
- Groups

There are two types of permissions:

- **Command permissions** Command permissions are linked to the Greenbone Management Protocol (GMP). Each command permission applies to a specific GMP command. The name of the permission is the relevant command.
A command permission is either a command level permission or a resource level permission.
 - **Command level** When no resource is specified, a command level permission is created. A command level permission allows the subject to run the given GMP command.
 - **Resource level** When a resource is specified, a resource level permission is created. A resource level permission allows the subject to run the given GMP command on a specific resource.
- **Super permissions** (see Chapter 9.4.2 (page 234))

9.4.1 Creating and Managing Permissions

Note: Usually, permissions are assigned in the web interface using the role management (see Chapter 9.2 (page 225)).

Creating and managing permissions using the page *Permissions* is only recommended to experienced users looking for a specific permission.

9.4.1.1 Creating a Permission

A new permission can be created as follows:

1. Select *Administration > Permissions* in the menu bar.
2. Create a new permission by clicking
3. Define the permission (see Fig. 9.6).
4. Click **Save**.
→ The permission is created and displayed on the page *Permissions*.

The following details of the permission can be defined:

Name Permission that should be granted.

Comment (optional) A comment describes the permission in more detail.

Subject Subject (user, role or group) that should be granted with the permission.



The screenshot shows a 'New Permission' dialog box. The 'Name' field contains 'create_group May create a new Group'. The 'Subject' section has 'Role' selected and 'Observer' chosen. The 'Description' field contains 'Role Observer may create a new Group'. At the bottom are 'Cancel' and 'Save' buttons.

Fig. 9.6: Creating a new permission

Note: The subjects for which permissions can be assigned depend on the role of the currently logged in user. Users can grant permissions to other users, whereas administrators can grant permissions to users, roles and groups.

Resource Type (only for the permission *Super (Has super access)*) Resource type (user, role or group) to which the user/role/group has super access.

User/role/group ID (only for the permission *Super (Has super access)*) ID of the user/role/group to which the user/role/group has super access.

Description Textual description of the permission.

9.4.1.2 Creating Permissions from the Resource Details Page

When accessing a resource details page, e.g., the detail page of a task, permissions for the resource can be granted directly on the details page as follows:

1. Open the details page of a resource.
Example: Select *Scans > Tasks* in the menu bar.
2. Click on the name of a task.
3. Click to open the details page of the task.
4. Click on the register *Permissions*.
5. Click in the opened section *Permissions*.
6. Define the permission (see Fig. 9.7).
7. Click *Save*.

→ The permission is created and displayed in the section *Permissions* on the resource details page.



The screenshot shows a modal dialog titled "Create Multiple Permissions". The "Grant" field is set to "write". The "to" field is set to "Role Admin". The "on" field is set to "Task DMZ Mail". A dropdown menu is open under "on", listing four options: "Scan Configuration", "Scanner Configuration", "Target URL including related resources", and "Port List for current resource only for related resources only". The last option is currently selected. At the bottom of the dialog are "Cancel" and "Save" buttons.

Fig. 9.7: Creating a permission from the resource details page

There are two types of permissions that can be granted directly on the resource details page:

- **read** Granting the permission *read* means allowing to view the resource on list pages and on its details page.
- **write** Granting the permission *write* means allowing to view and modify (but not delete) the resource.

Some resource types include additional permissions:

- **Tasks** When granting the permission *write* for a task, the permissions to start (*start_task*), stop (*stop_task*) and resume (*resume_task*) the task are added automatically.
- **Alerts** When granting the permission *write* for an alert, the permission to test the alert (*test_alert*) is added automatically.
- **Report formats and scanners** When granting the permission *write* for a report format or a scanner, the permissions to verify the report format (*verify_report_format*) or the scanner (*verify_scanner*) is added automatically.

For some resource types it can be selected whether the permissions should also be granted for related resources (see Fig. 9.7).

- **Tasks** For tasks this includes alerts and their filters, the target as well as its related credentials and port list, the schedule, the scanner and the scan configuration.
- **Targets** For targets this includes credentials and the port list.
- **Alerts** For alerts this includes the filter that is used on the report.

Note: Permissions can also be created only for the related resources.

The details of the related resources are displayed below the drop-down list.

9.4.1.3 Managing Permissions

List Page

All existing permissions can be displayed by selecting *Administration > Permissions* in the menu bar.

For all permissions the following information is displayed:

Name Name of the permission. A global permission is marked with .

Description Textual description of the permission.



Resource Type Resource type to which the user/role/group has access.

Resource Name of the resource to which the user/role/group has access.

Subject Type Subject type (user/role/group) that is granted with the permission.

Subject Subject that is granted with the permission.

For all permissions the following actions are available:

- trashcan icon Move the permission to the trashcan. Only self-created permissions can be moved to the trashcan.
- edit icon Edit the permission. Only self-created permissions can be edited.
- clone icon Clone the permission. Only self-created permissions can be cloned.
- export icon Export the permission as an XML file.

Note: By clicking trashcan or export below the list of permissions more than one permission can be moved to the trashcan or exported at a time. The drop-down list is used to select which permissions are moved to the trashcan or exported.

Details Page

Click on the name of a permission to display the details of the permission. Click to open the details page of the permission.

The following registers are available:

Information General information about the permission.

User Tags Assigned tags (see Chapter 8.5 (page 214)).

The following actions are available in the upper left corner:

- question mark icon Open the corresponding chapter of the user manual.
- list icon Show the list page of all permissions.
- create icon Create a new permission (see Chapter 9.4.1.1 (page 231)).
- clone icon Clone the permission. Only self-created permissions can be cloned.
- edit icon Edit the permission. Only self-created permissions can be edited.
- trashcan icon Move the permission to the trashcan. Only self-created permissions can be moved to the trashcan.
- export icon Export the permission as an XML file.

9.4.2 Granting Super Permissions

Any resource on the GSM (e.g., a user, a task, a target) is either global or owned by a specific user. Global resources are identified by .

Non-global resources can only be viewed and used by their owner. Individual permissions are necessary to make the resources available to other users which is quite tedious.

To avoid that, users, roles and groups can be assigned with super permissions. This makes all objects of other users, roles or groups accessible.

A user can get super permissions for:

- User
- Role



- Group
- Any

These super permissions allow complete access to any resource of the respective user, role, group or effectively all resources.

Note: The super permission *Any* cannot be set explicitly. It is restricted to the super administrator (see Chapter 9.2.5 (page 229)) and can only be set by creating such.

A user can only set super permissions for self-created objects. Only the super administrator can grant super permissions to any other user, role or group.

1. Click on the name of the user/role/group on the page *Users/Roles/Groups* for which super permissions should be assigned.
2. Open the details page by clicking .

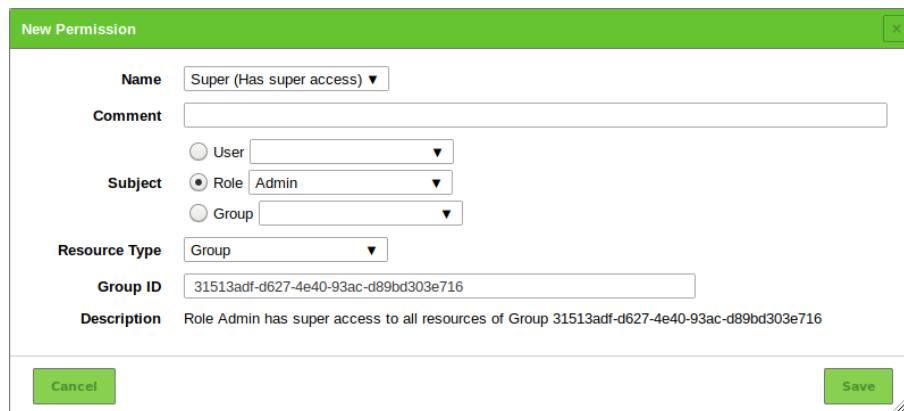
→ The resource ID can be found in the upper right corner (see Fig. 9.8).



The screenshot shows a user details page. At the top left is a user icon. Next to it, the text "User: user" is displayed. Below this, the resource ID "ID: b18d0e89-235d-4d1e-b47f-n2b7e96edbat" is shown. To the right of the ID are two timestamp fields: "Created: Mon, Jun 17, 2019 11:36 AM UTC" and "Modified: Mon, Jun 17, 2019 11:36 AM UTC".

Fig. 9.8: ID of a resource

3. Note or copy the ID.
4. Select *Administration > Permissions* in the menu bar.
5. Create a new permission by clicking .
6. In the drop-down list *Name* select *Super (Has super access)* (see Fig. 9.9).
7. Select the radio button of the subject type that should have super permissions.
8. In the according drop-down list select the user/role/group that should have super permissions.
9. Select the resource type for which super permissions should be assigned in the drop-down list *Resource Type*.
10. Enter or paste the previously determined resource ID into the input box *ID*.



The screenshot shows the "New Permission" dialog box. The "Name" field is set to "Super (Has super access)". The "Subject" section shows "Role Admin" selected. The "Resource Type" is set to "Group". The "Group ID" input field contains the value "31513adf-d627-4e40-93ac-d89bd303e716". The "Description" field contains the text "Role Admin has super access to all resources of Group 31513adf-d627-4e40-93ac-d89bd303e716". At the bottom are "Cancel" and "Save" buttons.

Fig. 9.9: Creating a new super permission

11. Click Save.

→ The super permission is created and displayed on the page *Permissions*.



Tip: Super permissions simplify the permission management on the GSM. They can easily be assigned for entire groups. This allows all users of a group to access all resources that are created by other members of the group.

9.4.3 Granting Read Access to Other Users

9.4.3.1 Requirements for Granting Read Access

Every user can share indefinite self-created resources. To do so, the user requires the **global get_users** permission as well as the **specific get_users** permission for the respective user who should obtain read access.

Note: The easiest and recommended way to share self-created resources is to use an administrator account and to create the user accounts that should receive read access with this administrator account.

All other ways described here are cumbersome and time-consuming.

Requirements for Administrators

By default, administrators already have the **global get_users** permission.

The administrator can get the specific **get_users** permission for the account that should obtain read access in two ways:

- Create the account oneself because administrators automatically have the specific **get_users** permission for accounts they created.
- With the help of a super administrator.

A super administrator can grant specific **get_users** permissions to an administrator as follows:

1. Log in to the web interface as a super administrator (see Chapters 7.2.1.5 (page 127) and 9.2.5 (page 229)).
2. Select *Administration > Users* in the menu bar.
3. Click on the name of the account who should obtain read access from the administrator.
4. Click .
5. Click on the register *Permissions*.
6. Create a new permission by clicking  in the section *Permissions*.
7. Select *read* in the drop-down list *Grant* (see Fig. 9.10).

The screenshot shows a dialog box titled "Create Multiple Permissions". It has a "Grant" dropdown set to "read". Below it, there are three radio buttons: "User" (selected), "Role", and "Group". Under "User", a dropdown shows "Admin". Below that, there's a "to" label followed by another dropdown showing "Admin". Under "on", there's a dropdown showing "User User_1" with the option "for current resource only" checked. At the bottom left is a "Cancel" button, and at the bottom right is a "Save" button.

Fig. 9.10: Granting an administrator a specific *get_users* permission

8. Select the radio button *User*.



9. Select the administrator that should be able to grant read access in the drop-down list *User*.

10. Click *Save*.

→ The specific *get_users* permission is created and displayed in the list (see Fig. 9.11).

The administrator is now able to grant read access to the respective user as described in Chapter 9.4.3.2 (page 239).

Name	Description	Resource Type	Resource	Subject Type	Subject	Actions
get_users (Automatically created when adding user)	User User_1 has read access to User User_1	User	User_1	User	User_1	
get_users	User Admin has read access to User User_1	User	User_1	User	Admin	

Fig. 9.11: Specific *get_users* permission for an administrator

Requirements for Regular Users

Regular users do not have the global *get_users* permission by default. It can be added as follows:

1. Log in to the web interface as an administrator.

2. Select *Administration > Roles* in the menu bar.

3. Create a new role by clicking .

4. Enter *GrantReadPriv* in the input box *Name*.

5. Click *Save*.

→ The role is created and displayed on the page *Roles*.

6. In the row of the newly created role click .

7. In the drop-down list *Name* in the section *New Permission* select *get_users* (see Fig. 9.12).

The screenshot shows the 'Edit Role GrantReadPriv' dialog. At the top, there are fields for 'Name' (GrantReadPriv), 'Comment' (This role allows access to the user data), and a dropdown for 'Users'. Below this is a section titled 'New Permission' with a dropdown for 'Name' set to 'get_users' and a 'Create Permission' button. Further down is a section titled 'New Super Permission' with a dropdown for 'Group' and a 'Create Permission' button. At the bottom is a section titled 'General Command Permissions' containing a table with one row for 'get_users'. The table columns are 'Name', 'Description', and 'Actions'. The 'Actions' column for the 'get_users' row contains a delete icon. At the very bottom are 'Cancel' and 'Save' buttons.

Fig. 9.12: Selecting permissions for a new role

8. Click *Create Permission*.

→ The permission is displayed in the section *General Command Permissions* (see Fig. 9.12).

9. Click *Save*.

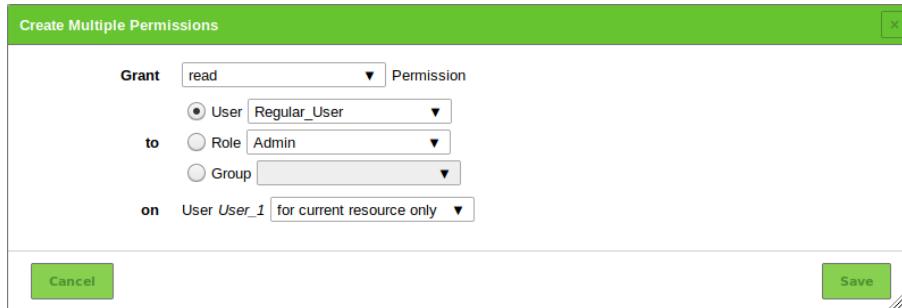
10. Select *Administration > Users* in the menu bar.



11. In the row of the user which should be assigned the newly created role click .
12. In the drop-down list *Roles* add the role *GrantReadPriv*.
13. Click *Save*.

A super administrator can grant specific *get_users* permissions to a user as follows:

1. Log in to the web interface as a super administrator (see Chapters 7.2.1.5 (page 127) and 9.2.5 (page 229)).
2. Select *Administration > Users* in the menu bar.
3. Click on the name of the account who should obtain read access from the user.
4. Click .
5. Click on the register *Permissions*.
6. In the section *Permissions* click .
7. Select *read* in the drop-down list *Grant* (see Fig. 9.13).



The screenshot shows the 'Create Multiple Permissions' dialog box. The 'Grant' dropdown is set to 'read'. The 'to' field has a radio button selected for 'User', with 'Regular_User' in the dropdown. The 'on' field has a dropdown set to 'User User_1 for current resource only'. At the bottom are 'Cancel' and 'Save' buttons.

Fig. 9.13: Granting a user a specific *get_users* permission

8. Select the radio button *User*.
9. Select the user that should be able to grant read access in the drop-down list *User*.
10. Click *Save*.

→ The specific *get_users* permission is created and displayed in the list (see Fig. 9.14).

The user is now able to grant read access to the respective user as described in Chapter 9.4.3.2 (page 239).

Name	Description	Resource Type	Resource	Subject Type	Subject	Actions
get_users (Automatically created when adding user)	User User_1 has read access to User User_1	User	User_1	User	User_1	   
get_users	User Regular_User has read access to User User_1	User	User_1	User	Regular_User	   

Fig. 9.14: Specific *get_users* permission for a user



9.4.3.2 Granting Read Access

When a user has the **global** and the **specific** `get_users` permission (see Chapter 9.4.3.1 (page 236)), the user can share resources as follows:

1. On the respective page click on the name of the resource which should be shared.
2. Open the details page by clicking .
- The object ID can be found in the upper right corner (see Fig. 9.15).



The screenshot shows a user profile with the name "User: user". Below it, the object ID is displayed as "ID: b18d0e89-235d-4d1e-b47f-d2b7e96edba". To the right, the creation and modification dates are listed as "Created: Mon, Jun 17, 2019 11:36 AM UTC" and "Modified: Mon, Jun 17, 2019 11:36 AM UTC".

Fig. 9.15: ID of a resource

3. Note or copy the ID.
4. Select *Administration > Permissions* in the menu bar.
5. Create a new permission by clicking .
6. In the drop-down list *Name* select the permission for the object to be shared.
 - Filter: `get_filters`
 - Scan configuration: `get_configs`
 - Alert: `get_alerts`
 - Note: `get_notes`
 - Override: `get_overrides`
 - Tag: `get_tags`
 - Target: `get_targets`
 - Task with report: `get_tasks`
 - Schedule: `get_schedules`
7. Select the radio button *User* (see Fig. 9.16).
8. In the according drop-down list select the user the object should be shared with.
9. Enter or paste the previously determined resource ID in the input box *ID*.



The screenshot shows the "New Permission" dialog. The "Name" field contains "get_filters Has read access to Filters". The "Comment" field contains "user can access the filter". The "Subject" section has a radio button selected for "User" with "user" chosen from the dropdown. The "Resource ID" field contains "63cf8f31-e816-47b1-8825-3f95763dd92c". The "Description" field contains "User user has read access to Filters". At the bottom are "Cancel" and "Save" buttons.

Fig. 9.16: Share objects with other users

10. Click *Save*.
→ The permission is created and displayed on the page *Permissions*.



Note: Additionally, resources can be shared with roles or groups.

For this, the global and specific permissions `get_groups` – granting read access to a group – or `get_roles` – granting read access to a role – are required and follow the same principle as described in Chapter 9.4.3.1 (page 236).

Exception: users with a default role already have the specific `get_roles` permissions for all default roles.

9.5 Using a Central User Management

Especially in larger environments with multiple users it is often difficult to achieve password synchronization. The effort to create new or reset passwords is often very high. To avoid this, the GSM supports the usage of a central password store using LDAP or RADIUS.

The GSM will use the service only for authentication on a per user basis, i.e., users who should be able to authenticate by the service have to be configured for authentication and to exist on the GSM as well.

Note: Prerequisite for using central authentication is the naming of the users with the same names as the objects in the LDAP tree or the RADIUS server.

9.5.1 LDAP

For the connection to an LDAP tree the GSM uses a very simple interface and a simple bind operation with a hard coded object path. The LDAP authentication is done as follows:

1. Log in as an administrator.
2. Select *Administration > LDAP* in the menu bar.
3. Click .
4. Activate the checkbox *Enable* (see Fig. 9.17).



Fig. 9.17: Configuring an LDAP authentication

5. Enter the LDAP host in the input box *LDAP Host*.

Note: Only one system can be entered by IP address or by name.

The GSM accesses the LDAP host using SSL/TLS. For verifying the host, the certificate of the host has to be uploaded to the GSM. Without SSL/TLS the LDAP authentication will not be accepted (see Chapter 9.5.2 (page 242)).



6. Enter the distinguished name (DN) of the objects in the input box *Auth. DN*.

Note: The wildcard `%s` replaces the user name.

Examples for the *Auth. DN* are:

- `cn=%s, ou=people, dc=domain, dc=de` This format works for any LDAP server with the correct attributes. The attribute `cn` (common name) is used. Users in different sub trees or different recursive depths of an LDAP tree are not supported. All users logging into the GSM must be in the same branch and in the same level of the LDAP tree.
- `uid=%s, ou=people, dc=domain, dc=de` This format works for any LDAP server with the correct attributes. The attribute `uid` (user ID) is used as a filter. It should be in the first place. The attributes `ou=people,dc=domain,dc=de` are used as base objects to perform a search and to retrieve the corresponding DN.
- `%s@domain.de` This format is typically used by Active Directory. The exact location of the user object is irrelevant.
- `domain.de\%s` This format is typically used by Active Directory. The exact location of the user object is irrelevant.

7. To verify the host, upload the certificate of the host by clicking *Browse*....

8. Click *OK*.

→ When the LDAP authentication is enabled, the option *LDAP Authentication Only* is available when creating or editing a user. By default, this option is disabled.

9. Create a new user or edit an existing user (see Chapter 9.1 (page 221)).

10. Activate the checkbox *LDAP Authentication Only* when the user should be allowed to authenticate using LDAP (see Fig. 9.18).

Edit User user	
Login Name	user
Comment	
Authentication	<input type="radio"/> Password: Use existing Password <input type="radio"/> New Password <input checked="" type="radio"/> LDAP Authentication Only
Roles	User
Groups	
Host Access	<input checked="" type="radio"/> Allow all and deny Deny all and allow 10.0.15.0/24
Interface Access	<input checked="" type="radio"/> Allow all and deny Deny all and allow
<input type="button" value="Cancel"/> <input type="button" value="Save"/>	

Fig. 9.18: Enabling authentication using LDAP

Note: The user has to exist with the same name in LDAP before the authentication with LDAP can be used. The GSM does not add, modify or remove users in LDAP and it does not automatically grant any user from LDAP access to the GSM.



9.5.2 LDAP with SSL/TLS

The GSM uses either the command StartTLS via LDAP on port 389 or SSL/TLS via LDAPS on port 636. The LDAP server must make its services available to SSL/TLS.

The following references are helpful for the exact configuration of all available LDAP servers:

- Microsoft: <https://social.technet.microsoft.com/wiki/contents/articles/2980.ldap-over-ssl-ldaps-certificate.aspx>
- OpenLDAP: <https://www.openldap.org/doc/admin24/tls.html>

To verify the identity of the LDAP server, the GSM has to trust the server's certificate. For this, the certificate of the issuing certificate authority (CA) must be stored on the GSM.

To do so, the certificate of the CA must be exported as a Base64 encoded file. A Base64 encoded certificate often has the file extension .pem. The file itself starts with -----BEGIN CERTIFICATE-----.

If the CA is an intermediate CA, the complete certificate chain needs to be imported. This is often true if an official CA is used because the Root CA is separated from the Issuing CA.

In these cases the contents of the file look as follows:

```
-----BEGIN CERTIFICATE-----
.....
Issuing CA
.....
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
.....
Root CA
.....
-----END CERTIFICATE-----
```

The actual location where the certificate can be found may vary based on the environment.

- Univention Corporate Server (UCS)

Here the CA certificate is retrieved from the file /etc/univention/ssl/ucsCA/CAcert.pem. This file already contains the certificate in the correct format and has to be uploaded when enabling LDAP.

- Active Directory LDAP

If the Active Directory LDAP service does not yet use LDAPS, the following article may be helpful: <https://social.technet.microsoft.com/wiki/contents/articles/2980.ldap-over-ssl-ldaps-certificate.aspx>.

The Active Directory LDAP CA certificate can then be exported as follows:

Note: The steps have to be executed from a desktop or server that has access to the CA console.

1. Open the CA console from any domain-joined computer or server.
2. Right click the name of the CA and select *Properties*.
3. In the CA certificates dialog box, select the tab *General*.
4. Select the certificate for the CA that should be accessed.
5. Click *View Certificate*.
6. In the dialog box *Certificate*, select the tab *Certification Authority*.
7. Select the name of the root CA and click *View Certificate*.
8. In the dialog box *Certificate*, select the tab *Details*.



9. Click *Copy to File*.
→ The certificate export wizard is opened.
10. Click *Next*.
11. Select *Base-64 encoded X.509 (.CER)* on the page *Export File Format*.
12. Click *Next*.
13. Enter the path and the name for the certificate in the input box *File to Export*.
14. Click *Next*.
15. Click *Finish*.
→ The CER file is created in the specified location. A dialog box informs that the export was successful.
16. Click *OK*.

The contents of the file must be uploaded when enabling LDAP.

Note: If the LDAP authentication does not work, verify that the entry in *LDAP Host* matches the commonName of the certificate of the LDAP server. If there are deviations, the GSM refuses using the LDAP server.

9.5.3 RADIUS

The RADIUS authentication is done as follows:

1. Log in as an administrator.
2. Select *Administration > Radius* in the menu bar.
3. Click .
4. Activate the checkbox *Enable* (see Fig. 9.19).
5. Enter the host name or IP address of the RADIUS server in the input box *RADIUS Host*.
6. Enter the common preshared secret key in the input box *Secret Key*.



Fig. 9.19: Configuring a RADIUS authentication

7. Click *OK*.
→ When the RADIUS authentication is enabled, the option *RADIUS Authentication Only* is available when creating or editing a user. By default, this option is disabled.
8. Create a new user or edit an existing user (see Chapter 9.1 (page 221)).



9. Activate the checkbox *RADIUS Authentication Only* when the user should be allowed to authenticate using RADIUS (see Fig. 9.20).

The screenshot shows the 'Edit User user' dialog box. In the 'Authentication' section, the 'RADIUS Authentication Only' radio button is selected. Other options like 'Password: Use existing Password', 'New Password', and 'LDAP Authentication Only' are available but not selected. The 'Save' button at the bottom right is highlighted.

Fig. 9.20: Enabling authentication using RADIUS

CHAPTER 10

Scanning a System

Note: This chapter documents all possible menu options.

However, not all GSM models support all of these menu options. Check the tables in Chapter 3 (page 18) to see whether a specific feature is available for the used GSM model.

10.1 Using the Task Wizard for a First Scan

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

10.1.1 Using the Task Wizard

A new task with the task wizard can be configured as follows:

1. Select *Scans > Tasks* in the menu bar.
 2. Start the wizard by moving the mouse over  and clicking *Task Wizard*.
 3. Enter the IP address or host name of the target system in the input box (see Fig. 10.1).
 4. Click *Start Scan*.
-

Note: If using a DNS name however, the GSM has to be able to resolve the name.

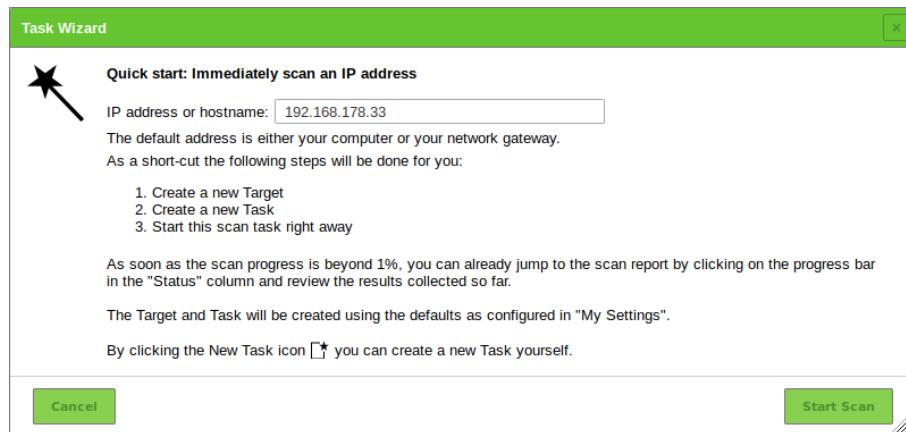


Fig. 10.1: Configuring the task wizard

→ The task wizard performs the following steps automatically:

1. Creating a new scan target on the GSM.
2. Creating a new scan task on the GSM.
3. Starting the scan task immediately.
4. Displaying the page *Tasks*.

After the task is started, the progress can be monitored (see Fig. 10.2).

Name	Status	Reports	Last Report	Severity	Trend	Actions
Immediate scan of IP 192.168.178.33	1%	1				<input type="checkbox"/> <input type="button" value="▶"/> <input type="button" value="✖"/> <input type="button" value="✎"/> <input type="button" value="↻"/>

(Applied filter: min_qod=70 apply_overrides=1 rows=10 first=1 sort=name) ◀◀ 1 - 1 of 1 ▶▶

Fig. 10.2: Page *Tasks* displaying the progress of the task

For the status of a task see Chapter 10.8 (page 288).

Tip: The report of a task can be displayed as soon as the task has been started by clicking the bar in the column *Status*. For reading, managing and downloading reports see Chapter 11 (page 315).

As soon as the status changes to *Done* the complete report is available. At any time the intermediate results can be reviewed (see Chapter 11.2.1 (page 320)).

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

10.1.2 Using the Advanced Task Wizard

Next to the simple wizard the GSM also provides an advanced wizard that allows for more configuration options.

A new task with the advanced task wizard can be configured as follows:

1. Select *Scans > Tasks* in the menu bar.
2. Start the wizard by moving the mouse over  and clicking *Advanced Task Wizard*.



3. Define the task (see Fig. 10.3).

Tip: For the information to enter in the input boxes see Chapters 10.2.1 (page 248) and 10.2.2 (page 251).

If an e-mail address is entered in the input box *Email report to* an alert is created sending an e-mail as soon as the task is completed (see Chapter 10.12 (page 305)).

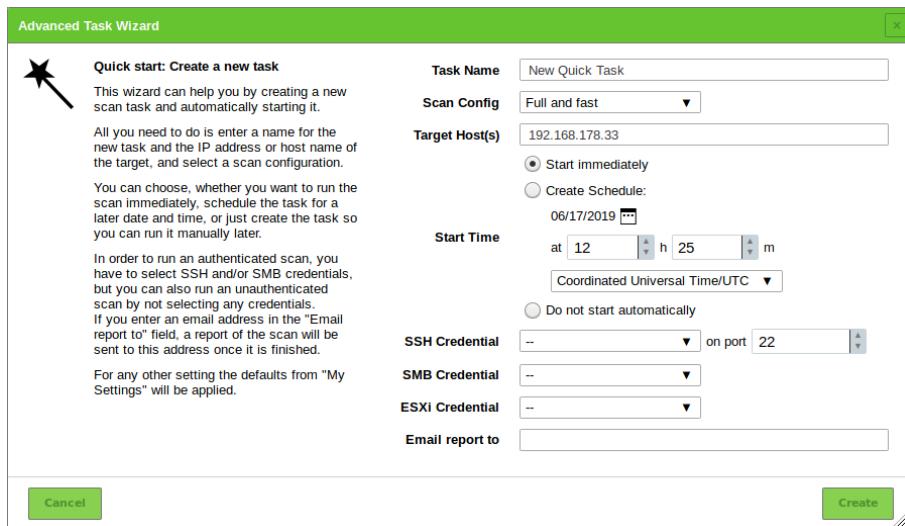


Fig. 10.3: Configuring the advanced task wizard

4. Click *Create*.

→ The advanced task wizard performs the following steps automatically:

1. Starting the scan task immediately.
2. Displaying the page *Tasks*.

For the status of a task see Chapter 10.8 (page 288).

Tip: The report of a task can be displayed as soon as the task has been started by clicking the bar in the column *Status*. For reading, managing and downloading reports see Chapter 11 (page 315).

As soon as the status changes to *Done* the complete report is available. At any time the intermediate results can be reviewed (see Chapter 11.2.1 (page 320)).

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

10.1.3 Using the Wizard to Modify a Task

An additional wizard can modify an existing task:

1. Select *Scans > Tasks* in the menu bar.
2. Start the wizard by moving the mouse over and clicking *Modify Task Wizard*.
3. Select the task which should be modified in the drop-down list *Task* (see Fig. 10.4).

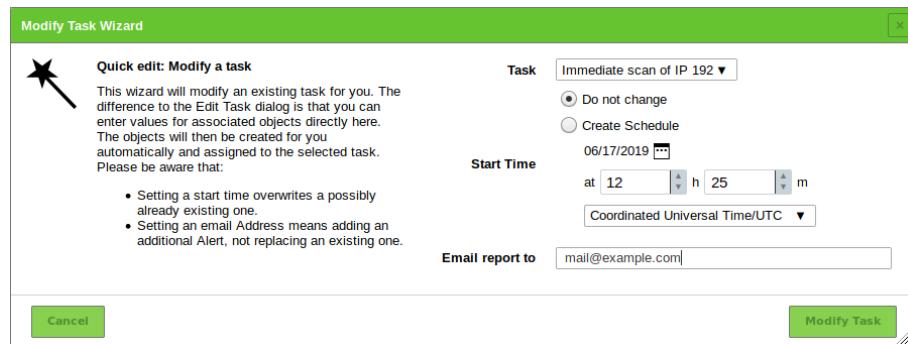


Fig. 10.4: Modifying a task using the wizard

4. Create a schedule for the task by selecting the radio button *Create Schedule* (see Chapter 10.10 (page 301)).
The date of the first scan can be selected by clicking and the time can be set using the input boxes.
5. Enter the e-mail address to which the report should be sent in the input box *Email report to*.
6. Click *Modify Task*.

10.2 Configuring a Simple Scan Manually

Generally speaking the GSM can use two different approaches to scan a target:

- Simple scan
- Authenticated scan using local security checks



The steps for configuring a simple scan manually which are described in the following chapters are briefly explained in a video based on GOS 5.0²⁰ (German only).

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

- Creating a target (see Chapter 10.2.1 (page 248))
- Creating a task (see Chapter 10.2.2 (page 251))
- Running the task (see Chapter 10.2.3 (page 253))

10.2.1 Creating a Target

The first step is to define a scan target as follows:

1. Select *Configuration > Targets* in the menu bar.
2. Create a new target by clicking .
3. Define the target (see Fig. 10.5).

²⁰ <https://youtu.be/fv3ypw5M5CY>



The screenshot shows the 'New Target' configuration dialog. Key settings include:

- Name:** Target1
- Hosts:** Manual entry of 192.168.15.5
- Exclude Hosts:** No entries
- Allow simultaneous scanning via multiple IPs:** Yes
- Port List:** All IANA assigned TCP 20
- Alive Test:** Scan Config Default
- Credentials for authenticated checks:** SSH on port 22

Fig. 10.5: Creating a new target

4. Click Save.

The following information can be entered:

Name The name can be chosen freely. A descriptive name should be chosen if possible. Possibilities are Mailserver, ClientNetwork, Webserverfarm, DMZ or describing the entered systems in more detail.

Comment The optional comment allows specifying background information. It simplifies understanding the configured targets later.

Hosts Manual entry of the hosts that should be scanned, separated by commas, or importing a list of hosts.

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

When entering manually the following options are available:

- Single IP address, e.g., 192.168.15.5
- Host name, e.g., mail.example.com
- IPv4 address range in long format, e.g., 192.168.15.5-192.168.15.27
- IPv4 address range in short format, e.g., 192.168.55.5-27
- IPv4 address range in CIDR notation, e.g., 192.168.15.0/24²³ (at most 4096 IP addresses)
- Single IPv6 address, e.g., fe80::222:64ff:fe76:4cea
- IPv6 address range in long format, e.g., ::12:fe5:fb50-::12:fe6:100
- IPv6 address range in short format, e.g., ::13:fe5:fb50-fb80
- IPv6 address range in CIDR notation, e.g., fe80::222:64ff:fe76:4cea/120 (at most 4096 IP addresses)

Multiple options can be mixed. If importing from a file, the same syntax can be used. Entries can be separated with commas or by line breaks. If many systems have to be scanned, using a file with the hosts is simpler than entering all hosts manually. The file should use UTF-8 text encoding.

²³ The maximum netmask is /20. This equals 4096 addresses.



Alternatively the systems can be imported from the host asset database.

Note: Importing a host from the asset database is only possible if a target is created from the page *Hosts* (see Chapter 13.1.3 (page 380)).

Exclude Hosts Manual entry of the hosts that should be excluded from the list mentioned above, separated by commas, or importing a list of hosts.

The same specifications as for *Hosts* apply.

Allow simultaneous scanning via multiple IPs Some services, especially IoT devices, may crash when scanned via multiple connections coming from the same host at the same time. This can happen, for example, if the device is connected via IPv4 and IPv6.

Selecting the radio button *No* will avoid scanning via several addresses at the same time.

Port list Port list used for the scan (see Chapter 10.7 (page 285)).

Note: A port list can be created on the fly by clicking next to the drop-down list.

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

- Scan Config Default (the alive test method *ICMP Ping* is used by default)
- ICMP Ping
- TCP-ACK Service Ping
- TCP-SYN Service Ping
- ICMP & TCP-ACK Service Ping
- ICMP & ARP Ping
- TCP-ACK Service & ARP Ping
- ICMP, TCP-ACK Service & ARP Ping
- Consider Alive

Sometimes there are problems with this test from time to time. In some environments routers and firewall systems respond to a TCP service ping with a TCP-RST even though the host is actually not alive (see Chapter 10.13 (page 313)).

Network components exist that support Proxy-ARP and respond to an ARP ping. Therefore this test often requires local customization to the environment.

SSH Credential Selection of a user that can log into the target system of a scan if it is a Linux or Unix system. This allows for an authenticated scan using local security checks (see Chapters 10.3.2 (page 255) and 10.3 (page 253)).

SMB Credential Selection of a user that can log into the target system of a scan if it is a Microsoft Windows system. This allows for an authenticated scan using local security checks (see Chapters 10.3.2 (page 255) and 10.3 (page 253)).

ESXi Credential Selection of a user that can log into the target system of a scan if it is a VMware ESXi system. This allows for an authenticated scan using local security checks (see Chapters 10.3.2 (page 255) and 10.3 (page 253)).

SNMP Credential Selection of a user that can log into the target system of a scan if it is an SNMP aware system. This allows for an authenticated scan using local security checks (see Chapters 10.3.2 (page 255) and 10.3 (page 253)).



Note: All credentials can be created on the fly by clicking next to the credential.

Reverse Lookup Only Only scan IP addresses that can be resolved into a DNS name.

Reverse Lookup Unify If multiple IP addresses resolve to the same DNS name the DNS name will only get scanned once.

Note: For reverse lookup unify, all target addresses are checked prior to the scan in order to reduce the number of actual scanned addresses. For large targets and for networks in which reverse lookup causes delays, this leads to a long phase where the task remains at 1 % progress.

This option is not recommended for large networks or networks in which reverse lookups cause delays.

10.2.2 Creating a Task

The second step is to create a task.

The GSM controls the execution of a scan using tasks. These tasks can be repeated regularly or run at specific times (see Chapter 10.10 (page 301)).

A task can be created as follows:

1. Select *Scans > Tasks* in the menu bar.
2. Create a new task by moving the mouse over and clicking *New Task*.
3. Define the task (see Fig. 10.6).

The screenshot shows the 'New Task' dialog box. The 'Name' field is set to 'DMZ Mail Scan'. The 'Scan Targets' dropdown is set to 'Target1'. The 'Schedule' dropdown shows 'Once' with a checkbox. Under 'Add results to Assets' and 'Apply Overrides', both 'Yes' radio buttons are selected. The 'Min QoD' slider is set to 70%. The 'Alterable Task' and 'Auto Delete Reports' sections both have 'No' selected. The 'Scanner' dropdown is set to 'OpenVAS Default' and the 'Scan Config' dropdown is set to 'Full and fast'. At the bottom are 'Cancel' and 'Save' buttons.

Fig. 10.6: Creating a new task

4. Click *Save*.

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

The following information can be entered:

Name The name can be chosen freely. A descriptive name should be chosen if possible. Possibilities are Mailserver, ClientNetwork, Webserverfarm, DMZ or describing the entered systems in more detail.



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

Scan Targets Select a previously configured target from the drop-down list (see Chapter 10.2.1 (page 248)).

Alternatively, the target can be created on the fly by clicking next to the drop-down list.

Alerts Select a previously configured alert from the drop-down list (see Chapter 10.12 (page 305)). Status changes of a task can be communicated via e-mail, Syslog, HTTP or a connector.

Alternatively, an alert can be created on the fly by clicking next to drop-down list.

Schedule Select a previously configured schedule from the drop-down list (see Chapter 10.10 (page 301)). The task can be run once or repeatedly at a predetermined time, e.g., every Monday morning at 6:00 a.m.

Alternatively, a schedule can be created on the fly by clicking next to the drop-down list.

Add results to Asset Management Selecting this option will make the systems available to the asset management of the GSM automatically (see Chapter 13 (page 378)). This selection can be changed at a later point as well.

Apply Overrides Overrides can be directly applied when adding the results to the asset database (see Chapter 11.8 (page 338)).

Min QoD Here the minimum quality of detection can be specified for the addition of the results to the asset database.

Alterable Task Allow for modification of the task even though reports were already created. The consistency between reports can no longer be guaranteed if tasks are altered.

Auto Delete Reports This option may automatically delete old reports. The maximum number of reports to store can be configured. If the maximum is exceeded, the oldest report is automatically deleted. The factory setting is *Do not automatically delete reports*.

Scanner By default, only the built-in OpenVAS and CVE scanners are supported (see Chapter 10.11 (page 303)). Sensors can be used as additional scanning engines but need to be configured first (see Chapter 16 (page 409)).

Note: The following options are only relevant for the OpenVAS scanner. The CVE scanner does not support any options.

Scan Config The GSM comes with seven pre-configured scan configurations for the OpenVAS scanner (see Chapter 10.9 (page 291)).

Network Source Interface Here a source interface name can be entered to tag the scan with the interface. Only users who are allowed to access this interface are able to use and run the scan.

Note: The entered interface must be a configured interface on the GSM, or the task will fail.

This setting has no impact on the actual routing of the scan. The routing can only be influenced by configuring the network settings (see Chapter 7.2.2 (page 132)).

Order for target hosts Select in which order the specified target hosts are processed during vulnerability tests. Available options are:

- Sequential
- Random
- Reverse



In order to improve the scan progress estimation, the setting *Random* is recommended (see Chapter 17.2.3 (page 421)).

This setting does not affect the alive test during which active hosts in a target network are identified. The alive test is always random.

Maximum concurrently executed NVTs per host/Maximum concurrently scanned hosts Select the speed of the scan on one host. The default values are chosen sensibly. If more VTs run simultaneously on a system or more systems are scanned at the same time, the scan may have a negative impact on either the performance of the scanned systems, the network or the GSM appliance itself. These values “maxhosts” and “maxchecks” may be tweaked.

Tag Select a previously configured tag from the drop-down list (see Chapter 8.5 (page 214)) to link it to the task.

10.2.3 Starting the Task

In the row of the newly created task click ▶.

Note: For scheduled tasks ⏱ is displayed. The task is starting at the time that was defined in the schedule (see Chapter 10.10 (page 301)).

→ The scan is running. For the status of a task see Chapter 10.8 (page 288).

Note: Scans are only started if there are enough system resources available. The most important resource is random-access memory (RAM). If too many scans are started and running at the same time and not enough RAM is available, scans are added to a waiting queue when clicking ▶.

When the required RAM is available again, scans from the waiting queue are started, following the principle “first in, first out”.

For more information see Chapter 17.3 (page 422).

The report of a task can be displayed as soon as the task has been started by clicking the bar in the column *Status*. For reading, managing and downloading reports see Chapter 11 (page 315).

As soon as the status changes to *Done* the complete report is available. At any time the intermediate results can be reviewed (see Chapter 11.2.1 (page 320)).

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

10.3 Configuring an Authenticated Scan Using Local Security Checks

An authenticated scan can provide more vulnerability details on the scanned system. During an authenticated scan the target is both scanned from the outside using the network and from the inside using a valid user login.

During an authenticated scan the GSM 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 GSM was able to log into the target system. The local security check VTs in the resulting scan are minimally invasive.



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

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

- **SMB** On Microsoft Windows systems the GSM can check the patch level and locally installed software such as Adobe Acrobat Reader or the Java suite.
- **SSH** This access is used to check the patch level on Unix and Linux systems.
- **ESXi** This access is used for testing of VMware ESXi servers locally.
- **SNMP** Network components like routers and switches can be tested via SNMP.

10.3.1 Advantages and Disadvantages of Authenticated Scans

The extent and success of the testing routines for authenticated scans depend heavily on the permissions of the used account.

On Linux systems an unprivileged user is sufficient and can access most interesting information while especially on Microsoft Windows systems unprivileged users are very restricted and administrative users provide more results. An unprivileged user does not have access to the Microsoft Windows registry and the Microsoft Windows system folder \windows which contains the information on updates and patch levels.

Local security checks are the most gentle method to scan for vulnerability details. While remote security checks try to be least invasive as well, they may have some impact.

Simply stated an authenticated scan is similar to a Whitebox approach. The GSM 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 GSM 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 GSM itself. During the test the GSM may provoke malfunctions to extract any available information on the used software, e.g., the scanner may send a malformed request to a service to trigger a response containing further information on the deployed product.

During a remote scan using the scan configuration *Full and fast* all remote checks are safe. The used VTs may have some invasive components but none of the used VTs try to trigger a defect or malfunction in the target (see example below). This is ensured by the scan preference `safe_checks=yes` in the scan configuration (see Chapter 10.9.4 (page 295)). All VTs with very invasive components or which may trigger a denial of service (DoS) are automatically excluded from the test.

Example for an Invasive VT

An example for an invasive but safe VT is the Heartbleed VT. It is executed even with `safe_checks` enabled because the VT does not have any negative impact on the target.

The VT is still invasive because it tests the memory leakage of the target. If the target is vulnerable, actual memory of the target is leaked. The GSM does not evaluate the leaked information. The information is immediately discarded.



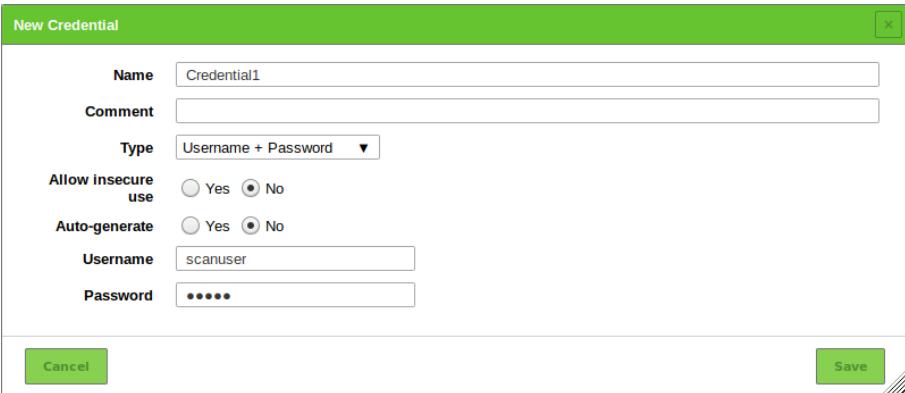
10.3.2 Using Credentials

Credentials for local security checks are required to allow VTs to log into target systems, e.g., for the purpose of locally checking the presence of all vendor security patches.

10.3.2.1 Creating a Credential

A new credential can be created as follows:

1. Select *Configuration > Credentials* in the menu bar.
2. Create a new credential by clicking .
3. Define the credential (see Fig. 10.7).



The screenshot shows the 'New Credential' dialog box. It has a green header bar with the title 'New Credential'. Below it is a form with the following fields:

- Name:** Credential1
- Comment:** (empty)
- Type:** Username + Password
- Allow insecure use:** No (radio button selected)
- Auto-generate:** No (radio button selected)
- Username:** scanneruser
- Password:** *****

At the bottom are two buttons: 'Cancel' on the left and 'Save' on the right.

Fig. 10.7: Creating a new credential

4. Click Save.

The following details of the credential can be defined:

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

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

- All English alphanumeric characters
- - (dash)
- _ (underscore)
- \ (backslash)
- . (full stop)
- @ (at sign)

This also excludes the German umlauts, which must be replaced as follows:

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

Comment An optional comment can contain additional information.



Type Definition of the credential type. The following types are possible:

- Username + Password
- Username + SSH Key
- Client Certificate
- SNMP
- S/MIME Certificate
- PGP Encryption Key
- Password only

Allow insecure use Select whether the GSM can use the credential for unencrypted or otherwise insecure authentication methods.

Depending on the selected type further options are shown:

Username + Password

- **Auto-generate** Select whether the GSM creates a random password.

Note: If the radio button Yes is selected, it is not possible to define a password in the input box *Password*.

- **Username** Definition of the login name used by the GSM to authenticate on the scanned target system.
- **Password** Definition of the password used by the GSM to authenticate on the scanned target system.

Username + SSH Key

- **Auto-generate** Select whether the GSM creates a random password.

Note: If the radio button Yes is selected, it is not possible to define a password in the input box *Password*.

- **Username** Definition of the login name used by the GSM 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.

Client Certificate

- **Passphrase** Definition of the passphrase of the private SSH key.
- **Certificate** Upload of the certificate file.
- **Private Key** Upload of the corresponding private key.



SNMP SNMPv3 requires a user name, an authentication password, and a privacy password, while all older SNMP versions (SNMPv1 and SNMPv2) only require an SNMP community.

Note: Due to the singular nature of the SNMP credential, it is currently not possible to configure either SNMPv1/v2 or SNMPv3 mode.

This means that the GSM will always try to log in with all SNMP protocol versions. It is possible to see both the result *SNMP Login Successful For Authenticated Checks* and the result *SNMP Login Failed For Authenticated Checks* for a scan, e.g., if the SNMPv3 login information in the credential is correct, but the SNMPv1/2 information is incorrect.

- **SNMP Community** Definition of the community for SNMPv1 or SNMPv2c.
- **Username** Definition of the user name for SNMPv3.
- **Password** Definition of the password for SNMPv3.
- **Privacy Password** Definition of the password for the encryption for SNMPv3.
- **Auth Algorithm** Selection of the authentication algorithm (MD5 or SHA1).
- **Privacy Algorithm** Selection of the encryption algorithm (AES, DES or none).

S/MIME Certificate

- **S/MIME Certificate** Upload of the certificate file.

PGP Encryption Key

- **PGP Public Key** Upload of the key file.

Password only

- **Password** Definition of the password used by the GSM to authenticate on the scanned target system.

Note: The credential has to be linked to at least one target. This allows the scan engine to apply the credential.

10.3.2.2 Managing Credentials

List Page

All existing credentials can be displayed by selecting *Configuration > Credentials* in the menu bar.

For all credentials the following information is displayed:

Name Name of the credential.

Type Chosen credential type.

Allow insecure use Indication whether the GSM can use the credential for unencrypted or otherwise insecure authentication methods.

Login User name for the credential if a credential type that requires a user name is chosen.

For all credentials the following actions are available:

- Move the credential to the trashcan. Only credentials which are currently not used can be moved to the trashcan.
- Edit the credential.
- Clone the credential.



- Export the credential as an XML file.

Depending on the chosen credential type (see Chapter 10.3.2.1 (page 255)) more actions may be available:

- Download an EXE package for Microsoft Windows. This action is available if *Username + Password* was chosen.
- Download an RPM package for Red Hat Enterprise Linux and its derivates. This action is available if *Username + SSH Key* was chosen.
- Download a Debian package for Debian GNU/Linux and its derivates. This action is available if *Username + SSH Key* was chosen.
- Download a public key. This action is available if *Username + SSH Key* or *Client Certificate* was chosen.

These installation packages simplify the installation and creation of accounts for authenticated scans. They create the user and the most important permissions for the authenticated scan and reset them during uninstalling.

Note: If the auto-generation of passwords is enabled (see Chapter 10.3.2.1 (page 255)), the packages have to be used, otherwise the usage is optional.

Note: By clicking or below the list of credentials more than one credential can be moved to the trashcan or exported at a time. The drop-down list is used to select which credentials are moved to the trashcan or exported.

Details Page

Click on the name of a credential to display the details of the credential. Click to open the details page of the credential.

The following registers are available:

Information General information about the credential.

User Tags Assigned tags (see Chapter 8.5 (page 214)).

Permissions Assigned permissions (see Chapter 9.4 (page 231)).

The following actions are available in the upper left corner:

- Open the corresponding chapter of the user manual.
- Show the list page of all credentials.
- Create a new credential (see Chapter 10.3.2.1 (page 255)).
- Clone the credential.
- Edit the credential.
- Move the credential to the trashcan. Only credentials which are currently not used can be moved to the trashcan.
- Export the credential as an XML file.

Depending on the chosen credential type (see Chapter 10.3.2.1 (page 255)) more actions may be available:

- Download an EXE package for Microsoft Windows. This action is available if *Username + Password* was chosen.



- Download an RPM package for Red Hat Enterprise Linux and its derivates. This action is available if *Username + SSH Key* was chosen.
- Download a Debian package for Debian GNU/Linux and its derivates. This action is available if *Username + SSH Key* was chosen.
- Download a public key. This action is available if *Username + SSH Key* or *Client Certificate* was chosen.

10.3.3 Requirements on Target Systems with Microsoft Windows

10.3.3.1 General Notes on the Configuration

- The remote registry service must be started in order to access the registry.

This is achieved by configuring the service to automatically start up. If an automatic start is not preferred, a manual startup can be configured. In that case the service is started while the system is scanned by the GSM and afterwards it is disabled again. To ensure this behaviour the following information about LocalAccountTokenFilterPolicy must be considered.

- It is necessary that for all scanned systems the file and printer sharing is activated. If using Microsoft Windows XP, take care to disable the setting *Use Simple File Sharing*.
- For individual systems not attached to a domain the following registry key must be set:

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\  
DWORD: LocalAccountTokenFilterPolicy = 1
```

- On systems with domain controller the user account in use must be a member of the group *Domain Administrators* to achieve the best possible results. Due to the permission concept it is not possible to discover all vulnerabilities using the *Local Administrator* or the administrators assigned by the domain. Alternatively follow the instructions in Chapter 10.3.3.2 (page 260).

→ 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 GSM 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 GSM. If the entry is confirmed, the firewall rule is configured. The service *File and Printer Sharing* will be enabled in the firewall rules.
- Powershell execution privileges on a target system may be required for the account utilized in an authenticated scan. Policy and vulnerability tests may occasionally execute Powershell commands to increase the accuracy of results, requiring privileges for the duration of a scan.
- For compliance audits targeting Windows operating systems, it is recommended to set the *Maximum concurrently executed NVTs per host/Maximum concurrently scanned hosts* to 1 in order to maximize the accuracy of the results (see Chapter 12.2.1.1 (page 352)).
- For a fully working Windows Management Instrumentation (WMI) access which is used for, e.g., file search or policy scans, the following settings are required:



- Allow WMI access in the Windows Firewall settings²¹ or a possible third-party firewall solution.
- Verify that the user or the group of the scan user is allowed to access WMI remotely.

10.3.3.2 Configuring a Domain Account for Authenticated Scans

For authenticated scans of Microsoft Windows target systems, it is highly recommended to use a domain account with a domain policy that grants local administrator privileges. This has several advantages:

- A domain policy only needs to be created once and can then be applied or revoked for different user accounts.
- Editing the Microsoft Windows registry locally is no longer required. User administration is thus centralized, which saves time in the long term and reduces possible configuration errors.
- From a vulnerability assessment perspective, only a domain account allows for the detection of domain-related scan results. These results will be missing if using a local user account.
- There are also several security advantages to using a domain account with the domain policy recommended by Greenbone Networks: the corresponding user may not log in locally or via the remote desktop protocol (RDP), limiting possible attack vectors. Additionally, the user credentials are secured via Kerberos, while the password of a local user account is at much greater risk of being exposed through exploits.

In order to use a domain account for host based remote audits on a Microsoft Windows target, the following configuration must be made under Windows XP Professional, Windows Vista, Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows 7, Windows 8, Windows 8.1 or Windows 10. The system must also be part of the domain.

Creating a Security Group

1. Log into a domain controller and open *Active Directory Users and Computers*.
2. Select *Action > New > Group* in the menu bar.
3. Enter `Greenbone Local Scan` in the input box *Name*.
4. Select *Global* for *Group Scope* and *Security* for *Group Type*.
5. Add the account used for the local authenticated scans by the GSM under Microsoft Windows to the group.
6. Click *OK*.

Creating a Group Policy Object (GPO)

1. In the left panel open the console *Group Policy Management*.
2. Right click *Group Policy Objects* and select *New*.
3. Enter `Greenbone Local SecRights` in the input box *Name* (see Fig. 10.8).
4. Click *OK*.

²¹ <https://docs.microsoft.com/en-us/windows/win32/wmisdk/connecting-to-wmi-remotely-starting-with-vista#windows-firewall-settings>

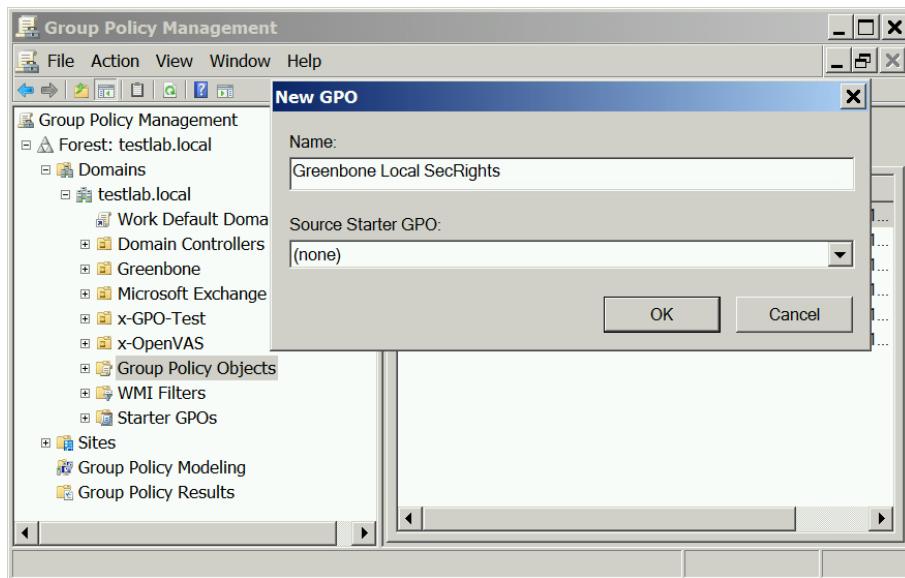


Fig. 10.8: Creating a new Microsoft Windows group policy object for Greenbone Networks scans

Configuring the Policy

1. Click the policy *Greenbone Local SecRights* and select *Edit*.
2. Select *Computer Configuration > Policies > Windows Settings > Security Settings* in the left panel.
3. Click *Restricted Groups* and select *Add Group*.
4. Click *Browse...* and enter *Greenbone Local Scan* in the input box (see Fig. 10.9).

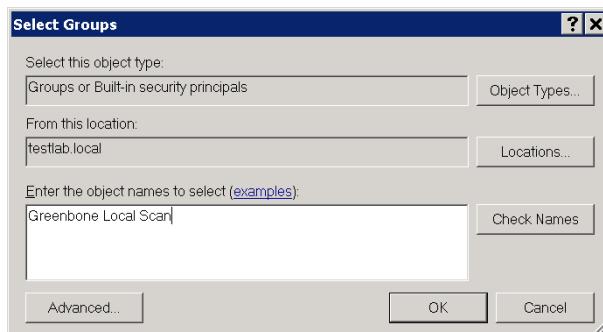


Fig. 10.9: Checking Microsoft Windows group names

5. Click *Check Names*.
6. Click *OK* twice to close the open windows.
7. At *This group is member of* click *Add*.
8. Enter *Administrators* in the input box *Group* (see Fig. 10.10) and click *OK* twice to close the open windows.

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

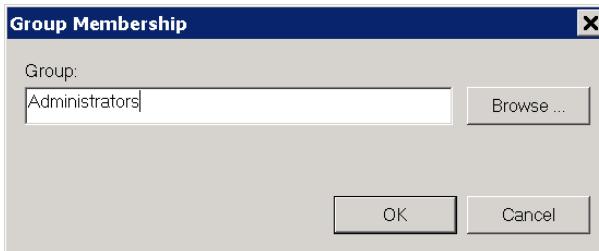


Fig. 10.10: Adding a group membership

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

1. Click the policy *Greenbone Local SecRights* and select *Edit*.
2. Select *Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment* in the left panel.
3. In the right panel double click *Deny log on locally*.
4. Activate the checkbox *Define these policy settings* and click *Add User or Group*.
5. Click *Browse...* and enter *Greenbone Local Scan* in the input box (see Fig. 10.11).
6. Click *Check Names*.

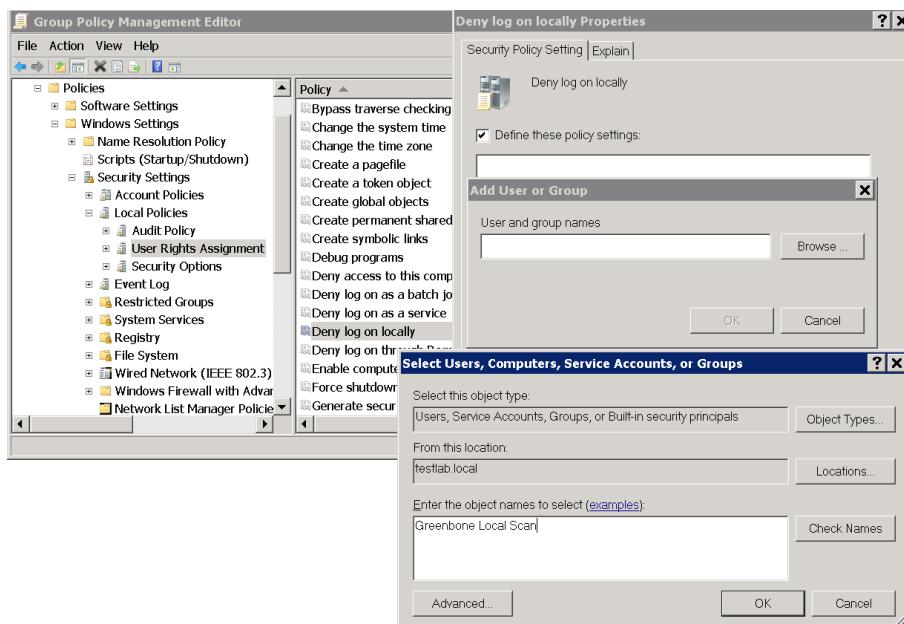


Fig. 10.11: Editing the policy

7. Click *OK* three times to close the open windows.

Configuring the Policy to Deny the Group Greenbone Local Scan Logging into the System 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 Remote Desktop Services*.
4. Activate the checkbox *Define these policy settings* and click *Add User or Group*.



5. Click *Browse...* and enter **Greenbone Local Scan** in the input box (see Fig. 10.12).
6. Click *Check Names*.

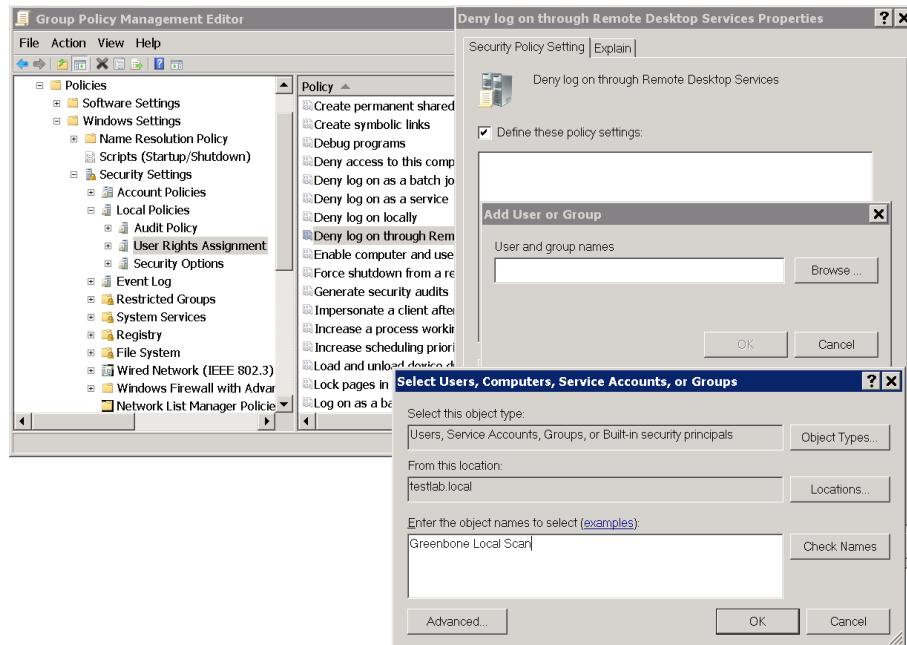


Fig. 10.12: Editing the policy

7. Click *OK* three times to close the open windows.

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

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

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

Research whether the settings are compatible with the environment.

Note: The following steps are optional.

1. In the left panel right click *Registry* and select *Add Key*.
2. Select *USERS* and click *OK* (see Fig. 10.13).
3. Click *Advanced* and *Add*.
4. Enter **Greenbone Local Scan** in the input box and click *OK* (see Fig. 10.14).
5. Select *This object and child objects* in the drop-down list *Apply to*.
6. Deactivate all checkboxes for *Allow* and activate the checkboxes *Set Value*, *Create Subkey*, *Create Link*, *Delete*, *Change Permissions* and *Take Ownership* for *Deny* (see Fig. 10.15).
7. Click *OK* twice and confirm the warning message by clicking *Yes*.
8. Click *OK*.
9. Select the radio buttons *Configure this key then* and *Propagate inheritable permissions to all subkeys* and click *OK* (see Fig. 10.16).

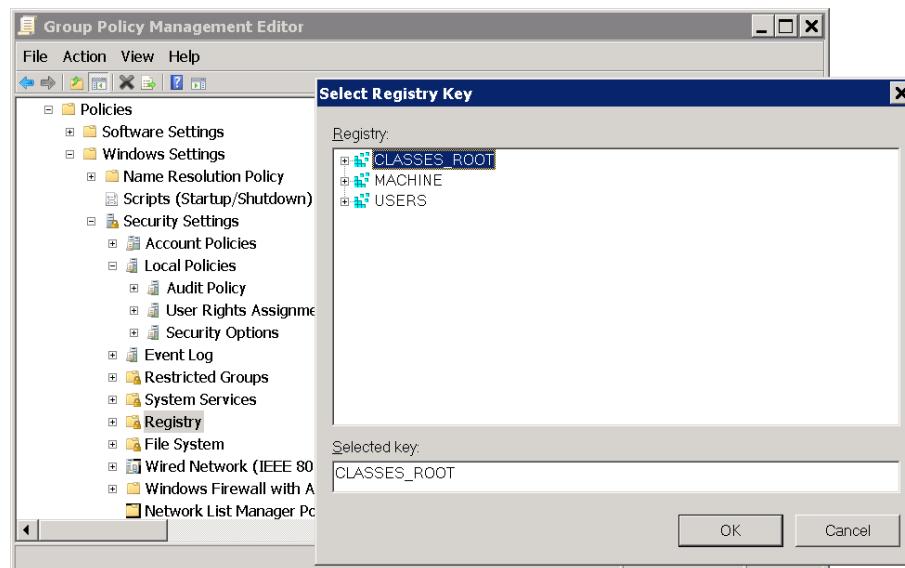
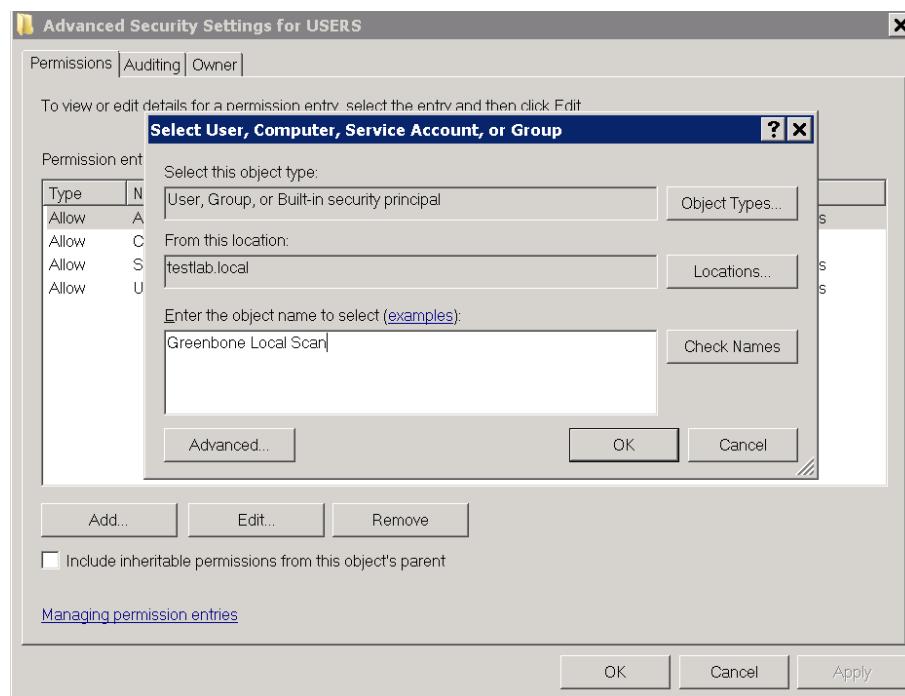


Fig. 10.13: Selecting the registry key

Fig. 10.14: Selecting the group *Greenbone Local Scan*

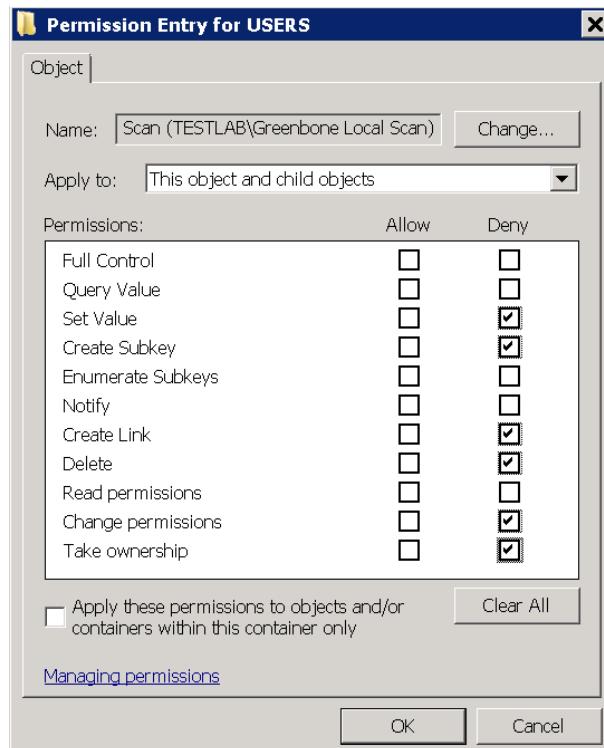


Fig. 10.15: Disallowing edition of the registry



Fig. 10.16: Making the permissions recursive



10. Repeat the steps 2 to 9 for *MACHINE* and *CLASSES_ROOT*.

Linking the Group Policy Object

1. In the right panel right click the domain and select *Link an Existing GPO...*
2. Select *Greenbone Local SecRights* in the section *Group Policy objects* and click *OK* (see Fig. 10.17).

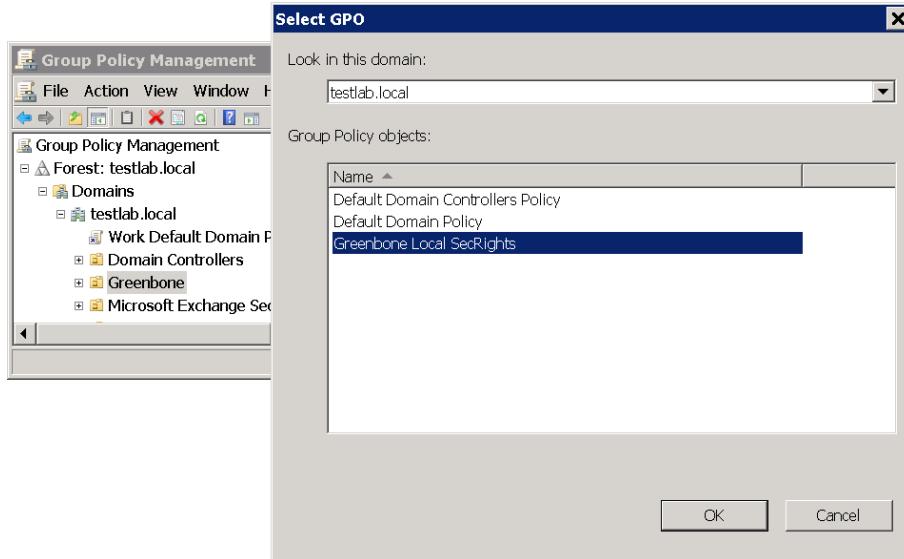


Fig. 10.17: Linking the policy

10.3.3.3 Restrictions

Based on the fact that write permissions to the registry and system drive have been removed, the following two tests will no longer work:

- **Leave information on scanned Windows hosts OID 1.3.6.1.4.1.25623.1.0.96171** This test, if desired, creates information about the start and end of a scan under HKLM\Software\VulScanInfo. Due to denying write access to HKLM this is no longer possible. If the test should be possible, the GPO must be adjusted respectively.
- **Windows file Checksums OID 1.3.6.1.4.1.25623.1.0.96180** This test, if desired, saves the tool Re-Hash under C:\Windows\system32 (for 32-bit systems) or C:\Windows\SysWOW64 (for 64-bit systems). Due to denying write access this is no longer possible. If the test should be possible, the tool must be saved separately or the GPO must be adjusted respectively.

More information can be found in Chapter 12.4.3 (page 363).

10.3.3.4 Scanning Without Domain Administrator and Local Administrator Permissions

It is possible to build a GPO in which the user also does not have any local administrator permissions. But the effort to add respective read permissions to each registry branch and folder is huge. Unfortunately, inheriting of permissions is deactivated for many folders and branches. Additionally, these changes can be set by GPO but cannot be removed again (tattooing GPO). Specific permissions could be overwritten so that additional problems could occur as well.

Building a GPO in which the user does not have any local administrator permissions does not make sense from a technical and administrative point of view.



10.3.4 Requirements on Target Systems with ESXi

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. This can be set up as follows:

1. Start the vSphere client.
2. Select *Administration > Roles* in the menu bar (see Fig. 10.18).

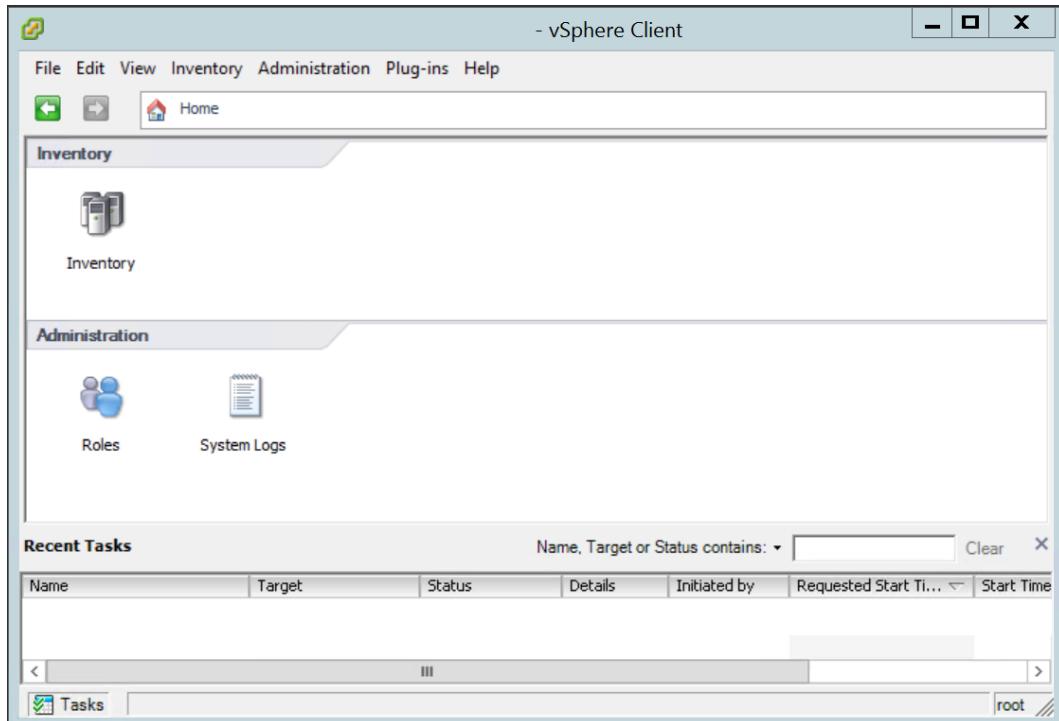


Fig. 10.18: vSphere client offering access to the roles

- The roles are displayed.
3. Right click *ReadOnly* and select *Clone* (see Fig. 10.19).
 - The cloned role is displayed as well.
 4. Right click the cloned role and select *Rename*.
 5. Enter the new name of the cloned role in the input box and click *OK*.
 6. Right click the cloned role and select *Edit Role...*
 7. Unfold *Global* and activate the checkbox *Settings* (see Fig. 10.20).
 8. Click *OK*.
 9. Select *Inventory > Inventory* in the menu bar.
 10. Open the tab *Permissions*.

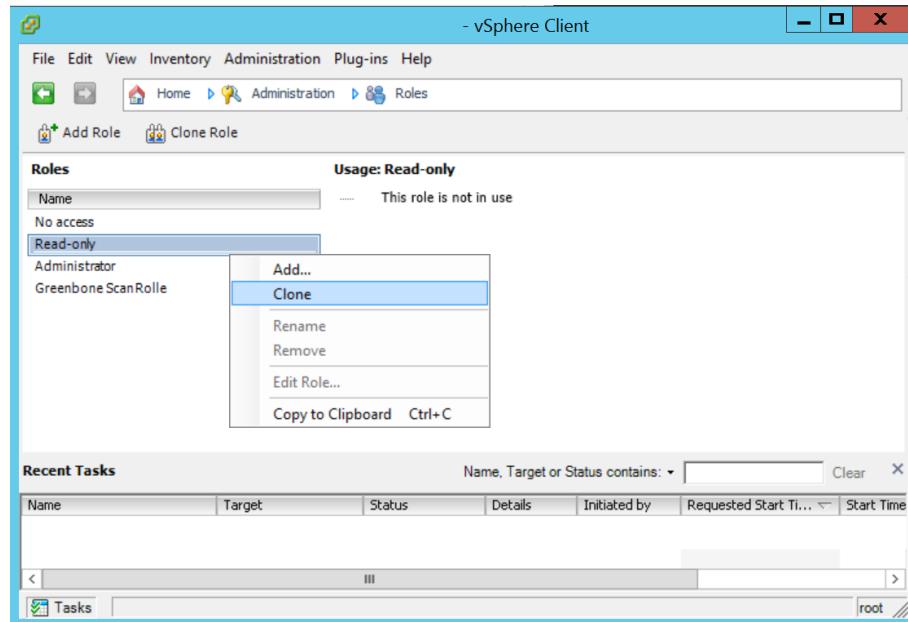


Fig. 10.19: Displaying the roles

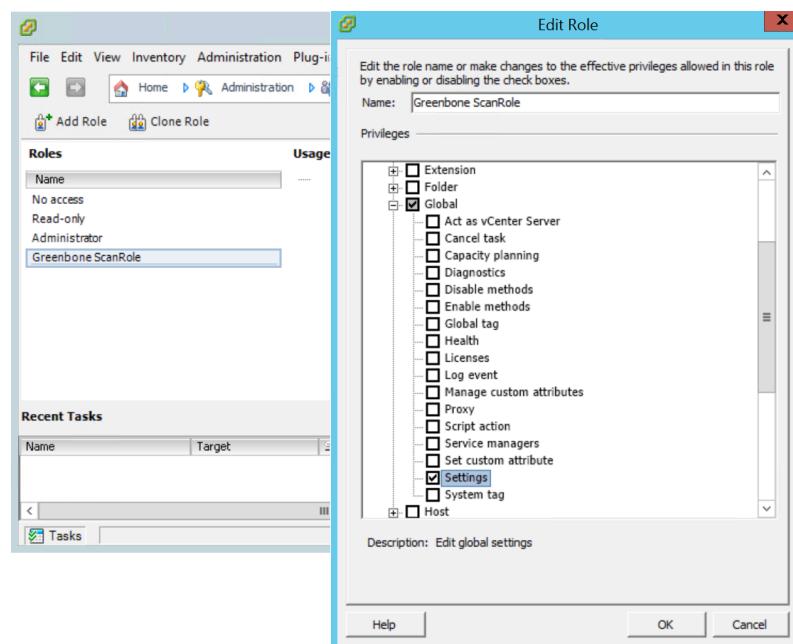


Fig. 10.20: Editing the role



11. Right click in the empty space and select *Add Permission...* (see Fig. 10.21).

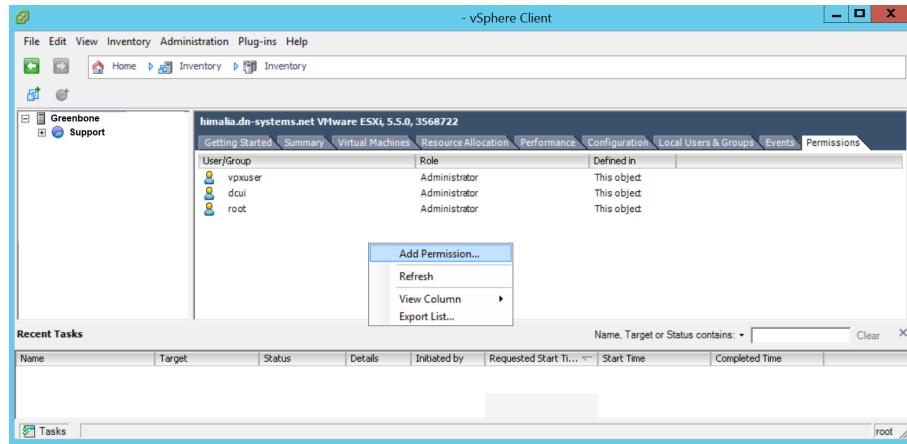


Fig. 10.21: Adding a permission to the scan user

12. Select the scan user account used by the GSM in the left section (see Fig. 10.22).
13. Select the created role in the drop-down list in the right section (see Fig. 10.22).
14. Click *OK*.

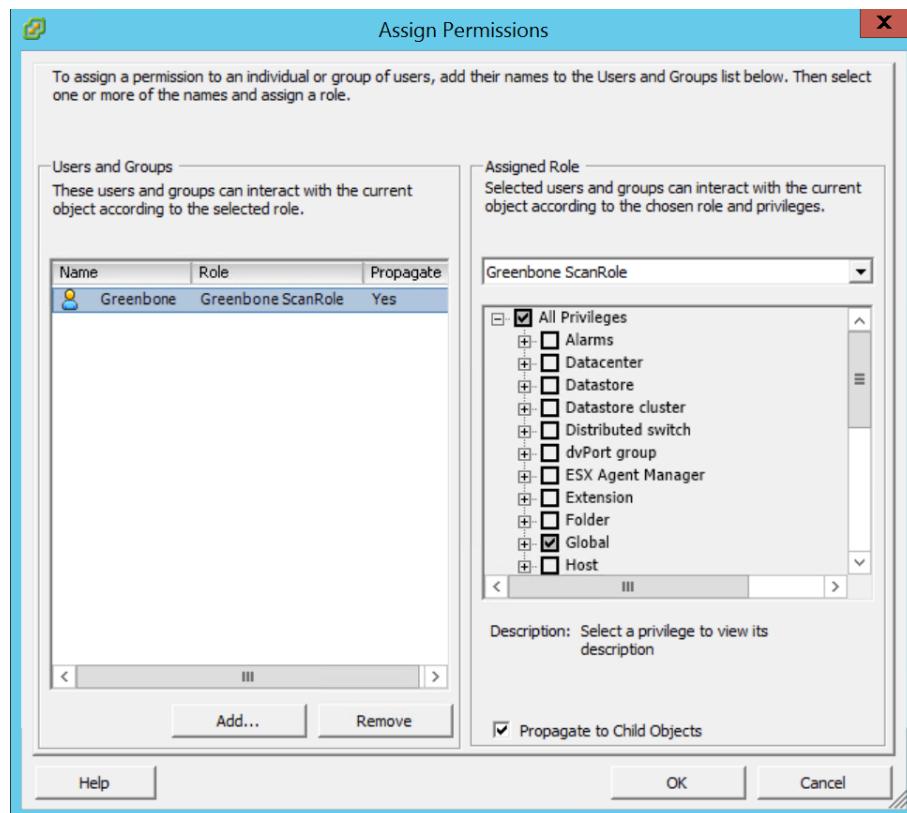


Fig. 10.22: Assigning the role to the scan user

10.3.5 Requirements on Target Systems with Linux/Unix

- For authenticated scans on Linux or Unix systems regular user access is usually enough. The login is performed via SSH. The authentication is done either with passwords or a private SSH key stored on the GSM.
- Generated installation package for credentials: the install package for Linux distributions based on Debian is a DEB file, the install package for Linux distributions based on Red Hat is an RPM file. Both install packages create a new user without any specific permissions. A public SSH key that is created on the GSM is stored in the user's home folder. For users of other Linux distributions or Unix derivatives the public key is offered for download. Creating a user and saving the public key with the proper file permissions is the responsibility of the user.
- In both cases it needs to be made sure that public key authentication is not prohibited by the SSH daemon. The line `PubkeyAuthentication no` must not be present.
- Existing SSH key pairs may also be used. SSH key pairs can be generated using the command `ssh-keygen` on Linux or `puttygen.exe` if using PuTTY on Microsoft Windows. To use an existing SSH key pair for authentication, the private key must be supplied when the credential is created. The private SSH key must be either in PEM or OpenSSH format. The key types Ed25519, ECDSA, RSA and DSA are supported.
- For scans that include policy testing, root permission or the membership in specific groups (often `wheel`) may be necessary. For security reasons many configuration files are only readable by super users or members of specific groups.
- The more permissions a user has, the more results and settings can be detected on a system. In some cases root user access may be required.
- The following commands are executed with root user access during an authenticated scan.

**Important:**

- This list is not static. New or changed VTs may add new commands at any time.
 - Depending on the found software, additional commands may be executed.
 - The executed commands depend on the Linux distribution and the selected scan configuration.
-

- bash
- cat
- date
- dpkg
- egrep
- find
- grep
- host
- id
- ifconfig
- lastlog
- locate
- ls
- md5sum
- mlocate
- netstat
- perl
- ps
- rpm
- sh
- sha1sum
- slocate
- uname
- uptime
- whereis
- which

- The installation of the package `locate` (alternatively `mlocate`) to provide the command `locate/mlocate` on the target system is recommended. The use of this command reduces calls to the command `find` used to search for files and thus, improves the search performance and lowers the resource usage on the target system.

For the commands to work, the corresponding database permissions and regular database updates, e.g., via a cron job, may need to be configured.



10.3.6 Requirements on Target Systems with Cisco OS

The GSM 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 GSM can use either SNMP or SSH.

10.3.6.1 SNMP

The GSM can use the SNMP protocol to access the Cisco network component. The GSM supports SNMPv1, v2c and v3. SNMP uses the port 161/udp. The default port list does not include any UDP port. Therefore, this port is ignored during the vulnerability test using *Full and fast* and no SNMP check is enabled. To scan network components the port list should be modified to include at least the following ports:

- 22/tcp SSH
- 80/tcp 8080/tcp HTTP
- 443/tcp 8443/tcp HTTPS
- 2000/tcp SCCP
- 2443/tcp SCCPS
- 5060/tcp 5060/udp SIP
- 5061/tcp 5061/udp SIPS
- 67/udp DHCP Server
- 69/udp TFTP
- 123/udp NTP
- 161/udp SNMP
- 162/udp SNMP Traps
- 500/udp IKE
- 514/udp Syslog
- 546/udp DHCPv6
- 6161/udp 6162/udp Unified CM

The administrator can set up special port lists used only for such network components.

The GSM needs to access only very few objects from the SNMP tree. For a less privileged access an SNMP view should be used to constrain the visibility of the SNMP tree for the GSM. The following two examples explain how to set up the view using either a community string or an SNMPv3 user.

To use an SNMP community string the following commands are required on the target:

```
# configure terminal
```

Using an access list the usage of the community can be restricted. The IP address of the GSM is 192.168.222.74 in this example:

```
(config) # access-list 99 permit 192.168.222.74
```

The view `gsm` should only allow accessing the system description:

```
(config) # snmp-server view gsm system included
(config) # snmp-server view gsm system.9 excluded
```



The last command links the community `gsm-community` with the view `gsm` and the access list 99:

```
(config) # snmp-server community gsm-community view gsm RO 99
```

If using an SNMPv3 user including encryption the following configuration lines are required on the target:

```
# configure terminal  
(config) # access-list 99 permit 192.168.222.74  
(config) # snmp-server view gsm system included  
(config) # snmp-server view gsm system.9 excluded
```

SNMPv3 requires the setup of a group first. Here the group `gsmgroup` is linked to the view `gsm` and the access list 99:

```
(config) # snmp-server group gsmgroup v3 priv read gsm access 99
```

Now the user can be created supplying the password `gsm-password` and the encryption key `gsm-encrypt`. The authentication is done using MD5 while the encryption is handled by AES128:

```
(config) # snmp-server user gsm-user gsm-group v3 auth md5 gsm-password priv  
aes 128 gsm-encrypt
```

To configure either the community or the SNMPv3 user in the GSM the administrator selects *Configuration > Credentials* in the menu bar (see Chapter 10.3.2 (page 255)).

10.3.6.2 SSH

The authenticated scan can be performed via SSH as well. If using SSH, the usage of a special unprivileged user is recommended. The GSM currently requires only the command `show version` to retrieve the current version of the firmware of the device.

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

Note: Before using the following example, make sure all side effects of the configuration are understood. If used without verification, the system may restrict further logins via SSH or console.

To use role-based access control AAA and views have to be enabled:

```
> enable  
# configure terminal  
(config) # aaa new-model  
(config) # exit  
> enable view  
# configure terminal
```

The following commands create a restricted view including just the command `show version`. The supplied password `view-pw` is not critical:

```
(config) # parser view gsm-view  
(config-view) # secret 0 view-pw  
(config-view) # commands exec include show version  
(config-view) # exit
```



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

```
(config) # username gsm-user view gsm-view password 0 gsm-pw  
(config) # aaa authorization console  
(config) # aaa authorization exec default local
```

If SSH is not enabled yet the following commands take care of that. Use the appropriate host name and domain:

```
(config) # hostname switch  
(config) # ip domain-name greenbone.net  
(config) # crypto key generate rsa general-keys modulus 2048
```

Finally, enable SSH logins using the following commands:

```
(config) # line vty 0 4  
(config-line) # transport input ssh  
(config-line) # Crt1-Z
```

The credentials of the user need to be entered on the GSM. Select *Configuration > Credentials* in the menu bar and create the appropriate user (see Chapter 10.3.2 (page 255)).

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

10.3.7 Requirements on Target Systems with Huawei VRP

The GSM 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 GSM can use either SNMP or SSH.

Note: The commands in this chapter serve as an example and should work on most Huawei routers.

Depending on the software version or hardware, some commands may differ (e.g., the order of the parameters or values), may not be necessary, or may not be available.

More information can be found in the related documentation for the respective device and software version.

10.3.7.1 SNMP

The GSM can use the SNMP protocol to access the Huawei network component. The GSM supports SNMPv1, v2c and v3. SNMP uses the port 161/udp. The default port list does not include any UDP port. Therefore, this port is ignored during the vulnerability test using *Full and fast* and no SNMP check is enabled. To scan network components the port list should be modified to include at least the following ports:

- 22/tcp SSH
- 80/tcp 8080/tcp HTTP
- 443/tcp 8443/tcp HTTPS
- 2000/tcp SCCP
- 2443/tcp SCCPS
- 5060/tcp 5060/udp SIP
- 5061/tcp 5061/udp SIPS
- 67/udp DHCP Server



- 69/udp TFTP
- 123/udp NTP
- 161/udp SNMP
- 162/udp SNMP Traps
- 500/udp IKE
- 514/udp Syslog
- 546/udp DHCPv6

The administrator can set up special port lists used only for such network components.

The GSM needs to access only very few objects from the SNMP tree. For a less privileged access an SNMP view should be used to constrain the visibility of the SNMP tree for the GSM. The following two examples explain how to set up the view using either a community string or an SNMPv3 user.

To use an SNMP community string the following commands are required on the target:

```
<HUAWEI>system-view
```

Using an access list the usage of the community can be restricted. The IP address of the GSM is 192.168.222.74 in this example:

```
[~HUAWEI]acl 2000  
[~HUAWEI-acl4-basic-2000]rule permit source 192.168.222.74 32  
[*HUAWEI-acl4-basic-2000]commit  
[~HUAWEI-acl4-basic-2000]quit
```

Allow Version 2c of SNMPv3:

```
[~HUAWEI]snmp-agent sys-info version v3 v2c  
[*HUAWEI]commit
```

The view gsm should only allow accessing the system description:

```
[~HUAWEI]snmp-agent mib-view included gsm system  
[*HUAWEI]snmp-agent mib-view excluded gsm system.9  
[*HUAWEI]commit
```

The last command links the community gsm-community with the view gsm and the access list 2000:

```
[~HUAWEI]snmp-agent community read gsm-community mib-view gsm acl 2000  
[*HUAWEI]commit
```

If using an SNMPv3 user including encryption, the following configuration lines are required on the target:

```
<HUAWEI>system-view  
[~HUAWEI]acl 2000  
[~HUAWEI-acl4-basic-2000]rule permit source 192.168.222.74 32  
[*HUAWEI-acl4-basic-2000]quit  
[*HUAWEI]snmp-agent sys-info version v3  
[*HUAWEI]snmp-agent mib-view included gsm system  
[*HUAWEI]snmp-agent mib-view excluded gsm system.9  
[*HUAWEI]commit
```



SNMPv3 requires the setup of a group first. Here the group `gsmgroup` is linked to the view `gsm` and the access list 2000:

```
[~HUAWEI]snmp-agent group v3 gsmgroup privacy read-view gsm acl 2000
[*HUAWEI]commit
```

Now the user can be created supplying the password `gsm-password` and the encryption key `gsm-encrypt`. The authentication is done using MD5 while the encryption is handled by AES128. This is done in three steps:

Configure the password `gsm-password`:

```
[~HUAWEI]snmp-agent usm-user v3 gsm-user authentication-mode md5
Please configure the authentication password (8-255)
[*HUAWEI]commit
```

Configure encryption key `gsm-encrypt`:

```
[~HUAWEI]snmp-agent usm-user v3 gsm-user privacy-mode aes128
Please configure the privacy password (8-255)
[*HUAWEI]commit
```

Add the user to the group:

```
[*HUAWEI]snmp-agent usm-user v3 gsm-user group gsmgroup
[*HUAWEI]commit
```

To configure either the community or the SNMPv3 user in the GSM the administrator selects *Configuration > Credentials* in the menu bar (see Chapter 10.3.2 (page 255)).

10.3.7.2 SSH

The authenticated scan can be performed via SSH as well. If using SSH, the usage of a special unprivileged user is recommended. The GSM currently requires only the commands `display device`, `display version` and `display patch-information` to retrieve the device's current firmware version.

Note: If a compliance scan is performed, the following additional commands may be used:

- `display arp speed-limit`
- `display arp-miss speed-limit source-ip`
- `display current-configuration`
- `display current-configuration configuration bgp`
- `display current-configuration configuration pim`
- `display current-configuration configuration user-interface`
- `display current-configuration configuration vpn-instance`
- `display current-configuration interface`
- `display current-configuration | include multicast`
- `display current-configuration | include ntp`
- `display current-configuration | include snmp`
- `display current-configuration | include ssh`
- `display ftp-server`
- `display isis peer`



- display mpls ldp session verbose
- display mpls rsvp-te interface
- display ospf peer brief
- display ospfv3 peer
- display snmp-agent sys-info version
- display ssh server status
- display telnet server
- display telnet server status
- display vrrp

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

Note: Before using the following example, make sure all side effects of the configuration are understood. If used without verification, the system may restrict further logins via SSH or console.

The following commands create a restricted view including just the commands `display device`, `display version` and `display patch-information`. The supplied password `Hello-secret123` is not critical.

```
<HUAWEI> system-view
[~HUAWEI]aaa
[~HUAWEI-aaa]local-user gsm-user password cipher Hello-secret123
[*HUAWEI-aaa]local-user gsm-user level 0
[*HUAWEI-aaa]local-user gsm-user service-type ssh
[*HUAWEI-aaa]commit
[~HUAWEI-aaa]quit
[~HUAWEI]ssh user gsm-user authentication-type password
[*HUAWEI]ssh user gsm-user service-type stelnet
[*HUAWEI]commit
```

The following commands add just the commands `display version`, `display patch-information` and `display device` to “level 0”, so that `gsm-user` is restricted:

```
[~HUAWEI] command-privilege level 0 view global display device
[*HUAWEI] command-privilege level 0 view global display version
[*HUAWEI] command-privilege level 0 view global display patch-information
[*HUAWEI]commit
```

If SSH is not enabled yet the following commands take care of that:

```
[~HUAWEI] rsa local-key-pair create
[*HUAWEI]commit
```

Enable SSH logins using the following commands:

```
[~HUAWEI] user-interface vty 0 4
[*HUAWEI-ui-vty0-4] authentication-mode aaa
[*HUAWEI-ui-vty0-4] protocol inbound ssh
[*HUAWEI-ui-vty0-4] quit
[*HUAWEI]commit
```



Enable the STelnet server:

```
[~HUAWEI] stelnet server enable  
[*HUAWEI] ssh authentication-type default password  
[*HUAWEI] commit
```

Using an access list, the usage of the SSH login can be restricted. The IP address of the GSM is 192.168.222.74 in this example.

Note: This may restrict any SSH logins from other IP addresses and render the device inaccessible via network.

```
[~HUAWEI]acl 2000  
[*HUAWEI-acl4-basic-2000] rule permit source 192.168.222.74 32  
[*HUAWEI-acl4-basic-2000] quit  
[*HUAWEI] HUAWEI acl 2000  
[*HUAWEI] commit
```

Depending on the security settings the password for gsm-view has to be changed on the first login. This should be checked by logging in manually once via SSH.

The credentials of the user need to be entered on the GSM. Select *Configuration > Credentials* in the menu bar and create the appropriate user (see Chapter 10.3.2 (page 255)).

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

10.3.8 Requirements on Target Systems with EulerOS

- For authenticated scans on EulerOS, regular user access is usually enough. The login is performed via SSH. The authentication is done either with passwords or a private SSH key stored on the GSM.
- Generated installation package for credentials: the install package for EulerOS is an RPM file. The install package creates a new user without any specific permissions. A public SSH key that is created on the GSM is stored in the user's home folder.
- In both cases it needs to be made sure that public key authentication is not prohibited by the SSH daemon. The line `PubkeyAuthentication no` must not be present.
- Existing SSH key pairs may also be used. SSH key pairs can be generated using the command `ssh-keygen` on EulerOS or `puttygen.exe` if using PuTTY on Microsoft Windows. To use an existing SSH key pair for authentication, the private key must be supplied when the credential is created. The private SSH key must be either in PEM or OpenSSH format. The key types Ed25519, ECDSA, RSA and DSA are supported.
- For scans that include policy testing, root permission or the membership in specific groups (often `wheel`) may be necessary. For security reasons many configuration files are only readable by super users or members of specific groups.
- The more permissions a user has, the more results and settings can be detected on a system. In some cases root user access may be required.



- The following commands are executed with root user access during an authenticated scan.

Important:

- This list is not static. New or changed VTs may add new commands at any time.
 - Depending on the found software, additional commands may be executed.
-

- bash
- cat
- date
- dpkg
- egrep
- find
- grep
- host
- id
- ifconfig
- lastlog
- locate
- ls
- md5sum
- mlocate
- netstat
- perl
- ps
- rpm
- sh
- sha1sum
- slocate
- uname
- uptime
- whereis
- which

- The installation of the package `locate` (alternatively `mlocate`) to provide the command `locate/mlocate` on the target system is recommended. The use of this command reduces calls to the command `find` used to search for files and thus, improves the search performance and lowers the resource usage on the target system.

For the commands to work, the corresponding database permissions and regular database updates, e.g., via a cron job, may need to be configured.



10.3.9 Requirements on Target Systems with GaussDB

Note: It has to be ensured that the scan is performed by a user that has GaussDB executing permissions.

10.3.9.1 Requirements for System User *root*

Note: Generally, scanning with the user *root* is not recommended.

A root user has the following requirements for scanning a target system with GaussDB:

- On the GSM:
 - Credentials for the target host(s), either as a password or as an SSH key
- On the target system:
 - Root user is able to execute `zsql/zengine` (e.g., `LD_LIBRARY_PATH` is set properly and not on default)
 - `PermitRootLogin yes` in `sshd_config` or `PermitRootLogin prohibit-password` in `sshd_config` for SSH key based credentials

10.3.9.2 Requirements for Database Administrator Accounts (e.g., *gaussdba*)

A database administrator has the following requirements for scanning a target system with GaussDB:

- On the GSM:
 - Credentials for the target host(s), either as a password or as an SSH key
- On the target system:
 - User *gaussdba* is the database installation user

10.3.9.3 Requirements for a Regular User Accounts

A regular user has the following requirements for scanning a target system with GaussDB:

- On the GSM:
 - Credentials for the target host(s), either as a password or as an SSH key
- On the target system:
 - User is able to execute `zsql/zengine` (e.g., `LD_LIBRARY_PATH` is set properly and not on default)

10.3.9.4 Requirements for a Regular Database User Accounts (e.g., *gauss*)

A regular database user has the following requirements for scanning a target system with GaussDB:

- On the GSM:
 - Credentials with the user name *gauss* and a password configured in each used scan configuration
- On the target system:
 - Public facing database server port



10.4 Configuring a Prognosis Scan

Not every vulnerability justifies a new scan of the network or of individual systems. If the GSM has already obtained information about vulnerabilities by former scans, it can make a prognosis of which security risks could exist.

Using the CVE scanner allows forecasting possible security risks based on current information about known security risks from the SecInfo management (see Chapter 14 (page 384)) without the need of a new scan. This is especially interesting for environments in which most vulnerabilities have been removed or remediated by using the GSM.

If security risks become known, an actual scan can be run to verify the prognosis.

Note: The asset database requires current data for the CVE scanner. A full scan, e.g., with the scan configuration *Full and fast*, has to be performed and the results have to be added to the assets.

The results of a prognosis scan rely on the availability of self-reported versions from exposed software found during a full scan. Using an authenticated scan may increase the results found by the prognosis scan.

A full scan of the systems should occur regularly in weekly or monthly intervals.

A prognosis scan can be run as follows:

1. Run a full scan (see Chapter 10.2 (page 248)).

Note: A full scan configuration has to be chosen, e.g., *Full and fast*.

Additionally, the radio button *Yes* has to be selected for *Add results to Assets*.

2. Select *Scans > Tasks* in the menu bar.
3. Create a new task by moving the mouse over and clicking *New Task*.
4. Define the task (see Chapter 10.2.2 (page 251)).
5. Select *CVE* in the drop-down list *Scanner*.
6. Click *Save*.
7. In the row of the task click .

→ The scan is running. For the status of a task see Chapter 10.8 (page 288).

Tip: The report of a task can be displayed as soon as the task has been started by clicking the bar in the column *Status*. For reading, managing and downloading reports see Chapter 11 (page 315).

As soon as the status changes to *Done* the complete report is available. At any time the intermediate results can be reviewed (see Chapter 11.2.1 (page 320)).

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

8. When the scan is completed select *Scans > Reports* in the menu bar.
9. Click on the date of the report to show the results.

→ The report shows each found CVE as a vulnerability (see Fig. 10.23).



Report: Fri, Jul 12, 2019 11:10 AM UTC Done

ID: 221d0336-2ed1-4d35-818c-47dc6348976f Created: Fri, Jul 12, 2019 11:10 AM UTC Modified:

Information	Results (155 of 291)	Hosts (10 of 58)	Ports (19 of 19)	Applications (0 of 0)	Operating Systems (0 of 0)	CVEs (10 of 10)	Closed CVEs (0 of 0)	TLS Certificates (6 of 6)	Error Messages (0 of 0)	User Tags (0)
◀ ◀ 1 - 100 of 155 ▶ ▶										
Vulnerability	Severity	QoD	Host		Location	Created ▾				
TWiki < 6.1.0 XSS Vulnerability	4.3 (Medium)	80 %	IP	Name		Fri, Jul 12, 2019 11:38 AM UTC				
TWiki XSS and Command Execution Vulnerabilities	10.0 (High)	80 %	192.168.117.83	scan-target-1.greenbone.net	80/tcp	Fri, Jul 12, 2019 11:38 AM UTC				
Tiki Wiki CMS Groupware 'fixedURLData' Local File Inclusion Vulnerability	5.0 (Medium)	80 %	192.168.117.83	scan-target-1.greenbone.net	80/tcp	Fri, Jul 12, 2019 11:38 AM UTC				
TWiki Cross-Site Request Forgery Vulnerability - Sep10	6.8 (Medium)	80 %	192.168.117.83	scan-target-1.greenbone.net	80/tcp	Fri, Jul 12, 2019 11:38 AM UTC				
Tiki Wiki CMS Groupware < 4.2 Multiple Unspecified Vulnerabilities	7.5 (High)	80 %	192.168.0.127	scan-target-4.greenbone.net	80/tcp	Fri, Jul 12, 2019 11:37 AM UTC				
Tiki Wiki CMS Groupware Input Sanitization Weakness Vulnerability	5.0 (Medium)	80 %	192.168.0.127	scan-target-4.greenbone.net	80/tcp	Fri, Jul 12, 2019 11:37 AM UTC				
Tiki Wiki CMS Groupware XSS Vulnerability	3.5 (Low)	80 %	192.168.0.127	scan-target-4.greenbone.net	80/tcp	Fri, Jul 12, 2019 11:37 AM UTC				

Fig. 10.23: Results of a prognosis scan

10. Click on a vulnerability and click

→ The details page of the vulnerability is opened.

The VT to which the result is assigned is displayed in the section *Detection Method* (see Fig. 10.24). By clicking on the VT the details page of the corresponding VT is opened.

Tip: For available actions on this page see Chapter 11.2.1 (page 320).

Result: OS End Of Life Detection

Information	User Tags (0)
Vulnerability	
Name	OS End Of Life Detection
Severity	10.0 (High)
QoD	80 %
Host	192.168.8.10
Location	general/tcp
Summary	
OS End Of Life Detection	
The Operating System on the remote host has reached the end of life and should not be used anymore.	
Detection Result	
The "Debian GNU/Linux" Operating System on the remote host has reached the end of life.	
CPE:	cpe:/o.debian:debian_linux:7
Installed version, build or SP:	7
EOL date:	2018-05-31
EOL info:	https://en.wikipedia.org/wiki/List_of_Debian_releases#Release_table
Detection Method	
Details:	OS End Of Life Detection OID: 1.3.6.1.4.1.25623.1.0.103674
Version used:	2018-02-22T15:42:48Z

Fig. 10.24: Details of a detected CVE

Note: The CVE scanner might show false positives as it does not check whether the vulnerability actually exists.



10.5 Using Container Tasks

10.5.1 Creating a Container Task

A container task can be used to import and provide reports created on other GSMS.

A container task can be created as follows:

1. Select *Scans > Tasks* in the menu bar.
2. Create a new container task by moving the mouse over and clicking *New Container Task*.
3. Enter the name of the container task in the input box *Name* (see Fig. 10.25).

New Container Task	
Name	<input type="text" value="Container_Task"/>
Comment	<input type="text" value="Imported results from older GSMS"/>
<input type="button" value="Cancel"/> <input type="button" value="Save"/>	

Fig. 10.25: Creating a container task

4. Click *Save*.
5. To add a report to the container task click in the row of the container task.
6. Click *Browse...* and select the XML file of a report (see Fig. 10.26).

Import Report	
Report	<input type="button" value="Browse..."/> report-437643e0-e82d-4c0f-97e2-011d1fc32e0e.pdf
Container Task	<input type="button" value="Container_Task"/>
Add to Assets	Add to Assets with QoD >= 70% and Overrides enabled <input checked="" type="radio"/> Yes <input type="radio"/> No
<input type="button" value="Cancel"/> <input type="button" value="Import"/>	

Fig. 10.26: Adding a report to a container task

7. Select the radio button *Yes* to add the report to the assets (see Chapter 13 (page 378)).
8. Click *Import*.

10.5.2 Managing Container Tasks

List Page

All existing container tasks can be displayed by selecting *Scans > Tasks* in the menu bar.

Note: Container tasks can be identified by in the column *Status*.

For all container tasks the following actions are available:

- Import reports to the container task.
- Move the container task to the trashcan.



- Edit the container task.
- Clone the container task.
- Export the container task as an XML file.

Note: By clicking or below the list of tasks more than one task can be moved to the trashcan or exported at a time. The drop-down list is used to select which tasks are moved to the trashcan or exported.

Details Page

Click on the name of a container task to display the details of the container task. Click to open the details page of the container task.

The following registers are available:

Information General information about the container task.

User Tags Assigned tags (see Chapter 8.5 (page 214)).

Permissions Assigned permissions (see Chapter 9.4 (page 231)).

The following actions are available in the upper left corner:

- Open the corresponding chapter of the user manual.
- Show the list page of all container tasks.
- Create a new task (see Chapter 10.2.2 (page 251)) or container task (see Chapter 10.5 (page 283)).
- Clone the container task.
- Edit the container task.
- Move the container task to the trashcan.
- Export the container task as an XML file.
- Import reports to the container task.
- Show the last report for the container task or show all reports for the container task.
- Show the results for the container task.
- Show the notes for the container task.
- Show the overrides for the container task.

10.6 Managing Targets

List Page

All existing targets can be displayed by selecting *Configuration > Targets* in the menu bar.

For all targets the following information is displayed:

Name Name of the target.

Hosts Hosts that are scanned if the target is used for a scan (see Chapter 10.2.2 (page 251)).

IPs Number of scanned hosts.

Port List Port list used if the target is used for a scan (see Chapter 10.2.2 (page 251)).

Credentials Credentials configured for the target.



For all targets the following actions are available:

- Move the target to the trashcan. Only targets which are currently not used can be moved to the trashcan.
- Edit the target.
- Clone the target.
- Export the target as an XML file.

Note: By clicking or below the list of targets more than one target can be moved to the trashcan or exported at a time. The drop-down list is used to select which targets are moved to the trashcan or exported.

Details Page

Click on the name of a target to display the details of the target. Click to open the details page of the target.

The following registers are available:

Information General information about the target.

User Tags Assigned tags (see Chapter 8.5 (page 214)).

Permissions Assigned permissions (see Chapter 9.4 (page 231)).

The following actions are available in the upper left corner:

- Open the corresponding chapter of the user manual.
- Show the list page of all targets.
- Create a new target (see Chapter 10.2.1 (page 248)).
- Clone the target.
- Edit the target.
- Move the target to the trashcan. Only targets which are currently not used can be moved to the trashcan.
- Export the target as an XML file.

10.7 Creating and Managing Port Lists

If applications run on unusual ports and they should be monitored and tested with the GSM, the default port lists should be adapted. If necessary, an individual port list including the desired port can be created.

All default port lists by Greenbone Networks are data objects that are distributed via the feed. They are downloaded and updated with each feed update.

If no default port lists are available, a feed update may be necessary, or the Feed Import Owner may need to be set (see Chapter 7.2.1.9.1 (page 130)).

Default port lists cannot be edited. Additionally, they can only be deleted temporarily by the Feed Import Owner or by a super administrator. During the next feed update, they will be downloaded again.

Note: To permanently delete a default port list, the Feed Import Owner has to delete it. Afterwards the Feed Import Owner has to be changed to (*Unset*) (see Chapter 7.2.1.9.1 (page 130)).



In addition to the default port lists, custom port lists can be created (see Chapter 10.7.1 (page 286)) or imported (see Chapter 10.7.2 (page 286)).

10.7.1 Creating a Port List

A new port list can be created as follows:

1. Select *Configuration > Port Lists* in the menu bar.
2. Create a new port list by clicking .
3. Define the port list (see Fig. 10.27).

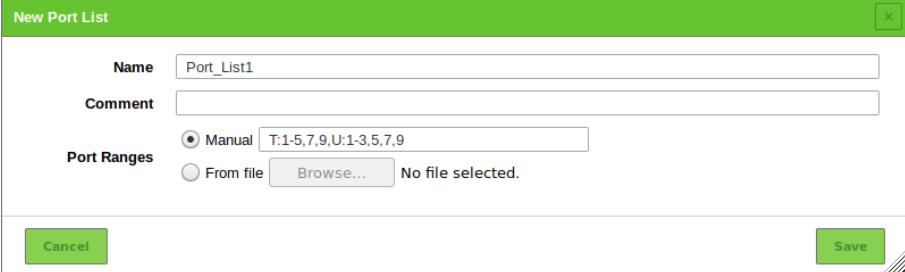


Fig. 10.27: Creating a new port list

4. Click *Save*.

The following details of the port list can be defined:

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

Comment An optional comment can contain additional information.

Port Ranges Manual entry of the port ranges or importing of a list of the port ranges. If entering manually, the port ranges are separated by commas. If importing from a file, the entries can be separated with commas or line breaks. The file should use UTF-8 text encoding.

Each value in the list can be a single port (e.g., 7) or a port range (e.g., 9–11). These options can be mixed (e.g., 5, 7, 9–11, 13).

An entry in the list can be preceded by a protocol specifier (T: for TCP, U: for UDP), e.g., T:1–3, U:7, 9–11 (TCP ports 1, 2 and 3, UDP ports 7, 9, 10 and 11). If no specifier is given, TCP is assumed.

10.7.2 Importing a Port List

A port list can be imported as follows:

1. Select *Configuration > Port Lists* in the menu bar.
 2. Click .
 3. Click *Browse...* and select the XML file of the port list.
 4. Click *Import*.
- The imported port list is displayed on the page *Port Lists*.



10.7.3 Managing Port Lists

List Page

All existing port lists can be displayed by selecting *Configuration > Port Lists* in the menu bar.

For all port lists the following information is displayed:

Name Name of the port list.

Total Total number of ports in the port list.

TCP Number of TCP ports in the port list.

UDP Number of UDP ports in the port list.

For all port lists the following actions are available:

- Move the port list to the trashcan. Only port lists which are currently not used can be moved to the trashcan. As long as the port list is not deleted from the trashcan, it is not downloaded anew during the next feed update.
- Edit the port list. Only self-created port lists which are currently not used can be edited.
- Clone the port list.
- Export the port list as an XML file.

Note: By clicking or below the list of port lists more than one port list can be moved to the trashcan or exported at a time. The drop-down list is used to select which port lists are moved to the trashcan or exported.

Details Page

Click on the name of a port list to display the details of the port list. Click to open the details page of the port list.

The following registers are available:

Information General information about the port list.

Port Ranges All port ranges included in this port list. The first and the last port of a range as well as the protocol specifier are displayed.

User Tags Assigned tags (see Chapter 8.5 (page 214)).

Permissions Assigned permissions (see Chapter 9.4 (page 231)).

The following actions are available in the upper left corner:

- Open the corresponding chapter of the user manual.
- Show the list page of all port lists.
- Create a new port list (see Chapter 10.7.1 (page 286)).
- Clone the port list.
- Edit the port list. Only self-created port lists which are currently not used can be edited.
- Move the port list to the trashcan. Only port lists which are currently not used can be moved to the trashcan. As long as the port list is not deleted from the trashcan, it is not downloaded anew during the next feed update.
- Export the port list as an XML file.



10.8 Managing Tasks

List Page

All existing tasks can be displayed by selecting *Scans > Tasks* in the menu bar.

Name	Status	Reports	Last Report	Severity	Trend	Actions
DMZ Mail Scan	✉️ New					▷ ▶ 🗑️ 🗑️ 🔍 🔍
Immediate scan of IP 192.168.178.33	⌚ 98 %	1				▷ ▶ 🗑️ 🗑️ 🔍 🔍

(Applied filter: min_qod=70 apply_overrides=1 rows=10 first=1 sort=name)

Fig. 10.28: Page *Tasks* displaying all tasks

For all tasks the following information is displayed:

Name Name of the task. The following icons may be displayed:

- ✎ The task is marked as alterable. Some properties that would otherwise be locked once reports exist can be edited.
- ⌚ The task is configured to run on a remote scanner (see Chapter 16 (page 409)).
- 👁 The task is visible to one or more other user(s).
- ✉️ The task is owned by another user.

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

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

Requested The task was just started. The GSM is preparing the scan.

21 % The task is currently running. The percent value is based on the number of VTs executed on the selected hosts. For this reason the value does not necessarily correlate with the time spent.

Queued The scan was added to a waiting queue (following the principle “first in, first out”) for one of the following reasons:

- Too many scans are already running and there is no memory available to start the scan. The scan will be started when the required resources are available again.
- The GSM is performing a feed update and is currently loading new VTs.
- The GSM was just started and is currently loading the VTs.

For more information see Chapter 17.3 (page 422).

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 at 84 % The task was stopped. The latest report is possibly not yet complete. Other reasons for this status could be the reboot of the GSM or a power outage. After restarting the scanner, the task will be resumed automatically.

Resume Requested The task was just resumed. The GSM is preparing the scan.

When resuming a scan, all unfinished hosts are scanned completely anew. The data of hosts that were already fully scanned is kept.



Interrupted at 42 % An error has occurred and the task was interrupted. The latest report is possibly not complete yet or is missing completely.

Done The task has been completed successfully.

Container The task is a container task.

Uploading The report is currently being uploaded into the container task.

Reports Number of reports for the task. By clicking on the number of reports the page *Reports* is opened. A filter is applied to show only the reports for the selected task.

Last Report Date and time of the latest report. By clicking it the details page of the latest report is opened.

Severity Highest severity found by a scan of the task.

Trend Change of vulnerabilities between the newest and the second newest report (see Chapter 11.5 (page 330)).

For all tasks the following actions are available:

- ▷ Start the task. Only currently not running tasks can be started.
- Stop the currently running task. All discovered results will be written to the database.
- ⌚ Show details of the assigned schedule (only available for scheduled tasks, see Chapter 10.10 (page 301)).
- ▷ Resume the stopped task. All unfinished hosts are scanned completely anew. The data of hosts that were already fully scanned is kept.
- trashcan Move the task to the trashcan.
- edit Edit the task.
- clone Clone the task.
- export Export the task as an XML file.

Note: By clicking trashcan or export below the list of tasks more than one task can be moved to the trashcan or exported at a time. The drop-down list is used to select which tasks are moved to the trashcan or exported.

Details Page

Click on the name of a task to display the details of the task. Click to open the details page of the task.

The following registers are available:

Information General information about the task.

User Tags Assigned tags (see Chapter 8.5 (page 214)).

Permissions Assigned permissions (see Chapter 9.4 (page 231)).

The following actions are available in the upper left corner:

- ?(?) Open the corresponding chapter of the user manual.
- list Show the list page of all tasks.
- new Create a new task (see Chapter 10.2.2 (page 251)) or container task (see Chapter 10.5 (page 283)).
- clone Clone the task.
- edit Edit the task.
- trashcan Move the task to the trashcan.



- ↗ Export the task as an XML file.
- ▷ Start the task. Only currently not running tasks can be started.
- ⏹ Stop the currently running task. All discovered results will be written to the database.
- ⏸ Resume the stopped task. All unfinished hosts are scanned completely anew. The data of hosts that were already fully scanned is kept.
- 📄 Show the last report for the task or show all reports for the task.
- 🎧 Show the results for the task.
- 📄 Show the notes for the task.
- ⌂ Show the overrides for the task.

10.8.1 Granting Permissions for a Task

On the details page of a task permissions for the task can be managed as follows:

Note: By default, regular users cannot create permissions for other users as they do not have access to the user database. To be able to create permissions for other users, a user must have the global and the specific `get_users` permission (see Chapter 9.4.3 (page 236)).

1. Select *Scans > Tasks* in the menu bar.
2. Click on the name of a task to display the details of the task. Click to open the details page of the task.
3. Click on the register *Permissions*.
4. In the section *Permissions* click .
5. Select the permission type in the drop-down list *Grant*.
6. Select the radio button *User*, *Group* or *Role* and select the user/role/group in the respective drop-down list (see Fig. 10.29).

The screenshot shows the 'Create Multiple Permissions' dialog box. At the top, it says 'Create Multiple Permissions'. Below that, there's a 'Grant' dropdown set to 'read' and a 'Permission' dropdown. Under 'to', there are three radio buttons: 'User' (selected), 'Role', and 'Group'. Below this, there's a section for 'Task' with a dropdown showing 'Immediate scan of IP 192.168.178.33 for current resource only'. Under 'on', there are four options listed:

- Scan Config Full and fast
- Scanner OpenVAS Default
- Target Target for immediate scan of IP 192.168.178.33 - 2019-06-17 12:20:39
- Port List OpenVAS Default

At the bottom, there are 'Cancel' and 'Save' buttons.

Fig. 10.29: Creating a new permission

7. Click *Save*.
→ The permission is displayed on the details page of the task (see Fig. 10.30).

After logging in the user can see the task and can access the respective reports.



Information	User Tags (0)	Permissions (1)					?
Name	Description	Resource Type	Resource	Subject Type	Subject	Actions	
get_tasks	User user has read access to Task Immediate scan of IP 192.168.178.33	Task	Immediate scan of IP 192.168.178.33	User	user		

Fig. 10.30: Permission displayed on the details page of a task

10.9 Configuring and Managing Scan Configurations

The GSM appliance comes with various predefined scan configurations. They can be customized and new scan configurations can be created.

10.9.1 Default Scan Configurations

All default scan configurations by Greenbone Networks are data objects that are distributed via the feed. They are downloaded and updated with each feed update.

If no default scan configurations are available, a feed update may be necessary, or the Feed Import Owner may need to be set (see Chapter 7.2.1.9.1 (page 130)).

Default scan configurations cannot be edited. Additionally, they can only be deleted temporarily by the Feed Import Owner or by a super administrator. During the next feed update, they will be downloaded again.

Note: To permanently delete a default scan configuration, the Feed Import Owner has to delete it. Afterwards the Feed Import Owner has to be changed to (*Unset*) (see Chapter 7.2.1.9.1 (page 130)).

In addition to the default scan configurations, custom scan configurations can be created (see Chapter 10.9.2 (page 292)) or imported (see Chapter 10.9.3 (page 295)).

By default, the following scan configurations are available:

Empty This scan configuration is an empty template containing no VTs. It can be cloned and used for a completely individual created scan configuration.

The VT families are static, i.e., new VTs of the chosen VT families are not added and used automatically.

Base This scan configuration only uses VTs which collect information about the target system. No vulnerabilities are being detected. It can be cloned and used for a completely individual created scan configuration.

The used port scanners are *Ping Host* and *Nmap* which detect whether a host is alive. Additionally, information about the operating system is collected.

The VT families are static, i.e., new VTs of the chosen VT families are not added and used automatically.

Discovery This scan configuration only uses VTs that provide information about the target system. No vulnerabilities are being detected.

Amongst others, the collected information contains information about open ports, used hardware, firewalls, used services, installed software and certificates. The system is inventoried completely.

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

Host Discovery This scan configuration is used to detect target systems. No vulnerabilities are being detected.

The used port scanner is *Ping Host* which detects whether a host is alive.

The VT families are static, i.e., new VTs of the chosen VT families are not added and used automatically.



System Discovery This scan configuration is used to detect target systems including installed operating systems and used hardware. No vulnerabilities are being detected.

The used port scanners are *Ping Host* and *Nmap* which detect whether a host is alive.

The VT families are static, i.e., new VTs of the chosen VT families are not added and used automatically.

Full and fast For many environments this is the best option to start with.

This scan configuration is based on the information gathered in the previous port scan and uses almost all VTs. Only VTs that will not damage the target system are used. VTs are optimized in the best possible way to keep the potential false negative rate especially low. The other “Full” configurations only provide more value in rare cases but with much higher effort.

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

Full and fast ultimate This scan configuration expands the scan configuration *Full and fast* with VTs that could disrupt services or systems or even cause shutdowns.

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

Full and very deep This scan configuration is based on the scan configuration *Full and fast* but the results of the port scan or the application/service detection do not have an impact on the selection of the VTs. Therefore, VTs that wait for a timeout or test for vulnerabilities of an application/service which were not detected previously are used. A scan with this scan configuration is very slow.

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

Full and very deep ultimate This scan configuration expands the scan configuration *Full and very deep* with dangerous VTs that could cause possible service or system disruptions. A scan with this scan configuration is very slow.

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

10.9.2 Creating a Scan Configuration

Tip: Greenbone Networks offers different scan configurations on their website (see Chapter 12 (page 346)).

A new scan configuration can be created as follows:

1. Select *Configuration > Scan Configs* in the menu bar.
2. Create a new scan configuration by clicking

Note: Alternatively, a scan configuration can be imported (see Chapter 10.9.3 (page 295)).

3. Enter the name of the scan configuration in the input box *Name* (see Fig. 10.31).
4. Select the radio button of the base that should be used.

It can be chosen between *Base with a minimum set of NVTs*, *Empty*, *static and fast*, *Full and fast* and an previously created scan configuration.

5. Click *Save*.
→ The scan configuration is created and displayed on the page *Scan Configs*.
6. In the row of the scan configuration click
7. In the section *Edit Network Vulnerability Test Families* select the radio button if newly introduced VT families should be included and activated automatically (see Fig. 10.32).



New Scan Config

Name	<input type="text" value="SNMP Scan Config"/>
Comment	<input type="text"/>
Base	<input checked="" type="radio"/> Base with a minimum set of NVTs <input type="radio"/> Empty, static and fast <input type="radio"/> Full and fast <input type="radio"/>
<input type="button" value="Cancel"/> <input type="button" value="Save"/>	

Fig. 10.31: Creating a new scan configuration

Edit Scan Config SNMP Scan Config

Name	<input type="text" value="SNMP Scan Config"/>																																																												
Comment	<input type="text" value="Empty and static configuration template."/>																																																												
Edit Network Vulnerability Test Families (65) <table border="1"> <thead> <tr> <th>Family</th> <th>NVTs selected</th> <th>Trend</th> <th>Select all NVTs</th> <th>Actions</th> </tr> </thead> <tbody> <tr><td>AIX Local Security Checks</td><td>0 of 1</td><td><input type="radio"/> ↗ <input checked="" type="radio"/> →</td><td><input type="checkbox"/></td><td><input checked="" type="checkbox"/></td></tr> <tr><td>Amazon Linux Local Security Checks</td><td>0 of 748</td><td><input type="radio"/> ↗ <input checked="" type="radio"/> →</td><td><input type="checkbox"/></td><td><input checked="" type="checkbox"/></td></tr> <tr><td>Brute force attacks</td><td>0 of 4</td><td><input type="radio"/> ↗ <input checked="" type="radio"/> →</td><td><input type="checkbox"/></td><td><input checked="" type="checkbox"/></td></tr> <tr><td>Buffer overflow</td><td>0 of 567</td><td><input type="radio"/> ↗ <input checked="" type="radio"/> →</td><td><input type="checkbox"/></td><td><input checked="" type="checkbox"/></td></tr> <tr><td>CISCO</td><td>0 of 1231</td><td><input type="radio"/> ↗ <input checked="" type="radio"/> →</td><td><input type="checkbox"/></td><td><input checked="" type="checkbox"/></td></tr> <tr><td>CentOS Local Security Checks</td><td>0 of 3212</td><td><input type="radio"/> ↗ <input checked="" type="radio"/> →</td><td><input type="checkbox"/></td><td><input checked="" type="checkbox"/></td></tr> <tr><td>Cisco Local Security Checks</td><td>0 of 221</td><td><input type="radio"/> ↗ <input checked="" type="radio"/> →</td><td><input type="checkbox"/></td><td><input checked="" type="checkbox"/></td></tr> <tr><td>Citrix Xenserver Local Security Checks</td><td>0 of 43</td><td><input type="radio"/> ↗ <input checked="" type="radio"/> →</td><td><input type="checkbox"/></td><td><input checked="" type="checkbox"/></td></tr> <tr><td>Compliance</td><td>0 of 12</td><td><input type="radio"/> ↗ <input checked="" type="radio"/> →</td><td><input type="checkbox"/></td><td><input checked="" type="checkbox"/></td></tr> <tr><td>Databases</td><td>0 of 579</td><td><input type="radio"/> ↗ <input checked="" type="radio"/> →</td><td><input type="checkbox"/></td><td><input checked="" type="checkbox"/></td></tr> <tr><td>Debian Local Security Checks</td><td>0 of 5366</td><td><input type="radio"/> ↗ <input checked="" type="radio"/> →</td><td><input type="checkbox"/></td><td><input checked="" type="checkbox"/></td></tr> </tbody> </table>		Family	NVTs selected	Trend	Select all NVTs	Actions	AIX Local Security Checks	0 of 1	<input type="radio"/> ↗ <input checked="" type="radio"/> →	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Amazon Linux Local Security Checks	0 of 748	<input type="radio"/> ↗ <input checked="" type="radio"/> →	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Brute force attacks	0 of 4	<input type="radio"/> ↗ <input checked="" type="radio"/> →	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Buffer overflow	0 of 567	<input type="radio"/> ↗ <input checked="" type="radio"/> →	<input type="checkbox"/>	<input checked="" type="checkbox"/>	CISCO	0 of 1231	<input type="radio"/> ↗ <input checked="" type="radio"/> →	<input type="checkbox"/>	<input checked="" type="checkbox"/>	CentOS Local Security Checks	0 of 3212	<input type="radio"/> ↗ <input checked="" type="radio"/> →	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Cisco Local Security Checks	0 of 221	<input type="radio"/> ↗ <input checked="" type="radio"/> →	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Citrix Xenserver Local Security Checks	0 of 43	<input type="radio"/> ↗ <input checked="" type="radio"/> →	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Compliance	0 of 12	<input type="radio"/> ↗ <input checked="" type="radio"/> →	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Databases	0 of 579	<input type="radio"/> ↗ <input checked="" type="radio"/> →	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Debian Local Security Checks	0 of 5366	<input type="radio"/> ↗ <input checked="" type="radio"/> →	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Family	NVTs selected	Trend	Select all NVTs	Actions																																																									
AIX Local Security Checks	0 of 1	<input type="radio"/> ↗ <input checked="" type="radio"/> →	<input type="checkbox"/>	<input checked="" type="checkbox"/>																																																									
Amazon Linux Local Security Checks	0 of 748	<input type="radio"/> ↗ <input checked="" type="radio"/> →	<input type="checkbox"/>	<input checked="" type="checkbox"/>																																																									
Brute force attacks	0 of 4	<input type="radio"/> ↗ <input checked="" type="radio"/> →	<input type="checkbox"/>	<input checked="" type="checkbox"/>																																																									
Buffer overflow	0 of 567	<input type="radio"/> ↗ <input checked="" type="radio"/> →	<input type="checkbox"/>	<input checked="" type="checkbox"/>																																																									
CISCO	0 of 1231	<input type="radio"/> ↗ <input checked="" type="radio"/> →	<input type="checkbox"/>	<input checked="" type="checkbox"/>																																																									
CentOS Local Security Checks	0 of 3212	<input type="radio"/> ↗ <input checked="" type="radio"/> →	<input type="checkbox"/>	<input checked="" type="checkbox"/>																																																									
Cisco Local Security Checks	0 of 221	<input type="radio"/> ↗ <input checked="" type="radio"/> →	<input type="checkbox"/>	<input checked="" type="checkbox"/>																																																									
Citrix Xenserver Local Security Checks	0 of 43	<input type="radio"/> ↗ <input checked="" type="radio"/> →	<input type="checkbox"/>	<input checked="" type="checkbox"/>																																																									
Compliance	0 of 12	<input type="radio"/> ↗ <input checked="" type="radio"/> →	<input type="checkbox"/>	<input checked="" type="checkbox"/>																																																									
Databases	0 of 579	<input type="radio"/> ↗ <input checked="" type="radio"/> →	<input type="checkbox"/>	<input checked="" type="checkbox"/>																																																									
Debian Local Security Checks	0 of 5366	<input type="radio"/> ↗ <input checked="" type="radio"/> →	<input type="checkbox"/>	<input checked="" type="checkbox"/>																																																									
<input type="button" value="Cancel"/> <input type="button" value="Save"/>																																																													

Fig. 10.32: Editing the new scan configuration



8. In the section *Edit Network Vulnerability Test Families* activate the checkboxes in the column *Select all NVTs* if all VTs of a family should be activated.
9. Click for a VT family to edit it (see Fig. 10.33).

Note: The following VT families cannot be edited:

- CentOS Local Security Checks
- Debian Local Security Checks
- Fedora Local Security Checks
- Huawei EulerOS Local Security Checks
- Oracle Linux Local Security Checks
- Red Hat Local Security Checks
- SuSE Local Security Checks
- Ubuntu Local Security Checks

Edit Scan Config Family Privilege escalation							
Config SNMP Scan Config							
Family Privilege escalation							
Edit Network Vulnerability Tests							
Name ▲	OID	Severity	Timeout	Prefs	Selected	Actions	
Adobe Flash Media Server Privilege Escalation Vulnerability	1.3.6.1.4.1.25623.1.0.800560	7.5 (High)	default	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Adobe FrameMaker Privilege Escalation Vulnerability (Windows)	1.3.6.1.4.1.25623.1.0.814315	6.8 (Medium)	default	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Adobe TCS Privilege Escalation Vulnerability (Windows)	1.3.6.1.4.1.25623.1.0.814313	6.8 (Medium)	default	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Apache <= 1.3.33 htpasswd local overflow	1.3.6.1.4.1.25623.1.0.14771	2.1 (Low)	default	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
ArcaVir AntiVirus Products Privilege Escalation Vulnerability	1.3.6.1.4.1.25623.1.0.800720	7.2 (High)	default	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Bournal Privilege Escalation Vulnerability	1.3.6.1.4.1.25623.1.0.800730	3.3 (Low)	default	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Cabletron Web View Administrative Access	1.3.6.1.4.1.25623.1.0.10962	7.5 (High)	default	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
ChangeTrack Local Privilege Escalation Vulnerability	1.3.6.1.4.1.25623.1.0.900868	7.2 (High)	default	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

Fig. 10.33: Editing a family of VTs

10. In the column *Selected* activate the checkboxes of the VTs that should be activated.
11. Click for a VT to edit it (see Fig. 10.34).

Note: If editing the VT includes uploading a text file, the file should use UTF-8 text encoding.

12. Click **Save** to save the VT.
13. Click **Save** to save the family of VTs.
14. Optional: edit scanner preferences (see Chapter 10.9.4 (page 295)).
15. Optional: edit VT preferences (see Chapter 10.9.5 (page 297)).
16. Click **Save** to save the scan configuration.



Edit Scan Config NVT Search for specified dirs

Name	Search for specified dirs
Config	BSI-TR-03116-4
Family	General
OID	1.3.6.1.4.1.25623.1.0.103437
Version	0
Notes	0
Overrides	0

Summary

This Plugin is searching for the specified webdirs.

Vulnerability Scoring

CVSS base	0.0 (Log)	
CVSS base vector	AV:N AC:L Au:N/C:N/I:N/A:N	
Name	New Value	Default Value
Timeout	<input checked="" type="radio"/> Apply default timeout <input type="radio"/>	
Run this Plugin	<input type="radio"/> Yes <input checked="" type="radio"/> No	no
Search for dir(s)	/admin:/manager	/admin:/manager
Valid http status codes indicating that a directory was found	200;301;302;401;403	200;301;302;401;403

Cancel **Save**

Fig. 10.34: Editing a VT

10.9.3 Importing a Scan Configuration

Note: Only scan configurations created with GOS 6 can be imported. Importing an older scan configuration is not possible and leads to an error message.

A scan configuration can be imported as follows:

1. Select *Configuration > Scan Configs* in the menu bar.
2. Click .
3. Click *Browse...* and select the XML file of the scan configuration.
4. Click *Import*.

Note: If the name of the imported scan configuration already exists, a numeric suffix is added to the name.

→ The imported scan configuration is displayed on the page *Scan Configs*.

5. Execute steps 6 to 16 of Chapter 10.9.2 (page 292) to edit the scan configuration.

10.9.4 Editing the Scanner Preferences

Scanner preferences can be edited as follows:

1. Select *Configuration > Scan Configs* in the menu bar.
2. In the row of the scan configuration click .
3. In the section *Edit Scanner Preferences* click  to edit the scanner preferences (see Fig. 10.35).
4. After editing the scanner preferences click *Save* to save the scan configuration.



Edit Scan Config BSI-TR-03116-4

Edit Scanner Preferences (20)

Name	New Value	Default Value
auto_enable_dependencies	<input checked="" type="radio"/> Yes <input type="radio"/> No	yes
cgi_path	/cgi-bin/scripts	/cgi-bin/scripts
checks_read_timeout	5	5
drop_privileges	<input type="radio"/> Yes <input checked="" type="radio"/> No	no
expand_vhosts	yes	yes
max_sysload	30	30
min_free_mem	1024	1024
network_scan	<input type="radio"/> Yes <input checked="" type="radio"/> No	no
non_simult_ports	139, 445	139, 445, 3389, Services/irc
open_sock_max_attempts	5	5
optimize_test	<input checked="" type="radio"/> Yes <input type="radio"/> No	yes
plugins_timeout	220	220

Cancel **Save**

Fig. 10.35: Editing the scanner preferences

10.9.4.1 Description of Scanner Preferences

Note: Documenting all scanner preferences is out of scope of this document. Only the most important preferences of the scanner are covered.

Undocumented preferences may also be deprecated despite still being visible. These preferences will be ignored by the scanner and should not be considered.

- *auto_enable_dependencies*: this defines whether VTs that are required by other VTs are activated automatically.
- *cgi_path*: path used by the VTs to access CGI scripts.
- *checks_read_timeout*: timeout for the network sockets during a scan.
- *test_empty_vhost*: the scanner also scans the target by using empty vhost values in addition to the target's associated vhost values.
- *max_sysload*: maximum load on the GSM. Once this load is reached, no further VTs are started until the load drops below this value again.
- *min_free_mem*: minimum available memory (in MB) which should be kept free on the GSM. Once this limit is reached, no further VTs are started until sufficient memory is available again.
- *non_simult_ports*: these ports are not being tested simultaneously by VTs.
- *optimize_test*: VTs will only be started if specific prerequisites are met (e.g., open ports or detected application).
- *plugins_timeout*: maximum run time of a VT.
- *safe_checks*: some VTs can cause damage on the host system. This setting disables those respective VTs.
- *scanner_plugins_timeout*: maximum run time (in seconds) for all VTs of the VT family *Port scanners*. If a VT runs longer, it is terminated.



- *expand_vhosts*: the target's host list of vhosts is expanded with values gathered from sources such as reverse lookup queries and VT checks for SSL/TLS certificates.
- *time_between_request*: wait time (in milliseconds) between two actions such as opening a TCP socket, sending a request through the open tcp socket and closing the TCP socket.
- *timeout_retry*: number of retries if a socket connection attempt times out.
- *unscanned_closed*: this defines whether TCP ports that were not scanned should be treated like closed ports.
- *unscanned_closed_udp*: this defines whether UDP ports that were not scanned should be treated as closed ports.

10.9.5 Editing the VT Preferences

1. Select *Configuration > Scan Configs* in the menu bar.
2. In the row of the scan configuration click .
3. In the section *Network Vulnerability Test Preferences* click  to edit the VT preferences.
4. In the row of the VT preference click .
5. Edit the VT preference.
6. Click *Save* to save the VT preference.
7. Click *Save* to save the scan configuration.

10.9.5.1 Description of VT Preferences

Note: Documenting all VT preferences is out of scope of this document. Only the VT preferences of the Nmap and Ping Host port scanners are covered for now.

Preferences of the VT *Ping Host*

The VT *Ping Host* in the VT family *Port scanners* contains the following configuration parameters:

Note: The *Alive Test* settings of a target can overwrite some settings of the ping scanner.

- *Do a TCP ping*: this defines whether the reachability of hosts should be tested using TCP. In this case the following ports will be tested: 21,22,23,25,53,80,135,137,139,143,443,445.
- *Do an ICMP ping*: this defines whether the reachability of hosts should be tested using ICMP.
- *Mark unreachable Hosts as dead*: this defines whether a host that is not discovered by this VT should be tested by other VTs later.
- *Report about reachable Hosts*: this defines whether a host discovered by this VT should be listed.
- *Report about unreachable Hosts*: this defines whether a host not discovered by this VT should be listed.
- *TCP ping tries also TCP-SYN ping*: the TCP ping uses a TCP-ACK packet by default. A TCP-SYN packet can be used additionally.
- *Use ARP*: this defines whether hosts should be searched for in the local network using the ARP protocol.
- *Use Nmap*: this defines whether the ping VT should use Nmap.



- *nmap: try also with only –sP*: if Nmap is used the ping scan is performed using the `-sP` option.
- *nmap additional ports for –PA*: additional ports for the TCP ping test. This is only the case if *Do a TCP ping* is selected.

Preferences of the VT *Nmap (NASL wrapper)*

The following options of the VT *Nmap (NASL wrapper)* in the VT family *Port scanners* will be directly translated into options for the execution of the Nmap command. Additional information can be found in the documentation for Nmap²².

- *Do not randomize the order in which ports are scanned*: Nmap will scan the ports in ascending order.
- *Do not scan targets not in the file*: see *File containing grepable results*.
- *Fragment IP packets*: Nmap fragments the packets for the attack. This allows bypassing simple packet filters.
- *Identify the remote OS*: Nmap tries to identify the operating system.
- *RPC port scan*: Nmap tests the system for Sun RPC ports.
- *Run dangerous ports even if safe checks are set*: UDP and RPC scans can cause problems and usually are disabled with the setting `safe_checks`. With this setting, they can be enabled anyway.
- *Service scan*: Nmap tries to identify services.
- *Use hidden option to identify the remote OS*: Nmap tries to identify more aggressively.
- *Data length*: Nmap adds random data of specified length to the packet.
- *Host Timeout*: host timeout.
- *Initial RTT timeout*: initial round trip timeout. Nmap can adjust this timeout dependent on the results.
- *Max RTT timeout*: maximum RTT.
- *Min RTT timeout*: minimum RTT.
- *Max Retries*: maximum number of retries.
- *Maximum wait between probes*: this regulates the speed of the scan.
- *Minimum wait between probes*: this regulates the speed of the scan.
- *Ports scanned in parallel (max)*: this defines how many ports should at most be scanned simultaneously.
- *Ports scanned in parallel (min)*: this defines how many ports should at least be scanned simultaneously.
- *Source port*: source port. This is of interest when scanning through a firewall if connections are in general allowed from a specific port.
- *File containing grepable results*: allows for the specification of a file containing line entries in the form of Host : IP address. If the option *Do not scan targets not in the file* is set at the same time only systems contained in the file will be scanned.
- *TCP scanning technique*: actual scan technique.
- *Timing policy*: instead of changing the timing values individually the timing policy can be modified.

²² <https://nmap.org/docs.html>



The timing policy uses the following values:

	Paranoid	Sneaky	Polite	Normal	Aggressive	Insane
initial_rtt_timeout	5 min	15 s	1 s	1 s	500 ms	250 ms
min_rtt_timeout	100 ms	100 ms	100 ms	100 ms	100 ms	50 ms
max_rtt_timeout	10 s	10 s	10 s	10 s	1250 ms	300 ms
max_parallelism	serial	serial	serial	parallel	parallel	parallel
scan_delay	5 min	15 s	400 ms	0 s	0 s	0 s
max_scan_delay	1 s	1 s	1 s	1 s	10 ms	5 ms

10.9.6 Managing Scan Configurations

List Page

All existing scan configurations can be displayed by selecting *Configuration > Scan Configs* in the menu bar (see Fig. 10.36).

For all scan configurations the following information is displayed:

Name Name of the scan configuration.

Type Type of the scan configuration.

Family – Total Number of activated VT families for the scan configuration.

Family – Trend Trend of VT families

↗ New VT families are included and activated automatically after a feed update. This ensures that new VTs are available immediately and without any interaction by the administrator.

→ New VT families are not included automatically after a feed update.

NVTs – Total Number of activated VTs for the scan configuration.

NVTs – Trend Trend of VTs.

↗ New VTs of the activated VT families are included and activated automatically after a feed update. This ensures that new VTs are available immediately and without any interaction by the administrator.

→ New VTs are not included automatically after a feed update.

Note: Greenbone Networks publishes new VTs regularly. New families of VTs can be introduced through the Greenbone Security Feed as well.



Scan Configs 12 of 12

Name ▲	Type	Family		NVTs		Actions
		Total	Trend	Total	Trend	
BSI-TR-03116-4	OpenVAS	5	→	9	→	
Discovery (Network Discovery scan configuration.)	OpenVAS	16	→	2785	↗	
empty (Empty and static configuration template.)	OpenVAS	0	→	0	→	
Full and fast (Most NVTs; optimized by using previously collected information.)	OpenVAS	65	↗	69525	↗	
Full and fast ultimate (Most NVT's including those that can stop services/hosts; optimized by using previously collected information.)	OpenVAS	65	↗	69525	↗	
Full and very deep (Most NVT's; don't trust previously collected information; slow.)	OpenVAS	65	↗	69525	↗	
Full and very deep ultimate (Most NVT's including those that can stop services/hosts; don't trust previously collected information; slow.)	OpenVAS	65	↗	69525	↗	
Host Discovery (Network Host Discovery scan configuration.)	OpenVAS	2	→	2	→	
IT-Grundschutz Scan Aktive Systeme (Version 2)	OpenVAS	2	→	3	→	
IT-Grundschutz Scan Aktive Systeme 2 (Version 2)	OpenVAS	2	→	3	→	
Policy Controls Scan Configuration (Start and verbose the Policy Controls.)	OpenVAS	3	→	3	→	
System Discovery (Network System Discovery scan configuration.)	OpenVAS	6	→	30	→	

Fig. 10.36: Page Scan Configs displaying all available scan configurations

For all scan configurations the following actions are available:

- Move the scan configuration to the trashcan. Only scan configurations which are currently not used can be moved to the trashcan. As long as the scan configuration is not deleted from the trashcan, it is not downloaded anew during the next feed update.
- Edit the scan configuration. Only self-created scan configurations which are currently not used can be edited.
- Clone the scan configuration.
- Export the scan configuration as an XML file.

Note: By clicking or below the list of scan configurations more than one scan configuration can be moved to the trashcan or exported at a time. The drop-down list is used to select which scan configurations are moved to the trashcan or exported.

Details Page

Click on the name of a scan configuration to display the details of the scan configuration. Click to open the details page of the scan configuration.

The following registers are available:

Scanner Preferences All scanner preferences for the scan configuration with current and default values (see Chapter 10.9.4.1 (page 296)).

NVT Families All VT families for the scan configuration with the number of activated VTs and the trend.

NVT Preferences All VT preferences for the scan configuration (see Chapter 10.9.5.1 (page 297)).

User Tags Assigned tags (see Chapter 8.5 (page 214)).

Permissions Assigned permissions (see Chapter 9.4 (page 231)).



The following actions are available in the upper left corner:

- ⓘ Open the corresponding chapter of the user manual.
- ⌂ Show the list page of all scan configurations.
- ⚡ Create a new scan configuration (see Chapter 10.9.2 (page 292)).
- ⌂ Clone the scan configuration.
- ⌂ Edit the scan configuration. Only self-created scan configurations which are currently not used can be edited.
- ⌂ Move the scan configuration to the trashcan. Only scan configurations which are currently not used can be moved to the trashcan. As long as the scan configuration is not deleted from the trashcan, it is not downloaded anew during the next feed update.
- ⌂ Export the scan configuration as an XML file.
- ⌂ Import a scan configuration (see Chapter 10.9.3 (page 295)).

10.10 Performing a Scheduled Scan

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

The GSM does not provide any schedules by default.

10.10.1 Creating a Schedule

A new schedule can be created as follows:

1. Select *Configuration > Schedules* in the menu bar.
2. Create a new schedule by clicking ⚡.
3. Define the schedule (see Fig. 10.37).
4. Click *Save*.
→ The schedule is created and can be selected when creating a new task (see Chapter 10.2.2 (page 251)).

The following details of the schedule can be defined:

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

Comment An optional comment can contain additional information.

Timezone Definition of the timezone the time refers to. UTC is default.

Note: Since the GSM runs in the UTC timezone internally, the chosen time zone is very important. For Eastern Standard Time (EST) America/New York has to be selected.

First Run Definition of the date and time for the first scan to start.

By clicking ⏱ the date can be chosen. By clicking *Now* the current date and time are set for the first run.

Run Until Definition of the date and time for the first scan to end.

By clicking ⏱ the date can be chosen. Activate the checkbox *Open End* to leave the end time open.



The screenshot shows the 'New Schedule' dialog box. It includes fields for Name (Schedule1), Comment, Timezone (Coordinated Universal Time/UTC), First Run (08/08/2019 12:00:00), Run Until (08/08/2019 10:00:00, with 'Open End' checked), Duration (Entire Operation), Recurrence (Custom...), Repeat (Every 2 weeks), and Repeat at (Mo., Tu., We., Th., Fr., Sa., Su.). At the bottom are 'Cancel' and 'Save' buttons.

Fig. 10.37: Creating a new schedule

Duration Definition of the maximum duration a task can take for its execution. The duration depends on the given start and end time. If an end time is defined and the assigned time is expired, the task is aborted and will be suspended until the next scheduled time slot becomes available. This way it can be ensured that the scan will always run with a specific (maintenance) time window.

Recurrence Definition of the repetition rate of the task. It can be selected between *Once*, *Hourly*, *Daily*, *Weekly*, *Monthly*, *Yearly*, *Workweeks (Monday till Friday)* or *Custom*. If the option *Custom* is selected, the repetition rate and the days on which the task should be run can be chosen.

10.10.2 Managing Schedules

List Page

All existing schedules can be displayed by selecting *Configuration > Schedules* in the menu bar.

For all schedules the following information is displayed:

Name Name of the schedule.

First Run Start time of the first run of the task.

Next Run Next run of the task according to the current date and time.

Recurrence Repetition rate of the task.

Duration Maximum duration a task can take for its execution. The duration depends on the given start and end time. If an end time is defined and the assigned time is expired, the task is aborted and will be suspended until the next scheduled time slot becomes available. This way it can be ensured that the scan will always run with a specific (maintenance) time window.

For all schedules the following actions are available:

- Move the schedule to the trashcan. Only schedules which are currently not used can be moved to the trashcan.
- Edit the schedule.
- Clone the schedule.
- Export the schedule as an XML file.



Note: By clicking or below the list of schedules more than one schedule can be moved to the trashcan or exported at a time. The drop-down list is used to select which schedules are moved to the trashcan or exported.

Details Page

Click on the name of a schedule to display the details of the schedule. Click to open the details page of the schedule.

The following registers are available:

Information General information about the schedule.

User Tags Assigned tags (see Chapter 8.5 (page 214)).

Permissions Assigned permissions (see Chapter 9.4 (page 231)).

The following actions are available in the upper left corner:

- Open the corresponding chapter of the user manual.
- Show the list page of all schedules.
- Create a new schedule (see Chapter 10.10.1 (page 301)).
- Clone the schedule.
- Edit the schedule.
- Move the schedule to the trashcan. Only schedules which are currently not used can be moved to the trashcan.
- Export the schedule as an XML file.

10.11 Creating and Managing Scanners

The GSM appliance comes with two predefined scanners. They can be managed and new scanners can be created.

The following scanners are already available:

- OpenVAS Default
- CVE: the CVE scanner allows forecasting possible security risks based on current information about known vulnerabilities from the SeclInfo management (see Chapter 14 (page 384)) without the need of a new scan (see Chapter 10.4 (page 281)).

Note: The desired scanner for a task is selected when creating the task (see Chapter 10.2.2 (page 251)).

10.11.1 Creating a Scanner

Note: The creation of a new scanner is only used in the following cases:

- Creating a new remote scanner (see Chapter 16.4 (page 415))
 - Creating an OSP scanner (see Chapter 18.1 (page 424))
-



10.11.2 Managing Scanners

List Page

All existing scanners can be displayed by selecting *Configuration > Scanners* in the menu bar (see Fig. 10.38).

For all scanners the following actions are available:

- Move the scanner to the trashcan. Only self-created scanners can be moved to the trashcan.
- Edit the scanner. Only self-created scanners can be edited.
- Clone the scanner. Only self-created scanners can be cloned.
- Export the scanner as an XML file.
- Verify that the scanner is online and that the manager can connect to it using the provided certificates and credentials.
- Download the certificate or CA certificate. The certificate or CA certificate can only be downloaded for self-created scanners.

Note: By clicking or below the list of scanners more than one scanner can be moved to the trashcan or exported at a time. The drop-down list is used to select which scanners are moved to the trashcan or exported.

Name	Host	Port	Type	Credential	Actions
CVE	60		CVE Scanner		
OpenVAS Default	60		OpenVAS Scanner		
Scanner_1	localhost	9391	GMP Scanner	Credential1	

Fig. 10.38: Page *Scanners* displaying all existing scanners

Details Page

Click on the name of a scanner to display the details of the scanner. Click to open the details page of the scanner.

The following registers are available:

Information General information about the scanner.

User Tags Assigned tags (see Chapter 8.5 (page 214)).

Permissions Assigned permissions (see Chapter 9.4 (page 231)).

The following actions are available in the upper left corner:

- Open the corresponding chapter of the user manual.
- Show the list page of all scanners.
- Create a new scanner (see Chapter 10.11.1 (page 303)).
- Clone the scanner. Only self-created scanners can be cloned.



- Edit the scanner. Only self-created scanners can be edited.
- Move the scanner to the trashcan. Only self-created scanners can be moved to the trashcan.
- Export the scanner as an XML file.
- Verify that the scanner is online and that the manager can connect to it using the provided certificates.

10.12 Using Alerts

Alerts are anchored within the system. If a configured event (e.g., a task is finished) happens, a specified condition is checked (e.g., vulnerability with a high severity category detected). If the conditions is met, an action is performed, e.g., an e-mail is sent to a defined address.

10.12.1 Creating an Alert

A new alert can be created as follows:

1. Select *Configuration > Alerts*.
2. Create a new alert by clicking .
3. Define the alert (see Fig. 10.39).
4. Click *Save*.

Fig. 10.39: Creating a new alert

The following details of the alert can be defined:

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

Comment An optional comment can contain additional information.



Event Definition of the event for which the alert message is sent. Alerts can be sent if the status of a task changes, if SeclInfo (VTs, CVEs, CPEs, CERT-Bund Advisories, DFN-CERT Advisories, OVAL Definition) is added or updated or if a ticket is assigned or edited (see Chapter 11.6 (page 331)).

Condition Definition of the additional conditions that have to be met.

Note: The options differ for task, for SeclInfo and for ticket related alerts.

The alert message can occur:

- Always
- If a specific severity level is reached.
- If the severity level changes, increases or decreases.
- If a Powerfilter matches at least the specified number of results more than in the previous scan.

Report Content (only for task related alerts) The report content can be limited with an additional filter. By clicking the scan report content composer is opened and a Powerfilter can be chosen (see Chapter 11.2.2 (page 324)). The filter must be created previously (see Chapter 8.4 (page 207)).

Details URL (only for SeclInfo related alerts) Definition of the URL from which the SeclInfo is obtained.

Delta Report (only for task related alerts) Optionally, a delta report can be created, either in comparison to a previous report or to a report with a certain ID.

Method Selection of the method for the alert. Only one method per alert can be chosen. If different alerts for the same event should be triggered, multiple alerts must be created and linked to the same event.

Note: Some methods cannot be used for SeclInfo or ticket related alerts.

The following methods are possible:

Email The report is sent to a given e-mail address.

To use this method the used mail server has to be configured using the GOS administration menu (see Chapter 7.2.10 (page 171)).

The settings *To Address*, *From Address* and *Content* have to be configured for the e-mail alert to work. The e-mail subject and encryption is optional.

- **To Address** E-mail address to which the e-mail is sent.
- **From Address** E-mail address that is stated as the e-mail's sender.
- **Subject** For the subject the following placeholders can be used:
 - \$d: the date of the last SeclInfo check or blank for task/ticket alerts.
 - \$e: the event description.
 - \$n: the task name or blank for SeclInfo/ticket alerts.
 - \$N: the alert name.
 - \$q: the type of SeclInfo event (*New*, *Updated*) or blank for task/ticket alerts.
 - \$s: the SeclInfo type (e.g., *NVT* or *CERT-Bund Advisory*) or blank for task/ticket alerts.
 - \$S: see \$s, but pluralized (e.g., *NVTs*, *CERT-Bund Advisories*) or blank for task/ticket alerts.
 - \$T: the total number of objects in the list for SeclInfo alerts or 0 for task/ticket alerts.
 - \$u: the owner of the alert or the name of the currently logged in user if the alert was triggered manually.



- \$U: the UUID of the alert.
 - \$\$: the dollar sign (\$).
- **Email Encryption** The e-mail can be encrypted using a configurable S/MIME or PGP key. The key can be selected in the drop-down list *Email Encryption* or created by clicking . The certificate files have to fulfill the following conditions:
 - PEM encoded (a binary DER file cannot be used)
 - Using the X.509 format
 - Issued for the recipient e-mail address (*To Address*) and valid (not expired)
 - If the certificate originally came in a bundled format that included the private key as well, only the unencrypted certificate has to be uploaded.

In case of S/MIME credentials, the certificate file additionally has to fulfill the following condition:

- Combines all certificates of the chain (root certificate and all intermediate certificates)
- **Content** The content of the e-mail can be a simple notice, an included or an attached report.
 - **Include Report** The report can be included directly in the e-mail. Any report format that uses a content type starting with *text/* can be chosen because e-mails do not support binary content directly.
 - **Attach Report** The report can be attached to the e-mail. Any report format can be chosen. The report will be attached to the generated e-mail in its correct MIME type.

The content of the e-mail message can be edited for both, the included and the attached report. For the message the following placeholders can be used:

- \$c: the condition description.
- \$d: the date of the last SeclInfo check or blank for task/ticket alerts.
- \$e: the event description.
- \$F: the name of filter.
- \$f: the filter term.
- \$H: the host summary.
- \$i: the report text or list of SeclInfo objects (only if including the report/list).
- \$n: the task name or blank for SeclInfo/ticket alerts.
- \$N: the alert name.
- \$q: the type of SeclInfo event (*New*, *Updated*) or blank for task/ticket alerts.
- \$r: the name of the report format.
- \$s: the SeclInfo type (e.g., *NVT* or *CERT-Bund Advisory*) or blank for task/ticket alerts.
- \$S: see \$s, but pluralized (e.g., *NVTs*, *CERT-Bund Advisories*) or blank for task/ticket alerts.
- \$t: the note if the report was truncated.
- \$T: the total number of objects in the list for SeclInfo alerts or 0 for task/ticket alerts.
- \$u: the owner of the alert or the name of the currently logged in user if the alert was triggered manually.
- \$U: the UUID of the alert.
- \$z: the timezone.
- \$\$: the dollar sign (\$).



HTTP Get The URL is issued as HTTP Get. For example, an SMS text message can be sent via HTTP Get gateway or a bug report can be created in an issue tracker. For the URL the following placeholders can be used:

- \$n: the task name or blank for SecInfo/ticket alerts.
- \$e: the event description.
- \$c: the condition description.
- \$\$: the dollar sign (\$).

Example: `https://example.com/$n` → `https://example.com/Scan_task_1`

SCP The report is copied to the given destination via Secure Copy Protocol (SCP) using the given login credentials for authentication.

All settings (*Credential*, *Host*, *Known Hosts*, *Path* and *Report*) have to be configured for the SCP alert to work.

- **Credential** A user name and password or user name and SSH key credential that contains valid login information for the destination system.
- **Host** The host name or IP address of the destination system. Only one destination system per SCP alert is supported.
- **Known Hosts** The SSH public key of the destination system in the format “host protocol public_key”, e.g., `localhost ssh-rsa AAAAB3NzaC1y...P3pCquVb`. The “host” part must match the host name or IP address respectively.
- **Path** The full path of the destination directory and file, e.g., `/home/user/Downloads/report.xml`. Shortening the path, e.g., by using `~` is not supported. For the file name the following placeholders can be used:
 - \$\$: the dollar sign (\$).
 - \$n: the task name.
- **Report** Format of the copied report.

Send to host The report is sent to an arbitrary host-port combination via TCP. The IP address or the host name is allowed.

The format of the report can be chosen from the installed report formats.

SMB The report is copied to the given destination via Server Message Block (SMB) protocol using the given login credentials for authentication.

The settings *Credential*, *Share path* and *File path* have to be configured for the SMB alert to work. The selection of a report format is optional.

- **Credential** A user name and password credential that contains valid login information for the destination system.
- **Share path** The share path contains the part of the UNC path containing the host and the share name, e.g., `\host\share`. The share path has to be created on the destination system before the alert can be used.
- **File path** Location of the report in the share folder that is defined by the share path.

Note: If the file path contains subdirectories which do not exist, the necessary subdirectories are created.

The file extension is appended corresponding to the format selected in the drop-down list *Report Format*.



The default report export file name (see Chapter 8.8 (page 218)) is appended to the file path if the file path ends with \.

Note: If a task uses the tag `smb-alert:file_path` with a value, then the value is used as the file path instead of the one that has been configured with the alert (see Chapter 8.5 (page 214)). Example: `smb-alert:file_path=alert_1` assigns the file path `alert_1`.

For the file path the following placeholders can be used:

- %C: the creation date in the format YYYYMMDD. Changed to the current date if a creation date is not available.
- %c: the creation time in the format HHMMSS. Changed to the current time if a creation time is not available.
- %D: the current date in the format YYYYMMDD.
- %F: the name of the used report format (XML for lists and types other than reports).
- %M: the modification date in the format YYYYMMDD. Changed to the creation date or to the current date if a modification date is not available.
- %m: the modification time in the format HHMMSS. Changed to the creation time or to the current time if a modification time is not available.
- %N: the name for the object or the associated task for reports. Lists and types without a name will use the type (see %T).
- %T: the object type, e.g., “task”, “port_list”. Pluralized for list pages.
- %t: the current time in the format HHMMSS.
- %U: the unique ID of the object or “list” for lists of multiple objects.
- %u: the name of the currently logged in user.
- %%: the percent sign (%).

- **Report Format** Format of the copied report. If no report format is defined, XML is used by default.

SNMP An SNMP trap is sent to the given agent. The provided community string is used to authenticate the SNMP trap. The agent is the targeted SNMP trap receiver. For the message the following placeholders can be used:

- \$\$: the dollar sign (\$).
- \$d: the date of the last SecInfo check or blank for task/ticket alerts.
- \$e: the event description.
- \$n: the task name or blank for SecInfo/ticket alerts.
- \$q: the type of SecInfo event (*New*, *Updated*) or blank for task/ticket alerts.
- \$s: the SecInfo type (e.g., *NVT* or *CERT-Bund Advisory*) or blank for task/ticket alerts.
- \$S: see \$s, but pluralized (e.g., *NVTs*, *CERT-Bund Advisories*) or blank for task/ticket alerts.
- \$T: the total number of objects in the list for SecInfo alerts or 0 for task/ticket alerts.

Sourcefire Connector The data can be sent to a Cisco Firepower Management Center (formerly known as Sourcefire Defense Center) automatically. For more information see Chapter 18.4 (page 432).

Start Task The alert can start an additional task. The task is selected in the drop-down list.



System Logger The alert is sent to a Syslog daemon. The Syslog server is defined using the GOS administration menu (see Chapter 7.2.11 (page 173)).

verinice.PRO Connector The data can be sent to a verinice.PRO installation automatically. For more information see Chapter 18.2 (page 424).

TippingPoint SMS An HTTPS API is used to upload a report in CSV format to the TippingPoint Security Management System (SMS).

- **Hostname / IP** The CSV report is sent to `https://$SMS_ADDRESS/vulnscanner/import` where `$SMS_ADDRESS` is replaced by the host name/IP address from the input field.
- **Credentials** A user name and password credential that contains valid login information for the TippingPoint SMS.
- **SSL / TLS Certificate** A CA certificate used to verify that the host the alert connects to is the TippingPoint SMS.
- **Use workaround for default certificate** By default, the certificate uses *Tippingpoint* as the common name (CN) which does not match the host name/IP address of the TippingPoint SMS in most cases. If enabled, the workaround temporarily changes the CN and resolves it to the actual host name/IP address within the internal connector script.

Alemba vFire A new ticket in the service management application vFire is created. The report can be attached in one or more formats. For more information see Chapter 18.5 (page 434).

10.12.2 Assigning an Existing Alert to a Task

If an alert should be used afterwards, the alert has to be defined for a specific task as follows:

Note: Already defined and used tasks can be edited as well as it does not have any effect on already created reports.

1. Select *Scans > Tasks* in the menu bar.
2. In the row of the task click .
3. Select the alert in the drop-down list *Alerts* (see Fig. 10.40).

Note: A new alert can be created by clicking .

4. Click *Save*.
→ Afterwards the task using the alert appears on the details page of the alert (see Fig. 10.41).

10.12.3 Managing Alerts

List Page

All existing alerts can be displayed by selecting *Configuration > Alerts* in the menu bar.

For all alerts the following information is displayed:

Name Name of the alert.

Event Event for that the alert is triggered.

Condition Condition that has to be fulfilled to trigger the alert.



Edit Task DMZ Mail Scan

Name	DMZ Mail Scan
Comment	
Scan Targets	Target1
Alerts	
Schedule	
Add results to Assets	Dispatch reports via e-mail
Apply Overrides	<input checked="" type="radio"/> Yes <input type="radio"/> No
Min QoD	70
Alterable Task	<input type="radio"/> Yes <input checked="" type="radio"/> No
Auto Delete Reports	<input checked="" type="radio"/> Do not automatically delete reports <input type="radio"/> Automatically delete oldest reports but always keep newest 5 reports
Scanner	OpenVAS Default
Scan Config	Full and fast

Cancel **Save**

Fig. 10.40: Configuring a task with an alert

Alert: Dispatch reports via e-mail

Information	User Tags (0)	Permissions (0)
Condition	Always	
Event	Task run status changed to Done	
Email	To address	mail@example.com
Method	From address	gsm@example.com
	Content	Simple Notice
	Subject	[GVM] Task '\$n': \$e
Results Filter	filter1	
Active	Yes	
Task using this Alert DMZ Mail Scan		

Fig. 10.41: Task using a specific alert



Method Chosen alert method with additional information, e.g., to which IP address or e-mail address the alert message is sent.

Filter (only for task related alerts) Filter that is applied to the report content.

Active Indication whether the alert is enabled or disabled.

For all alerts the following actions are available:

- Move the alert to the trashcan. Only alerts which are currently not used can be moved to the trashcan.
- Edit the alert.
- Clone the alert.
- Export the alert as an XML file.
- Test the alert.

Note: By clicking or below the list of alerts more than one alert can be moved to the trashcan or exported at a time. The drop-down list is used to select which alerts are moved to the trashcan or exported.



Details Page

Click on the name of an alert to display the details of the alert. Click to open the details page of the alert.

The following registers are available:

Information General information about the alert.

User Tags Assigned tags (see Chapter 8.5 (page 214)).

Permissions Assigned permissions (see Chapter 9.4 (page 231)).

The following actions are available in the upper left corner:

- Open the corresponding chapter of the user manual.
- Show the list page of all alerts.
- Create a new alert (see Chapter 10.12.1 (page 305)).
- Clone the alert.
- Edit the alert.
- Move the alert to the trashcan. Only alerts which are currently not used can be moved to the trashcan.
- Export the alert as an XML file.

10.13 Obstacles While Scanning

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

10.13.1 Hosts not Found

During a typical scan (either *Discovery* or *Full and fast*) the GSM will by default first use the ping command to check the availability of the configured targets. If the target does not reply to the ping request it is presumed to be dead and will not be scanned by the port scanner or any VT.

In most LAN environments this does not pose any problems because all devices will respond to a ping request. But sometimes (local) firewalls or other configuration might suppress the ping response. If this happens the target will not be scanned and will not be included in the results and the scan report.

To remediate this problem, both the target configuration and the scan configuration support the setting of the alive test (see *Alive Test* (page 250)).

If the target does not respond to a ping request, a TCP ping may be tested. If the target is located within the same broadcast domain, an ARP ping may be tried as well.

10.13.2 Long Scan Periods

Once the target is discovered to be alive using the ping command the GSM uses a port scanner to scan the target. By default, a TCP port list containing around 5000 ports is used. If the target is protected by a (local) firewall dropping most of these packets the port scan will need to wait for the timeout of each individual port. If the hosts are protected by (local) firewalls the port lists or the firewalls may be tuned. If the firewall does not drop the request but rejects the request the port scanner does not have to wait for the timeout. This is especially true if UDP ports are included in the scan.



10.13.3 VT not Used

This happens especially very often if UDP based VTs like VTs using the SNMP protocol are used. If the default configuration *Full and fast* is used, the SNMP VTs are included. But if the target is configured using the default port list, the VTs are not executed. This happens because the default port list does not include any UDP ports. Therefore, the port 161/udp (SNMP) is not discovered and excluded from further scans. Both the discovery scans and the recommended scan configuration *Full and fast* optimize the scan based on the discovered services. If the UDP port is not discovered, no SNMP VTs are executed.

Do not enable all ports per default in the port lists. This will prolong the scans considerably. Best practice is the tuning of the port lists to the ports which are used in the environment and are supported by the firewalls.

10.13.4 Scanning vhosts

The scanner is able to find all relationships of host names and IP addresses without needing additional user input.

In environments with virtual hosts, the scan reports will have less results because duplicates are avoided.

Two scanner preferences handle vhost scanning (see Chapter 10.9.4 (page 295)):

test_empty_vhost If this preference is enabled, the scanner also tests the target by using empty vhost values in addition to the target's associated vhost values.

expand_vhosts If this preference is enabled, the target's host list of vhosts is expanded with values gathered from sources such as reverse lookup queries and VT checks for SSL/TLS certificates.

Reports and Vulnerability Management

Note: This chapter documents all possible menu options.

However, not all GSM models support all of these menu options. Check the tables in Chapter 3 (page 18) to see whether a specific feature is available for the used GSM model.

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

The GSM saves all reports of all scans in a local database. Not only is the last report of a scan saved but all reports of all scans ever run. This allows access to information from the past. The reports contain the discovered vulnerabilities and information of a scan.

Once a scan has been started, the report of the results found so far can be viewed. When a scan is completed, the status changes to *Done* and no more results will be added.

11.1 Configuring and Managing Report Formats

Report formats are defined as the formats a report is created from, based on the scan results. Many report formats reduce the available data in order to display it in a meaningful way.

The report formats can be used to export report information into other document formats so they can be processed by other third party applications (connectors).

The name of the exported report is configurable in the user settings (see Chapter 8.8 (page 218)).

The native GSM XML format contains all data and can be used to import exported reports on another GSM. To do so, create a container task (see Chapter 10.5 (page 283)).

Greenbone Networks supports the creation of additional report formats via report format plug-ins. Requests, suggestions and concrete templates are welcome.

The report format plug-in framework has the following properties:

Simple import/export A report format plug-in is always a single XML file. The import can be performed easily.



Parameterized Plug-ins can contain parameters that can be used to adapt the plug-in to specific requirements using the web interface.

Content type For every plug-in it is determined of which type the result is. Depending on the content type the plug-ins are displayed in contextual relation. For example, the types `text/*` for the sending as e-mail inline.

Signature support The Greenbone Security Feed provides signatures for trusted plug-ins. By that it can be verified that an imported plug-in was verified by Greenbone Networks.

11.1.1 Default Report Formats

All default report formats by Greenbone Networks are data objects that are distributed via the feed. They are downloaded and updated with each feed update.

If no default report formats are available, a feed update may be necessary, or the Feed Import Owner may need to be set (see Chapter 7.2.1.9.1 (page 130)).

Default report formats cannot be edited. Furthermore, they can only be deleted temporarily by the Feed Import Owner or by a super administrator. During the next feed update, they will be downloaded again.

Note: To permanently delete a default report format, the Feed Import Owner has to delete it. Afterwards the Feed Import Owner has to be changed to `(Unset)` (see Chapter 7.2.1.9.1 (page 130)).

By default, the following report formats are available:

Anonymous XML This is the anonymous version of the XML format. IP addresses are replaced by random IP addresses.

ARF: Asset Reporting Format v1.0.0 This format creates a report that represents the NIST Asset Reporting Format.

CPE – Common Platform Enumeration CSV Table This report selects all CPE tables and creates a single comma-separated file.

CSV Hosts This report creates a comma-separated file containing the systems discovered.

CSV Results This report creates a comma-separated file with the results of a scan.

GCR PDF – Greenbone Compliance Report This is the complete Greenbone Compliance Report for compliance audits (see Chapter 12.2 (page 352)) with all vulnerabilities in graphical format as a PDF file. The language of the report is English.

GSR HTML – Greenbone Security Report This is the complete Greenbone Security Report with all vulnerabilities and results. It can be opened with any web browser and contains dynamically sortable lists as known from the web interface. The language of the report is English.

GSR PDF – Greenbone Security Report This is the complete Greenbone Security Report with all vulnerabilities in graphical format as a PDF file. The topology graph is not included if more than 100 hosts are covered in the report. The language of the report is English.

GXCR PDF – Greenbone Executive Compliance Report This is the shortened Greenbone Compliance Report for compliance audits (see Chapter 12.2 (page 352)) with all vulnerabilities in graphical format as a PDF file for management. The language of the report is English.

GXR PDF – Greenbone Executive Report This is the shortened Greenbone Security Report with all vulnerabilities in graphical format as a PDF file for management. The topology graph is not included if more than 100 hosts are covered in the report. The language of the report is English.

ITG – IT-Grundschutz catalog This report is guided by the BSI IT-Grundschutz catalog. It provides an overview of the discovered results in tabular view in CSV format. The language of the report is German.



LaTeX This report is offered as LaTeX source text. The language of the report is English.

NBE This is the old OpenVAS/Nessus report format. It does not have support for notes, overrides and some additional information.

PDF This is a complete report in PDF. Like the HTML format it is neutral. The language of the report is English.

TLS Map This is the report format for TLS Map scans (see Chapter 12.6 (page 376)).

Topology SVG This presents the results in an SVG picture.

TXT This creates a text file. This format is especially useful when being sent by e-mail. The language of the report is English.

Verinice ISM Creates an import file for the ISMS tool *verinice* (see Chapter 18.2 (page 424)).

Verinice ITG (obsolete) Creates an import file for the ISMS tool *verinice* (see Chapter 18.2 (page 424)).

Vulnerability Report HTML (recommended) This is the new complete Greenbone Security Report with all vulnerabilities and results. It can be opened with any web browser. The language of the report is English.

Vulnerability Report PDF (recommended) This is the new complete Greenbone Security Report with all vulnerabilities in graphical format as a PDF file. The language of the report is English.

Reports with this report format are limited to the first 500 results per host. Subsequent results per host will be left out and a warning will be shown on the title page of the report.

XML The report is exported in the native XML format. Contrary to the other formats this format contains all results and does not format them at all.

11.1.2 Managing Report Formats

List Page

All existing report formats can be displayed by selecting *Configuration > Report Formats* in the menu bar.

For all report formats the following information is displayed:

Name Name of the report format.

Extension The file name of the downloaded report consists of the UUID (unique internal ID of the report) and this extension. Among others, the extension supports the browser to start a compatible application in case the specified content type is not recognized.

Content Type The content type specifies the format in use and is transmitted when being downloaded. By this, a compatible application can be launched by the browser.

Additionally, the content type is important internally: it is used to offer suitable plug-ins within its context. For example, when sending a report via e-mail all plug-ins of the type `text/*` are offered as they can be embedded in an e-mail in a humanly readable way.

Trust Some report formats only convert data, while others perform more complex operations and also execute programs. To prevent abuse, each report format plug-in has to be digitally signed by Greenbone Networks. The digital signatures are distributed via the Greenbone Security Feed. If a signature is authentic and the publisher is trusted, it is ensured that the report format exists in the exact format as certified by the publisher. The trust check is automatic and the result can be seen in the column *Trust (Last Verified)*.

Active The report formats are only available in the respective selection menus if they are activated. Newly imported report formats are always deactivated at first. A report format can only be activated if it is trusted.

For all report formats the following actions are available:

- Move the report format to the trashcan. As long as the report format is not deleted from the trashcan, it is not downloaded anew during the next feed update.



- Edit the report format. Only self-created report formats can be edited.

Note: By clicking  below the list of report formats more than one report format can be moved to the trashcan at a time. The drop-down list is used to select which report formats are moved to the trashcan.

Details Page

Click on the name of a report format to display the details of the report format. Click  to open the details page of the report format.

The following actions are available in the upper left corner:

-  Open the corresponding chapter of the user manual.
-  Show the list page of all report formats.
- Add a new report format (see Chapter 11.1.3 (page 318)).
- Edit the report format. Only self-created report formats can be edited.
-  Move the report format to the trashcan. As long as the report format is not deleted from the trashcan, it is not downloaded anew during the next feed update.



Report Formats 21 of 21

Name	Extension	Content Type	Trust (Last Verified)	Active	Actions
Anonymous XML (Anonymous version of the raw XML report)	xml	text/xml	Yes (11/27/2019)	Yes	 <input checked="" type="checkbox"/>
ARF (Asset Reporting Format v1.0.0.)	xml	text/xml	Yes (11/27/2019)	Yes	 <input checked="" type="checkbox"/>
CPE (Common Platform Enumeration CSV table.)	csv	text/csv	Yes (11/27/2019)	Yes	 <input checked="" type="checkbox"/>
CSV Hosts (CSV host summary.)	csv	text/csv	Yes (11/27/2019)	Yes	 <input checked="" type="checkbox"/>
CSV Results (CSV result list.)	csv	text/csv	Yes (11/27/2019)	Yes	 <input checked="" type="checkbox"/>
GCR PDF (Greenbone Compliance Report.)	pdf	application/pdf	Yes (11/27/2019)	Yes	 <input checked="" type="checkbox"/>
GSR HTML (Greenbone Security Report (HTML).)	html	text/html	Yes (11/27/2019)	Yes	 <input checked="" type="checkbox"/>
GSR PDF (Greenbone Security Report.)	pdf	application/pdf	Yes (11/27/2019)	Yes	 <input checked="" type="checkbox"/>

Fig. 11.1: Page *Report Formats* displaying all available report formats

11.1.3 Adding a Report Format

Note: To prevent abuse, all additionally imported report formats have to be reviewed and digitally signed by Greenbone Networks. Report formats that are not signed by Greenbone Networks are not supported in GOS, and cannot be used.

For more information see Chapter 11.1.2 (page 317) – *Trust*.

A new report format can be imported as follows:

1. Provide or obtain a report format plug-in that has been reviewed and accepted by Greenbone Networks.



2. Select *Configuration > Report Formats* in the menu bar.
3. Click .
4. Click *Browse...* and select the report format plug-in (see Fig. 11.2).

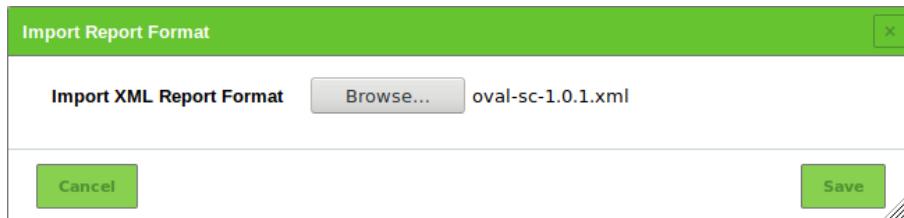


Fig. 11.2: Importing a report format plug-in

5. Click *Save*.
→ The imported report format is displayed on the page *Report Formats*.
6. In the row of the report format click .
7. For *Active* select the radio button *Yes* (see Fig. 11.3).
8. Click *Save*.



Fig. 11.3: Activating a new report format

11.2 Using and Managing Reports

All existing reports for all scans can be displayed by selecting *Scans > Reports* in the menu bar.

The total number of reports of a specific task is displayed on the page *Tasks* in the column *Reports*.

The reports for a specific task can be displayed as follows:

1. Select *Scans > Tasks* in the menu bar.
2. For the desired task click on the total number of reports in the column *Reports* to display all reports.
→ The page *Reports* is opened. A filter is applied to show only the reports for the selected task.

Tip: By clicking on the date in the column *Last Report* the details page of the latest report is opened (see Chapter 11.2.1 (page 320)).

For every report the following information is displayed:

Date Date and time of report creation.

Status Status of the corresponding task.



Reports	Last Report
1	Mon, Jun 17, 2019 1:13 PM UTC
3	Mon, Jun 17, 2019 1:14 PM UTC

Fig. 11.4: Number of reports saved in total and date of the last report

Task Corresponding task.

Severity Highest severity found by the scan.

High/Medium/Low/Log/False Pos. Number of found vulnerabilities for each severity.

For all reports the following actions are available:

- Create a delta report (see Chapter 11.2.5 (page 326)).
- Delete the report.

Note: By clicking below the list of reports more than one report can be deleted at a time. The drop-down list is used to select which reports are deleted.

11.2.1 Reading a Report

Click on the date of a report to display the details of the report.

The following registers are available:

Information General information about the corresponding scan.

Results List of all results in this report (see Chapter 11.2.1.1 (page 321)).

Hosts Scanned hosts with host names and IP addresses. The detected operating systems, the number of found vulnerabilities for each severity and the highest severity found by the scan are displayed.

Ports Scanned ports with port name, number of hosts and highest severity found by the scan.

Applications Scanned applications with CPE of the application, number of hosts, number of occurrences of results that detected this CPE and highest severity found by the scan.

Operating Systems Scanned operating systems with system name, host name, number of scanned hosts and highest severity found by the scan.

CVEs CVEs found with the scan.

Closed CVEs CVEs of originally detected vulnerabilities which were already confirmed as solved during the scan.

TLS Certificates TLS certificates found with the scan.

Error Messages Error messages that occurred during the scan.

User Tags Assigned tags (see Chapter 8.5 (page 214)).

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

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



The following actions are available in the upper left corner:

- ⓘ Open the corresponding chapter of the user manual.
- ⚡ Show the list page of all report formats.
- + Add the report contents that have at least a QoD of 70 % and enabled overrides to the assets.
- - Remove the report contents from the assets.
- ⌂ Show the corresponding task.
- ⓘ Open the page *Results*. A filter is applied to show only the results for this report.
- ⚡ Open the page *Vulnerabilities*. A filter is applied to show only the vulnerabilities for this report.
- ⓘ Open the page *TLS Certificates*. A filter is applied to show only the TLS certificates for this report.
- ⚡ Open the page *Performance*. The system performance for the scan's duration is displayed.
- ⬇ Download a filtered report (see Chapter 11.2.2 (page 324)).
- ⚡ Trigger an alert to send a report (see Chapter 11.2.4 (page 325)).

11.2.1.1 Results of a Report

The register *Results* contains a list of all vulnerabilities detected by the GSM (see Fig. 11.5).

Information	Results (241 of 381)	Hosts (11 of 11)	Ports (20 of 20)	Applications (2 of 2)	Operating Systems (1 of 1)	CVEs (1 of 1)	Closed CVEs (0 of 0)	TLS Certificates (1 of 1)	Error Messages (0 of 0)	User Tags (0)
◀ ◀ 1 - 100 of 241 ▶ ▶										
Vulnerability	Severity	QoD	Host IP	Name	Location	Created				
OpenVAS Framework Components End Of Life Detection	10.0 (High)	80 %	192.168.117.12	scan-target.greenbone.net	general/tcp	Thu, Oct 18, 2018 2:09 PM UTC				
OS End Of Life Detection	10.0 (High)	80 %	192.168.126.4	scan-target-3.greenbone.net	general/tcp	Thu, Oct 18, 2018 2:07 PM UTC				
OS End Of Life Detection	10.0 (High)	80 %	192.168.117.12	scan-target.greenbone.net	general/tcp	Thu, Oct 18, 2018 2:08 PM UTC				
Anonymous FTP Login Reporting	6.4 (Medium)	80 %	192.168.126.52		21/tcp (IANA: ftp)	Thu, Oct 18, 2018 2:12 PM UTC				
Cleartext Transmission of Sensitive Information via HTTP	4.8 (Medium)	80 %	192.168.0.127	scan-target-4.greenbone.net	80/tcp (IANA: www-https)	Thu, Oct 18, 2018 2:09 PM UTC				
SSH Weak Encryption Algorithms Supported	4.3 (Medium)	95 %	192.168.116.4		22/tcp (IANA: ssh)	Thu, Oct 18, 2018 2:07 PM UTC				
SSH Weak Encryption Algorithms Supported	4.3 (Medium)	95 %	192.168.0.12	scan-target-2.greenbone.net	22/tcp (IANA: ssh)	Thu, Oct 18, 2018 2:11 PM UTC				
SSH Weak MAC Algorithms Supported	2.6 (Low)	95 %	192.168.116.9		22/tcp (IANA: ssh)	Thu, Oct 18, 2018 2:07 PM UTC				

Fig. 11.5: Register *Results* showing a list of discovered vulnerabilities

Note: By default, overrides are not applied. They can be applied by filtering the report (see Chapter 11.2.1.3 (page 323)).

For every result the following information is displayed:

Vulnerability Name of the found vulnerability. By clicking on the name of a vulnerability details of the vulnerability are shown (see Fig. 11.6). The details page of the vulnerability is opened by clicking ⓘ.

Vulnerabilities with an attached note are marked with ⓘ. Vulnerabilities with an attached ticket are marked with ⓘ.



Note: If the column of the vulnerability still appears empty the respective VT has not been updated yet.

CPE Inventory

⊕ **Summary**

This routine uses information collected by other routines about CPE identities of operating systems, services and applications detected during the scan.

Detection Result

192.168.178.33|cpe:/a:openbsd:openssh:7.4p1
192.168.178.33|cpe:/o:debian:debian_linux:9

Detection Method

Details: CPE Inventory OID: 1.3.6.1.4.1.25623.1.0.810002
Version used: 2019-03-19T13:31:53Z

Fig. 11.6: Detailed information about the vulnerability

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

- A vendor patch is available.
- A workaround is available.
- A mitigation by configuration is available.
- No fix is and will be available.
- No solution exists.

Severity The severity of the vulnerability (CVSS, see Chapter 14.2.4 (page 393)) is displayed as a bar to support the analysis of the results.

QoD QoD is short for Quality of Detection and shows the reliability of the detection of a vulnerability. The QoD was introduced with GOS 3.1. Results created with earlier versions are assigned a QoD of 75 % during migration.

By default, only results that were detected by VTs 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 8.4.1 (page 207)).

Host Host for which the result was found. The IP address and the name of the host are displayed separately.

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

Created Date and time of the report creation.

11.2.1.2 Interpreting a Report

To interpret the results note the following information:

- **False Positives** A false positive is a finding that describes a problem that does not really exist. Vulnerability scanners often find evidence that point at a vulnerability but a final judgment cannot be made. There are two options available:
 - Reporting of a potentially non-existent vulnerability (false positive).
 - Ignoring reporting of a potentially existing vulnerability (false negative).



Since a user can identify, manage and as such deal with false positives compared to false negatives, the GSM vulnerability scanner reports all potentially existing vulnerabilities. If the user knows that false positives exist an override can be configured (see Chapter 11.8 (page 338)).

- **Multiple findings can have the same cause.** If an especially old software package is installed, often multiple vulnerabilities exist. Each of these vulnerabilities is tested by an individual VT and causes an alert. The installation of a current package will remove a lot of vulnerabilities at once.
- **High [High] and Medium [Medium]** Findings of the severity levels *High* and *Medium* are most important and should be addressed with priority. Before addressing medium level findings, high level findings should get addressed. Only in exceptional cases this approach should be deviated from, e.g., if it is known that the high level findings need to be less considered because the service cannot be reached through the firewall.
- **Low [Low] and Log [Log]** Findings of the severity levels *Low* and *Log* are mostly interesting for detail understanding. These findings are filtered out by default but can hold very interesting information. Considering them will increase the security of the network and the systems. Often a deeper knowledge of the application is required for their understanding. Typical for a result with the severity *Log* is that a service uses a banner with its name and version number. This could be useful for an attacker when this version has a known vulnerability.

11.2.1.3 Filtering a Report

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

The report can be filtered as follows:

1. Click in the filter bar.
2. Enter a keyword which should be searched for in the input box *Filter* (see Fig. 11.7).

Fig. 11.7: Adjusting the filter for the report



3. For *Apply Overrides* select the radio button *Yes* to enable overrides (see Chapter 11.8 (page 338)).
For *Apply Overrides* select the radio button *No* to disable overrides.
4. Activate the checkbox *Only show hosts that have results* if only the hosts with results should be included.
5. For *QoD* select the desired QoD.
6. For *Severity (Class)* activate the checkboxes of the desired severity classes.
7. For *Solution Type* select the radio buttons of the desired solution types.
8. Enter the (part of a) vulnerability's name, host or location in the according input box.
9. Click *Update*.

11.2.2 Exporting a Report

For supported export formats see Chapter 11.1 (page 315).

A report can be exported as follows:

1. Select *Scans > Reports* in the menu bar.
2. Click on the date of a report to open the details page of the report.
3. Click ↓.
→ The scan report content composer is opened (see Fig. 11.8).

Note: The applied filter is displayed in the input box *Filter* and cannot be changed. For changing the filter see Chapter 11.2.1.3 (page 323).



Fig. 11.8: Composing the content of a report export

4. For *Include* activate the checkbox *Notes* to include attached notes and the checkbox *Overrides* to label enabled overrides and include their text field.
- Note:** Overrides are only considered if they are enabled when filtering the report (see Chapter 11.2.1.3 (page 323)).
5. Select the report format in the drop-down list *Report Format*.
6. Activate the checkbox *Store as default* to save the settings for future exports.
7. Click *OK*.
8. Save the report by clicking *Save File*.



11.2.3 Importing a Report

Reports can be imported to the GSM as follows:

1. Select *Scans > Reports* in the menu bar.
2. Click .
3. Click *Browse...* and select the XML file of a report (see Fig. 11.9).

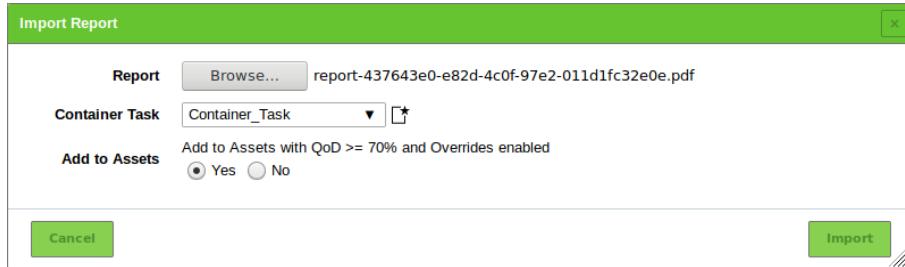


Fig. 11.9: Importing a report

4. Select the container task to which the report should be added in the drop-down list *Container Task*.

Tip: By clicking a new container task can be created (see Chapter 10.5 (page 283)).

5. Select the radio button *Yes* to add the report to the assets.
6. Click *Import*.

11.2.4 Triggering an Alert for a Report

Often an alert includes the sending of a report. The report sent by an alert is subject to a filter defined in the alert content composer (see Chapter 10.12 (page 305)). Triggering an alert for a report adds a second filter originating from the scan report content composer (see Chapter 11.2.2 (page 324)).

The alert can be triggered manually as follows:

1. Select *Scans > Reports* in the menu bar.
2. Click on the date of a report to show the results.
3. Filter the report so that only the results that should be sent are displayed by using the Powerfilter (see Chapter 11.2.1.3 (page 323)) or selecting a register.

Note: The filter that is configured in the alert content composer (see Chapter 10.12 (page 305)) is applied additionally.

To mimic the behaviour of this filter, adjust the filter of the report in a way that no results are filtered out.

4. Click .
- The scan report content composer is opened (see Fig. 11.8).

Note: The applied filter for displaying the results is entered in the input box *Filter* and cannot be changed. For changing the filter see Chapter 11.2.1.3 (page 323).



5. For *Include* activate the checkbox *Notes* to include attached notes and the checkbox *Overrides* to label enabled overrides and include their text field.

Note: Overrides are only considered if they are enabled when filtering the report (see Chapter 11.2.1.3 (page 323)).

6. Select the alert in the drop-down list *Alert*.

Tip: A new alert can be created by clicking . For the information to enter in the input boxes see Chapter 10.12 (page 305).

7. Activate the checkbox *Store as default* to save the settings for future sendings of the report.

8. Click *OK*.

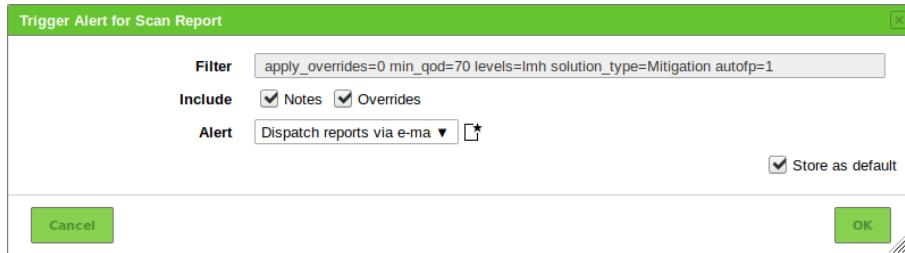


Fig. 11.10: Triggering an alert manually

11.2.5 Creating a Delta Report

If more than one report of a single task is available (see Chapter 11.2 (page 319)) a delta report can be created as follows:

1. Select *Scans > Tasks* in the menu bar.
2. Click on the total number of reports in the column *Reports*.
→ The page *Reports* is opened. A filter is applied to show only the reports for the selected task.
3. Select the first report by clicking in the column *Actions* of the respective report (see Fig. 11.11).
→ The icon is grayed out for the selected report.

Date ▾	Status	Task	Severity	High	Medium	Low	Log	False Pos.	Actions
Fri, Jul 12, 2019 1:00 PM UTC	Done	DMZ Mail Scan	4.8 (Medium)	0	3	0	129	0	
Mon, Jun 17, 2019 2:24 PM UTC	Done	DMZ Mail Scan	10.0 (High)	4	10	3	158	0	

Fig. 11.11: Selecting the first report

4. Select the second report by clicking in the column *Actions* of the respective report (see Fig. 11.12).
→ The delta report with the delta results is displayed (see Fig. 11.13) and can be exported.



Date ▼	Status	Task	Severity	High	Medium	Low	Log	False Pos.	Actions
Fri, Jul 12, 2019 1:00 PM UTC	Done	DMZ Mail Scan	4.8 (Medium)	0	3	0	129	0	△ X
Mon, Jun 17, 2019 2:24 PM UTC	Done	DMZ Mail Scan	10.0 (High)	4	10	3	158	0	▲ X

(Applied filter: apply_overrides=0 min_qod=70 task_id=32c5f618-cd56-4ff-bb69-0a833cb0a79b sort-reverse=date first=1 rows=10) [Apply to page contents ▾] [Print] [X]

Fig. 11.12: Selecting the second report

1 - 34 of 35 ▶▶							
Delta	Vulnerability	Severity ▼	QoD	Host IP	Name	Location	Created
[=]	SSL/TLS: HTTP Strict Transport Security (HSTS) Missing	10.0 (High)	100 %	192.168.0.12		443/tcp	Fri, Aug 16, 2019 8:07 AM UTC
[+]	OS End Of Life Detection	10.0 (High)	80 %	192.168.126.4		general/tcp	Fri, Aug 16, 2019 7:44 AM UTC
[+]	SSH Brute Force Logins With Default Credentials Reporting	7.5 (High)	95 %	192.168.117.12		22/tcp	Fri, Aug 16, 2019 7:52 AM UTC
[~]	TCP timestamps	2.6 (Low)	80 %	127.0.0.8		general/tcp	Fri, Aug 16, 2019 8:05 AM UTC
[-]	SSL/TLS: Hostname discovery from server certificate	0.0 (Log)	98 %	192.168.0.127		general/tcp	Fri, Aug 16, 2019 8:05 AM UTC

Fig. 11.13: Delta report with delta results

The type of the delta result is displayed in the column *Delta*. There are four types of delta results:

- **Gone [-]** The result exists in the first report but not in the second report (according to order of selection).
- **New [+]** The result exists in the second report but not in the first report (according to order of selection).
- **Same [=]** The result exists in both reports and is equal.
- **Changed [~]** The result exists in both reports but is different.

The term `delta_states=` can be entered into the filter bar to show only a specific type of delta results (see Chapter 8.4 (page 207)).

- `delta_states=g` shows all results of the type *Gone*.
- `delta_states=n` shows all results of the type *New*.
- `delta_states=s` shows all results of the type *Same*.
- `delta_states=c` shows all results of the type *Changed*.

Tip: Multiple types can be displayed at the same time, e.g., `delta_states=gs` shows all results of the type *Gone* and *Same*.



11.3 Displaying all Existing Results

List Page

While the reports only contain the results of one single scan, all results are saved in the internal database and can be viewed by selecting *Scans > Results* in the menu bar.

Powerfilters can be used to display only interesting results (see Chapter 8.4 (page 207)).

Vulnerability	Severity	QoD	Host	Location	Created
			IP	Name	
OS End Of Life Detection	10.0 (High)	80 %	192.168.0.12	scan-target-2.greenbone.net	general/tcp Fri, Jul 12, 2019 11:30 AM UTC
phpinfo() output Reporting	7.5 (High)	80 %	192.168.126.4	scan-target-3.greenbone.net	80/tcp Fri, Jul 12, 2019 11:36 AM UTC
Tiki Wiki CMS Groupware < 4.2 Multiple Unspecified Vulnerabilities	7.5 (High)	80 %	192.168.117.12	scan-target.greenbone.net	80/tcp Fri, Jul 12, 2019 11:37 AM UTC
TWiki Cross-Site Request Forgery Vulnerability - Sep 10	6.8 (Medium)	80 %	192.168.0.12	scan-target-2.greenbone.net	80/tcp Fri, Jul 12, 2019 11:38 AM UTC
Tiki Wiki CMS Groupware < 17.2 SQL Injection Vulnerability	6.5 (Medium)	80 %	192.168.117.83	scan-target-1.greenbone.net	80/tcp Fri, Jul 12, 2019 11:38 AM UTC

Fig. 11.14: Page *Results* showing all results of all scans

For all results the following information is displayed:

Vulnerability Name of the found vulnerability.

Vulnerabilities with an attached note are marked with . Vulnerabilities with an attached ticket are marked with .

Note: If the column of the vulnerability still appears empty the respective VT has not been updated yet.

Note: Even though the results contain a lot of information, external references are always listed in the details.

These refer to webpages on which the vulnerability was already discussed.

Additional background information is available such as who discovered the vulnerability, what effects it could have and how it can be remediated.

Solution type To simplify the elimination of vulnerabilities every result offers a solution for problems. The column *Solution type* displays the existence of a solution. The following the solutions are possible:

- A vendor patch is available.
- A workaround is available.
- A mitigation by configuration is available.
- No fix is and will be available.
- No solution exists.

Severity Severity of the vulnerability. The severity of the vulnerability (CVSS, see Chapter 14.2.4 (page 393)) is displayed as a bar to support the analysis of the results.

QoD QoD is short for Quality of Detection and shows the reliability of the detection of a vulnerability. The QoD was introduced with GOS 3.1. Results created with earlier versions are assigned a QoD of 75 % during migration.



By default, only results that were detected by VTs 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 8.4.1 (page 207)).

Host Host for which the result was found. The IP address and the name of the host are displayed separately.

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

Created Date and time of the report creation.

Note: By clicking below the list of results more than one result can be exported at a time. The drop-down list is used to select which results exported.

Details Page

Click on the name of a result to display the details of the result. Click to open the details page of the result.

The following registers are available:

Information General information about the result.

User Tags Assigned tags (see Chapter 8.5 (page 214)).

The following actions are available in the upper left corner:

- Open the corresponding chapter of the user manual.
- Show the list page of all results.
- Export the result as an XML file.
- Create a new note for the result (see Chapter 11.7.1 (page 335)).
- Create a new override for the result (see Chapter 11.8.1 (page 338)).
- Create a new ticket for the result (see Chapter 11.6.1 (page 331)).
- Show the corresponding task.
- Show the corresponding report.

11.4 Displaying all Existing Vulnerabilities

List Page

While the reports only contain the vulnerabilities of one single scan, all vulnerabilities are saved in the internal database and can be viewed by selecting *Scans > Vulnerabilities* in the menu bar.

Powerfilters can be used to display only interesting vulnerabilities (see Chapter 8.4 (page 207)).

For all vulnerabilities the following information is displayed:

Name Title of the vulnerability.

Oldest Result Date and time of the oldest result that was found for the vulnerability.

Newest Result Date and time of the newest result that was found for the vulnerability.

Severity Severity of the vulnerability. To support the administrator with the analysis of the results, the severity of a vulnerability (CVSS, see also Chapter 14.2.4 (page 393)) is displayed as a bar.

QoD QoD is short for Quality of Detection and shows the reliability of the detection of a vulnerability. The QoD was introduced with GOS 3.1. Results created with earlier versions are assigned a QoD of 75 % during migration.



Name	Oldest Result	Newest Result	Severity ▾	QoD	Results	Hosts
SMB NativeLanMan	Fri, Jul 12, 2019 11:38 AM UTC	Fri, Jul 12, 2019 11:38 AM UTC	10.0 (High)	80 %	1	1
OS End Of Life Detection	Fri, Jul 12, 2019 11:30 AM UTC	Fri, Jul 12, 2019 11:30 AM UTC	10.0 (High)	80 %	1	1
Tiki Wiki CMS Groupware < 4.2 Multiple Unspecified Vulnerabilities	Fri, Jul 12, 2019 11:37 AM UTC	Fri, Jul 12, 2019 11:37 AM UTC	7.5 (High)	80 %	1	1
phpinfo() output Reporting	Fri, Jul 12, 2019 11:36 AM UTC	Fri, Jul 12, 2019 11:36 AM UTC	7.5 (High)	80 %	1	1
TWiki Cross-Site Request Forgery Vulnerability - Sep10	Fri, Jul 12, 2019 11:38 AM UTC	Fri, Jul 12, 2019 11:38 AM UTC	6.8 (Medium)	80 %	1	1
Tiki Wiki CMS Groupware < 17.2 SQL Injection Vulnerability	Fri, Jul 12, 2019 11:38 AM UTC	Fri, Jul 12, 2019 11:38 AM UTC	6.5 (Medium)	80 %	1	1
TWiki Cross-Site Request Forgery Vulnerability	Fri, Jul 12, 2019 11:38 AM UTC	Fri, Jul 12, 2019 11:38 AM UTC	6.0 (Medium)	80 %	1	1
Tiki Wiki CMS Groupware 'fixedURLData' Local File Inclusion Vulnerability	Fri, Jul 12, 2019 11:38 AM UTC	Fri, Jul 12, 2019 11:38 AM UTC	5.0 (Medium)	80 %	1	1
Tiki Wiki CMS Groupware Input Sanitation Weakness Vulnerability	Fri, Jul 12, 2019 11:37 AM UTC	Fri, Jul 12, 2019 11:37 AM UTC	5.0 (Medium)	80 %	1	1
Cleartext Transmission of Sensitive Information via HTTP	Fri, Jul 12, 2019 11:19 AM UTC	Fri, Jul 12, 2019 1:04 PM UTC	4.8 (Medium)	80 %	6	3

Fig. 11.15: Page *Vulnerabilities* showing all vulnerabilities of all scans

By default, only vulnerabilities that were detected by VTs 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 8.4.1 (page 207)).

Results Number of results found for this vulnerability. By clicking on the number of results the page *Results* is opened. A filter is applied to show only the results for the selected vulnerability.

Note: By clicking ↗ below the list of results more than one result can be exported at a time. The drop-down list is used to select which results exported.

Details Page

Click on the name of a vulnerability to open the details page of the vulnerability.

The following actions are available in the upper left corner:

- ⓘ Open the corresponding chapter of the user manual.
- ⚡ Show the list page of all vulnerabilities.
- ↗ Export the vulnerability as an XML file.
- ⌂ Create a new note for the vulnerability (see Chapter 11.7.1 (page 335)).
- ⌂ Create a new override for the vulnerability (see Chapter 11.8.1 (page 338)).
- ⓘ Show the corresponding results.
- ⓘ Show the corresponding vulnerability.

11.5 Trend of Vulnerabilities

If a task has been run multiple times the trend of discovered vulnerabilities is displayed on the page *Tasks* (see Fig. 11.16).

To get there select *Scans > Tasks* in the menu bar.

The trend describes the change of vulnerabilities between the newest and the second newest report. It is displayed in the column *Trend*.



Name	Status	Reports	Last Report	Severity	Trend	Actions
Container_Task	Container					
DMZ Mail Scan	Done	2	Mon, Jun 17, 2019 1:22 PM UTC	7.5 (High)	→	
Unnamed	Done	3	Mon, Jun 17, 2019 1:14 PM UTC	6.8 (Medium)	↗	

(Applied filter: min_qod=70 apply_overrides=1 rows=10 first=1 sort=name)

Apply to page contents

◀◀ 1 - 3 of 3 ▶▶

Fig. 11.16: Task with trend

The following trends are possible:

- ↗ In the newest report the highest severity is higher than the highest severity in the second newest report.
- ↖ The highest severity is the same for both reports. However, the newest report contains more security issues of this severity than the second newest report.
- The highest severity and the amount of security issues are the same for both reports.
- ↘ The highest severity is the same for both reports. However, the newest report contains less security issues of this severity than the second newest report.
- ↙ In the newest report the highest severity is lower than the highest severity in the second newest report.

11.6 Using Tickets

Users can task other users or themselves to resolve findings of a scan.

11.6.1 Creating a Ticket

A ticket can be created as follows:

1. Select *Scans > Reports* in the menu bar and click on the date of a report to show the results.
2. Click on an item in the column *Vulnerability* and to open the details page of the result.
or
1. Select *Scans > Results* in the menu bar.
2. Click on an item in the column *Vulnerability* and to open the details page of the result.
3. Create a new ticket by clicking .
4. Select the user to whom the ticket should be assigned in the drop-down list *Assign to User* (see Fig. 11.17).
5. Enter a note for the ticket in the input box *Note*.
6. Click *Save*.
→ The number of tickets for a result are displayed in the upper left corner of the details page of the result (see Fig. 11.18). By clicking the corresponding tickets are displayed.



Fig. 11.17: Creating a new ticket



Fig. 11.18: Number of assigned tickets

11.6.2 Changing the Status of a Ticket

A ticket can have the following status:

- Open: the vulnerability has not been fixed yet.
- Fixed: the vulnerability has been fixed.
- Fixed verified: the task has been run again and the vulnerability was not found anymore. This status is set automatically.
- Closed: the fix of the vulnerability was verified or the ticket is not required anymore.

The status of a ticket can be changed as follows:

1. Select *Resilience > Remediation Tickets* in the menu bar.
2. In the row of the ticket click .
3. Select the new status in the drop-down list *Status* (see Fig. 11.19).
4. Select the user to whom the ticket with the new status should be assigned in the drop-down list *Assigned User*.
5. Enter a note for the new status in the respective input box.
6. Click *Save*.



Edit Ticket TCP timestamps

Status	Fixed
Assigned User	user
Note for Open	Solve until 2019-08-01
Note for Fixed	Solved by user on 2019-06-25
Note for Closed	
<input type="button" value="Cancel"/> <input type="button" value="Save"/>	

Fig. 11.19: Changing the status of a ticket

11.6.3 Setting an Alert for a Ticket

Alerts for tickets can be set for the following events:

- A new ticket is received.
- The status of an assigned ticket changed.
- The status of an own ticket changed.

An alert for tickets is set up as follows:

1. Select *Configuration > Alerts* in the menu bar.
2. Create a new alert by clicking .
3. Define the alert (see Fig. 11.20).
4. Click *Save*.

New Alert

Name	Ticket received
Comment	
Event	<input type="radio"/> Task run status changed to Done <input type="radio"/> New <input type="radio"/> NVTs <input checked="" type="radio"/> Ticket Received <input type="radio"/> Assigned Ticket Changed <input type="radio"/> Owned Ticket Changed
Condition	<input checked="" type="radio"/> Always
Method	Email
To Address	mail@example.com
From Address	gsm@example.com
Email Encryption	-- 
Active	<input checked="" type="radio"/> Yes <input type="radio"/> No
<input type="button" value="Cancel"/> <input type="button" value="Save"/>	

Fig. 11.20: Setting an alert for a ticket



The following details of the alert can be defined:

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

Comment An optional comment can contain additional information.

Event Select *Ticket Received* if an alert should be sent when a new ticket is assigned to oneself.

Select *Assigned Ticket Changed* if an alert should be sent when the status of a ticket assigned to oneself changes.

Select *Owned Ticket Changed* if an alert should be sent when the status of ticket assigned to another user changes.

Method Selection of the method for the alert. Only one method per alert can be chosen.

If different alerts for the same event should be triggered, multiple alerts must be created and linked to the same task.

The following methods are possible:

Email An e-mail is sent to the given address.

The transmission of the e-mail can be encrypted using a configurable S/MIME or GPG key. The encryption can be selected in the drop-down list *Email Encryption* or created by clicking .

Start Task The alert can start an additional task. The task is selected in the drop-down list *Start Task*.

System Logger The alert is sent to a Syslog daemon.

The Syslog server is defined using the console (see Chapter 7.2.11 (page 173)).

11.6.4 Managing Tickets

List Page

All existing tickets can be displayed by selecting *Resilience > Remediation Tickets* in the menu bar.

For all tickets the following information is displayed:

Vulnerability Vulnerability for which the ticket is created.

Severity Severity of the vulnerability for which the ticket is created.

Host Host on which the vulnerability was found.

Solution Type Solution type of the vulnerability for which the ticket is created.

Assigned User User to which the ticket is assigned.

Modification Time Date and time of the last modification of the ticket.

Status Status of the ticket.

For all tickets the following actions are available:

-  Move the ticket to the trashcan.
-  Edit the ticket.
-  Clone the ticket.

Note: By clicking  or  below the list of tickets more than one ticket can be moved to the trashcan or exported at a time. The drop-down list is used to select which tickets are moved to the trashcan or exported.



Details Page

Click on the name of a ticket to display the details of the ticket. Click to open the details page of the ticket.

The following registers are available:

Information General information about the ticket.

User Tags Assigned tags (see Chapter 8.5 (page 214)).

The following actions are available in the upper left corner:

- Open the corresponding chapter of the user manual.
- Show the list page of all tickets.
- Clone the ticket.
- Edit the ticket.
- Move the ticket to the trashcan.
- Export the ticket as an XML file.

11.7 Using Notes

Notes allow adding comments to a VT and are displayed in the reports as well. A note can be added to a specific result, task, severity, port or host and as such will only appear in specific reports. A note can be generalized as well so that it will be displayed in all reports.

11.7.1 Creating a Note

11.7.1.1 Creating a Note Through a Scan Result

Notes can be created in different ways. The simplest way is through the respective scan result in a report:

1. Select *Scans > Reports* in the menu bar.
 2. Click on the date of the report to show the results.
 3. Select the register *Results*.
 4. Click on a result in the column *Vulnerability*.
 5. Click to open the details page of the result.
 6. Click in the upper left corner of the page.
 7. Define the note (see Fig. 11.21).
 8. Click *Save*.
- The note is displayed on the details page of the result (see Fig. 11.22).



New Note

NVT	TCP timestamps
<input type="radio"/> yes, always	
<input checked="" type="radio"/> yes, for the next	20
<input type="radio"/> no	days
Hosts	<input type="radio"/> Any <input checked="" type="radio"/> 192.168.178.33
Location	<input type="radio"/> Any <input checked="" type="radio"/> general/tcp
Severity	<input type="radio"/> Any <input checked="" type="radio"/> > 0.0
Task	<input type="radio"/> Any <input checked="" type="radio"/> Container
Result	<input type="radio"/> Any <input checked="" type="radio"/> Only selected result (TCP timestamps)
Text	
Repeat scan after 7 days.	
<input type="button" value="Cancel"/>	<input type="button" value="Save"/>

Fig. 11.21: Creating a new note

Timestamp options when initiating TCP connections, but use them in the
that is initiating communication includes them in their synchronize (SYN)
See the references for more information.

Notes

Note	
Repeat scan after 7 days.	
Modified Mon, Jun 24, 2019 4:13 PM	

Fig. 11.22: Report containing a note



11.7.1.2 Creating a Note on the Page Notes

Notes can be created on the page *Notes* as well:

1. Select *Scans > Notes* in the menu bar.
2. Create a new note by clicking .
3. Enter the ID of the VT in the input box *NVT OID*.
4. Define the note.

Tip: It is possible to enter ranges of IP addresses and CIDR blocks in the input box *Hosts*. In that way, notes for entire subnets can be created without having to specify every host in a comma-separated list.

Notes can be generalized by selecting the radio button *Any* for hosts, locations, severities, tasks or results.

5. Click *Save*.

11.7.2 Managing Notes

List Page

All existing notes can be displayed by selecting *Scans > Notes* in the menu bar (see Fig. 11.23).

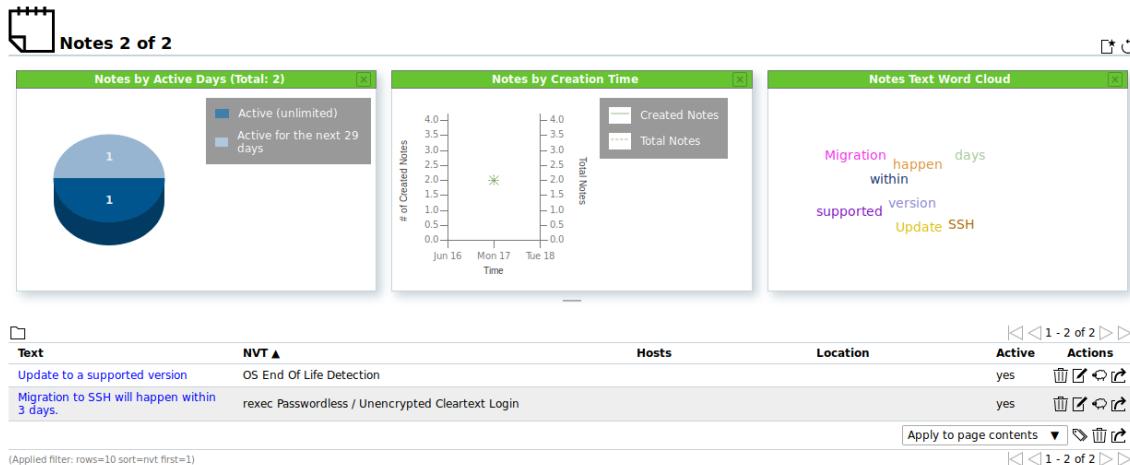


Fig. 11.23: Managing notes

For all notes the following actions are available:

- Move the note to the trashcan.
- Edit the note.
- Clone the note.
- Export the note as an XML file.

Note: By clicking or below the list of notes more than one note can be moved to the trashcan or exported at a time. The drop-down list is used to select which notes are moved to the trashcan or exported.



Details Page

Click on the name of a note to display the details of the note. Click  to open the details page of the note.

The following registers are available:

Information General information about the note.

User Tags Assigned tags (see Chapter 8.5 (page 214)).

Permissions Assigned permissions (see Chapter 9.4 (page 231)).

The following actions are available in the upper left corner:

-  Open the corresponding chapter of the user manual.
-  Show the list page of all notes.
-  Create a new note (see Chapter 11.7.1 (page 335)).
-  Clone the note.
-  Edit the note.
-  Move the note to the trashcan.
-  Export the note as an XML file.

11.8 Using Overrides and False Positives

The severity of a result can be modified. This is called override.

Overrides are especially useful to manage results that are detected as a false positive and that have been given a critical severity but should be given a different severity in the future.

The same applies to results that only have been given the severity *Log* but should be assigned a higher severity locally. This can be managed with an override as well.

Overrides are also used to manage acceptable risks.

11.8.1 Creating an Override

11.8.1.1 Creating an Override Through a Scan Result

Overrides can be created in different ways. The simplest way is through the respective scan result in a report:

1. Select *Scans > Reports* in the menu bar.
2. Click on the date of the report to show the results.
3. Select the register *Results*.
4. Click on a result in the column *Vulnerability*.
5. Click  to open the details page of the result.
6. Click  in the upper left corner of the page.
7. Define the override. Select the new severity in the drop-down list *New Severity* (see Fig. 11.24).
8. Click *Save*.



Fig. 11.24: Creating a new override

The following information can be entered:

Note: If an override is created through a scan result, some settings are already filled in.

NVT VT for which the override is applied.

Active Selection whether the override should be activated. An activation for an arbitrary number of days is possible as well.

Hosts Host or range of hosts for which the result must be found for the override to apply.

Tip: It is possible to enter ranges of IP addresses and CIDR blocks. In that way, overrides for entire subnets can be created without having to specify every host in a comma-separated list.

Host ranges are specified with a minus, e.g. 198.168.1.1–198.168.1.25. A range bigger than 4096 is not supported.

Note: Conflicting overrides, e.g. an override for a host range and another override for a host inside that range, are not permitted.

Location Port for which the result must be found for the override to apply. Only a specific port or the setting Any are supported per override. A specific port must be supplied as a number followed by /tcp or /udp.

Severity Range of severity of the VT for which the overrides should be applied.

New Severity Severity the VT should have after the override is applied.

Task Selection of tasks for which the override should be applied.

Result Selection of results for which the override should be applied.

Note: The radio button Any has to be selected if the override should be applied to reports in the future.

Text A text describes the override in more detail.



Note: If several overrides apply to the same VT in the same report the most recent override is used and applied.

11.8.1.2 Creating an Override on the Page Overrides

Overrides can be created on the page *Overrides* as well:

1. Select *Scans > Overrides* in the menu bar.
2. Create a new override by clicking .
3. Enter the ID of the VT in the input box *NVT OID*.
4. Define the override.

Note: For the information to enter in the input boxes see Chapter 11.8.1.1 (page 338).

5. Select the new severity in the drop-down list *New Severity*.
6. Click *Save*.

11.8.2 Managing Overrides

List Page

All existing overrides can be displayed by selecting *Scans > Overrides* in the menu bar.

For all overrides the following actions are available:

-  Move the override to the trashcan.
-  Edit the override.
-  Clone the override.
-  Export the override as an XML file.

Note: By clicking  or  below the list of overrides more than one override can be moved to the trashcan or exported at a time. The drop-down list is used to select which overrides are moved to the trashcan or exported.

Details Page

Click on the name of an override to display the details of the override. Click  to open the details page of the override.

The following registers are available:

Information General information about the override.

User Tags Assigned tags (see Chapter 8.5 (page 214)).

Permissions Assigned permissions (see Chapter 9.4 (page 231)).

The following actions are available in the upper left corner:

-  Open the corresponding chapter of the user manual.
-  Show the list page of all overrides.
-  Create a new override (see Chapter 11.8.1 (page 338)).



- Clone the override.
- Edit the override.
- Move the override to the trashcan.
- Export the override as an XML file.

11.8.3 Disabling and Enabling Overrides

If overrides change the display of the results, the overrides can be enabled or disabled.

This is done by setting the filter as follows:

1. Click in the filter bar.
2. For *Apply Overrides* select the radio button *Yes* to enable overrides.
For *Apply Overrides* select the radio button *No* to disable overrides.
3. Click *Update*.

Tip: Overrides can be labelled in exported reports (see Chapter 11.2.2 (page 324)).

11.9 Using Business Process Maps

A Business Process Map (BPM) is used to illustrate the impact of collected results on a business.

Business processes are modeled using nodes (= processes) and edges (= connections).

Each node is assigned with the host on which the process takes place. The node is colored according to the highest severity of the host.

The following colors are possible:

- Red: one or more host(s) has/have the severity *High*
- Yellow: one or more host(s) has/have the severity *Medium* but no host has a higher severity
- Blue: one or more host(s) has/have the severity *Low* but no host has a higher severity
- Light gray: one or more host(s) has/have the severity *Log* but no host has a higher severity
- Dark gray: no severities are available for the host(s) (*N/A*)
- White: no hosts are associated with this process

If a process is vulnerable and might affect a following process, the coloration of this following process is adjusted.

By this, it is possible to detect the vulnerabilities of processes and their impact on subsequent processes.

The following rules apply for the color overriding:

- Higher severities override lower severities: *High > Medium > Low > Log*
- *Log* does not override the missing assignment of hosts
- *N/A* does not override *Log*

Loading and saving the BMP is completely automatic. The map is loaded when the page *Business Process Map* is opened. Changes are saved as soon as they are done.

The BPM cannot be shared or exported/imported.



11.9.1 Navigating the Business Process Map

The map can be moved by clicking and dragging the background.

The map can be zoomed from a scale of 0.3 to 1.6 by using the mouse wheel or clicking + and -. The font size will adjust for better readability.

Clicking jumps to the starting position in the map and resets the zoom.

11.9.2 Creating a Business Process Map

1. Select *Resilience > Business Process Map* in the menu bar.
2. Click to create a process node.
→ The process node is created and displayed on the map (see Fig. 11.25).

For each process a standard tag is created on the page *Tags* (see Chapter 8.5.4 (page 215)). The name of the tag corresponds to the name of the process, preceded by “myBP:”. If the process is renamed, the tag’s name is changed as well, while the tag’s ID remain the same.

Note: The created tags should not be edited manually.

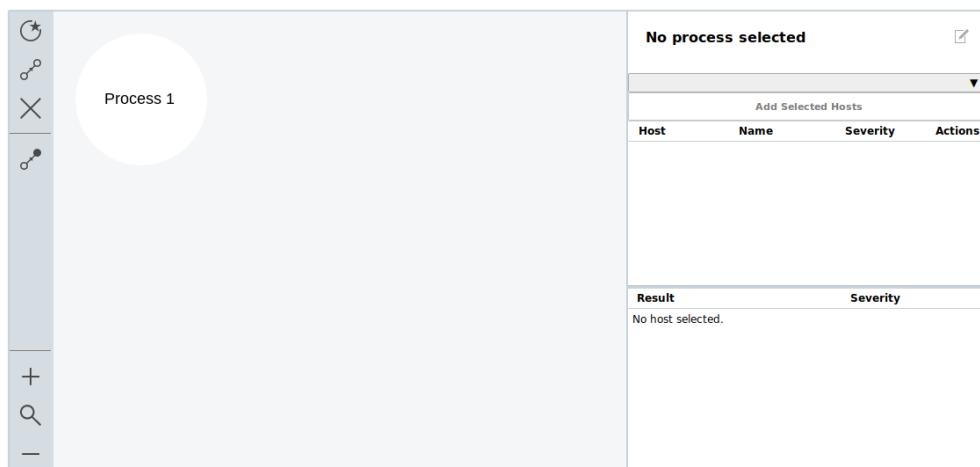


Fig. 11.25: Creating a new process

Note: At most 50 processes can be created for a BPM.

3. Select the process node by clicking it.
→ The node is marked by a blue border.
4. Select the hosts that should be assigned to the process in the drop-down list (see Fig. 11.26).
5. Click *Add Selected Hosts*.

→ The process node is colored according to the host’s highest severity.

When the process node is selected, the hosts are displayed in the table on the right (see Fig. 11.27).

By clicking the details page of the host is opened (see Chapter 13.1.2 (page 379)).

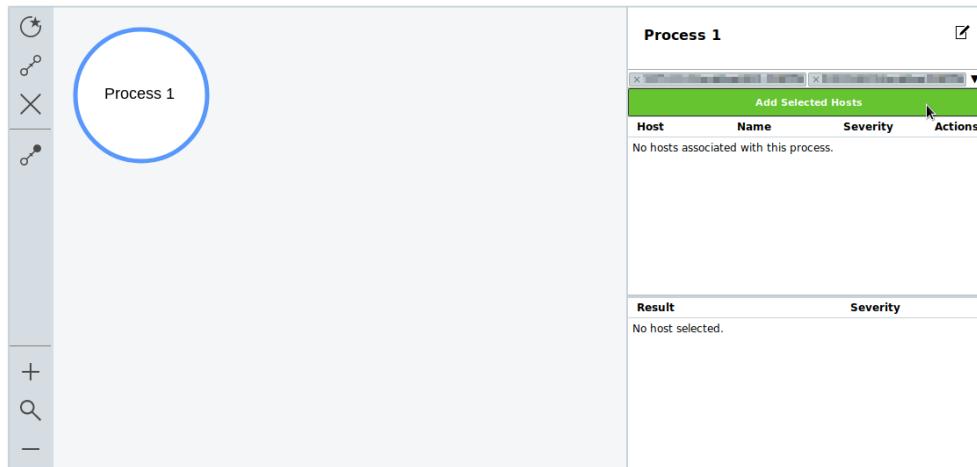


Fig. 11.26: Assigning hosts to a process

By clicking on a host, the results found for this hosts are displayed in a table below (see Fig. 11.27). Clicking on a result opens its details page (see Chapter 11.3 (page 328)).

The screenshot shows the 'Process 1' configuration page with assigned hosts and their results. The results table is expanded to show four items:

Result	Severity
TightVNC ClientConnection Multiple Integer Overflow Vulnerabilities (Linux)	10.0 (High)
PHP-CGI-based setups vulnerability when parsing query string parameters from php files.	7.5 (High)
SSH Brute Force Logins With Default Credentials Reporting	7.5 (High)
Ubuntu Update for apache2 vulnerability USN-990-2	5.8 (Medium)

Fig. 11.27: Hosts and results of a process

Note: Each host assigned to a process is tagged with the standard tag created for the corresponding process (see step 2) (see Chapter 8.5.4 (page 215)).



Note: While it is possible to assign unlimited hosts to a process, there is a maximum of 100 hosts per process that will actually be shown in the table on the right and considered when estimating the node's color.

If the limit is exceeded, a warning is shown above the host table.

6. Create a second (or more) process node(s) (see steps 2 – 5).
7. Click to create a new connection.
→ The “draw” mode is activated.
8. Click the source process node.
→ The node is marked by a blue border (see Fig. 11.28).

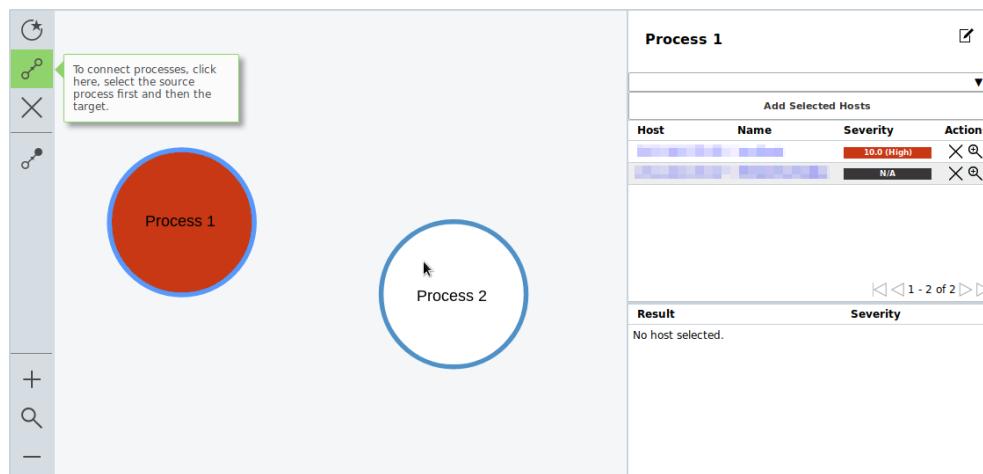


Fig. 11.28: Creating a connection

9. Click the target process node.
→ The connection is created. The arrow indicates the direction of influence (see Fig. 11.29).

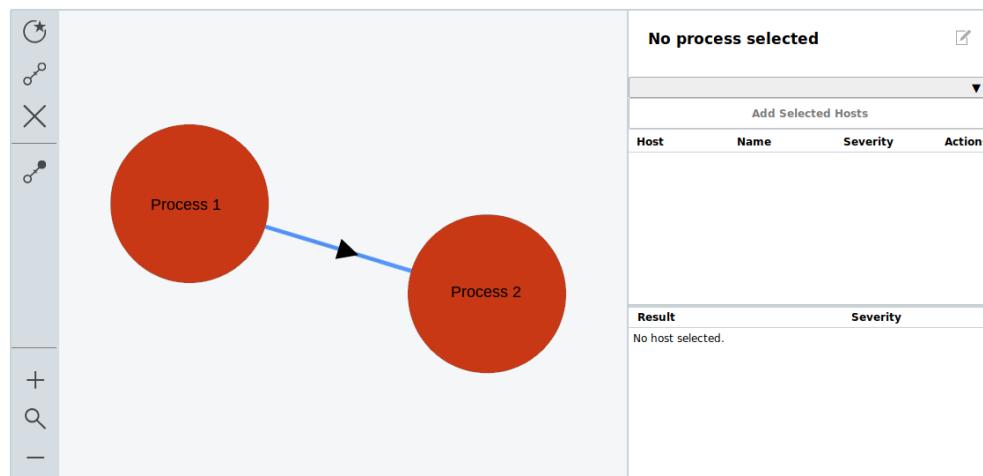


Fig. 11.29: Newly created connection

If conditional colorization is enabled, the color of the primary process is assigned to the following process(es) as well, i.e., the color of the following process node(s) is the same as that of the primary process



node. A tooltip shows the original severity of the process.

To find a source process easily, the conditional colorization can be disabled by clicking . The icon is highlighted in green if the conditional colorization is disabled.

10. Leave the “draw” mode by clicking any empty space in the map or by pressing Esc.

11.9.3 Editing a Business Process Map

11.9.3.1 Editing a Process

A process can be edited as follows:

1. Select *Resilience > Business Process Map* in the menu bar.
2. Click the desired process node.
3. Click to change the name or the description of the process.
4. Select additional hosts that should be assigned to the process in the drop-down list and click *Add Selected Hosts*.
5. Click to remove a host from the process.

11.9.3.2 Deleting Elements

Elements of the map (process nodes and connections) can be deleted by selecting the element and pressing Delete or clicking .

If a process is deleted that is either the source or the target of a connection, the connection is removed as well.

CHAPTER 12

Performing Compliance Scans and Special Scans

In information technology (IT) compliance is the main approach for organizations to keep their information and assets protected and secure.

With cybercrime on the rise, governments see the need to protect the identities and assets of their citizens by passing rules and regulations on privacy and IT security. Information security bodies such as the Information Systems Audit and Control Association (ISACA) or the International Organization for Standardization (ISO) publish IT security standards, frameworks and guidelines.

These standards, frameworks and guidelines require organizations to implement the appropriate safeguards to protect themselves and their information assets from attacks. For implementation the organization has to create an IT security framework consisting of policies, standards, baselines, guidelines and detailed procedures.

Vulnerability assessment systems such as the Greenbone Security Manager (GSM) can assist IT security professionals to check their IT security safeguards for the standards, frameworks and guidelines mentioned above.

The GSM supports performing audits based on policies.

The Chapters 12.4 (page 357), 12.5 (page 372) and 12.6 (page 376) show some examples for policy audits.

Note: The policies used in these chapters are provided via the feed.

Some policies may not be available yet, but will be added at a later time.

In case a policy is not available, contact the Greenbone Networks Support (support@greenbone.net).



12.1 Configuring and Managing Policies

Policies are scan configurations with the flag *policy*.

All default policies by Greenbone Networks are data objects that are distributed via the feed. They are downloaded and updated with each feed update.

If no default policies are available, a feed update may be necessary, or the Feed Import Owner may need to be set (see Chapter 7.2.1.9.1 (page 130)).

Default policies cannot be edited. Furthermore, they can only be deleted temporarily by the Feed Import Owner or by a super administrator. During the next feed update, they will be downloaded again.

Note: To permanently delete a default policy, the Feed Import Owner has to delete it. Afterwards the Feed Import Owner has to be changed to (*Unset*) (see Chapter 7.2.1.9.1 (page 130)).

In addition to the default policies, custom policies can be created (see Chapter 12.1.1 (page 347)) or imported (see Chapter 12.1.2 (page 350)).

12.1.1 Creating a Policy

A new policy can be created as follows:

1. Select *Resilience > Compliance Policies* in the menu bar.
2. Create a new policy by clicking .

Note: Alternatively, a policy can be imported (see Chapter 12.1.2 (page 350)).

3. Enter the name of the policy in the input box *Name* (see Fig. 12.1).

Fig. 12.1: Creating a new policy

4. Click *Save*.
→ The policy is created and displayed on the page *Policies*.
5. In the row of the policy click .
6. In the sections *Edit Network Vulnerability Test Families* select the radio button  if newly introduced VT families should be included and activated automatically (see Fig. 12.2).
7. In the section *Edit Network Vulnerability Test Families* activate the checkboxes in the column *Select all NVTs* if all VTs of a family should be activated.



Edit Policy IT Grundschutz Policy

Name	IT Grundschutz Policy
Comment	Empty and static configuration template.

Edit Network Vulnerability Test Families (65)

Family	NVTs selected	Trend	Select all NVTs	Actions
AIX Local Security Checks	0 of 1	<input type="radio"/> ↗ <input checked="" type="radio"/> ↘ →	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Amazon Linux Local Security Checks	0 of 748	<input type="radio"/> ↗ <input checked="" type="radio"/> ↘ →	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Brute force attacks	0 of 7	<input type="radio"/> ↗ <input checked="" type="radio"/> ↘ →	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Buffer overflow	0 of 567	<input type="radio"/> ↗ <input checked="" type="radio"/> ↘ →	<input type="checkbox"/>	<input checked="" type="checkbox"/>
CISCO	0 of 1314	<input type="radio"/> ↗ <input checked="" type="radio"/> ↘ →	<input type="checkbox"/>	<input checked="" type="checkbox"/>
CentOS Local Security Checks	0 of 3245	<input type="radio"/> ↗ <input checked="" type="radio"/> ↘ →	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Cisco Local Security Checks	0 of 221	<input type="radio"/> ↗ <input checked="" type="radio"/> ↘ →	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Citrix Xenserver Local Security Checks	0 of 44	<input type="radio"/> ↗ <input checked="" type="radio"/> ↘ →	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Compliance	0 of 12	<input type="radio"/> ↗ <input checked="" type="radio"/> ↘ →	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Databases	0 of 611	<input type="radio"/> ↗ <input checked="" type="radio"/> ↘ →	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Debian Local Security Checks	0 of 5521	<input type="radio"/> ↗ <input checked="" type="radio"/> ↘ →	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Fig. 12.2: Editing the new policy

8. Click for a VT family to edit it (see Fig. 12.3).

Note: The following VT families cannot be edited:

- CentOS Local Security Checks
- Debian Local Security Checks
- Fedora Local Security Checks
- Huawei EulerOS Local Security Checks
- Oracle Linux Local Security Checks
- Red Hat Local Security Checks
- SuSE Local Security Checks
- Ubuntu Local Security Checks

9. In the column *Selected* activate the checkboxes of the VTs that should be activated.

10. Click for a VT to edit it (see Fig. 12.4).

Note: If system-specific VTs of the VT family *Policy* are used (e.g., beginning with “Linux”, “Microsoft Windows”, “Microsoft Office”), the radio button *Yes* has to be selected for *Verbose Policy Controls* in the VT *Compliance Tests* (VT family *Compliance*).

Note: If editing the VT includes uploading a text file, the file should use UTF-8 text encoding.



Edit Policy Family Firewalls

Policy IT Grundschutz Policy
Family Firewalls

Edit Network Vulnerability Tests

Name ▲	OID	Severity	Timeout	Prefs	Selected	Actions
Arkoon identification	1.3.6.1.4.1.25623.1.0.14377	0.0 (Log)	default	0	<input type="checkbox"/>	<input checked="" type="checkbox"/>
BlueCoat ProxySG console management detection	1.3.6.1.4.1.25623.1.0.16363	5.0 (Medium)	default	0	<input type="checkbox"/>	<input checked="" type="checkbox"/>
CheckPoint Firewall-1 Telnet Authentication Detection	1.3.6.1.4.1.25623.1.0.10675	5.0 (Medium)	default	0	<input type="checkbox"/>	<input checked="" type="checkbox"/>
CheckPoint Firewall-1 Web Authentication Detection	1.3.6.1.4.1.25623.1.0.10676	5.0 (Medium)	default	0	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Checkpoint Firewall open Web administration	1.3.6.1.4.1.25623.1.0.11518	4.3 (Medium)	default	0	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Checkpoint SecuRemote information leakage	1.3.6.1.4.1.25623.1.0.10710	5.0 (Medium)	default	0	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Checkpoint SecureRemote detection	1.3.6.1.4.1.25623.1.0.10617	1.2 (Low)	default	0	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Checkpoint VPN-1 PAT information disclosure	1.3.6.1.4.1.25623.1.0.80096	5.0 (Medium)	default	0	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Firewall ECF hit bypass	1.3.6.1.4.1.25623.1.0.12119	7.5 (High)	default	0	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Buttons: Cancel, Save

Fig. 12.3: Editing a family of VTs

Edit Policy NVT Linux: Rsyslog configuration

Name: Linux: Rsyslog configuration
Policy: IT Grundschutz Policy
Family: Policy
OID: 1.3.6.1.4.1.25623.1.0.109789
Last Modified: Mon, Feb 11, 2019 2:35 PM UTC

Summary

The 'rsyslog' service is the replacement for 'syslog' daemon with many improvements (connection oriented transmission or log to database formats). This script tests the correct configuration of the 'rsyslog' package.

Vulnerability Scoring

Name	New Value	Default Value
CVSS base	0.0 (Log)	
CVSS base vector	AV:L/A/C:H/Au:S/C:N/I:N/A:N	
Timeout	<input checked="" type="radio"/> Apply default timeout <input type="radio"/>	
File permissions	640	640
Remote log host	.* @@host.example.com	.* @@host.example.com
Accept remote rsyslog messages	<input checked="" type="radio"/> Yes <input type="radio"/> No	Yes

Buttons: Cancel, Save

Fig. 12.4: Editing a VT



11. Click **Save** to save the VT.
12. Click **Save** to save the family of VTs.
13. Optional: edit scanner preferences (see Chapter 10.9.4 (page 295)).
14. Optional: edit VT preferences (see Chapter 10.9.5 (page 297)).
15. Click **Save** to save the policy.

12.1.2 Importing a Policy

A policy can be imported as follows:

1. Select *Resilience > Compliance Policies* in the menu bar.
2. Click .
3. Click *Browse...* and select the XML file of the policy (see Fig. 12.5).



Fig. 12.5: Importing a policy

4. Click *Import*.

Note: If the name of the imported policy already exists, a numeric suffix is added to the name.

→ The imported policy is displayed on the page *Policies*.

5. Execute steps 5 to 15 of Chapter 12.1.1 (page 347) to edit the policy.

12.1.3 Managing Policies

List Page

All existing policies can be displayed by selecting *Resilience > Compliance Policies* in the menu bar (see Fig. 12.6).

For all policies the following information is displayed:

Name Name of the policy.

For all policies the following actions are available:

-  Move the policy to the trashcan. Only policies which are currently not used can be moved to the trashcan. As long as the policy is not deleted from the trashcan, it is not downloaded anew during the next feed update.
-  Edit the policy. Only self-created policies which are currently not used can be edited.
-  Clone the policy.
-  Create a new audit for the policy (see Chapter 12.2.1.2 (page 353)).
-  Export the policy as an XML file.



 Policies 4 of 4	
Name	Actions
Microsoft Office 2013 (Audit for a hardened Microsoft Office 2013 installation.)	    
Microsoft Office 2016 (Audit for a hardened Microsoft Office 2016 installation.)	    
Microsoft Windows 10 (Audit for a hardened Microsoft Windows 10 system.)	    
Microsoft Windows 8.1 (Audit for a hardened Microsoft Windows 8.1 system.)	    

Apply to page contents ▾  

(Applied filter: first=1 rows=10 sort=name)   1 - 4 of 4  

Fig. 12.6: Page *Policies* displaying all available policies

Note: By clicking  or  below the list of policies more than one policy can be moved to the trashcan or exported at a time. The drop-down list is used to select which policies are moved to the trashcan or exported.

Details Page

Click on the name of a policy to display the details of the policy. Click  to open the details page of policy.

The following registers are available:

Information General information about the policy.

Scanner Preferences All scanner preferences for the policy with current and default values.

NVT Families All VT families for the policy with the number of activated VTs and the trend.

NVT Preferences All VT preferences for the policy.

Permissions Assigned permissions (see Chapter 9.4 (page 231)).

The following actions are available in the upper left corner:

-  Open the corresponding chapter of the user manual.
-  Show the list page of all policies.
-  Create a new policy (see Chapter 12.1.1 (page 347)).
-  Clone the policy.
-  Edit the policy. Only self-created policies which are currently not used can be edited.
-  Move the policy to the trashcan. Only policies which are currently not used can be moved to the trashcan. As long as the policy is not deleted from the trashcan, it is not downloaded anew during the next feed update.
-  Export the policy as an XML file.
-  Import a policy (see Chapter 12.1.2 (page 350)).



12.2 Configuring and Managing Audits

Audits are scan tasks with the flag *audit*.

12.2.1 Creating an Audit

12.2.1.1 Creating an Audit on the Page Audits

An audit can be created on the page *Audits* as follows:

1. Select *Resilience > Compliance Audits* in the menu bar.
2. Create an audit by clicking .
3. Define the audit (see Fig. 12.7).
4. Click *Save*.

→ The audit is created and displayed on the page *Audits*.

The following information can be entered:

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

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

Scan Targets Select a previously configured target from the drop-down list (see Chapter 10.2.1 (page 248)).

Additionally, the target can be created on the fly by clicking  next to the drop-down list.

Alerts Select a previously configured alert from the drop-down list (see Chapter 10.12 (page 305)). Status changes of an audit can be communicated via e-mail, Syslog, HTTP or a connector.

Additionally, an alert can be created on the fly by clicking  next to drop-down list.

Schedule Select a previously configured schedule from the drop-down list (see Chapter 10.10 (page 301)).

The audit can be run once or repeatedly at a predetermined time, e.g., every Monday morning at 6:00 am.

Additionally, a schedule can be created on the fly by clicking  next to the drop-down list.

Add results to Assets Selecting this option will make the systems available to the asset management of the GSM automatically (see Chapter 13 (page 378)). This selection can be changed at a later point as well.

Alterable Audit Allow for modification of the audit even though reports were already created. The consistency between reports can no longer be guaranteed if audits are altered.

Auto Delete Reports This option may automatically delete old reports. The maximum number of reports to store can be configured. If the maximum is exceeded, the oldest report is automatically deleted. The factory setting is *Do not automatically delete reports*.

Policy The GSM comes with four pre-configured policies.

Network Source Interface Here the source interface of the GSM for the scan can be chosen.

Order for target hosts Select in which order the specified target hosts are processed during vulnerability tests. Available options are:

- Sequential
- Random
- Reverse



In order to improve the scan progress estimation, the setting *Random* is recommended (see Chapter 17.2.3 (page 421)).

This setting does not affect the alive test during which active hosts in a target network are identified. The alive test is always random.

Maximum concurrently executed NVTs per host/Maximum concurrently scanned hosts Select the speed of the scan on one host. The default values are chosen sensibly. If more VTs run simultaneously on a system or more systems are scanned at the same time, the scan may have a negative impact on either the performance of the scanned systems, the network or the GSM appliance itself. These values “maxhosts” and “maxchecks” may be tweaked.

The screenshot shows the 'New Audit' dialog box. The 'Name' field is set to 'Windows 10 Scan'. Under 'Scan Targets', 'Target_1' is selected. The 'Schedule' dropdown shows 'Once'. In the 'Add results to Assets' section, 'Yes' is selected. For 'Alterable Audit', 'No' is selected. Under 'Auto Delete Reports', 'Do not automatically delete reports' is chosen. The 'Policy' dropdown is set to 'Microsoft Windows 10'. The 'Network Source Interface' field is empty. The 'Order for target hosts' is set to 'Sequential'. The 'Maximum concurrently executed NVTs per host' is set to '4'. The 'Maximum concurrently scanned hosts' is set to '20'. At the bottom left is a 'Cancel' button and at the bottom right is a 'Save' button.

Fig. 12.7: Creating a new audit

12.2.1.2 Creating an Audit Through a Policy

An audit can directly be created for a policy as follows:

1. Select *Resilience > Compliance Policies* in the menu bar.
2. In the row of the desired policy click .
→ The policy is already selected in the drop-down list *Policy*.
3. Define the audit.

Tip: For the information to enter in the input boxes see Chapter 12.2.1.1 (page 352).

4. Click *Save*.
→ The audit is created and displayed on the page *Audits*.



12.2.2 Starting an Audit

In the row of the newly created audit click ▶.

Note: For scheduled audits ⏱ is displayed. The audit is starting at the time that was defined in the schedule (see Chapter 10.10 (page 301)).

→ The scan is running. For the status of an audit see Chapter 12.2.3 (page 354).

Note: Scans are only started if there are enough system resources available. The most important resource is random-access memory (RAM). If too many scans are started and running at the same time and not enough RAM is available, scans are added to a waiting queue when clicking ▶.

When the required RAM is available again, scans from the waiting queue are started, following the principle “first in, first out”.

The number of scans in the waiting queue is limited as well, i.e., scans beyond that are not started at all.

For more information see Chapter 17.3 (page 422).

The report of an audit can be displayed as soon as the audit has been started by clicking the bar in the column *Status*. For reading, managing and downloading reports see Chapter 11 (page 315).

As soon as the status changes to *Done* the complete report is available. At any time the intermediate results can be reviewed (see Chapter 11.2.1 (page 320)).

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

12.2.3 Managing Audits

List Page

All existing audits can be displayed by selecting *Resilience > Compliance Audits* in the menu bar (see Fig. 12.8).

Name	Status	Report	Compliance Status	Actions
Windows 10 Scan	Done		21 %	▶ ▷ 🗑️ 📁 🗑️ 🗑️
Windows 8.1 Scan	New			▶ ▷ 🗑️ 📁 🗑️ 🗑️

(Applied filter: apply_overrides=0 min_qod=70 first=1 rows=10 sort=name)

Fig. 12.8: Page *Audits* displaying all available audits

For all audits the following information is displayed:

Name Name of the audit. The following icons may be displayed:

- 📝 The audit is marked as alterable. Some properties that would otherwise be locked once reports exist can be edited.



- The audit is configured to run on a remote scanner (see Chapter 16 (page 409)).
- The audit is visible to one or more other user(s).
- The audit is owned by another user.

Status Current status of the audit. The following status bars are possible:

New

The audit has not been run since it was created.

Requested

The audit was just started. The GSM is preparing the scan.

21 %

The audit is currently running. The percent value is based on the number of VTs executed on the selected hosts. For this reason the value does not necessarily correlate with the time spent.

Queued

The scan was added to a waiting queue (following the principle “first in, first out”) for one of the following reasons:

- Too many scans are already running and there is no memory available to start the scan. The scan will be started when the required resources are available again.
- The GSM is performing a feed update and is currently loading new VTs.
- The GSM was just started and is currently loading the VTs.

For more information see Chapter 17.3 (page 422).

Delete Requested

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

Stop Requested

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

Stopped at 84 %

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

Resume Requested

The audit was just resumed. The GSM is preparing the scan.

When resuming a scan, all unfinished hosts are scanned completely anew. The data of hosts that were already fully scanned is kept.

Interrupted at 42 %

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

Done

The audit has been completed successfully.

Report Date and time of the latest report. By clicking it the details page of the latest report is opened.

Compliance Status Relation of requirements identified as compliant to requirements identified as non-compliant (percentage).

For all audits the following actions are available:

- ▶ Start the audit. Only currently not running audits can be started.
- ⚡ Stop the currently running audit. All discovered results will be written to the database.
- ⏱ Show details of the assigned schedule (only available for scheduled audits, see Chapter 10.10 (page 301)).
- ⏵ Resume the stopped audit. All unfinished hosts are scanned completely anew. The data of hosts that were already fully scanned is kept.
- 🗑 Move the audit to the trashcan.
- 🎁 Edit the audit.



- Clone the audit.
- Export the audit as an XML file.
- Download the report of the audit as a GCR file (Greenbone Compliance Report as PDF format).

Note: By clicking or below the list of audits more than one audit can be moved to the trashcan or exported at a time. The drop-down list is used to select which audits are moved to the trashcan or exported.

Details Page

Click on the name of an audit to display the details of the audit. Click to open the details page of the audit.

The following registers are available:

Information General information about the audit.

Permissions Assigned permissions (see Chapter 9.4 (page 231)).

The following actions are available in the upper left corner:

- Open the corresponding chapter of the user manual.
- Show the list page of all audits.
- Create a new audit (see Chapter 12.2.1.1 (page 352)).
- Clone the audit.
- Edit the audit.
- Move the audit to the trashcan.
- Export the audit as an XML file.
- Start the audit. Only currently not running audits can be started.
- Stop the currently running audit. All discovered results will be written to the database.
- Resume the stopped audit. All unfinished hosts are scanned completely anew. The data of hosts that were already fully scanned is kept.
- Show the last report for the audit or show all reports for the audit.
- Show the results for the audit.



12.3 Using and Managing Policy Reports

Reports for audits are similar to reports of all other tasks.

Once a scan has been started, the report of the results found so far can be viewed. When a scan is completed, the status changes to *Done* and no more results will be added.

12.3.1 Using a Policy Report

A policy report can be used in the same way as any other report. Chapter 11.2 (page 319) contains information about reading, interpreting, filtering, exporting, importing and comparing reports.

For further information about results and vulnerabilities see Chapters 11.3 (page 328) and 11.4 (page 329).

12.3.2 Exporting a Policy Report

Note: A policy report always has the report format *Greenbone Compliance Report PDF (GCR PDF)*. Changing the report format is not possible.

Additionally, the report can be downloaded from the page *Audits* as follows:

1. Select *Resilience > Compliance Audits* in the menu bar.
2. In the row of the desired audit click .
3. Download the PDF file.

12.4 Generic Policy Scans

When performing policy scans, there are groups of four VTs in the VT family *Policy* that can be configured accordingly.

At least the base VT and one additional VT are required to run a policy scan.

The four VT types are:

Base This VT performs the actual scan of the policy.

Errors This VT summarizes any items in which some errors occurred when running the base VT.

Matches This VT summarizes any items which match the checks performed by the base VT.

Violations This VT summarizes any items which did not match the checks performed by the base VT.

Note: The base VT must always be selected for a policy check since it performs the actual tests. The other three VTs may be selected according to the needs. For example, if matching patterns are of no concern then only a VT of the type *Violations* should be selected additionally.

12.4.1 Checking File Content

File content checks belong to policy audits which do not explicitly test for vulnerabilities but rather test the compliance of file contents (e.g., configuration files) regarding a given policy.

The GSM provides a policy module to check if a file content is compliant with a given policy.



In general, this is an authenticated scan, i.e., the scan engine will have to log into the target system to perform the check (see Chapter 10.3 (page 253)).

The file content check can only be performed on systems supporting the command `grep`. Normally this means Linux or Linux-like systems.

Four different VTs in the VT family *Policy* provide the file content check:

- *File Content*: this VT performs the actual file content check.
- *File Content: Errors*: this VT shows the files in which errors occurred (e.g., the file is not found on the target system).
- *File Content: Matches*: this VT shows the patterns and files which passed the file content check (the predefined pattern matches in the file).
- *File Content: Violations*: this VT shows the patterns and files which did not pass the file content check (the predefined pattern does not match in the file).

12.4.1.1 Checking File Content Patterns

1. Create a reference file with the patterns to check. Following is an example:

```
filename|pattern|presence/absence
/tmp/filecontent_test|^parameter1=true.*$|presence
/tmp/filecontent_test|^parameter2=true.*$|presence
/tmp/filecontent_test|^parameter3=true.*$|absence
/tmp/filecontent_notthere|^parameter3=true.*$|absence
```

Note: This file must contain the row `filename|pattern|presence/absence`.

The subsequent rows each contain a test entry.

Each row contains three fields which are separated by `|`.

The first field contains the path and file name, the second field contains the pattern to check (as a regular expression) and the third field indicates if a pattern has to be present or absent.

2. Select *Resilience > Compliance Policies* in the menu bar.
3. In the row of the desired policy click .
→ The cloned policy is displayed on the page *Policies*.
4. In the row of the cloned policy click .
5. In the section *Edit Network Vulnerability Test Families* click for the VT family *Policy*.
→ All VTs that allow special configuration are listed (see Fig. 12.9).
6. Click for *File Content*.
7. Activate the checkbox *Upload file* (see Fig. 12.10).

Tip: If a reference file was already uploaded, the checkbox *Replace existing file* is displayed instead. The possibility to change the reference file is only available if the policy is currently not used.

8. Click *Browse...* and select the previously created reference file.
9. Click *Save* to save the VT.
10. Click *Save* to save the family of VTs.



Edit Policy Family Policy						
Skipped						
EU General Data Protection Regulation	1.3.6.1.4.1.25623.1.0.109180	0.0 (Log)	default	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
File Checksums	1.3.6.1.4.1.25623.1.0.103940	0.0 (Log)	default	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
File Checksums: Errors	1.3.6.1.4.1.25623.1.0.103943	0.0 (Log)	default	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
File Checksums: Matches	1.3.6.1.4.1.25623.1.0.103941	0.0 (Log)	default	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
File Checksums: Violations	1.3.6.1.4.1.25623.1.0.103942	10.0 (High)	default	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
File Content	1.3.6.1.4.1.25623.1.0.103944	0.0 (Log)	default	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
File Content: Errors	1.3.6.1.4.1.25623.1.0.103947	0.0 (Log)	default	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
File Content: Matches	1.3.6.1.4.1.25623.1.0.103945	0.0 (Log)	default	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
File Content: Violations	1.3.6.1.4.1.25623.1.0.103946	10.0 (High)	default	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Linux: AIDE configuration status	1.3.6.1.4.1.25623.1.0.109731	0.0 (Log)	default	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Linux: Accept IPv6 router advertisements	1.3.6.1.4.1.25623.1.0.109765	0.0 (Log)	default	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Linux: Accept source routed packets	1.3.6.1.4.1.25623.1.0.109757	0.0 (Log)	default	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Linux: Access /etc/group	1.3.6.1.4.1.25623.1.0.109812	0.0 (Log)	default	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Fig. 12.9: Editing the family of VTs

Edit Policy NVT File Content						
Name	File Content					
Policy	Base policy					
Family	Policy					
OID	1.3.6.1.4.1.25623.1.0.103944					
Last Modified	Mon, Nov 20, 2017 8:54 AM UTC					
Summary						
Checks for policy violations of file content						
Vulnerability Scoring						
CVSS base	0.0 (Log)					
CVSS base vector	AV:N AC:L Au:N/C:N/I:N/A:N					
Name	New Value	Default Value				
Timeout	<input checked="" type="radio"/> Apply default timeout <input type="radio"/>					
Target File Policies	<input checked="" type="checkbox"/> Upload file <input type="button" value="Browse..."/> ref_file					

Fig. 12.10: Uploading the reference file



11. Click Save to save the policy.

12.4.1.2 Changing the Severity

The severities of the VTs depend on the GOS version used. Since GOS 4.2, the VTs of the type *Violations* have a default severity of 10.

In the past, these VTs had a default severity of 0 (log message) and overrides were required for different severities. The new default severity of 10 can be changed using overrides as well (see Chapter 11.8 (page 338)).

By sectioning into three different VTs, it is possible to create distinct overrides for the severity according to the needs.

In the following example the severities of *File Content: Violations* and *File Content: Errors* have been changed which will be shown in the reports accordingly (see Fig. 12.11).

Text	NVT ▲	Hosts	Location	From	To	Active	Actions
File Content Violation	File Content: Violations			Any	5.0 (Medium)	yes	
Error on File System	File Content: Errors			Any	10.0 (High)	yes	

(Applied filter: rows=10 sort=nvt first=1) ◀ ◀ 1 - 2 of 2 ▶ ▶

Fig. 12.11: Overrides changing the severity

12.4.2 Checking Registry Content

The registry²⁴ is a database in Microsoft Windows containing important information about system hardware, installed programs, settings and user accounts on the computer. Microsoft Windows continually refers to the information in the registry.

Due to the nature of the Microsoft Windows registry every program/application installed under Microsoft Windows will register itself in the Microsoft Windows registry. Even malware and other malicious code usually leave traces within the registry.

The registry can be utilized to search for specific applications or malware related information such as version levels and numbers. Also, missing or changed registry settings could point to a potential security policy violation on an endpoint.

The GSM provides a policy module to verify registry entries on target systems. This module checks for the presence or absence of registry settings as well as registry violations.

Since the registry is unique to Microsoft Windows systems, this check can only be run on these systems.

To access the registry on the target system an authenticated scan has to be run.

Four different VTs in the VT family *Policy* provide the registry content check:

- *Windows Registry Check*: this VT performs the actual registry content check on the files.
- *Windows Registry Check: Errors*: this VT shows the files in which errors occurred (e.g., registry content not found on the target system).
- *Windows Registry Check: OK*: this VT shows the registry settings which passed the registry check (right registry content).
- *Windows Registry Check: Violations*: this VT shows the registry content which did not pass the registry check (wrong registry content).

²⁴ <https://docs.microsoft.com/en-us/windows/win32/sysinfo/registry>



12.4.2.1 Checking Registry Content Patterns

1. Create a reference file with the reference registry content. Following is an example:

```
Present|Hive|Key|Value|ValueType|ValueContent
TRUE|HKLM|SOFTWARE\Macromedia\FlashPlayer\SafeVersions|8.0|REG_DWORD|33
TRUE|HKLM|SOFTWARE\Microsoft\Internet Explorer
TRUE|HKLM|SOFTWARE\Microsoft\Internet Explorer\Version|REG_SZ|9.11.10240.16384
TRUE|HKLM|SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\
    System\LocalAccountTokenFilterPolicy|REG_DWORD|1
FALSE|HKLM|SOFTWARE\Virus
TRUE|HKLM|SOFTWARE\ShouldNotBeHere
TRUE|HKLM|SOFTWARE\Macromedia\FlashPlayer\SafeVersions|8.0|REG_DWORD|*
```

Note: This file must contain the row Present|Hive|Key|Value|ValueType|ValueContent.

The subsequent rows each contain a test entry.

Each row contains six fields which are separated by |.

The first field sets whether a registry entry should be present or not, the second the hive the registry entry is located in, the third the key, the fourth the value, the fifth the value type and the sixth the value content. If a star * is used in the last column any value is valid and accepted for existence or non-existence.

2. Select *Resilience > Compliance Policies* in the menu bar.
3. In the row of the policy *Microsoft Windows Registry Check* click .
- The cloned policy is displayed on the page *Policies*.
4. In the row of the cloned policy click .
5. In the section *Edit Network Vulnerability Test Families* click  for the VT family *Policy*.
- All VTs that allow special configuration are listed (see Fig. 12.12).

Edit Policy Family Policy						
rules						
Windows Defender Firewall: Public Profile: Allow unicast response	1.3.6.1.4.1.25623.1.0.109936		default	1	<input checked="" type="checkbox"/>	
Windows Defender Firewall: Public Profile: Apply local connection security rules	1.3.6.1.4.1.25623.1.0.109194		default	1	<input checked="" type="checkbox"/>	
Windows Defender Firewall: Public Profile: Apply local firewall rules	1.3.6.1.4.1.25623.1.0.109193		default	1	<input checked="" type="checkbox"/>	
Windows Registry Check	1.3.6.1.4.1.25623.1.0.105988		default	1	<input checked="" type="checkbox"/>	
Windows Registry Check: Errors	1.3.6.1.4.1.25623.1.0.105991		default	0	<input checked="" type="checkbox"/>	
Windows Registry Check: OK	1.3.6.1.4.1.25623.1.0.105989		default	0	<input checked="" type="checkbox"/>	
Windows Registry Check: Violations	1.3.6.1.4.1.25623.1.0.105990		default	0	<input checked="" type="checkbox"/>	
Windows file Checksums	1.3.6.1.4.1.25623.1.0.96180		default	5	<input checked="" type="checkbox"/>	
Windows file Checksums: Errors	1.3.6.1.4.1.25623.1.0.96182		default	0	<input checked="" type="checkbox"/>	
Windows file Checksums: Matches	1.3.6.1.4.1.25623.1.0.96181		default	0	<input checked="" type="checkbox"/>	
Windows file Checksums:	1.3.6.1.4.1.25623.1.0.96183		default	0	<input checked="" type="checkbox"/>	
<input type="button" value="Cancel"/>			<input type="button" value="Save"/>			

Fig. 12.12: Editing the family of VTs

6. Click  for *Windows Registry Check*.



7. Activate the checkbox *Upload file* (see Fig. 12.13).

Tip: If a reference file was already uploaded, the checkbox *Replace existing file* is displayed instead. The possibility to change the reference file is only available if the policy is currently not used.

Fig. 12.13: Uploading the reference file

8. Click *Browse...* and select the previously created reference file.
9. Click *Save* to save the VT.
10. Click *Save* to save the family of VTs.
11. Click *Save* to save the policy.

12.4.2.2 Changing the Severity

The severities of the VTs depend on the GOS version used. Since GOS 4.2, the VTs of the type *Violations* have a default severity of 10.

In the past, these VTs had a default severity of 0 (log message) and overrides were required for different severities. The new default severity of 10 can be changed using overrides as well (see Chapter 11.8 (page 338)).

By sectioning into three different VTs, it is possible to create distinct overrides for the severity according to the needs.

In the following example the severities of *Windows Registry Check: Violations* and *Windows Registry Check: Errors* have been changed which will be shown in the reports accordingly (see Fig. 12.14).

Text	NVT ▲	Hosts	Location	From	To	Active	Actions
Windows Registry Check: Violations	Windows Registry Check: Violations			Any	5.0 (Medium)	yes	
Windows Registry Check: Errors	Windows Registry Check: Errors			Any	10.0 (High)	yes	

Fig. 12.14: Overrides changing the severity



12.4.3 Checking File Checksums

File checksum checks belong to policy audits which do not explicitly test for vulnerabilities but rather for file integrity.

The GSM provides a policy module to verify file integrity on target systems. This module checks the file content by MD5 or SHA1 checksums.

In general, this is an authenticated check, i.e., the scan engine will have to log into the target system to perform the check.

The file checksum check can only be performed on systems supporting checksums. Normally this means Linux or Linux-like systems. However, the GSM provides a module for checksum checks for Microsoft Windows systems as well (see Chapter 12.4.3.3 (page 365)).

Four different VTs in the VT family *Policy* provide the file checksum check:

- *File Checksums*: this VT performs the actual checksum check on the files.
- *File Checksums: Errors*: this VT shows the files in which errors occurred (e.g., file not found on the target system).
- *File Checksums: Matches*: this VT shows the files which passed the checksum check (checksum matches).
- *File Checksums: Violations*: this VT shows the files which did not pass the checksum check (wrong checksum).

12.4.3.1 Checking File Checksum Patterns

1. Create a reference file with the reference checksums. Following is an example:

```
Checksum|File|Checksumtype
6597ecf8208cf64b2b0eaa52d8169c07|/bin/login|md5
ed3ed98cb2efa9256817948cd27e5a4d9be2bdb8|/bin/bash|sha1
7c59061203b2b67f2b5c51e0d0d01c0d|/bin/pwd|md5
```

Note: This file must contain the row `Checksum|File|Checksumtype`.

The subsequent rows each contain a test entry.

Each row contains three fields which are separated by `|`.

The first field contains the checksum in hex, the second field the path and file name and the third field the checksum type. Currently MD5 and SHA1 checksums are supported.

Important: Checksums and checksum types must be lowercase.

2. Select *Resilience > Compliance Policies* in the menu bar.
3. In the row of the desired policy click .
→ The cloned policy is displayed on the page *Policies*.
4. In the row of the cloned policy click .
5. In the section *Edit Network Vulnerability Test Families* click  for the VT family *Policy*.
→ All VTs that allow special configuration are listed (see Fig. 12.15).
6. Click  for *File Checksums*.



Edit Policy Family Policy						
Docker Compliance Check: Failed	1.3.6.1.4.1.25623.1.0.140122	10.0 (High)	default	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Docker Compliance Check: Passed	1.3.6.1.4.1.25623.1.0.140123	0.0 (Log)	default	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Docker Compliance Check: Skipped	1.3.6.1.4.1.25623.1.0.140125	0.0 (Log)	default	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
EU General Data Protection Regulation	1.3.6.1.4.1.25623.1.0.109180	0.0 (Log)	default	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
File Checksums	1.3.6.1.4.1.25623.1.0.103940	0.0 (Log)	default	3	<input checked="" type="checkbox"/>	<input type="checkbox"/>
File Checksums: Errors	1.3.6.1.4.1.25623.1.0.103943	0.0 (Log)	default	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
File Checksums: Matches	1.3.6.1.4.1.25623.1.0.103941	0.0 (Log)	default	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
File Checksums: Violations	1.3.6.1.4.1.25623.1.0.103942	10.0 (High)	default	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
File Content	1.3.6.1.4.1.25623.1.0.103944	0.0 (Log)	default	1	<input checked="" type="checkbox"/>	<input type="checkbox"/>
File Content: Errors	1.3.6.1.4.1.25623.1.0.103947	0.0 (Log)	default	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
File Content: Matches	1.3.6.1.4.1.25623.1.0.103945	0.0 (Log)	default	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
File Content: Violations	1.3.6.1.4.1.25623.1.0.103946	10.0 (High)	default	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Linux: AIDE configuration status	1.3.6.1.4.1.25623.1.0.109731	0.0 (Log)	default	1	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Fig. 12.15: Editing the family of VTs

7. Activate the checkbox *Upload file* (see Fig. 12.16).

Tip: If a reference file was already uploaded, the checkbox *Replace existing file* is displayed instead. The possibility to change the reference file is only available if the policy is currently not used.

Edit Policy NVT File Checksums						
Name	File Checksums					
Policy	Base policy					
Family	Policy					
OID	1.3.6.1.4.1.25623.1.0.103940					
Last Modified	Mon, Jul 30, 2018 9:29 AM UTC					
Summary						
Checks the checksums (MD5 or SHA1)of specified files.						
The SSH protocol is used to log in and to gather the needed information						
Vulnerability Scoring						
CVSS base	0.0 (Log)	CVSS base vector	AV:N AC:L Au:N C:N I:N A:N			
Name	New Value	Default Value				
Timeout	<input checked="" type="radio"/> Apply default timeout <input type="radio"/>					
timeout	600	600				
Target checksum File	<input checked="" type="checkbox"/> Upload file <input type="button" value="Browse..."/>	ref_file				
List all and not only the first 100 entries	<input type="radio"/> Yes <input checked="" type="radio"/> No	no				

Fig. 12.16: Uploading the reference file

8. Click *Browse...* and select the previously created reference file.



9. Click Save to save the VT.
10. Click Save to save the family of VTs.
11. Click Save to save the policy.

12.4.3.2 Changing the Severity

The severities of the VTs depend on the GOS version used. Since GOS 4.2, the VTs of the type *Violations* have a default severity of 10.

In the past, these VTs had a default severity of 0 (log message) and overrides were required for different severities. The new default severity of 10 can be changed using overrides as well (see Chapter 11.8 (page 338)).

By sectioning into three different VTs, it is possible to create distinct overrides for the severity according to the needs.

In the following example the severities of *File Checksum: Violations* and *File Checksum: Errors* have been changed which will be shown in the reports accordingly (see Fig. 12.17).

Text	NVT ▲	Hosts	Location	From	To	Active	Actions
File Checksum Violations	File Checksums: Violations	Any			5.0 (Medium)	yes	
File Checksum Errors	File Checksums: Errors	Any			10.0 (High)	yes	

(Applied filter: rows=10 sort=nvt first=1) 1 - 2 of 2

Fig. 12.17: Overrides changing the severity

12.4.3.3 Checking File Checksum Patterns for Microsoft Windows

The GSM provides a similar module for Microsoft Windows systems for file checksum checks.

Since Microsoft Windows does not provide an internal program for creating checksums it has to be installed one either manually or automatically by the VT. The GSM uses ReHash²⁵ for creating checksums on Microsoft Windows systems.

Note: There are two operating modes for these checks:

- Using a tool that was installed on the target system manually.
- The tool ReHash will automatically be installed and deinstalled as well if requested on the target system during the checking routine.

As for Linux systems the VTs for checksum checks are located in the VT family *Policy*.

1. Create a reference file with the patterns to check. Following is an example:

```
Checksum|File|Checksumtype
6597ecf8208cf64b2b0eaa52d8169c07|/bin/login|md5
ed3ed98cb2efa9256817948cd27e5a4d9be2bdb8|/bin/bash|sha1
7c59061203b2b67f2b5c51e0d0d01c0d|/bin/pwd|md5
```

2. In the row of the respective policy click .
3. In the section *Edit Network Vulnerability Test Families* click for the VT family *Policy*.
→ All VTs that allow special configuration are listed (see Fig. 12.18).

²⁵ <http://rehash.sourceforge.net/>



Edit Policy Family Policy						
Windows Defender Firewall: Public Profile: Apply local firewall rules	1.3.6.1.4.1.25623.1.0.109193	0.0 (Log)	default	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Windows Registry Check	1.3.6.1.4.1.25623.1.0.105988	0.0 (Log)	default	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Windows Registry Check: Errors	1.3.6.1.4.1.25623.1.0.105991	0.0 (Log)	default	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Windows Registry Check: OK	1.3.6.1.4.1.25623.1.0.105989	0.0 (Log)	default	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Windows Registry Check: Violations	1.3.6.1.4.1.25623.1.0.105990	10.0 (High)	default	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Windows file Checksums	1.3.6.1.4.1.25623.1.0.96180	0.0 (Log)	default	5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Windows file Checksums: Errors	1.3.6.1.4.1.25623.1.0.96182	0.0 (Log)	default	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Windows file Checksums: Matches	1.3.6.1.4.1.25623.1.0.96181	0.0 (Log)	default	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Windows file Checksums: Violations	1.3.6.1.4.1.25623.1.0.96183	10.0 (High)	default	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Windows: disabled domain users	1.3.6.1.4.1.25623.1.0.109026	0.0 (Log)	default	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Windows: domain users password age	1.3.6.1.4.1.25623.1.0.109030	0.0 (Log)	default	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Windows: domain users password never expires	1.3.6.1.4.1.25623.1.0.109025	0.0 (Log)	default	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Fig. 12.18: Editing the family of VTs

4. Click for *Windows file Checksums*.
5. For *Delete hash test Programm after the test* select the radio button *Yes* if the checksum program ReHash should be deleted after the check (see Fig. 12.19).

Tip: The program can be left on the target system, e.g., to speed up recurring tests and therefore does not have to be transferred each time.

6. For *Install hash test Programm on the Target* select the radio button *Yes* if the checksum program ReHash should be installed on the target system automatically.

Note: If it is not installed automatically, it has to be installed manually under C:\Windows\system32 (on 32-bit systems) or C:\Windows\SysWOW64 (on 64-bit systems) and has to be executable for the authenticated user.

7. Activate the checkbox *Upload file*.

Tip: If a reference file was already uploaded, the checkbox *Replace existing file* is displayed instead. The possibility to change the reference file is only available if the policy is currently not used.

8. Click *Browse...* and select the previously created reference file.
9. Click *Save* to save the VT.
10. Click *Save* to save the family of VTs.
11. Click *Save* to save the policy.



Edit Policy NVT Windows file Checksums

Name	Windows file Checksums
Policy	Base policy
Family	Policy
OID	1.3.6.1.4.1.25623.1.0.96180
Last Modified	Wed, Mar 13, 2019 7:32 AM UTC

Summary

Checks the checksums (MD5 or SHA1) of specified files in Windows

Vulnerability Scoring

CVSS base	0.0 (Log)	
CVSS base vector	AV:N AC:L Au:N/C:N/I:N/A:N	
Name	New Value	Default Value
Timeout	<input checked="" type="radio"/> Apply default timeout <input type="radio"/>	
timeout	600	600
List all and not only the first 100 entries	<input type="radio"/> Yes <input checked="" type="radio"/> No	no
Install hash test Programm on the Target	<input checked="" type="radio"/> Yes <input type="radio"/> No	no
Delete hash test Programm after the test	<input checked="" type="radio"/> Yes <input type="radio"/> No	yes
Target checksum File	<input checked="" type="checkbox"/> Upload file <input type="button" value="Browse..."/> ref_file	

Buttons: Cancel, Save

Fig. 12.19: Uploading the reference file

12.4.4 Performing CPE-Based Checks

For detailed information about Common Platform Enumeration (CPE) see Chapter 14.2.2 (page 389).

12.4.4.1 Simple CPE-Based Checks for Security Policies

With any executed scan, CPEs for the identified products are stored. This happens independently of whether the product actually reveals a security problem or not. On this basis it is possible to describe simple security policies and the checks for compliance with these.

With the Greenbone Security Manager it is possible to describe policies to check for the presence as well as for the absence of a product. These cases can be associated with a severity to appear in the scan report.

The examples demonstrate how to check the compliance of a policy regarding specific products in an IT infrastructure and how the reporting with the corresponding severity can be done.

The information about whether a certain product is present on the target system is gathered by a single Vulnerability Test (VT) or even independently by a number of special VTs. This means that for a certain product an optimized policy that only concentrates on this product and does not do any other scan activity can be specified.

12.4.4.2 Detecting the Presence of Problematic Products

This example demonstrates how the presence of a certain product in an IT infrastructure is classified as a severe problem and reported as such.

1. Select *Resilience > Compliance Policies* in the menu bar.
 2. Create a new policy by clicking
 3. Define the name of the policy.
 4. Click *Save*.
- The policy is created and displayed on the page *Policies*.



5. In the row of the policy click .
6. Unfold the section *Network Vulnerability Test Preferences* by clicking .
→ All VTs that allow special configuration are listed (see Fig. 12.20).

Edit Policy CPE based compliance			
OPTIONS for Brute Force INV IS	Disable default account checks	no	<input checked="" type="checkbox"/>
SSL/TLS: Version Detection Report	Report TLS version	no	<input checked="" type="checkbox"/>
Response Time / No 404 Error Code Check	Maximum response time (in seconds)	60	<input checked="" type="checkbox"/>
File Checksums	Target checksum File		<input checked="" type="checkbox"/>
File Checksums	List all and not only the first 100 entries	no	<input checked="" type="checkbox"/>
File Content	Target File Policies		<input checked="" type="checkbox"/>
CPE Policy Check	Single CPE	cpe:/	<input checked="" type="checkbox"/>
CPE Policy Check	CPE List		<input checked="" type="checkbox"/>
CPE Policy Check	Check for	present	<input checked="" type="checkbox"/>
Checks for open UDP ports	Silent	yes	<input checked="" type="checkbox"/>
Create System Characteristics	Create OVAL System Characteristics	no	<input checked="" type="checkbox"/>
Launch Nmap for Network Scanning	Source port		<input checked="" type="checkbox"/>
Launch Nmap for Network Scanning	Timing policy	Normal	<input checked="" type="checkbox"/>
Launch Nmap for Network Scanning	Host Timeout (ms)		<input checked="" type="checkbox"/>
Launch Nmap for Network Scanning	Min RTT Timeout (ms)		<input checked="" type="checkbox"/>
Launch Nmap for Network Scanning	Max RTT Timeout (ms)		<input checked="" type="checkbox"/>
<input type="button" value="Cancel"/>		<input type="button" value="Save"/>	

Fig. 12.20: Overview of VTs

7. A single CPE (Internet Explorer 6) will be searched.

Click for the VT *CPE Policy Check – Single CPE*.

Tip: This short-cut avoids having to click through the family structures in the section *Edit Network Vulnerability Test Families* to get to the desired VT (the here used VT is in the VT family *Policy*).

8. Enter `cpe:/a:microsoft:ie:6` in the input box *Single CPE* (see Fig. 12.21).
9. For this example the stated CPEs must be present to comply.
Select the radio button *present*.
10. Click **Save** to save the VT.
11. Click **Save** to save the policy.

Note: The severities of the VTs depend on the GOS version used. Since GOS 4.2, the VTs of the type *Violations* have a default severity of 10.

In the past, these VTs had a default severity of 0 (log message) and overrides were required for different severities. The new default severity of 10 can be changed using overrides as well (see Chapter 11.8 (page 338)).

Note: In case the mere availability of a product should be considered it is required to configure remote access using credentials to apply local security checks (see Chapter 10.3.2 (page 255)). If just running network services should be searched it normally does not help but rather increase the number of false positives.



Edit Policy NVT CPE Policy Check

Name	CPE Policy Check
Policy	CPE based compliance
Family	Policy
OID	1.3.6.1.4.1.25623.1.0.103962
Last Modified	Fri, Sep 21, 2018 7:07 PM UTC

Summary

This NVT is running CPE-based Policy Checks.

Vulnerability Scoring

CVSS base	0.0 (Log)	
CVSS base vector	AV:N AC:L Au:N C:N I:N A:N	
Name	New Value	Default Value
Timeout	<input checked="" type="radio"/> Apply default timeout <input type="radio"/>	
Single CPE	cpe:/a:microsoft:ie:6	cpe:/
CPE List	<input type="checkbox"/> Upload file <input type="button" value="Browse..."/> No file selected.	
Check for	<input checked="" type="radio"/> present <input type="radio"/> missing	present

Buttons: Cancel, Save

Fig. 12.21: Editing *CPE Policy Check – Single CPE*

12. Create a new target (see Chapter 10.2.1 (page 248)), create a new audit (see Chapter 12.2.1.1 (page 352)) and run the audit (see Chapter 12.2.2 (page 354)).
When creating the audit, use the previously created policy.
13. When the scan is completed select *Scans > Reports* in the menu bar.

Tip: To show only the results of the CPE-based policy checks, a suitable filter can be applied.

14. Enter `cpe` in the input box *Filter*.
→ The reports for CPE-based policy checks are displayed.
15. Click on the date of a report.
→ The report for CPE-based policy checks is displayed.
The report can be used as described in Chapter 11.2.1 (page 320).
In this example: if Internet Explorer 6 was found on one of the target systems it is reported as a problem.

12.4.4.3 Detecting the Absence of Important Products

This example shows how the absence of a certain product in the IT infrastructure is defined and reported as a severe problem.

1. Select *Resilience > Compliance Policies* in the menu bar.
2. Create a new policy by clicking .
3. Define the name of the policy.
4. Click *Save*.
→ The policy is created and displayed on the page *Policies*.
5. In the row of the policy click .



6. Unfold the section *Network Vulnerability Test Preferences* by clicking □.

→ All VTs that allow special configuration are listed (see Fig. 12.22).

Edit Policy CPE based compliance			
Options for Brute Force Inv Is	Disable default account checks	no	<input checked="" type="checkbox"/>
SSL/TLS: Version Detection Report	Report TLS version	no	<input checked="" type="checkbox"/>
Response Time / No 404 Error Code Check	Maximum response time (in seconds)	60	<input checked="" type="checkbox"/>
File Checksums	Target checksum File		<input checked="" type="checkbox"/>
File Checksums	List all and not only the first 100 entries	no	<input checked="" type="checkbox"/>
File Content	Target File Policies		<input checked="" type="checkbox"/>
CPE Policy Check	Single CPE	cpe:/	<input checked="" type="checkbox"/>
CPE Policy Check	CPE List		<input checked="" type="checkbox"/>
CPE Policy Check	Check for	present	<input checked="" type="checkbox"/>
Checks for open UDP ports	Silent	yes	<input checked="" type="checkbox"/>
Create System Characteristics	Create OVAL System Characteristics	no	<input checked="" type="checkbox"/>
Launch Nmap for Network Scanning	Source port		<input checked="" type="checkbox"/>
Launch Nmap for Network Scanning	Timing policy	Normal	<input checked="" type="checkbox"/>
Launch Nmap for Network Scanning	Host Timeout (ms)		<input checked="" type="checkbox"/>
Launch Nmap for Network Scanning	Min RTT Timeout (ms)		<input checked="" type="checkbox"/>
Launch Nmap for Network Scanning	Max RTT Timeout (ms)		<input checked="" type="checkbox"/>
<input type="button" value="Cancel"/>		<input type="button" value="Save"/>	

Fig. 12.22: Overview of VTs

7. A single CPE (Norton Antivirus) will be searched.

Click for the VT *CPE Policy Check – Single CPE*.

Tip: This short-cut avoids having to click through the family structures in the section *Edit Network Vulnerability Test Families* to get to the desired VT (the here used VT is in the VT family *Policy*).

8. Enter `cpe:/a:symantec:norton_antivirus` in the input box *Single CPE* (see Fig. 12.23).

9. For this example the stated CPEs must be missing to comply.

Select the radio button *missing*.

10. Click *Save* to save the VT.

11. Click *Save* to save the policy.

Note: The severities of the VTs depend on the GOS version used. Since GOS 4.2, the VTs of the type *Violations* have a default severity of 10.

In the past, these VTs had a default severity of 0 (log message) and overrides were required for different severities. The new default severity of 10 can be changed using overrides as well (see Chapter 11.8 (page 338)).

Note: In case the mere availability of a product should be considered it is required to configure remote access using credentials to apply local security checks (see Chapter 10.3.2 (page 255)). If just running network services should be searched it normally does not help but rather increase the number of false positives.



Edit Policy NVT CPE Policy Check

Name	CPE Policy Check
Policy	CPE based compliance
Family	Policy
OID	1.3.6.1.4.1.25623.1.0.103962
Last Modified	Fri, Sep 21, 2018 7:07 PM UTC

Summary

This NVT is running CPE-based Policy Checks.

Vulnerability Scoring

CVSS base	0.0 (Log)	
CVSS base vector	AV:N AC:L Au:N C:N I:N A:N	
Name	New Value	Default Value
Timeout	<input checked="" type="radio"/> Apply default timeout <input type="radio"/>	
Single CPE	cpe:/a:symantec:norton_antivirus	cpe:/
CPE List	<input type="checkbox"/> Upload file <input type="button" value="Browse..."/> No file selected.	
Check for	<input type="radio"/> present <input checked="" type="radio"/> missing	present

Buttons: Cancel, Save

Fig. 12.23: Editing *CPE Policy Check – Single CPE*

12. Create a new target (see Chapter 10.2.1 (page 248)), create a new audit (see Chapter 12.2.1.1 (page 352)) and run the audit (see Chapter 12.2.2 (page 354)).
When creating the audit, use the previously created policy.
13. When the scan is completed select *Scans > Reports* in the menu bar.

Tip: To show only the results of the CPE-based policy checks, a suitable filter can be applied.

14. Enter `cpe` in the input box *Filter*.
→ The reports for CPE-based policy checks are displayed.
15. Click on the date of a report.
→ The report for CPE-based policy checks is displayed.
The report can be used as described in Chapter 11.2.1 (page 320).
In this example: if Norton Antivirus was not found on one of the target systems it is reported as missing.



12.5 Checking Standard Policies

12.5.1 IT-Grundschatz

The German Federal Office for Information Security (BSI)²⁶ publishes the IT-Grundschatz catalogs²⁷, a collection of documents that provide useful information for detecting weaknesses and combating attacks on IT environments.

Greenbone Networks provides a policy for testing the compliance with the following modules of the IT-Grundschatz compendium:

- SYS.1.2.2 Windows Server 2012
- SYS.1.3 Server on Linux and Unix
- SYS.2.2.2 Clients on Windows 8.1
- SYS.2.2.3 Clients on Windows 10
- SYS.2.3 Clients on Linux and Unix

An IT-Grundschatz scan can be carried out as follows:

1. Create a new target (see Chapter 10.2.1 (page 248)), create a new audit (see Chapter 12.2.1.1 (page 352)) and run the audit (see Chapter 12.2.2 (page 354)).

When creating the audit, use the policy *IT-Grundschatz*.

2. When the scan is completed select *Scans > Reports* in the menu bar.

3. Click on the date of the report.

→ The report for the IT-Grundschatz scan is displayed.

The report can be used as described in Chapter 11.2.1 (page 320). The report contains detailed information about compliant, not compliant and incomplete requirements.

4. To export the report click .

5. For *Include* activate the checkbox *Notes* to include attached notes and the checkbox *Overrides* to label enabled overrides and include their text field (see Chapter 11.2.2 (page 324)).

6. Select *GCR PDF* in the drop-down list *Report Format*.

7. Click *OK* and download the PDF file.

²⁶ https://www.bsi.bund.de/EN/TheBSI/thebsi_node.html

²⁷ https://www.bsi.bund.de/EN/Topics/ITGrundschatz/itgrundschatz_node.html



12.5.2 BSI TR-03116: Kryptographische Vorgaben für Projekte der Bundesregierung

The German Federal Office for Information Security (BSI) published a technical guideline TR-03116: Kryptographische Vorgaben für Projekte der Bundesregierung²⁸. Part 4 of this guideline describes the security requirements for services of the federal government using the cryptographic protocols SSL/TLS, S/MIME and OpenPGP.

The requirements are based on forecasts for the security of the algorithms and key lengths for the next years.

Greenbone Networks provides a policy for testing the compliance of services with the technical guideline “TR-03116”.

The policy tests if the scanned hosts and services use SSL/TLS. If this is the case, the compliance with the guideline is tested.

The policy states three main requirements:

TLS version TLS versions lower than 1.2 are not allowed.

Supported ciphers If TLS 1.2 is enabled, one of the following ciphers has to be supported:

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

If TLS 1.3 is enabled, cipher TLS_AES_128_GCM_SHA256 has to be supported.

Allowed cipher suites If TLS 1.2 is enabled, only the following cipher suites are allowed:

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA

²⁸ https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03116/TR-03116_node.html



If TLS 1.3 is enabled, only the following cipher suites are allowed:

- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384
- TLS_AES_128_CCM_SHA256

A BSI TR-03116 scan can be carried out as follows:

1. Create a new target (see Chapter 10.2.1 (page 248)), create a new audit (see Chapter 12.2.1.1 (page 352)) and run the audit (see Chapter 12.2.2 (page 354)).

When creating the audit, use the policy *BSI TR-03116: Part 4*.

2. When the scan is completed select *Scans > Reports* in the menu bar.

3. Click on the date of the report.

→ The report for the BSI TR-03116 scan is displayed.

The report can be used as described in Chapter 11.2.1 (page 320). The report contains detailed information about compliant, not compliant and incomplete requirements.

4. To export the report click

5. For *Include* activate the checkbox *Notes* to include attached notes and the checkbox *Overrides* to label enabled overrides and include their text field (see Chapter 11.2.2 (page 324)).

6. Select *GCR PDF* in the drop-down list *Report Format*.

7. Click *OK* and download the PDF file.

12.5.3 BSI TR-02102: Kryptographische Verfahren: Empfehlungen und Schlüssellängen

The German Federal Office for Information Security (BSI) published a technical guideline TR-02102: Kryptographische Verfahren: Empfehlungen und Schlüssellängen²⁹. Part 4 of this guideline describes the recommendations for the use of the Secure Shell (SSH) cryptographic protocol.

Greenbone Networks provides a policy for testing the compliance of services with the technical guideline “TR-02102”.

The following SSH settings in the file `/etc/ssh/sshd_config` are tested in the policy:

- Protocol (OID: 1.3.6.1.4.1.25623.1.0.150066): SSH version 2 has to be used.
- KexAlgorithms (OID: 1.3.6.1.4.1.25623.1.0.150077): the following algorithms are allowed for key exchange during SSH connection establishment: diffie-hellman-group-exchange-sha256, diffie-hellman-group14-sha256, diffie-hellman-group15-sha512, diffie-hellman-group16-sha512, rsa2048-sha256, ecdh-sha2-*
- ReKeyLimit (OID: 1.3.6.1.4.1.25623.1.0.150560): the key material of a connection must be renewed after 1 hour or 1 GiB of transferred data.
- Ciphers (OID: 1.3.6.1.4.1.25623.1.0.150225): the following encryption methods are allowed: AEAD_AES_128_GCM, AEAD_AES_256_GCM, aes256-cbc, aes192-cbc, aes128-cbc, aes128-ctr, aes192-ctr, aes256-ctr
- MACs (OID: 1.3.6.1.4.1.25623.1.0.109795): the following MACs are allowed: hmac-sha1, hmac-sha2-256, hmac-sha2-512

²⁹ <https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr-02102.html?nn=451438>



- HostKeyAlgorithms (OID: 1.3.6.1.4.1.25623.1.0.150559): the following methods for server authentication are allowed: pgp-sign-rsa, pgp-sign-dss, ecdsa-sha2-, x509v3-rsa2048-sha256, x509v3-ecdsa-sha2-
- AuthenticationMethods (OID: 1.3.6.1.4.1.25623.1.0.150561): the public key authentication (*publickey*) has to be used.
- PubkeyAuthentication (OID: 1.3.6.1.4.1.25623.1.0.150222): the public key authentication (*publickey*) has to be allowed.

A BSI TR-02102 scan can be carried out as follows:

1. Create a new target (see Chapter 10.2.1 (page 248)), create a new audit (see Chapter 12.2.1.1 (page 352)) and run the audit (see Chapter 12.2.2 (page 354)).

When creating the audit, use the policy *BSI TR-02102-4*.

2. When the scan is completed select *Scans > Reports* in the menu bar.

3. Click on the date of the report.

→ The report for the BSI TR-02102 scan is displayed.

The report can be used as described in Chapter 11.2.1 (page 320). The report contains detailed information about compliant, not compliant and incomplete requirements.

4. To export the report click ↴.

5. For *Include* activate the checkbox *Notes* to include attached notes and the checkbox *Overrides* to label enabled overrides and include their text field (see Chapter 11.2.2 (page 324)).

6. Select *GCR PDF* in the drop-down list *Report Format*.

7. Click *OK* and download the PDF file.



12.6 Running a TLS Map Scan

The TLS (Transport Layer Security) protocol ensures the confidentiality, authenticity and integrity of communication in insecure networks. It establishes confidential communication between sender and receiver, e.g., web server and web browser.

With the Greenbone Security Manager (GSM) it is possible to identify systems that offer services using SSL/TLS protocols. Additionally, the GSM detects the protocol versions and offers encryption algorithms. Further details about the service can be achieved in case it can be properly identified.

12.6.1 Checking for TLS and Exporting the Scan Results

For an overview on TLS usage in the network or on single systems, Greenbone Networks recommends using the scan configuration *TLS-Map*. This scan configuration identifies the used protocol versions and the offered encryption algorithms. Additionally, it tries to identify in-depth details of the service.

1. Select *Configuration > Port Lists* in the menu bar to have a look at the pre-configured port lists.

Note: By clicking own port lists can be created (see Chapter 10.7.1 (page 286)).

2. Choose a suitable list of ports that should be scanned.

Note: Pay attention that all ports of interest are covered by the list.

The more extensive the list the longer the scan will take but this may also detect services at unusual ports.

Consider that the TLS protocol is based on the TCP protocol. A port list with UDP ports will slow down the scan without benefits. If any TCP ports should be covered *All TCP* should be selected.

3. Create a new target (see Chapter 10.2.1 (page 248)), create a new task (see Chapter 10.2.2 (page 251)) and run the task (see Chapter 10.2.3 (page 253)).

When creating the task, use the scan configuration *TLS-Map*.

4. When the scan is completed select *Scans > Reports* in the menu bar.

5. Click on the date of the report.

→ The report for the TLS-Map scan is displayed.

The report can be used as described in Chapter 11.2.1 (page 320).

6. To export the report click .

7. For *Include* activate the checkbox *Notes* to include attached notes and the checkbox *Overrides* to label enabled overrides and include their text field (see Chapter 11.2.2 (page 324)).

8. Select *TLS Map* in the drop-down list *Report Format*.

9. Click *OK* and download the CSV file.

→ The report can be used in spreadsheet applications.

The file contains one line per port and systems where an SSL/TLS protocol is offered:

```
IP,Host,Port,TLS-Version,Ciphers,Application-CPE
192.168.12.34,www.local,443,TLSv1.0;SSLv3,SSL3_RSA_RC4_128_SHA;TLS1_RSA_RC4_128_SHA,
cpe:/a:apache:http_server:2.2.22;cpe:/a:php:php:5.4.4
```

(continues on next page)



(continued from previous page)

```
192.168.56.78, www2.local, 443, TLSv1.0;SSLv3,SSL3_RSA_RC4_128_SHA;TLS1_RSA_RC4_128_SHA,  
cpe:/a:apache:http_server:2.2.22
```

Separated by commas, each line contains the following information:

- **IP** The IP address of the system where the service was detected.
- **Host** The DNS name of the system in case it is available.
- **Port** The port where the service was detected.
- **TLS-Version** The protocol version offered by the service. In case more than one is offered, the versions are separated with semicolons.
- **Ciphers** The encryption algorithms offered by the service. In case more than one is offered, the algorithms are separated with semicolons.
- **Application-CPE** The detected application in CPE format. In case more than one is identified, the applications are separated with semicolons.

CHAPTER 13

Managing Assets

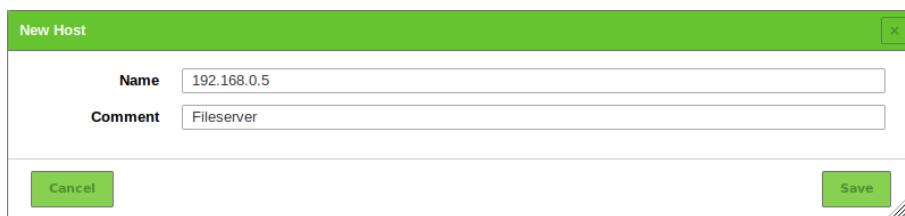
When creating a new task it can be defined whether the results of the scan should be stored in the assets (see Chapter 10.2.2 (page 251)).

13.1 Creating and Managing Hosts

13.1.1 Creating a Host

Hosts can be added to the asset management as follows:

1. Select *Assets > Hosts* in the menu bar.
2. Create a new host by clicking  in the upper left corner of the page.
3. Enter the IP address of the host in the input box *Name* (see Fig. 13.1).



New Host	
Name	192.168.0.5
Comment	Fileserver
<input type="button" value="Cancel"/>	<input type="button" value="Save"/>

Fig. 13.1: Creating a new host

4. Click *Save*.

This feature is also available via GMP (see Chapter 15 (page 399)). The import of hosts from a configuration management database can be achieved using this option.



13.1.2 Managing Hosts

List Page

All existing hosts can be displayed by selecting *Assets > Hosts* in the menu bar (see Fig. 13.2).

Name	Hostname ▲	IP Address	OS	Severity	Modified	Actions
192.168.0.12	scan-target-2.greenbone.net	192.168.0.12	Windows	0.0 (Log)	Thu, Oct 18, 2018 3:03 PM UTC	X Edit Create Export
192.168.126.4	scan-target-3.greenbone.net	192.168.126.4	Ubuntu	0.0 (Log)	Fri, Jul 12, 2019 1:05 PM UTC	X Edit Create Export
192.168.117.12	scan-target.greenbone.net	192.168.117.12	Ubuntu	0.0 (Log)	Fri, Jul 12, 2019 1:05 PM UTC	X Edit Create Export
127.0.0.8	localhost	127.0.0.8	Ubuntu	4.8 (Medium)	Fri, Jul 12, 2019 1:05 PM UTC	X Edit Create Export
192.168.0.127	scan-target-4.greenbone.net	192.168.0.127	Ubuntu	0.0 (Log)	Fri, Jul 12, 2019 1:05 PM UTC	X Edit Create Export
127.0.0.8	localhost	127.0.0.8	Ubuntu	0.0 (Log)	Thu, Oct 18, 2018 3:03 PM UTC	X Edit Create Export
192.168.117.83	scan-target-1.greenbone.net	192.168.117.83	Ubuntu	0.0 (Log)	Thu, Oct 18, 2018 3:03 PM UTC	X Edit Create Export

Fig. 13.2: Page *Hosts* displaying all scanned hosts

For all hosts the following actions are available:

- X Delete the host.
- Edit the host.
- Create a new target from the host (see Chapter 13.1.3 (page 380)).
- Export the host as an XML file.

Note: By clicking X, Export or Create below the list of hosts more than one host can be deleted, exported or used to create a new target at a time. The drop-down list is used to select which hosts are deleted, exported or used to create a new target.

Details Page

Click on the name of a host to display the details of the host. Click + to open the details page of the host.

The following registers are available:

Information General information about the host.

Any identifying information collected for the host during scans, e.g., host names, IP and MAC addresses, operating systems, SSH keys and X.509 certificates, is displayed in the section *All Identifiers* (see Fig. 13.3).

Note: If identifiers have duplicates, only the latest identifiers are shown. In this case, the section is named *Latest Identifiers* and all identifiers can be displayed by clicking *Show all Identifiers* below the table.

For all host identifiers the following action is available:

- X Delete the identifier.

User Tags Assigned tags (see Chapter 8.5 (page 214)).



Information	User Tags (1)	Permissions (0)		
Hostname DCHV1R01.local				
IP Address 10.1.11.111				
Comment				
OS	Microsoft Windows			
Route	• 10.1.15.189 ► 10.1.11.111			
Severity	5.0 (Medium)			
All Identifiers				
Name	Value	Created	Source	Actions
MAC	00:50:56:92:00:70	Fri, Feb 28, 2020 1:30 PM UTC	Report 8e909664-ddab-4de6-83f5-fb6731ace1d9 (NVT 1.3.6.1.4.1.25623.1.0.10150)	X
OS	cpe:/o:microsoft:windows	Fri, Feb 28, 2020 1:30 PM UTC	Report 8e909664-ddab-4de6-83f5-fb6731ace1d9 (NVT 1.3.6.1.4.1.25623.1.0.102011)	X
MAC	00:50:56:92:00:70	Fri, Feb 28, 2020 1:30 PM UTC	Report 8e909664-ddab-4de6-83f5-fb6731ace1d9 (NVT 1.3.6.1.4.1.25623.1.0.96215)	X
hostname	DCHV1R01.local	Fri, Feb 28, 2020 1:30 PM UTC	Report 8e909664-ddab-4de6-83f5-fb6731ace1d9 (NVT 1.3.6.1.4.1.25623.1.0.103996)	X
OS	cpe:/o:microsoft:windows	Fri, Feb 28, 2020 1:30 PM UTC	Report 8e909664-ddab-4de6-83f5-fb6731ace1d9 (NVT 1.3.6.1.4.1.25623.1.0.102002)	X
ip	10.1.11.111	Fri, Feb 28, 2020 1:30 PM UTC	Report 8e909664-ddab-4de6-83f5-fb6731ace1d9 (Target Host)	X
os	cpe:/o:microsoft:windows_server_2008:r2::sp1	Fri, Feb 28, 2020 1:30 PM UTC	Report 8e909664-ddab-4de6-83f5-fb6731ace1d9 (NVT 1.3.6.1.4.1.25623.1.0.103621)	X

Fig. 13.3: All identifiers

Permissions Assigned permissions (see Chapter 9.4 (page 231)).

The following actions are available in the upper left corner:

- ⓘ Open the corresponding chapter of the user manual.
- ⚡ Show the list page of all hosts.
- ⚡ Create a new host (see Chapter 13.1.1 (page 378)).
- 🖊 Edit the host.
- 🗑 Delete the host.
- 📁 Export the host as an XML file.
- ⓘ Show the corresponding results.

13.1.3 Creating a Target from Hosts

A target with a set of hosts can be created as follows:

1. Filter the hosts so that only the hosts that should be used for the target (e.g., only Microsoft Windows hosts) are displayed (see Chapter 8.4 (page 207)).
2. Create a new target by clicking ⚡ below the list of hosts (see Fig. 13.4).

→ The window for creating a target is opened. The input box *Hosts* is prefilled with the set of displayed hosts.

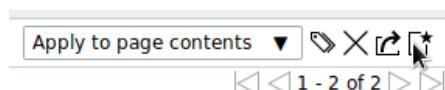


Fig. 13.4: Creating a target with the displayed hosts



3. Define the target and click **Save**.

Tip: For the information to enter in the input boxes see Chapter 10.2.1 (page 248).

Note: If additional suitable hosts show up in further scans they will **not** be added to the target.

13.2 Managing Operating Systems

The operating systems view within the asset management provides a different view on the stored data. While the hosts view is centered on the individual hosts, this view concentrates on the used operating systems.

List Page

All operating systems can be displayed by selecting *Assets > Operating Systems* in the menu bar (see Fig. 13.5).

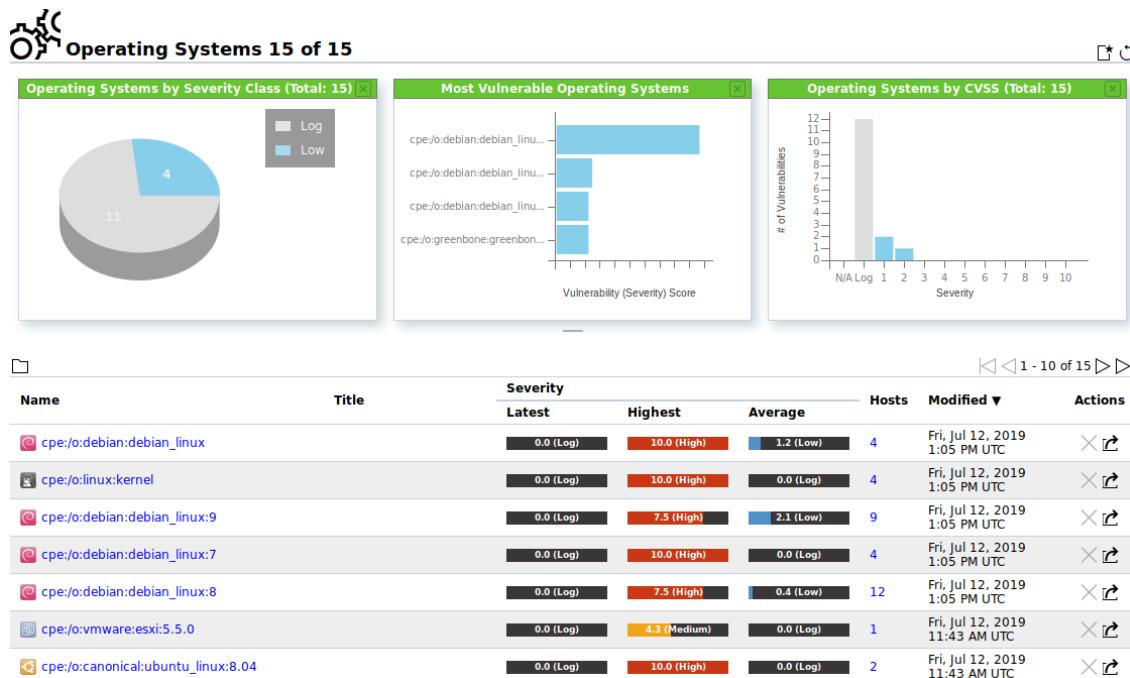


Fig. 13.5: Page *Operating Systems* displaying all scanned operating systems

For all operating systems the following actions are available:

- ✗ Delete the operating system. Only operating systems which are currently not used can be deleted.
- ↗ Export the operating system as an XML file.

Note: By clicking ✗ or ↗ below the list of operating systems more than one operating system can be deleted or exported at a time. The drop-down list is used to select which operating systems are deleted or exported.



Details Page

Click on the name of an operating system to open the details page of the operating system.

The following registers are available:

Information General information about the operating system.

User Tags Assigned tags (see Chapter 8.5 (page 214)).

Permissions Assigned permissions (see Chapter 9.4 (page 231)).

The following actions are available in the upper left corner:

- ② Open the corresponding chapter of the user manual.
- >Show the list page of all operating systems.
- >Delete the operating system. Only operating systems which are currently not used can be deleted.
- Export the operating system as an XML file.
- Show the corresponding hosts.

13.3 Managing TLS Certificates

TLS certificates are collected during scanning.

List Page

All existing TLS certificates can be displayed by selecting *Assets > TLS Certificates* in the menu bar (see Fig. 13.6).

For all TLS certificates the following actions are available:

- Delete the TLS certificate.
- Download the TLS certificate.
- Export the TLS certificate as an XML file.

Note: By clicking or below the list of TLS certificates more than one TLS certificate can be deleted or exported at a time. The drop-down list is used to select which TLS certificates are deleted or exported.

Issuer DN	Serial ▲	Activates	Expires	Last seen	Actions
CN=dclap001,OU=xSeries,O=IBM,L=RTP,ST=NORTH CAROLINA,C=US	00B66B68ACFCB795F5	Mon, Aug 21, 2006 7:55 AM UTC	Thu, Jan 3, 2008 7:55 AM UTC	Mon, Oct 21, 2019 1:41 PM UTC	
CN=EM2_CA	00BAC9	Wed, Oct 23, 2013 1:12 PM UTC	Wed, Oct 19, 2033 1:12 PM UTC	Mon, Oct 21, 2019 1:41 PM UTC	
CN=dcfr2001,OU=xSeries,O=IBM,L=RTP,ST=NORTH CAROLINA,C=US	00DCE9C3769DE0FA87	Tue, Sep 23, 2008 9:18 AM UTC	Fri, Feb 5, 2010 9:18 AM UTC	Mon, Oct 21, 2019 1:41 PM UTC	
C=XX,ST=There is no such thing outside US,L=Everywhere,O=OCOSA,OU=Office for Compilation of Otherwise Simple Affairs,CN=ubuntu804-base.localdomain,EMAIL=root@ubuntu804-base.localdomain	00FFFFFFFAFFFFF93A4	Wed, Mar 17, 2010 2:07 PM UTC	Fri, Apr 16, 2010 2:07 PM UTC	Mon, Oct 21, 2019 1:38 PM UTC	
CN=EM2_CA	0147C9	Tue, May 28, 2013 11:40 PM UTC	Tue, May 24, 2033 11:40 PM UTC	Mon, Oct 21, 2019 1:41 PM UTC	
CN=EM2_CA	0147CD	Wed, May 29, 2013 12:02 AM UTC	Wed, May 25, 2033 12:02 AM UTC	Mon, Oct 21, 2019 1:41 PM UTC	

Fig. 13.6: Page *TLS Certificates* displaying all collected TLS certificates



Details Page

Click on the name of a TLS certificate to display the details of the TLS certificate. Click to open the details page of the TLS certificate.

The following registers are available:

Information General information about the TLS certificate.

User Tags Assigned tags (see Chapter 8.5 (page 214)).

Permissions Assigned permissions (see Chapter 9.4 (page 231)).

The following actions are available in the upper left corner:

- Open the corresponding chapter of the user manual.
- Show the list page of all TLS certificates.
- Delete the TLS certificate.
- Download the TLS certificate.
- Export the TLS certificate as an XML file.

CHAPTER 14

Managing SecInfo

The SecInfo management provides centralized access to a wide range of information technology (IT) security information including the following categories:

Vulnerability Tests (VT) VTs test the target system for potential vulnerabilities.

Common Vulnerabilities and Exposures (CVE) CVEs are vulnerabilities published by vendors and security researchers.

Common Platform Enumeration (CPE) CPE offers standardized names for products used in the IT.

Open Vulnerability Assessment Language (OVAL) Definitions OVAL offers a standardized language for testing vulnerabilities. OVAL definitions use this language to discover vulnerabilities.

CERT-Bund Advisories CERT-Bund Advisories are published by the CERT-Bund³⁰, the Computer Emergency Response Team of the German Federal Office for Information Security (BSI)³¹ (German: Bundesamt für Sicherheit in der Informationstechnik, abbreviated as BSI). The main task of the CERT-Bund is the operation of a warning and information service publishing information regarding new vulnerabilities and security risks as well as threats for IT systems.

DFN-CERT Advisories DFN-CERT advisories are published by the DFN-CERT³², the Computer Emergency Response Team of the German National Research and Education Network³³ (German: Deutsches Forschungsnetz, abbreviated as DFN).

CVEs, CPEs and OVAL definitions are published and made accessible by the National Institute of Standards and Technology (NIST)³⁴ as part of the National Vulnerability Database (NVD)³⁵ (see Chapter 14.2 (page 386)).

Note: Greenbone Networks is also offering all SecInfo data online, accessible via the SecInfo portal³⁶. The SecInfo portal provides all SecInfo described in the following chapters and the CVSS calculator.

Access to the SecInfo Portal is provided by activating a guest access (see Chapter 9.1.3 (page 225)).

³⁰ <https://www.cert-bund.de/>

³¹ https://www.bsi.bund.de/EN/TheBSI/thebsi_node.html

³² <https://www.dfn-cert.de/>

³³ <https://www.dfn.de/en/>

³⁴ <https://www.nist.gov>

³⁵ <https://nvd.nist.gov/>

³⁶ <https://secinfo.greenbone.net>



14.1 Vulnerability Tests (VT)

VTs are test routines used by the GSM. They are part of the Greenbone Security Feed (GSF) which is updated regularly. VTs include information about development date, affected systems, impact of vulnerabilities and remediation.

List Page

All existing VTs can be displayed by selecting *SecInfo > NVTs* in the menu bar.

For all VTs the following information is displayed:

Name Name of the VT.

Family Family of VTs to which the VT belongs.

Created Date and time of creation.

Modified Date and time of last modification.

CVE CVE that is checked for using the VT.

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

- A vendor patch is available.
- A workaround is available.
- A mitigation by configuration is available.
- No fix is and will be available.
- No solution exists.

Severity The severity of the vulnerability (CVSS, see Chapter 14.2.4 (page 393)) is displayed as a bar to support the analysis of the results.

QoD QoD is short for Quality of Detection and represents how reliable the detection of a vulnerability is. The QoD concept was introduced with GOS 3.1. Results created with GOS versions before GOS 3.1 were assigned a QoD of 75 % during migration.

With the introduction of the QoD, the parameter *Paranoid* in the scan configuration (see Chapter 10.9 (page 291)) is removed without replacement. In the past a scan configuration without this parameter only used VTs with a QoD of at least 70%. Now all VTs are used and executed in a scan configuration.

Note: By clicking below the list of VTs more than one VT can be exported at a time. The drop-down list is used to select which VTs are exported.

Details Page

Click on the name of a VT to display the details of the VT. Click to open the details page of the VT.

The following actions are available in the upper left corner:

- Open the corresponding chapter of the user manual.
- Show the list page of all VTs.
- Export the VT as an XML file.
- Create a new note for the VT (see Chapter 11.7.1 (page 335)).
- Create a new override for the VT (see Chapter 11.8.1 (page 338)).
- Show the corresponding results.



- ☀ Show the corresponding vulnerability.

14.2 Security Content Automation Protocol (SCAP)

The National Institute of Standards and Technology (NIST)³⁷ provides the National Vulnerability Database (NVD)³⁸. The NVD is a data repository for the vulnerability management of the US government. The goal is the standardized provision of the data for automated processing. By that, vulnerability management is supported and the implementation of compliance guidelines is verified.

The NVD provides different databases including the following:

- Checklists
- Vulnerabilities
- Misconfigurations
- Products
- Threat metrics

The NVD utilizes the Security Content Automation Protocol³⁹ (SCAP). SCAP is a combination of different interoperable standards. Many standards were developed or derived from public discussion.

The public participation of the community in the development is an important aspect for accepting and spreading SCAP standards. SCAP is currently specified in version 1.3 and includes the following components:

- **Languages**
 - XCCDF: Extensible Configuration Checklist Description Format
 - OVAL: Open Vulnerability and Assessment Language
 - OCIL: Open Checklist Interactive Language
 - Asset Identification
 - ARF: Asset Reporting Format
- **Collections**
 - CCE: Common Configuration Enumeration
 - CPE: Common Platform Enumeration
 - CVE: Common Vulnerabilities and Exposure
- **Metrics**
 - CVSS: Common Vulnerability Scoring System
 - CCSS: Common Configuration Scoring System
- **Integrity**
 - TMSAD: Trust Model for Security Automation Data

OVAL, CCE, CPE and CVE are trademarks of NIST.

The Greenbone Security Manager (GSM) uses OVAL, CVE, CPE and CVSS. By utilizing these standards the interoperability with other systems is guaranteed. The standards also allow comparing the results.

³⁷ <https://www.nist.gov>

³⁸ <https://nvd.nist.gov/>

³⁹ <https://csrc.nist.gov/projects/security-content-automation-protocol/>



Vulnerability assessment systems such as the GSM can be validated by NIST respectively. The GSM has been validated with respect to SCAP version 1.0⁴⁰.

14.2.1 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, MITRE⁴¹ founded the Common Vulnerabilities and Exposure (CVE) project⁴². 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 NVD refers to the CVE database and complements the content with information regarding the elimination, severity, possible impact and affected products of the vulnerability. Greenbone Networks refers to the CVE database of the NVD. At the same time the GSM combines the information, VTs and CERT-Bund/DFN-CERT advisories.

List Page

All existing CVEs can be displayed by selecting *SecInfo > CVEs* in the menu bar.

Columns like *Severity* may display *N/A* for one of the following reasons:

- The CVE was published but no vulnerability analysis/severity assessment was carried out by the NVD yet. This can take a few days up to a few weeks.
Such CVEs can be identified when browsing the related entry⁴³. As long as *Undergoing Analysis* is displayed there, *N/A* is shown in the columns for the CVE.
- There is always a delay of 1 – 2 working days between the vulnerability analysis/severity assessment and the time the updated information is displayed in the SecInfo.

The column *CVSS Base Vector* shows the CVSS vector used for calculating the severity of a CVE. This vector includes the CVSS version defined for the CVE.

By clicking on the vector, the page *CVSSv2/CVSSv3 Base Score Calculator* is opened. The fields of the corresponding calculator are already filled in, depending on which CVSS version is used to calculate the severity of the CVE.

Note: By clicking  below the list of CVEs more than one CVE can be exported at a time. The drop-down list is used to select which CVEs are exported.

⁴⁰ <https://csrc.nist.gov/Projects/Security-Content-Automation-Protocol/SCAP-Releases>

⁴¹ <https://www.mitre.org/>

⁴² <https://cve.mitre.org/>

⁴³ <https://nvd.nist.gov/vuln/full-listing>



Details Page

Click on the name of a CVE to display the details of the CVE. Click to open the details page of the CVE (see Fig. 14.1).

Information	User Tags (0)
--------------------	------------------

Description

There's a flaw in the BFD library of binutils in versions before 2.36. An attacker who supplies a crafted file to an application linked with BFD, and using the DWARF functionality, could cause an impact to system availability by way of excessive memory consumption.

CVSS

Base Score	6.5 (Medium)
Base Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H
Attack Vector	NETWORK
Attack Complexity	LOW
Privileges Required	NONE
User Interaction	REQUIRED
Scope	UNCHANGED
Confidentiality Impact	NONE
Integrity Impact	NONE
Availability Impact	HIGH

References

MISC https://bugzilla.redhat.com/show_bug.cgi?id=1947111

FEDORA [FEDORA-2021-d23d016509](#)

FEDORA [FEDORA-2021-9bd201dd4d](#)

FEDORA [FEDORA-2021-7ca24ddc86](#)

CERT Advisories referencing this CVE

Name	Title
DFN-CERT-2021-0742	GNU Binutils: Eine Schwachstelle ermöglicht einen Denial-of-Service-Angriff

Fig. 14.1: Details page of a CVE

The following registers are available:

Information General information about the CVE.

User Tags Assigned tags (see Chapter 8.5 (page 214)).

The following actions are available in the upper left corner:

- ② Open the corresponding chapter of the user manual.
- ≡ Show the list page of all CVEs.
- ↗ Export the CVE as an XML file.



14.2.2 CPE

The Common Platform Enumeration (CPE)⁴⁴ is modelled after CVE. It is a structured naming scheme for applications, operating systems and hardware devices.

The CPE was initiated by MITRE⁴⁵ and is maintained by NIST as a part of the NVD. 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).

Common Platform Enumeration (CPE) Version 2.2: Name Structure

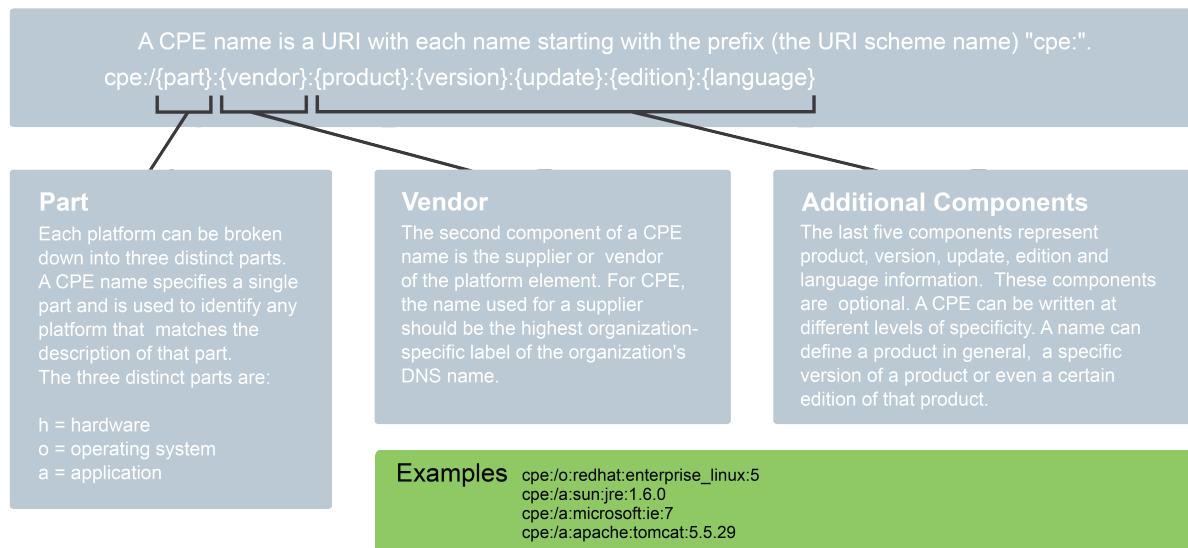


Fig. 14.2: Name structure of a CPE name

The combination of CPE and CVE standards enables the conclusion of existing vulnerabilities when discovering a platform or product.

CPE is composed of the following components:

- **Naming** The name specification describes the logical structure of well-formed names (WFNs), their binding to URIs and formatted character strings as well as their conversion.
- **Name Matching** The name matching specification describes the methods to compare WFNs with each other. This allows for the testing whether some or all WFNs refer to the same product.
- **Dictionary** The dictionary is a repository of CPE names and metadata. Every name defines a single class of an IT product. The dictionary specification describes the processes for using the dictionary, e.g., searching for a specific name or for entries belonging to a more general class.
- **Applicability Language** The applicability language specification describes the creation of complex logical expressions with the help of WFNs. These applicability statements can be used for tagging checklists, guidelines or other documents and, by that, for describing for which products the documents are relevant.

⁴⁴ <https://csrc.nist.gov/projects/security-content-automation-protocol/specifications/cpe>

⁴⁵ <https://www.mitre.org/>



List Page

All existing CPEs can be displayed by selecting *SecInfo > CPEs* in the menu bar.

Note: By clicking ↗ below the list of CPEs more than one CPE can be exported at a time. The drop-down list is used to select which CPEs are exported.

Details Page

Click on the name of a CPE to display the details of the CPE. Click 🔎 to open the details page of the CPE.

The following registers are available:

Information General information about the CPE.

User Tags Assigned tags (see Chapter 8.5 (page 214)).

The following actions are available in the upper left corner:

- ⓘ Open the corresponding chapter of the user manual.
- ⚡ Show the list page of all CPEs.
- ↗ Export the CPE as an XML file.

14.2.3 OVAL Definitions

The Open Vulnerability and Assessment Language (OVAL)⁴⁶ is a MITRE⁴⁷ 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.

Example: the OVAL definition 22272 has the following structure:

```
<definition id="oval:org.mitre.oval:def:22272" version="4" class="vulnerability">
<metadata>
  <title>Vulnerability in Google Chrome before 32.0.1700.76 on Windows allows
    attackers to trigger a sync with an arbitrary Google account by
    leveraging improper handling of the closing of an untrusted signin
    confirm dialog</title>
<affected family="windows">
  <platform>Microsoft Windows 2000</platform>
  <platform>Microsoft Windows XP</platform>
  <platform>Microsoft Windows Server 2003</platform>
  <platform>Microsoft Windows Server 2008</platform>
  <platform>Microsoft Windows Server 2008 R2</platform>
  <platform>Microsoft Windows Vista</platform>
  <platform>Microsoft Windows 7</platform>
  <platform>Microsoft Windows 8</platform>
  <platform>Microsoft Windows 8.1</platform>
  <platform>Microsoft Windows Server 2012</platform>
  <platform>Microsoft Windows Server 2012 R2</platform>
  <product>Google Chrome</product>
</affected>
```

(continues on next page)

⁴⁶ <https://oval.cisecurity.org/>

⁴⁷ <https://www.mitre.org/>



(continued from previous page)

```

<reference source="CVE" ref_id="CVE-2013-6643"
ref_url="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-6643"/>
<description>The OneClickSigninBubbleView::WindowClosing function in
browser/ui/views/sync/one_click_signin_bubble_view.cc in Google
Chrome before 32.0.1700.76 on Windows and before 32.0.1700.77 on Mac
OS X and Linux allows attackers to trigger a sync with an arbitrary
Google account by leveraging improper handling of the closing of an
untrusted signin confirm dialog.</description>
<oval_repository>
  <dates>
    <submitted date="2014-02-03T12:56:06">
      <contributor organization="ALTX-SOFT">Maria Kedovskaya</contributor>
    </submitted>
    <status_change date="2014-02-04T12:25:48.757-05:00">DRAFT</status_change>
    <status_change date="2014-02-24T04:03:01.652-05:00">INTERIM</status_change>
    <status_change date="2014-03-17T04:00:17.615-04:00">ACCEPTED</status_change>
  </dates>
  <status>ACCEPTED</status>
</oval_repository>
</metadata>
<criteria>
  <extend_definition comment="Google Chrome is installed"
definition_ref="oval:org.mitre.oval:def:11914"/>
  <criteria operator="AND" comment="Affected versions of Google Chrome">
    <criterion comment="Check if the version of Google Chrome is greater than
or equals to 32.0.1651.2" test_ref="oval:org.mitre.oval:tst:100272"/>
    <criterion comment="Check if the version of Google Chrome is less than
or equals to 32.0.1700.75" test_ref="oval:org.mitre.oval:tst:99783"/>
  </criteria>
</criteria>
</definition>

```

This information is graphically processed by the web interface and presented easily readable.

List Page

All existing OVAL definitions can be displayed by selecting *SecInfo > OVAL Definitions* in the menu bar.

Note: By clicking below the list of OVAL definitions more than one OVAL definition can be exported at a time. The drop-down list is used to select which OVAL definitions are exported.

Details Page

Click on the name of an OVAL definition to display the details of the OVAL definition. Click to open the details page of the OVAL definition (see Fig. 14.3).

The following registers are available:

Information General information about the OVAL definition.

User Tags Assigned tags (see Chapter 8.5 (page 214)).

The following actions are available in the upper left corner:

- Open the corresponding chapter of the user manual.
- Show the list page of all OVAL definitions.
- Export the OVAL definition as an XML file.



OVAL OVAL Definition:
oval:org.mitre.oval:def:19168

Information User Tags (0)

Title Use-after-free vulnerability in Google Chrome before 31.0.1650.48 via vectors involving the string values of id attributes

Version 3

Definition Class vulnerability

Referenced CVEs 1

Severity **7.5 (High)**

File /oval/5.10/org.mitre.oval/v/family/windows.xml

Affected

Family windows

Type	Name
Product	Google Chrome
Platform	Microsoft Windows 2000
Platform	Microsoft Windows 7
Platform	Microsoft Windows Server 2003
Platform	Microsoft Windows Server 2008
Platform	Microsoft Windows Server 2008 R2
Platform	Microsoft Windows Vista
Platform	Microsoft Windows XP
Platform	Microsoft Windows 8
Platform	Microsoft Windows Server 2012

Criteria

- Check if the version of Google Chrome is less than 31.0.1650.48 ([oval:org.mitre.oval:tst:86556](#))
- Google Chrome is installed ([oval:org.mitre.oval:def:11914](#))

Fig. 14.3: Details page of an OVAL definition



14.2.4 CVSS

To support the interpretation of a vulnerability, the Common Vulnerability Scoring System (CVSS) was invented. The CVSS is an industry standard for describing the severity of security risks in computer systems.

Security risks are rated and compared using different criteria. This allows for the creation of a priority list of counter measures.

The CVSS is developed by the CVSS Special Interest Group (CVSS-SIG)⁴⁸ of the Forum of Incident Response and Security Teams (FIRST)⁴⁹. The current CVSS score version is 3.1.

The CVSS score supports base score metrics, temporal score metrics, and environmental score metrics.

Base score metrics Base score metrics test the exploitability of a vulnerability and their impact on the target system. Access, complexity and requirement of authentication are rated. Additionally, they rate whether the confidentiality, integrity or availability is threatened.

Temporal score metrics Temporal score metrics test whether a completed example code exists, the vendor already supplied a patch and confirmed the vulnerability. The score will be changing drastically in the course of time.

Environmental score metrics Environmental score metrics describe the effect of a vulnerability within an organization. They take damage, target distribution, confidentiality, integrity and availability into account. This assessment strongly depends on the environment in which the vulnerable product is used.

Since the base score metrics are merely meaningful in general and can be determined permanently, the GSM provides them as part of the SecInfo data.

The CVSS calculator can be opened by selecting *Help > CVSS Calculator* in the menu bar (see Fig. 14.4). Both the calculator for CVSS version 2.0 and the calculator for CVSS version 3.0/3.1 are displayed.

The screenshot shows two side-by-side CVSS calculators. On the left is the 'CVSSv2 Base Score Calculator' and on the right is the 'CVSSv3 Base Score Calculator'. Both calculators have sections for 'From Metrics', 'From Vector', and 'Results'.

CVSSv2 Base Score Calculator:

- From Metrics:**
 - Access Vector: Local
 - Access Complexity: Low
 - Authentication: None
 - Confidentiality: None
 - Integrity: None
 - Availability: None
- From Vector:**
 - Vector: AV:L/AC:L/Au:N/C:N/I:N/A:N
- Results:**
 - CVSS Base Vector: AV:L/AC:L/Au:N/C:N/I:N/A:N
 - Severity: 0.0 (Low)

CVSSv3 Base Score Calculator:

- From Metrics:**
 - Attack Vector: Local
 - Attack Complexity: Low
 - Privileges Required: None
 - User Interaction: Required
 - Scope: Unchanged
 - Confidentiality: High
 - Integrity: None
 - Availability: None
- From Vector:**
 - CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:N/U
- Results:**
 - CVSS Base Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R:S:U/C:H/I:N/A:N
 - Severity: 5.5 (Medium)

Fig. 14.4: CVSS calculator for calculating severity scores

⁴⁸ <https://www.first.org/cvss/>

⁴⁹ <https://www.first.org/>



14.2.4.1 CVSS Version 2.0

The following formula is used by the CVSS calculator for version 2.0:

```
BaseScore = roundTo1Decimal( ( ( 0.6 * Impact ) +
    ( 0.4 * Exploitability ) - 1.5 ) * f( Impact ) )
```

“Impact” is calculated as follows:

```
Impact = 10.41 * (1 - (1 - ConfImpact) *
    (1 - IntegImpact) * (1 - AvailImpact))
```

“Exploitability” is calculated as follows:

```
Exploitability = 20 * AccessVector * AccessComplexity * Authentication
```

Note: The function `f(Impact)` is 0, if the impact is 0.

In all other cases the value is 1.176.

The other values are constants:

- **Access Vector**
 - Requires local access: 0.395
 - Adjacent network accessible: 0.646
 - Network accessible: 1.0
- **Access Complexity**
 - High: 0.35
 - Medium: 0.61
 - Low: 0.71
- **Authentication**
 - Requires multiple instances of authentication: 0.45
 - Requires single instance of authentication: 0.56
 - Requires no authentication: 0.704
- **ConfImpact**
 - None: 0.0
 - Partial: 0.275
 - Complete: 0.660
- **IntegImpact**
 - None: 0.0
 - Partial: 0.275
 - Complete: 0.660
- **AvailImpact**
 - None: 0.0
 - Partial: 0.275



- Complete: 0.660

14.2.4.2 CVSS Version 3.0/3.1

The following formula is used by the CVSS calculator for version 3.0/3.1:

```
* If Impact <= 0, BaseScore = 0  
  
* If Scope is "Unchanged":  
  BaseScore = Roundup (Minimum ((Impact + Exploitability), 10))  
  
* If Scope is "Changed":  
  BaseScore = Roundup (Minimum (1.08 * (Impact + Exploitability), 10))
```

“ISS” (Impact Sub-Score) is calculated as follows:

```
ISS = 1 - ((1 - Confidentiality) * (1 - Integrity) * (1 - Availability))
```

“Impact” is calculated as follows:

```
* If Scope is "Unchanged":  
  Impact = 6.42 * ISS  
  
* If Scope is "Changed":  
  Impact = 7.52 * (ISS - 0.029) - 3.25 * (ISS - 0.02)15
```

“Exploitability” is calculated as follows:

```
Exploitability = 8.22 * Attack Vector * Attack Complexity  
               * Privileges Required * User Interaction
```

The other values are constants:

- **Attack Vector**
 - Network: 0.85
 - Adjacent: 0.62
 - Local: 0.55
 - Physical: 0.2
- **Attack Complexity**
 - Low: 0.77
 - High: 0.44
- **Privileges Required**
 - None: 0.85
 - Low: 0.62 (or 0.68 if Scope is “Changed”)
 - High: 0.27 (or 0.5 if Scope is “Changed”)
- **User Interaction**
 - None: 0.85
 - Required: 0.62
- **Confidentiality**
 - None: 0.0



- Low: 0.22
- High: 0.56

- **Integrity**

- None: 0.0
- Low: 0.22
- High: 0.56

- **Availability**

- None: 0.0
- Low: 0.22
- High: 0.56

14.3 CERT-Bund Advisories

The CERT-Bund⁵⁰, 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 Centre⁵¹.

The services of CERT-Bund are primarily available to federal authorities and include the following:

- 24 hour on call duty in cooperation with the IT Situation Centre
- Analyzing incoming incident reports
- Creating recommendations derived from incidents
- Supporting federal authorities during IT security incidents
- Operating a warning and information service
- Active alerting of the federal administration in case of imminent danger

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

Advisories This information service is only available to federal agencies as a closed list. The advisories describe current information about security critical incidents in computer systems and detailed measures to remediate security risks.

Short Information Short information features the short description of current information regarding security risks and vulnerabilities. This information is not always verified and could be incomplete or even inaccurate.

⁵⁰ <https://www.cert-bund.de/>

⁵¹ https://www.bsi.bund.de/EN/Topics/IT-Crisis-Management/IT-Situation-Centre/itsituationcentre_node.html



The Greenbone Security Feed contains the CERT-Bund Short Information. They can be identified by the "K" in the message (CB-K14/1296).

List Page

All existing CERT-Bund advisories can be displayed by selecting *SecInfo > CERT-Bund Advisories* in the menu bar.

Note: By clicking  below the list of CERT-Bund advisories more than one CERT-Bund advisory can be exported at a time. The drop-down list is used to select which CERT-Bund advisories are exported.

Details Page

Click on the name of a CERT-Bund advisory to display the details of the CERT-Bund advisory. Click  to open the details page of the CERT-Bund advisory.

The following registers are available:

Information General information about the CERT-Bund advisory.

User Tags Assigned tags (see Chapter 8.5 (page 214)).

The following actions are available in the upper left corner:

- ⓘ Open the corresponding chapter of the user manual.
- ⌂ Show the list page of all CERT-Bund advisories.
- ↗ Export the CERT-Bund advisory as an XML file.

14.4 DFN-CERT Advisories

While the individual VTs, CVEs, CPEs and OVAL definitions are created primarily to be processed by computer systems, the DFN-CERT⁵² publishes new advisories regularly.

The DFN-CERT is responsible for hundreds of universities and research institutions that are associated with the German Research and Education Network⁵³ (German: Deutsches Forschungsnetz, abbreviated as DFN). Additionally, it provides key security services to government and industry.

An advisory describes especially critical security risks that require fast reacting. The DFN-CERT advisory service includes the categorization, distribution and rating of advisories issued by different software vendors and distributors. Advisories are obtained by the Greenbone Security Manager and stored in the database for reference.

List Page

All existing DFN-CERT advisories can be displayed by selecting *SecInfo > DFN-CERT Advisories* in the menu bar.

Note: By clicking  below the list of DFN-CERT advisories more than one DFN-CERT advisory can be exported at a time. The drop-down list is used to select which DFN-CERT advisories are exported.

Details Page

Click on the name of a DFN-CERT advisory to display the details of the DFN-CERT advisory. Click  to open the details page of the DFN-CERT advisory.

⁵² <https://www.dfn-cert.de/>

⁵³ <https://www.dfn.de/en/>



The following registers are available:

Information General information about the DFN-CERT advisory.

User Tags Assigned tags (see Chapter 8.5 (page 214)).

The following actions are available in the upper left corner:

- ⓘ Open the corresponding chapter of the user manual.
- ⚡ Show the list page of all DFN-CERT advisories.
- ↗ Export the DFN-CERT advisory as an XML file.

CHAPTER 15

Using the Greenbone Management Protocol

The vulnerability management functionality of the Greenbone Security Manager (GSM) is also available via the Greenbone Management Protocol (GMP).

Greenbone Networks provides the Greenbone Vulnerability Management Tools (gvm-tools) to access the functionality made available by GMP (see Chapter 15.3 (page 400)). This user manual covers gvm-tools up to version 2.0.0 beta.

The newest version of GMP is documented at <https://docs.greenbone.net/API/GMP/gmp-21.04.html>.

15.1 Changes to GMP

GMP is regularly updated to apply changes in the functionality provided by the underlying service and to provide a consistent and comprehensive interface.

Updates result in a new version of GMP. Each new version includes a list of added, modified and removed protocol elements, e.g., commands or attributes. The most recent version of the list is available at <https://docs.greenbone.net/API/GMP/gmp-21.04.html#changes>.

Depending on the changes, the old version may be available for some time. During this transitional phase, the new and the old version are available at the same time.

This list helps to prepare for upcoming changes as soon as possible. It does not represent the complete list of upcoming changes.

15.2 Activating GMP

Before GMP can be used, it has to be activated on the GSM.

While the web interface uses GMP locally on the appliance, GMP is not remotely accessible via the network by default.

The remote GMP service can be activated using the GOS administration menu (see Chapter 7.2.4.2 (page 153)).



In general, the access to GMP is authenticated and encrypted with SSL/TLS. The same users as for the web interface are used. The users are subject to the same restrictions and have the same permissions.

15.3 Using gvm-tools

The Greenbone Vulnerability Management Tools (gvm-tools) are a collection of tools that provide access to the functionalities of the Greenbone Management Protocol (GMP). GMP scripts executed with `gvm-script` use the API provided by the library `python-gvm`⁵⁴.

Note: `python-gvm` is automatically installed when installing gvm-tools.

gvm-tools are available as a command line interface (CLI) and as a Python shell for Microsoft Windows and any operating system that supports Python, including Linux.

Note: Both gvm-tools and `python-gvm` use a different version scheme than GOS, so the versions of gvm-tools, `python-gvm` and GOS are not necessarily the same.

It is recommended to use the latest versions of gvm-tools and `python-gvm`.

gvm-tools can be downloaded at the project's official GitHub repository⁵⁵. Python 3.5 or later is required. To install gvm-tools, follow the instructions provided at <https://github.com/greenbone/gvm-tools#installation>.

In addition, gvm-tools are available as statically linked EXE files for all currently supported versions of Microsoft Windows⁵⁶.

The EXE versions of gvm-tools do not require Python and may be downloaded directly from Greenbone Networks at:

- CLI: `gvm-cli.exe`⁵⁷
- Python shell: `gvm-pyshell.exe`⁵⁸

Important: External links to the Greenbone download website are case-sensitive.

Note that upper cases, lower cases and special characters have to be entered exactly as they are written in the footnotes.

Note: gvm-tools are licensed under the GNU General Public License v3.0 and may be adapted and built for other uses cases, based on the source code.

15.3.1 Accessing with `gvm-cli.exe`

GMP is XML based. Every command and every response is a GMP object.

The command line tool `gvm-cli.exe` supplied by Greenbone Networks offers direct sending and receiving of XML commands and responses.

⁵⁴ <https://python-gvm.readthedocs.io/en/latest/>

⁵⁵ <https://github.com/greenbone/gvm-tools>

⁵⁶ <https://docs.microsoft.com/en-us/lifecycle/faq/windows>

⁵⁷ <https://download.greenbone.net/tools/gvm-cli.exe>

⁵⁸ <https://download.greenbone.net/tools/gvm-pyshell.exe>



gvm-cli.exe supports the following connections:

- SSH
- TLS
- Unix Domain Socket

gvm-cli.exe supports several command line switches which can be displayed using:

```
$ gvm-cli -h
usage: gvm-cli [-h] [-c [CONFIG]]
                [--log {{DEBUG,INFO,WARNING,ERROR,CRITICAL}}]
                [--timeout TIMEOUT] [--gmp-username GMP_USERNAME]
                [--gmp-password GMP_PASSWORD] [-V] [--protocol {GMP,OSP}]
                CONNECTION_TYPE ...

optional arguments:
-h, --help            show this help message and exit
-c [CONFIG], --config [CONFIG]
                    Configuration file path (default: ~/.config/gvm-tools.conf)
--log {{DEBUG,INFO,WARNING,ERROR,CRITICAL}}
                    Activate logging (default level: None)
--timeout TIMEOUT    Response timeout in seconds, or -1 to wait
                    indefinitely (default: 60)
--gmp-username GMP_USERNAME
                    Username for GMP service (default: '')
--gmp-password GMP_PASSWORD
                    Password for GMP service (default: '')
-V, --version         Show version information and exit
--protocol {GMP,OSP}  Service protocol to use (default: GMP)

connections:
valid connection types

CONNECTION_TYPE      Connection type to use
ssh                  Use SSH to connect to service
tls                  Use TLS secured connection to connect to service
socket               Use UNIX Domain socket to connect to service
```

While gvm-cli.exe supports more command line switches the additional options are only displayed when the connection type is specified:

```
$ gvm-cli ssh -h
usage: gvm-cli ssh [-h] --hostname HOSTNAME [--port PORT]
                   [--ssh-username SSH_USERNAME]
                   [--ssh-password SSH_PASSWORD] [-X XML] [-r] [--pretty]
                   [--duration]
                   [infile]

positional arguments:
infile              File to read XML commands from.

optional arguments:
-h, --help           show this help message and exit
--hostname HOSTNAME Hostname or IP address
--port PORT          SSH port (default: 22)
--ssh-username SSH_USERNAME
                    SSH username (default: 'gmp')
--ssh-password SSH_PASSWORD
```

(continues on next page)



(continued from previous page)

-X XML, --xml XML	SSH password (default: 'gmp') XML request to send
-r, --raw	Return raw XML
--pretty	Pretty format the returned xml
--duration	Measure command execution time

All current GSM appliances supporting GOS 6 use SSH to encrypt GMP. The use of TLS is deprecated, not officially supported and may be removed in a future version.

The gvm-tools are mostly helpful for batch mode (batch processing, scripting).

With `gvm-cli.exe` GMP can be used in a simple way:

```
gvm-cli --xml "<get_version/>"  
gvm-cli --xml "<get_tasks/>"  
gvm-cli < file
```

15.3.1.1 Configuring the Client

For using command `gvm-cli` logging into the appliance is required.

The needed information is supplied either using command line switches or a configuration file (`~/.config/gvm-tools.conf`).

To provide the GMP user with command line switches use:

- `--gmp-username`
- `--gmp-password`

Alternatively a configuration file `~/.config/gvm-tools.conf` containing the information can be created:

```
[Auth]  
gmp_username=webadmin  
gmp_password=kennwort
```

This configuration file is not read by default. The command line switch `--config` or `-c` has to be added to read the configuration file.

15.3.1.2 Starting a Scan Using the Command `gvm-cli`

A typical example for using GMP is the automatic scan of a new system.

In the example it is assumed that an Intrusion Detection System (IDS) is used that monitors the systems in the Demilitarized Zone (DMZ) and immediately discovers new systems and unusual TCP ports that are not used already. If such an event is discovered, the IDS should automatically initiate a scan of the new system with the help of a script.

For this, the command `gvm-cli` can be used although the command `gvm-pyshell` or using self written python scripts may be more suitable (see Chapter 15.3.2.1 (page 404)). The processing of the XML output is better supported by python than by using the shell.

Starting point is the IP address of the new suspected system. A target needs to be created for this IP address on the GSM.

The command `create_target` is described at:

https://docs.greenbone.net/API/GMP/gmp-21.04.html#command_create_target.



1. If the IP address is saved in the variable `IPADDRESS`, create the respective target as follows:

```
$ gvm-cli --gmp-username webadmin --gmp-password kennwort ssh \
--hostname 192.168.222.115 \
--xml "<create_target><name>Suspect Host</name>\n<hosts>$IPADDRESS</hosts></create_target>\n\n<create_target_response status='201' status_text='OK, resource created' id='4574473f-a5d0-494c-be6f-3205be487793'>"
```

2. Create the task as follows:

```
$ gvm-cli --gmp-username webadmin --gmp-password kennwort ssh \
--hostname 192.168.222.115 \
--xml "<create_task><name>Scan Suspect Host</name> \
<target id='4574473f-a5d0-494c-be6f-3205be487793'></target> \
<config id='daba56c8-73ec-11df-a475-002264764cea'></config></create_task>\n\n<create_task_response status='201' status_text='OK, resource created' id='ce225181-c836-4ec1-b83f-a6fcba70e17d'>"
```

→ The output is the ID of the task. It is required to start and monitor the task.

The other IDs used by the command can be retrieved using the following commands which display the available targets and scan configs:

```
$ gvm-cli --gmp-username webadmin --gmp-password kennwort ssh \
--hostname 192.168.222.115 --xml "<get_targets/>"\n\n$ gvm-cli --gmp-username webadmin --gmp-password kennwort ssh \
--hostname 192.168.222.115 --xml "<get_configs/>"
```

Note: The output of the commands above is XML.

3. Start the task as follows:

```
$ gvm-cli --gmp-username webadmin --gmp-password kennwort ssh \
--hostname 192.168.222.115 \
--xml '<start_task task_id="ce225181-c836-4ec1-b83f-a6fcba70e17d"/>'
```

→ The connection will be closed by the GSM. The task is running.

4. Display the status of the task as follows:

```
$ gvm-cli --gmp-username webadmin --gmp-password kennwort ssh \
--hostname 192.168.222.115 \
--xml '<get_tasks task_id="ce225181-c836-4ec1-b83f-a6fcba70e17d"/>\n\n<get_tasks_response status="200" status_text="OK"><apply_overrides>
...<status>Running</status><progress>98<host_progress>
<host>192.168.255.254</host>98</host_progress></progress>...>'
```

→ As soon as the scan is completed, the report can be downloaded.

For this the ID that was output when the task was created is required and a meaningful report format has to be entered.



5. Display the IDs for the report formats as follows:

```
$ $ gvm-cli --gmp-username webadmin --gmp-password kennwort ssh \
--hostname 192.168.222.115 --xml '<get_report_formats/>'
```

6. Load the report as follows:

```
$ gvm-cli --gmp-username webadmin --gmp-password kennwort ssh \
--hostname 192.168.222.115 \
--xml '<get_reports report_id="23a335d6-65bd-4be2-a83e-be330289eef7" \
format_id="35ba7077-dc85-42ef-87c9-b0eda7e903b6"/>'
```

Tip: To fully and automatically process the data, the task can be combined with an alert that forwards the report based on a given condition.

15.3.2 Accessing with `gvm-pyshell.exe`

The command line tool `gvm-pyshell.exe` supplied by Greenbone Networks offers the direct sending and receiving of XML commands and XML responses using python commands. The commands take care of the generation and parsing of the XML data.

The tool supports the following connections:

- TLS
- SSH
- Socket

While the current GSM appliances (GOS 6) use SSH to protect GMP, older appliances used TLS and Port 9390 to transport GMP. The `gvm-tools` can be used with both the older and the current GOS.

The `gvm-tools` are mostly helpful for batch mode (batch processing, scripting).

The authentication configuration of the command `gvm-pyshell` can be stored in a file in the home directory of the user. The syntax is explained in Chapter 15.3.1.1 (page 402).

The Python implementation follows the GMP API (<https://docs.greenbone.net/API/GMP/gmp-21.04.html>). Optional arguments in the API are identified by a ?. The following example explains the usage of the Python functions:

```
gmp.create_task("Name", "Config", "Scanner", "Target", comment="comment")
```

Tip: While mandatory arguments can be supplied in the correct order and are identified automatically they can also be specified using their identifier:

```
gmp.create_task(name="Name", config_id="Config", scanner_id="Scanner",
target_id="Target", comment="comment")
```

15.3.2.1 Starting a Scan Using the Command `gvm-pyshell`

A typical example for using GMP is the automatic scan of a new system.

In the example it is assumed that an Intrusion Detection System (IDS) is used that monitors the systems in the Demilitarized Zone (DMZ) and immediately discovers new systems and unusual TCP ports that are not used



already. If such an event is discovered, the IDS should automatically initiate a scan of the new system with the help of a script.

For this, the command `gvm-pyshell` is very suitable. The processing of the XML output is better supported by python than by using the shell.

Starting point is the IP address of the new suspected system. A target needs to be created for this IP address on the GSM.

The command `create_target` is described at:

https://docs.greenbone.net/API/GMP/gmp-21.04.html#command_create_target.

1. The following lines illustrate the commands required when using `gvm-pyshell`:

```
$ gvm-pyshell \
--gmp-username webadmin --gmp-password kennwort \
ssh --hostname 192.168.222.115
GVM Interactive Console 2.0.0 API 1.1.0. Type "help" to get information about
functionality.
>>> res=gmp.create_target("Suspect Host", make_unique=True, \
hosts=['192.168.255.254'])
>>> target_id = res.xpath('@id')[0]
```

The variable `target_id` contains the ID of the created target. This ID can be used to create the corresponding task.

Note: The task creation requires the following input:

- `target_id`
 - `config_id`
 - `scanner_id`
 - `task_name`
 - `task_comment`
-

2. All existing scan configurations can be displayed as follows:

```
>>> res = gmp.get_configs()
>>> for i, conf in enumerate(res.xpath('config')):
...     id = conf.xpath('@id')[0]
...     name = conf.xpath('name/text()')[0]
...     print('\n{0} {1}: ({2})'.format(i, name, id))
```

3. All existing scanners can be displayed using the same technique. If only the built-in scanners are used the following IDs are hard coded:

- OpenVAS scanner: 08b69003-5fc2-4037-a479-93b440211c73
- CVE scanner: 6acd0832-df90-11e4-b9d5-28d24461215b



4. Create the task as follows:

```
>>> res=gmp.create_task(name="Scan Suspect Host",
... config_id="daba56c8-73ec-11df-a475-002264764cea",
... scanner_id="08b69003-5fc2-4037-a479-93b440211c73",
... target_id=target_id)
>>> task_id = res.xpath('@id')[0]
```

5. Start the task as follows:

```
>>> gmp.start_task(task_id)
```

→ The current connection is closed immediately. Further commands are not required.

All commands can be put in a Python script which may be invoked by the Python shell:

```
len_args = len(args.script) - 1
if len_args is not 2:
    message = """
    This script creates a new task with specific host and vt!
    It needs two parameters after the script name.
    First one is name of the target and the second one is the
    chosen host. The task is called target-task

    Example:
        $ gvm-pyshell ssh newtask target host
    """
    print(message)
    quit()

target = args.script[1]
host = args.script[2]
task = target + " Task"

# Full and Fast
myconfig_id = "daba56c8-73ec-11df-a475-002264764cea"

# OpenVAS Scanner
myscanner_id = "08b69003-5fc2-4037-a479-93b440211c73"

res=gmp.create_target(target, True, hosts=host)
mytarget_id = res.xpath('@id')[0]

res=gmp.create_task(name=task,
                     config_id=myconfig_id,
                     scanner_id=myscanner_id,
                     target_id=mytarget_id)
mytask_id = res.xpath('@id')[0]

gmp.start_task(mytask_id)
```



15.3.3 Example Scripts

The gvm-tools come with a collection of example scripts which can be used by the command `gvm-script`.

Currently the following scripts are available for gvm-tools version 2.0.0 (<https://github.com/greenbone/gvm-tools/tree/master/scripts>):

- `application-detection.gmp.py`: this script displays all hosts with the searched application.
- `cfg-gen-for-certs.gmp.py`: this script creates a new scan configuration with VTs based on a given CERT-Bund advisory.
- `clean-sensor.gmp.py`: this script removes all resources from a sensor except active tasks.
- `create-dummy-data.gmp.py`: this script generates dummy data.
- `DeleteOverridesByFilter.gmp.py`: this script deletes overrides using a filter.
- `monthly-report2.gmp.py`: this script displays all vulnerabilities based on the reports of a given months. Made for GOS 4.x.
- `monthly-report.gmp.py`: this script will display all vulnerabilities based on the reports of a given months. Made for GOS 3.1.
- `nvt-scan.gmp.py`: this script creates a new task with a specific host and VT using a hardcoded base configuration.
- `startNVTScan.gmp.py`: this script creates a new task with a specific host and VT interactively.
- `SyncAssets.gmp.py`: this script uploads assets to the asset database.
- `SyncReports.gmp.py`: this script pulls reports and uploads them to a second GSM using container tasks.

Tip: These scripts can serve as a starting point for the development of custom scripts.

15.4 Status Codes

GMP uses status codes similar to HTTP status codes. The following codes are used:

2xx: The command was sent, understood and accepted successfully.

200: OK

201: Resource created

202: Request submitted

4xx: A user error occurred.

400: Syntax error This includes different syntax errors. Often elements or attributes in the GMP command are missing. The status text shows additional information.

Currently this status code is also used for missing or wrong authentication.

401: Authenticate First This is the error code that is used for missing or wrong authentication. Currently the value 400 is still used.

403: Access to resource forbidden This is the error code that is used for not having enough permissions. Often *400: Permission denied* is displayed instead as well.

404: Resource missing The resource could not be found. The resource ID was empty or wrong.

409: Resource busy This error code happens, for example, if the feed synchronization is started while it is already in progress.



5xx: A server error occurred.

500: Internal Error This can be caused by entries that exceed an internal buffer size.

503: Scanner loading NVTs The scanner is currently busy loading the VTs from its cache. The request should be made again at a later time.

503: Service temporarily down Possibly the scanner daemon is not running. Often the problem are expired certificates.

503: Service unavailable The GMP command is blocked on the GSM.

CHAPTER 16

Using a Master-Sensor Setup

Note: This chapter documents all possible menu options.

However, not all GSM models support all of these menu options. Check the tables in Chapter 3 (page 18) to see whether a specific feature is available for the used GSM model.

Due to security reasons it is often not possible to scan specific network segments directly. For example, direct access to the internet may be prohibited. To overcome this issue, the Greenbone Security Manager (GSM) supports the setup of a distributed scan system: two or more GSMS in different network segments can be connected securely in order to run vulnerability tests for those network segments that are otherwise not accessible.

In this case one GSM controls one or more other GSMS remotely. A controlling GSM is referred to as a “master” and a controlled GSM is referred to as a “sensor”.

Master

- All GSM models of the Midrange Class (physical and virtual) and the Enterprise Class can be used as a master (see Chapter 3 (page 18)).

Sensor

- All GSM models except for GSM ONE can be used as a sensor.
- The GSM models GSM 35 and 25V can only be used as a sensor and are always controlled by a master.
- All sensors can be managed directly by the master including automatic or manual feed updates as well as upgrades of the Greenbone Operating System (GOS).
- A sensor does not require any network connectivity other than to the master and the scan targets.
- A sensor does not require any further administrative steps after the initial setup.
- If a sensor should perform scans remotely, it has to be configured as a remote scanner.
 - The user can configure a scan for the remote scanner individually using the web interface of the master depending on requirements and permissions.
 - The remote scanner runs the scan and relays the results to the master where all vulnerability information is managed.



- The connection to a remote scanner is established by using the Open Scanner Protocol (OSP) via SSH.

The connection between master and sensor is established using the Secure Shell (SSH) protocol via port 22/TCP.

To distinguish between the sensor and remote scanner terminology:

- **Sensors** This feature requires the setup of the master-sensor link using the GOS administration menu of both the master and the sensor. This feature then supports the remote feed synchronization and the upgrade management of the sensor.
- **Remote Scanners** This feature requires the setup of the remote scanner using the web interface on the master. This feature then supports the execution of scans via the sensor.

16.1 Configuring a Master-Sensor Setup

16.1.1 Connecting a Master to a Sensor

A master can be linked to a sensor as follows:

1. Open the GOS administration menu of both the master and the sensor (see Chapter 7.1.2.2 (page 121)).
2. In the GOS administration menu of the master, select *Setup* and press *Enter*.
3. Select *Master* and press *Enter*.
4. Select *Master Identifier* and press *Enter*.
5. Select *Download* and press *Enter* (see Fig. 16.1).



Fig. 16.1: Configuring the master

6. Open the web browser and enter the displayed URL.
7. Download the PUB file.
 - When the key is downloaded, the GOS administration menu of the master displays the fingerprint of the key for verification.



Important: Do not confirm the fingerprint until the key is uploaded to the sensor.

8. In the GOS administration menu of the sensor, select *Setup* and press **Enter**.
9. Select *Sensor* and press **Enter**.
10. Select *Configure Master* and press **Enter** (see Fig. 16.2).

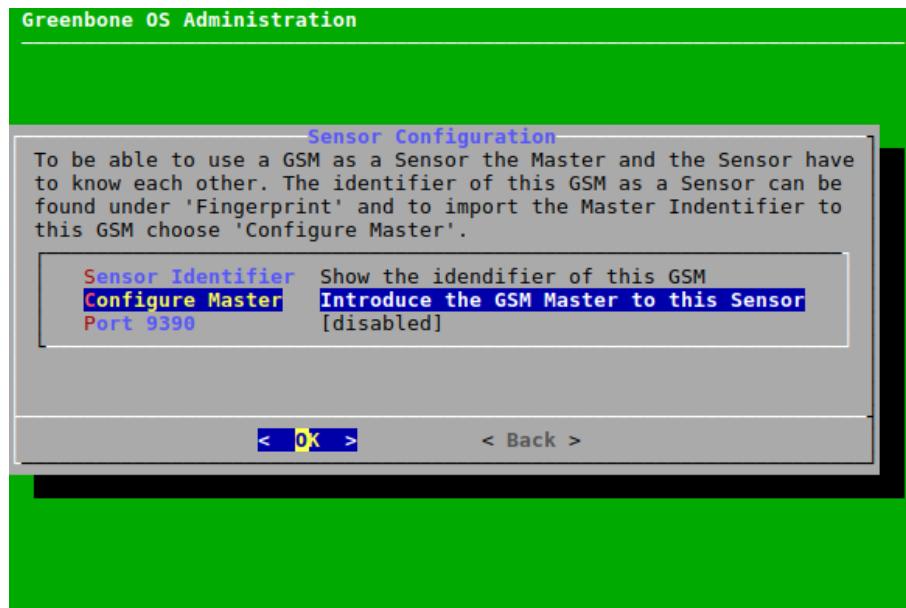


Fig. 16.2: Configuring the sensor

11. Select *Upload* and press **Enter**.
12. Open the web browser and enter the displayed URL.
13. Click *Browse...*, select the previously downloaded PUB file and click *Upload*.
→ When the key is uploaded, the GOS administration menu of the sensor displays the fingerprint of the key for verification.
14. Compare the fingerprint to the fingerprint displayed in the GOS administration menu of the master.
If the fingerprints match, press **Enter** in both GOS administration menus.
15. In the GOS administration menu of the sensor, select *Save* and press **Enter**.
16. Perform twice: press **Tab** and press **Enter**.
17. Select *Services* and press **Enter**.
18. Select *SSH* and press **Enter**.
19. Select *SSH State* and press **Enter**.
→ SSH is enabled on the sensor.
20. Select *Save* and press **Enter**.
21. Press **Tab** to select *Back* and press **Enter**.
22. Select *OSP* and press **Enter**.
23. Press **Enter** to enable OSP.
→ A message informs that the changes have to be saved (see Chapter 7.1.3 (page 122)).



24. Press **Enter** to close the message.
25. Select **Save** and press **Enter**.
→ OSP is enabled on the sensor.
26. In the GOS administration menu of the master, select **Setup** and press **Enter**.
27. Select **Master** and press **Enter**.
28. Select **Sensors** and press **Enter**.
29. Select **Add a new sensor** and press **Enter**.
30. Enter the IP address or the host name of the sensor in the input box and press **Enter**.
→ Additional menu options for the sensor configuration are shown (see Fig. 16.3, see Chapter 16.2 (page 413)).

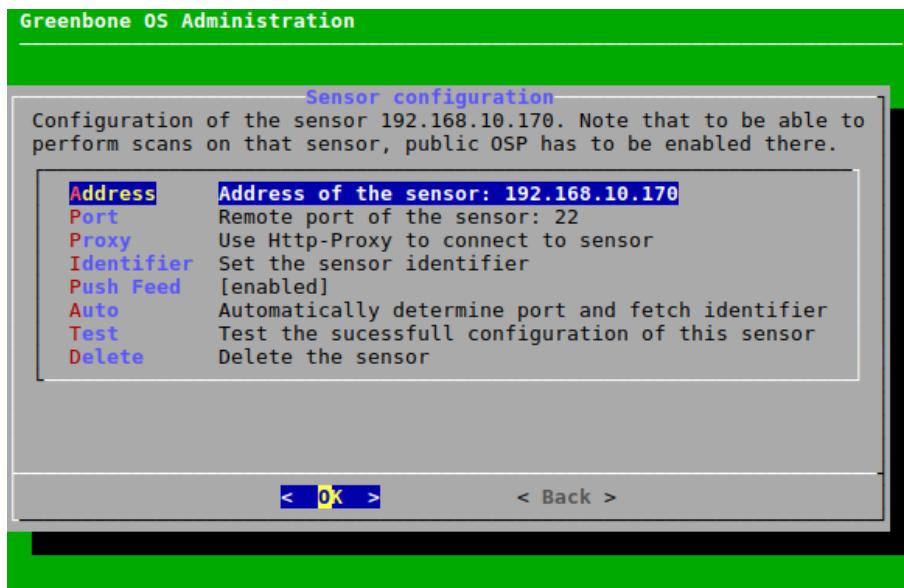


Fig. 16.3: Sensor configuration menu

31. Select **Auto** and press **Enter**.
→ The master connects to the sensor automatically and retrieves the identifier.
The fingerprint of the identifier is displayed in the GOS administration menu of the master.
32. In the GOS administration menu of the sensor, select **Setup** and press **Enter**.
33. Select **Sensor** and press **Enter**.
34. Select **Sensor Identifier** and press **Enter**.
35. Select **Fingerprint** and press **Enter**.
36. Compare the fingerprint to the fingerprint displayed in the GOS administration menu of the master.
If the fingerprints match, press **Enter** in the GOS administration menu of the master.
37. Select **Save** and press **Enter**.
38. Select **Test** and press **Enter**.
→ The configuration of the sensor is tested.
If the test fails, a warning with instructions is displayed (see Fig. 16.4).

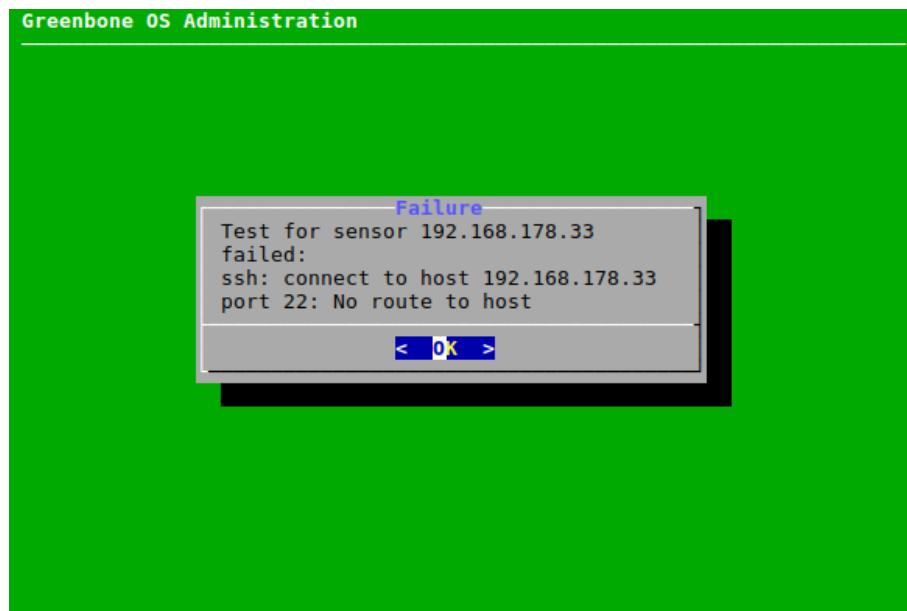


Fig. 16.4: Testing the sensor configuration

Note: Once configured successfully, sensors can be managed directly on the master using the GOS administration menu (see Chapters 7.3.5 (page 188) and 7.3.7 (page 189)).

16.1.2 Creating a Scan User Account

Note: The creation of a scan user account is not required for the GSM models GSM 35 and GSM 25V.

In addition to linking the master and the sensor, a scan user account on the sensor is required for using the sensor as a remote scanner (see Chapter 16.4 (page 415)). The scan user can be created as follows:

1. In the GOS administration menu of the sensor, select *Setup* and press **Enter**.
2. Select *User* and press **Enter**.
3. Select *Users* and press **Enter**.
4. Select *Admin User* and press **Enter**.
5. Determine the user name and the password of the scan user and press **Tab**.
6. Press **Enter**.

16.2 Managing all Configured Sensors

All sensors configured on a master can be displayed as follows:

1. Select *Setup* and press **Enter**.
2. Select *Master* and press **Enter**.
3. Select *Sensors* and press **Enter**.



→ Actions for all configured sensors are displayed (see Fig. 16.5).

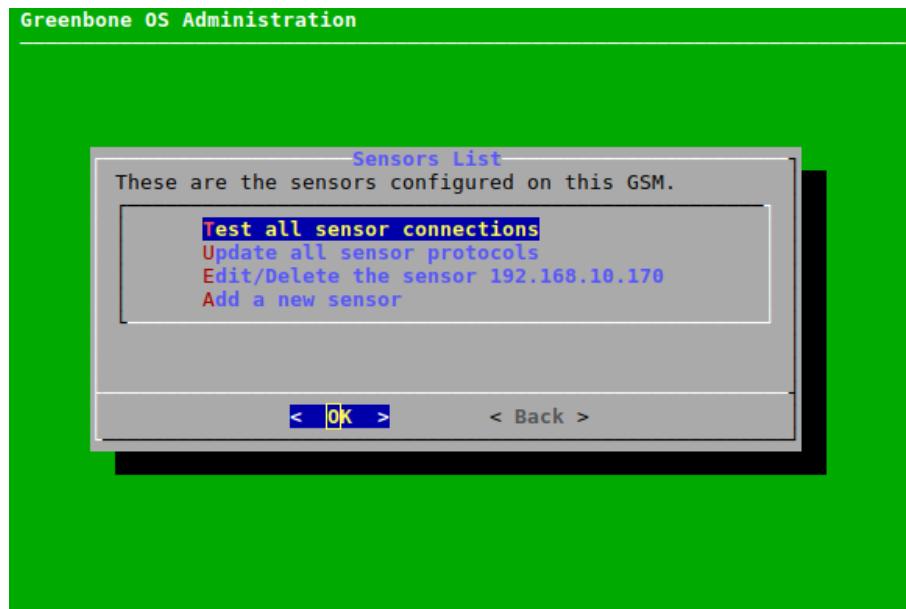


Fig. 16.5: Managing all configured sensors

The following actions are available:

Testing all sensor connections Test whether all sensors are configured correctly. If the test fails, a warning with instructions is displayed.

Update all sensor protocols Update all sensor protocol configurations on the master.

Edit/Delete the sensor ... Open the menu for configuring a specific sensor (see Fig. 16.3). The following actions are available:

- Setting the address of the sensor.
- Setting the remote port of the sensor.
- Setting the proxy for the sensor.
- Setting the sensor identifier.
- Enabling/disabling automatic feed updates on the sensor if the feed is updated on the master.
- Setting the port and the identifier automatically.
- Testing the correct configuration of the sensor.
- Deleting the sensor.

Add a new sensor Configure a new sensor (see Chapter 16.1.1 (page 410)).

16.3 Deploying Sensors in Secure Networks

For master-sensor setups the master stores all vulnerability information and credentials. A sensor does not store any information permanently (except for NVTs).

Due to this the master needs to be placed in the highest security zone with communication to the outside (to the sensors). All communication is initiated from the master in the higher security zone down to the sensor in the lower security zone.



Note: A firewall separating the different zones only needs to allow connections from the master to the sensor. No additional connections need to be allowed into the higher security zone.

Master and sensor appliances communicate via the SSH protocol. Port 22/TCP is used by default. For backward compatibility port 9390/TCP can be used. This can be configured as follows:

1. In the GOS administration menu of the sensor, select *Setup* and press **Enter**.
2. Select *Sensor* and press **Enter**.
3. Select *Port 9390* and press **Enter**.
4. Select *Save* and press **Enter**.

On sensors Greenbone Security Feed (GSF) updates and GOS upgrades can be downloaded either directly from the Greenbone Networks servers or using the master. In the second case only the master contacts the Greenbone Networks servers and distributes the corresponding files to all connected sensors. To prevent the sensor from contacting the Greenbone Networks servers, automatic synchronization can be disabled as follows:

1. In the GOS administration menu of the sensor, select *Setup* and press **Enter**.
2. Select *Feed* and press **Enter**.
3. Select *Synchronisation* and press **Enter**.
4. Select *Save* and press **Enter**.

Tip: As an additional layer of security a source and destination NAT rule on a firewall using stateful packet inspection (SPI) can be used to avoid the need of default routes on the GSM appliances.

16.4 Configuring a Sensor as a Remote Scanner

Note: In order to configure a sensor as a remote scanner, all steps in Chapter 16.1.1 (page 410) have to be completed first.

Sensors can be used as remote scanning engines (scanners) on the master in addition to the default OpenVAS and CVE scanners. For this, the sensor must be configured as a remote scanner using the web interface of the master.

A new remote scanner can be configured as follows:

1. Log into the web interface of the master.
2. Select *Configuration > Scanners* in the menu bar.
3. Create a new scanner by clicking
4. Enter the name of the remote scanner in the input box *Name* (see Fig. 16.6).
5. Select *Greenbone Sensor* in the drop-down list *Type*.
6. Enter the IP address or the host name of the sensor in the input box *Host*.
7. Create a new credential by clicking
8. Enter the name of the credential in the input box *Name*.
9. Select *Username + Password* in the drop-down list *Type*.



The screenshot shows a configuration dialog titled "New Scanner". It contains the following fields:

- Name: Remote_Scanner1
- Comment: (empty)
- Type: Greenbone Sensor
- Host: localhost
- Credential: Credential1

At the bottom are two buttons: "Cancel" and "Save".

Fig. 16.6: Configuring the remote scanner on the master

10. Enter the account information of the scan user account (see Chapter 16.1.2 (page 413)) in the input boxes *Username* and *Password*.
11. Click **Save** to create the credential.
12. Click **Save** to create the remote scanner.
 - The scanner is created and displayed on the page *Scanners*.
13. In the row of the newly created remote scanner click to verify the scanner.
 - If the setup is correct, the scanner is successfully verified.

Tip: Scanners are configured on a per-user basis. Scanners can be created for each user or permissions can be used to grant usage rights to other users (see Chapter 9.4 (page 231)).

16.5 Using a Remote Scanner

After a sensor is configured as a remote scanner, scan tasks can be configured on the master to run on the sensor (see Chapter 10.2.2 (page 251)).

The screenshot shows a configuration dialog titled "Reports". It contains the following settings:

- A checkbox labeled "Automatically delete oldest reports but all" is checked.
- A "Scanner" dropdown menu is open, showing "Remote_Scanner1" as the selected option.
- A "Scan Config" dropdown menu is open, showing "Full and fast" as the selected option.

Fig. 16.7: Selecting the remote scanner for a task

If an existing task is marked as alterable in the column *Name* on the page *Tasks* (see Chapter 10.8 (page 288)) the task can be sent to a remote scanner as follows:

1. Select *Scans > Tasks* in the menu bar.
2. In the row of the task click .
3. Select the remote scanner in the drop-down list *Scanner* (see Fig. 16.7).
4. Click **Save**.
5. Start the task by clicking

Managing the Performance

When operating the Greenbone Security Manager (GSM), significant amounts of data can be transferred between the GSM, the scan targets and any sensor appliances. In addition to that, the scan results have to be analyzed, filtered and processed by the GSM. Depending on the GSM model, the number of users and the configuration of the scan tasks, many of these processes will run concurrently.

17.1 Monitoring the Appliance Performance

The overall performance of the Greenbone Security Manager (GSM) can be monitored by selecting *Administration > Performance* in the menu bar (see Fig. 17.1).

The resource utilization of the GSM for the last hour, day, week, month or year can be displayed.

Note: The performance of a configured sensor can be displayed on the master as well.

The following sections are important:

Processes A high amount of processes is not critical. However, primarily only sleeping and running processes should be displayed.

System Load An ongoing high utilization is critical. A load of 4 on a system with 4 cores is considered acceptable.

CPU Usage Especially a high Wait-IO is critical.

Memory Usage The GSM uses aggressive caching. The usage of most of the memory as cache is acceptable.

Swap Usage A use of the swap memory points to a potential system overload.

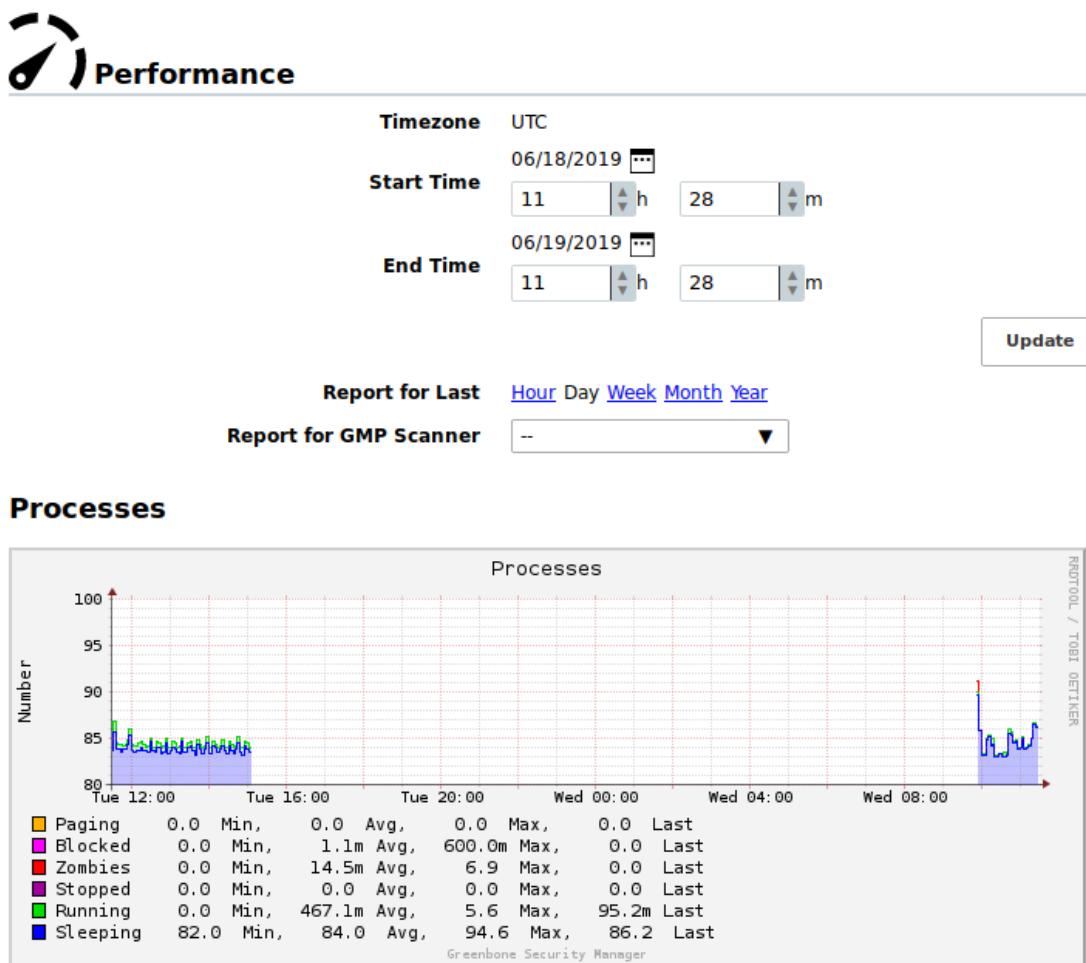


Fig. 17.1: Displaying the performance of the GSM



17.2 Optimizing the Scan Performance

The speed of a scan depends on many parameters:

- Selected ports
- Selected scan configuration
- Scanning order of targets

17.2.1 Selecting a Port List for a Task

The port list configured for a target has a large impact on the duration of the alive test and the vulnerability scan of this target.

17.2.1.1 General Information about Ports and Port Lists

Ports are the connection points of network communication. Each port of a system connects with the port on another system.

Transmission Control Protocol (TCP) ports

- 65535 TCP ports for each system
- Data transmission occurs in both directions between two TCP ports.
- The scan of TCP ports is usually performed simply and fast.

User Datagram Protocol (UDP) ports

- 65535 UDP ports for each system
- Data transmission occurs only in one direction 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 applications⁶¹.

The Internet Assigned Numbers Authority (IANA)⁵⁹ 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. Nmap⁶⁰, 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 GSM:

- All IANA assigned TCP 2012-02-10: all TCP ports assigned by IANA on 10th of February 2012
- All IANA assigned TCP and UDP 2012-02-10: all TCP and UDP ports assigned by IANA on 10th of February 2012
- All privileged TCP

⁶¹ 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.

⁵⁹ <https://www.iana.org/>

⁶⁰ <https://nmap.org/>



- All privileged TCP and UDP
- All TCP
- All TCP and Nmap 5.51 top 100 UDP: all TCP ports and the top 100 UDP ports according to Nmap 5.51
- 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
- OpenVAS Default: the TCP ports which are scanned by the OpenVAS scanner when passing the default port range preference

Note: Additional port lists can be created as described in Chapter 10.7 (page 285).

17.2.1.2 Selecting the Right Port List

When choosing a port list discovery performance and scan duration have to be taken into account.

The duration of a scan is mostly determined by the network configuration and the amount of ports to be tested.

Services not bound to ports on the list are not tested for vulnerabilities. Additionally, malicious applications that are bound to such ports will not be discovered. Malicious applications mostly use open ports that are usually not used and are far from the system ports.

Other criteria are the defence mechanisms that are activated by exhaustive port scans and initiate counter measures or alerts. Even with normal scans, firewalls can simulate that all 65535 ports are active and as such slow down the actual scan with so called time-outs.

Additionally, for each port that is queried the service behind it reacts at least with one log entry. For organizational reasons some services may only be scanned at a specific time.

Scan Duration

In some situations with port throttling, scanning all TCP and UDP ports can take up to 24 hours or more for a single system. Since the scans are performed in parallel, two systems will only take marginally more time than a single system. However, the parallelizing has its limits due to system resources and network performance.

All IANA TCP ports usually require only a couple of minutes to be scanned.

Since some counter measures can increase the duration of a scan, throttling can be prevented by making configuration changes on the defense system.

In suspected cases of a compromise or highest security breaches a fully inclusive scan is unavoidable.

Total Security

For port scans total security does not exist, i.e., even when all TCP and all UDP ports are scanned the preset timeout of the port testing can be too short to force a hidden malicious application to respond.

If an initial suspicion exists, an experienced penetration tester should be consulted.



17.2.2 Selecting a Scan Configuration for a Task

The scan configuration has an impact on the scan duration as well. The GSM offers four different scan configurations for vulnerability scans:

- Full and fast
- Full and fast ultimate
- Full and very deep
- Full and very deep ultimate

The scan configurations *Full and fast* and *Full and fast ultimate* optimize the scan process by using information found earlier in the scan. Only NVTs that are useful are executed, resulting in a reduced scan duration.

Scans using the scan configurations *Full and very deep* and *Full and very deep ultimate* ignore already discovered information and execute all available NVTs without exception.

17.2.3 Selecting the Scanning Order of Targets

During a scan the corresponding status bar on the page *Tasks* reflects the progress of the scan in percent (see Chapter 10.8 (page 288)).

In most cases this progress is a rough estimation since it is difficult for the GSM to project how the systems or services that have not been scanned yet behave compared to the already scanned systems and services.

Example A target network 192.168.0.0/24 that has only 5 alive hosts with the IP addresses 192.168.0.250–254 should be scanned. When creating a task with default settings for this target, the scanner will try to scan all possible hosts in the target network sequentially.

Since no hosts can be scanned for the IP addresses 192.168.0.1–249, the scanner skips these hosts and the scan progress reaches 95 % very quickly, indicating that the scan is almost finished.

Then the hosts with the IP addresses 192.168.0.250–254 are scanned and for each host, the vulnerability tests take some time. As a consequence, the scan progress is noticeably slower between 95 % and 100 %.

In order to improve the progress estimation, the setting *Order for target hosts* can be adjusted when creating a new task (see Chapter 10.2.2 (page 251)).

The setting *Random* is recommended (see Fig. 17.2).

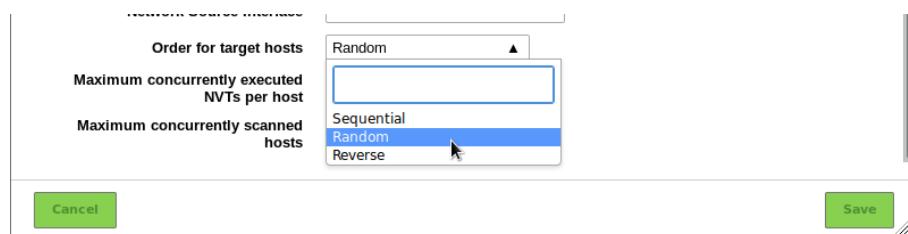


Fig. 17.2: Selecting the order for targets



17.3 Scan Queueing

Scans are only started if sufficient system resources are available. The available resources depend on the GSM model, the GOS version used, and the current workload of the system.

The most relevant resource for scanning is random-access memory (RAM). Each scan requires a certain minimum of RAM to be executed properly because the same scan process cannot handle multiple scans from different users or even from the same user. RAM has physical limits and cannot be shared in a satisfactory way.

CPU, network connection and disk I/O are relevant system resources as well. However, unlike RAM, they can be shared at the cost of slower scan execution.

The system performance charts provide detailed information about the RAM over time (see Chapter 17.1 (page 417)).

If too many scans are started and running at the same time and not enough RAM is available, scans are added to a waiting queue when clicking ▶. When the required RAM is available again, scans from the waiting queue are started, following the principle “first in, first out”.

The workload management is subject to the scanner. If a master-sensor setup is used, each sensor manages its available resources on its own. Sensor scans affect the scanning capacity of the master only minimally.

CHAPTER 18

Connecting the Greenbone Security Manager to Other Systems

The Greenbone Security Manager (GSM) can be connected to other systems.

Some systems have already been integrated into the GSM by Greenbone Networks:

- verinice ITSM system (see Chapter 18.2 (page 424))
- Nagios Monitoring System (see Chapter 18.3 (page 428))
- Cisco Firepower Management Center (see Chapter 18.4 (page 432))

The GSM offers numerous interfaces that allow for the communication with other systems:

Greenbone Management Protocol (GMP) The Greenbone Management Protocol allows to remote control the GSM completely. The protocol supports the creating of users, creating and starting of scan tasks and exporting of reports.

Connecting additional scanners using OSP The Open Scanner Protocol (OSP) is a standardized interface for different vulnerability scanners. Arbitrary scanners can be integrated seamlessly into the GSM vulnerability management. Controlling the scanners and handling the results works in the same way for all scanners.

Report format The GSM can present the scan results in any format. To do so, the GSM already comes with a multitude of pre-installed report formats (see Chapter 11.1 (page 315)). Additional report formats can be downloaded from the Greenbone download webpage or developed in collaboration with Greenbone Networks.

Alert via Syslog, e-mail, SNMP trap or HTTP (see Chapter 10.12 (page 305))

Automatic result forwarding through connectors These connectors are created by Greenbone Networks, verified and integrated into the GSM.

Monitoring via SNMP The webpage <https://docs.greenbone.net/API/SNMP/snmp-gos-20.08-21.04.en.html> provides the current Management Information Base (MIB) file. MIB files describe the files that can be queried by SNMP about the equipment.



18.1 Using an OSP Scanner

The Open Scanner Protocol (OSP) resembles the Greenbone Management Protocol (GMP, see Chapter 15 (page 399)). It is XML based, stateless and does not require a permanent connection for communication. The design allows for embedding additional scanners seamlessly into the GSM.

The open format allows developing custom OSP scanners. Greenbone Networks provides the protocol documentation at <https://docs.greenbone.net/API/OSP/osp-21.04.html>.

18.2 Using Verinice

Verinice⁶² is a free Open Source Information Security Management System (ISMS) developed by SerNet⁶³.

Greenbone Security Manager: Verinice Integration

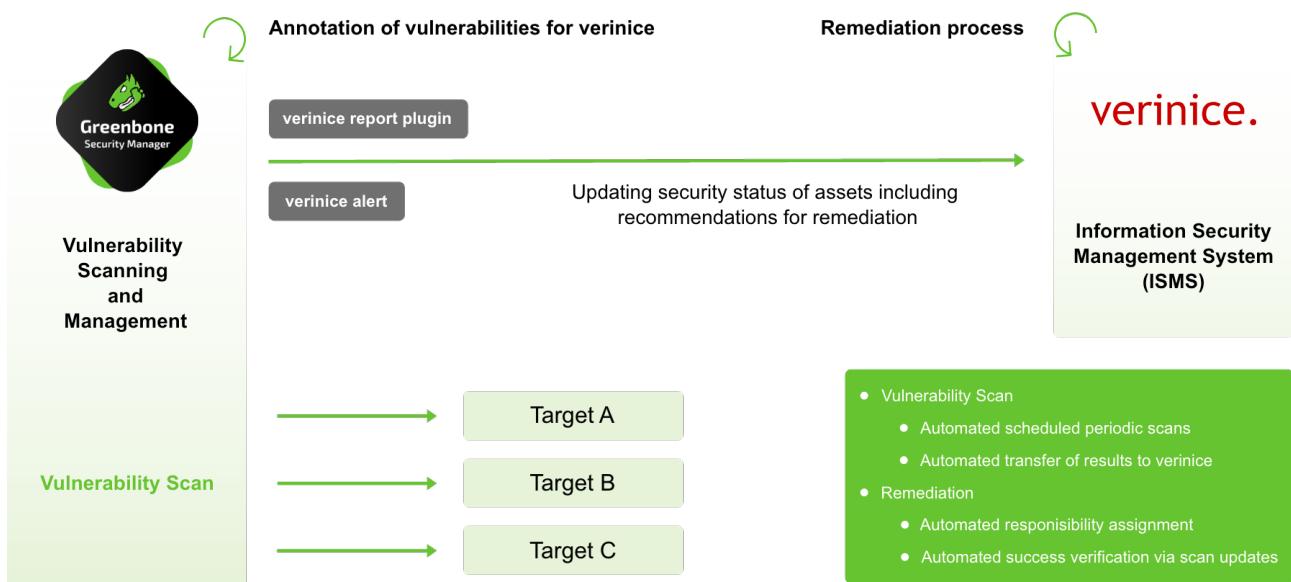


Fig. 18.1: Integrating the GSM with verinice

Verinice is suitable for:

- Vulnerability remediation workflow
- Performing risk analysis based on ISO 27005
- Operating an ISMS based on ISO 27001
- Performing an IS assessment per VDA specifications
- Proof of compliance with standards such as ISO 27002, IDW PS 330

The GSM can support the operation of an ISMS. For this, Greenbone Networks offers a report format for the export of data from the GSM into verinice:

- Verinice-ISM

⁶² <https://verinice.com/en/>

⁶³ <https://www.sernen.de/en/>



It is possible to transfer data completely automated from the GSM to verinice.PRO, the server extension of verinice.

Note: For support with the use of the connector contact SerNet or Greenbone Networks.

18.2.1 IT Security Management

The report format *Verinice ISM* for verinice is preinstalled on the GSM.

With this report format Greenbone Networks supports the vulnerability remediation workflow in verinice.

Verinice uses the notes (see Chapter 11.7 (page 335)) of the scan results to create objects for processing. If there are no notes in a task only the assets will be imported as well as the complete vulnerability report. Exclusively such vulnerabilities that have a note will be imported by verinice as vulnerabilities. This allows controlling the import in fine detail.

Note: Within the entire security process it has to be decided which vulnerabilities have to be solved and which can be tolerated. This decision is made by tagging the vulnerabilities accordingly in the vulnerability management.

The remediation workflow targets at solving any of the managed issues. Within the remediation workflow it is not allowed to decide about tolerating an issue.

After the scan is completed the report has to be exported using the report format *Verinice ISM* (see Chapter 11.2.2 (page 324)). A VNA file is created. This is a ZIP file containing the data of the scan.

Note: For the following example SerNet verinice 1.18.1 was used.

If another version is used, the steps may differ. Contact the verinice support for help.

18.2.1.1 Importing the ISM Scan Report

The report can be imported in verinice as follows:

1. Start verinice.
2. Select *View > Show Perspective > Information Security Management* in the menu bar (see Fig. 18.2).

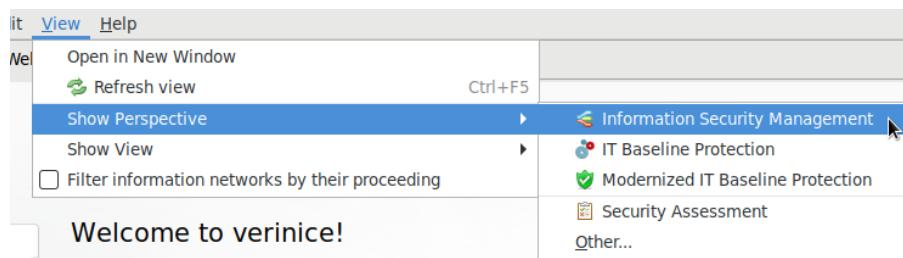


Fig. 18.2: Opening the perspective *Information Security Management*

3. Click in the window *Catalogs* to import the desired catalog.
4. Create an organization by clicking



Note: The window for defining the details of the organization can simply be closed.

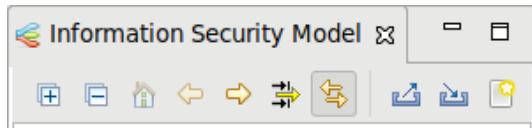


Fig. 18.3: Creating a new organization

5. In the window *Information Security Model* click .
6. Click *Select file...* and select the ISM report. The remaining parameters can be kept with their default settings (see Fig. 18.4).

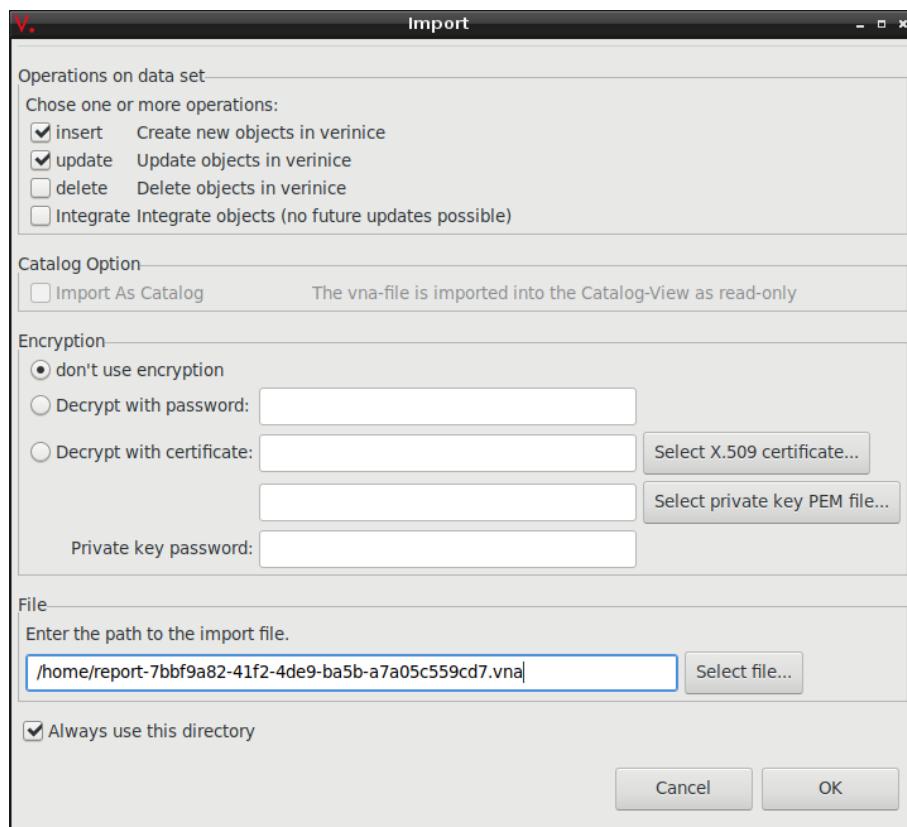


Fig. 18.4: Selecting the ISM report

7. Click *OK*.

→ The results of the ISM report are imported and can be unfolded in verinice (see Fig. 18.5).

The process to track vulnerabilities for the imported organization can be separated into two sub processes:

- Creation of tasks
- Remediation of vulnerabilities

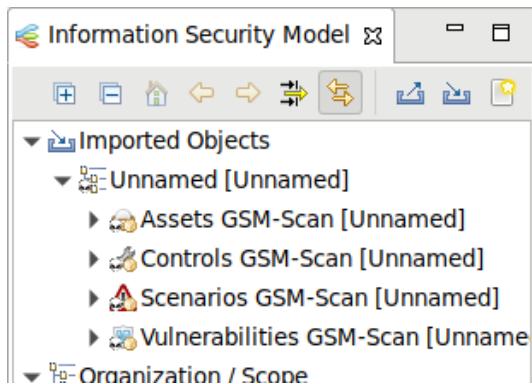


Fig. 18.5: Unfolding the results of the ISM report

18.2.1.2 Creating Tasks

Before creating tasks the data for the organization must be prepared as follows:

1. After the first import of an organization it must be moved from the group of imported objects to the top level.
Right click on the organization and select *Cut*. Click right in the top level in the window *Information Security Model* and select *Paste*.
2. The assets and controls must be grouped.
Right click on *Assets GSM-Scan* and select *Group by Tags...* (see Fig. 18.6).

Confirm the message by clicking *OK*.

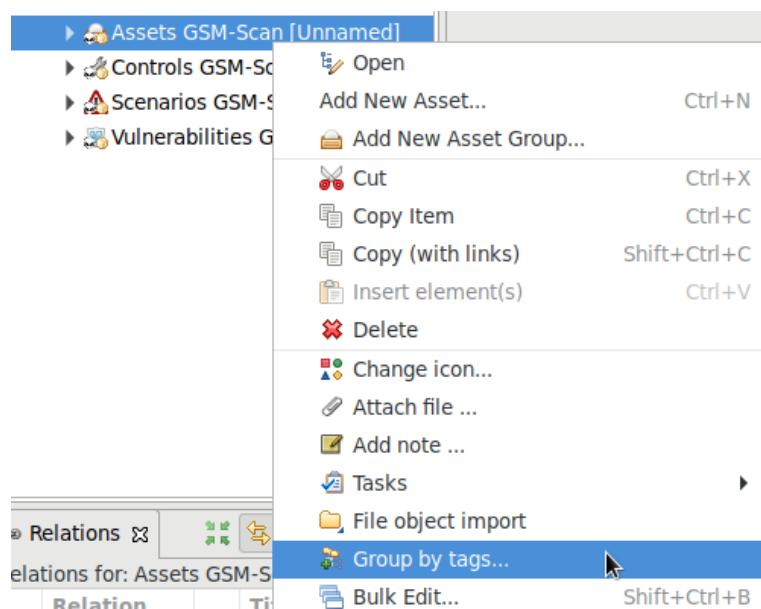


Fig. 18.6: Grouping the assets

3. Right click on *Controls GSM-Scan* and select *Group by Tags...*
Confirm the message by clicking *OK*.
4. All assets groups must be assigned a responsible person.
Expand the organization, right click on *Persons* and select *Add Person...*



5. Assign the newly created person per drag and drop to the assets group.

→ The successful assignment can be displayed in the window *Relations* by clicking *Assets GSM-Scan* (see Fig. 18.7).

Relations			
Relations for: Assets GSM-Scan			
Relation	Title	Scope	Desc
responsible	Person1	Organization	/

Fig. 18.7: Displaying the relations for a group

6. Right click on the organization and select *Tasks > Greenbone: Start vulnerability process....*

→ It is verified whether all assets and controls are grouped and whether all asset groups are assigned to a person. A message displays the result of the verification.

7. Continue with creating a task or cancel the creation.

The task to remediate vulnerabilities is called “Remediate Vulnerabilities”.

18.2.1.3 Remediating Vulnerabilities

The created tasks can be managed with the help of the view *Task* (*View > Show View > Tasks* in the menu bar) or the web frontend of the verinice.PRO version (under: ISO 27000 tasks).

A task contains controls, scenarios and assets that are connected to a control group and are assigned to a responsible person. The responsible person remediates the vulnerabilities for all assets.

Note: If the deadline for the task “Remediate Vulnerabilities” expires, a reminder e-mail is sent to the responsible person.

After the task is completed all connections between assets and scenarios that were assigned to a task are deleted.

The following states of a control are possible:

- Implemented: no asset is assigned to the scenario anymore.
- Partly: other connections to assets still exist.

18.3 Using Nagios

Nagios can integrate the scan results as an additional test in its monitoring tasks. The scanned systems are automatically matched with the monitored systems. With this the scan results are eventually available for the alert rules and other processes of Nagios.

When linking Nagios with the GSM, Nagios will assume the controlling role.

Nagios retrieves the newest scan results from the GSM regularly and automatically. This is done via a Nagios command which uses the tool `gvm-script` to call the script `check-gmp.gmp.py`.

Note: Other products compatible with Nagios such as Open Monitoring Distribution, Icinga, Centreon etc. should generally work but may require small adjustments to the described steps.



Greenbone Security Manager: Nagios/Centreon Integration

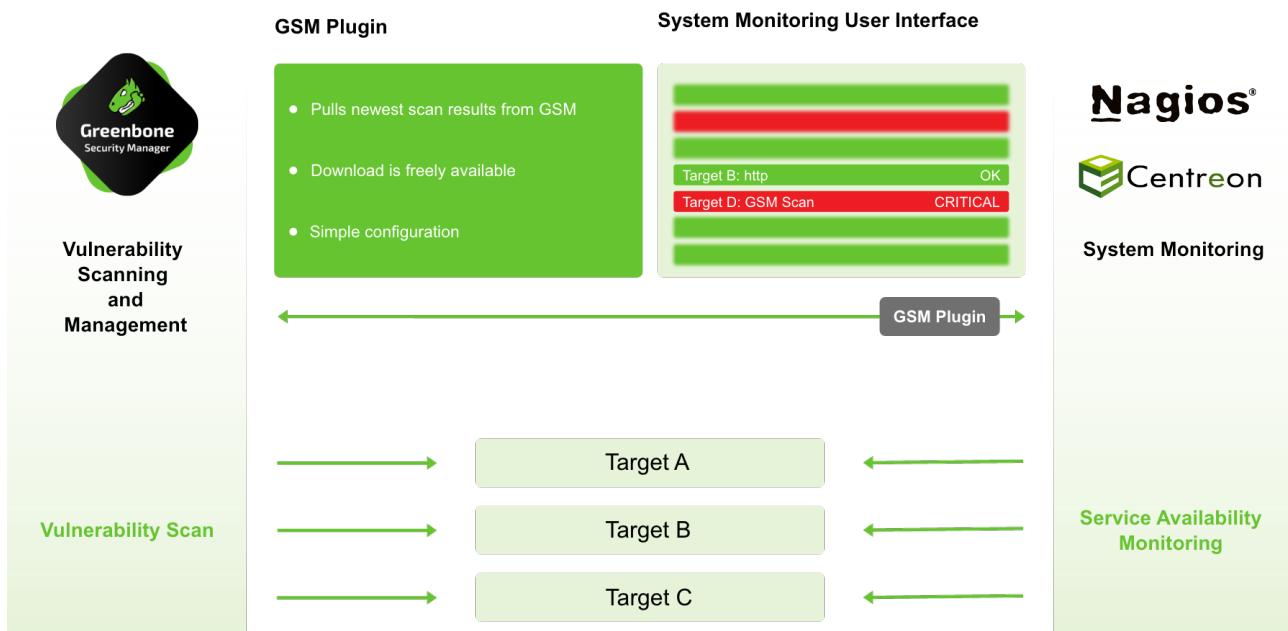


Fig. 18.8: Linking Nagios with the GSM

18.3.1 Configuring the GSM User

For access Nagios requires a user to log in to the GSM. For this user a scan target (or multiple scan targets) has to be set up with all hosts of which the security status should be monitored.

Note: The sample configuration used here assumes that there is only one relevant target but technically it is possible to link complex setups with multiple targets and multiple GSMS.

The GSM user account provided for queries by the GMP script must be owner of the relevant scan targets or at least have unrestricted reading access to them.

The tasks should be run as scheduled scans regularly.

Additionally, network access via GMP to the GSM must be possible. Therefore, the GMP access must be activated in the GOS administration menu (see Chapter 15.2 (page 399)).

18.3.2 Configuring the Script

Greenbone Networks provides the script `check-gmp.gmp.py` as part of the script collection of the gvm-tools (see Chapter 15.3 (page 400)). This script can be called by the monitoring solution using `gvm-script`.

Note: The following assumes Nagios is installed in `/usr/local/nagios/`, afterwards referred to as `/.../`. Adjust the file location if necessary.

1. Copy the plug-in to `/.../libexec/`.



2. Check if the script can reach the GSM through the network, GMP was activated and the user was created properly:

Note: In the following command replace the IP address with the IP address of the GSM and provide the user name and the created password.

```
nagios-host# gvm-script --gmp-username="user name" --gmp-password="password" \
ssh --hostname 192.168.10.169 /.../libexec/check-gmp.gmp.py --ping \
GMP OK: Ping successful
```

3. Check whether there is access to the data:

```
nagios-host# gvm-script --gmp-username="user name" --gmp-password="password" \
ssh --hostname 192.168.10.169 /.../libexec/check-gmp.gmp.py \
-F 192.168.10.130 --last-report -T "Scan Suspect Host" --status
GMP CRITICAL: 284 vulnerabilities found - High: 118 Medium: 153 Low: 13
Report did contain 1 errors for IP 192.168.10.130
|High=118 Medium=153 Low=13
```

The script supports several command line switches. These can be displayed using:

```
nagios-host# gvm-script -c /.../etc/gvm-tools.conf ssh --hostname
 192.168.10.169 scripts/check-gmp.gmp.py -H
usage: check-gmp [-H] [-V] [--cache [CACHE]] [--clean] [-F HOSTADDRESS] [-T TASK]
...
Check-GMP Nagios Command Plugin 2.0.0 (C) 2017-2019 Greenbone Networks GmbH
...
optional arguments:
-H           Show this help message and exit.
-V, --version      Show program's version number and exit
--cache [CACHE]    Path to cache file. Default: /tmp/check_gmp/reports.db.
--clean          Activate to clean the database.
...
```

4. If the tests were successful the check can be integrated into Nagios monitor.

Add the host to be monitored to the section `HOST DEFINITIONS` in the Nagios configuration file `/.../etc/objects/localhost.cfg`.

In this example the host is a Metasploitable Linux.

```
define host{
  use                  linux-server
  host_name            metasploitable
  alias                metasploitable
  address              192.168.10.130
}
```

5. In the same configuration file, in the section `SERVICE DEFINITIONS`, define a new service which calls the Nagios command `check_gmp_status`.

As the example shows, the name of the task where to fetch the report from is passed to the command as an argument.

```
define service{
  use                  local-service ; Name of service template to use
}
(continues on next page)
```



(continued from previous page)

```
host_name          metasploitable
service_description GMP task last report status
check_command      check_gmp_status!metasploitable
}
```

6. Create the `check_gmp_status` command in the file `/.../etc/objects/commands.cfg`.

```
define command{
    command_name      check_gmp_status
    command_line      gvm-script -c /.../etc/gvm-tools.conf ssh
                      --hostname 192.168.10.169 $USER1$/check-gmp.gmp.py -F $HOSTADDRESS$
                      --last-report -T $ARG1$ --status
}
```

Note: In the command line it can be seen that no user name and password options but a configuration file are passed to the tool `gvm-script` (see Chapter 15.3 (page 400)).

7. Restart the Nagios service to apply the new configuration.

```
nagios-host# systemctl restart nagios
```

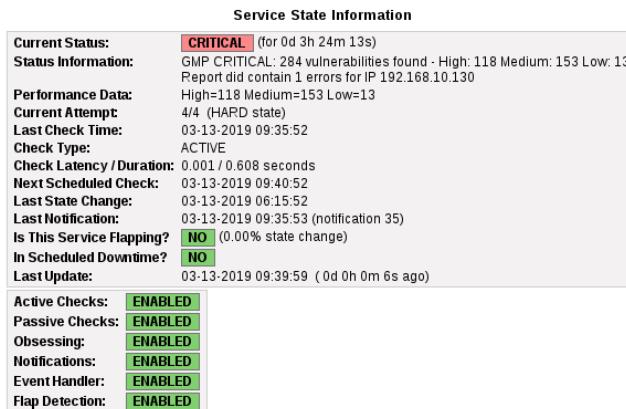


Fig. 18.9: Nagios displaying the monitored host status

18.3.3 Caching and Multiprocessing

The script `check-gmp.gmp.py` supports caching. All new reports will be cached in a SQLite database. The first call with an unknown host will take longer because the report needs to be retrieved from the GSM. Subsequent calls will only retrieve the current report from the GSM if the end time of the scan differs. Otherwise, the information from the database is used. This will greatly reduce the load both on the monitoring server and the GSM.

The cache file is written to `/tmp/check_gmp/reports.db` by default. A different location of the database can be specified using the command line switch `--cache`.

To further reduce the load both on the monitoring server and the GSM the plug-in can restrict the maximum number of simultaneously running plug-in instances. Additionally started instances are stopped and wait for their continuation. The default value of `MAX_RUNNING_INSTANCES` is 10. The default can be modified using the command line switch `-I`.



18.4 Using the Cisco Firepower Management Center

The Cisco Firepower Management Center (former Sourcefire Intrusion Prevention System (IPS)) is one of the leading solutions for intrusion detection and defense in computer networks. As a Network Intrusion Detection System (NIDS) it is tasked with the discovery, alerting and the defense against attacks on the network.

To identify and classify attacks correctly, the Firepower Management Center requires as much information as possible about the systems in the network, the applications installed on them, and the potential vulnerabilities for both. For this purpose the Firepower Management Center has its own asset database that can be augmented with information from the GSM. Additionally, the Firepower Management Center can start an automatic scan if it suspects anything.

The following connection methods are available:

Automatic data transfer from the GSM to the NIDS/IPS If the GSM and NIDS/IDS are configured respectively the data transfer from the GSM to the NIDS/IPS can be utilized easily, like any other alert functionality of the GSM. After completion of the scan, the report will be forwarded as an alert to the NIDS/IPS with respect to the desired criteria. If the scan task is run automatically on a weekly basis, a fully automated alerting and optimization system is obtained.

Active control of the GSM by the NIDS/IPS In the operation of the NIDS/IPS suspected incidents on systems with high risk can occur. In such a case the NIDS/IPS can instruct the GSM to check the system⁶⁵.

To use the connection methods the GSM as well as the Firepower Management Center have to be prepared. On the GSM a report format plug-in has to be installed. In the Firepower Management Center the option to receive the data must be enabled.

Note: The report format *Sourcefire* is provided via the feed.

Report formats may not be available yet, but will be added at a later time.

In case a report format is not available, contact the Greenbone Networks Support (support@greenbone.net).

18.4.1 Configuring the Host-Input-API Clients

The Host-Input-API is an interface through which the Firepower Management Center accepts data from other applications for its asset database.

1. Log into the Firepower Management Center.
2. Select *System > Local > Registration* in the menu bar.
3. Select the register *Host Input Client*.
4. Enter the IP address of the GSM in the input box *Hostname* (see Fig. 18.10).
5. Enter the password in the input box *Password*.

Note: The connection is TLS encrypted.

→ The Firepower Management Center creates a private key and certificate automatically.

In the certificate the IP address entered above will be used as common name and verified when the client is establishing a connection. If the client uses a different IP address, the connection fails.

The created PKCS#12 file is optionally secured by a password.

⁶⁵ This control does not exist as a finalized *Remediation* for the Firepower Management Center but it can be implemented via GMP (see Chapter 15 (page 399)).



Last login on Friday, 2014-05-09 at 10:11:19 AM from 192.168.111.6

SOURCEfire

Fig. 18.10: Creating a host input client

Afterwards the certificate and the key are created and made available as a download.

6. Click to download the file (see Fig. 18.11).

Hostname	
192.168.255.12	

https://192.168.111.20/estreamer_admin/downloadcert.cgi?client=192.168.255.12&host_input=1

SOURCEfire

Fig. 18.11: Downloading the created PKCS#12 file

18.4.2 Configuring a Sourcefire Connector Alert

Now the respective alert must be set up on the GSM.

1. Select *Configuration > Alerts* in the menu bar.
2. Create a new alert by clicking .
3. Define the alert (see Fig. 18.12).

Tip: For the information to enter in the input boxes see Chapter 10.12 (page 305).

4. Choose *Sourcefire Connector* in the drop-down list *Method*.



Fig. 18.12: Creating an alert with Sourcefire Connector

5. Supply the PKCS#12 file by clicking *Browse*....

Note: If a password was entered when the client was created, the PKCS#12 file has to be decrypted before loading it into the GSM.

To do so, the following command in Linux can be used:

```
$ openssl pkcs12 -in encrypted.pkcs12 -nodes -out decrypted.pkcs12
Enter Import Password : password
MAC verified OK
$
```

6. Click *Save*.

18.5 Using Alemba vFire

vFire is an Enterprise Service Management application, developed by Alemba⁶⁴.

The GSM can be configured to create tickets in an instance of vFire based on events like finished scans.

18.5.1 Prerequisites for Alemba vFire

For the integration to work properly, the following prerequisites must be met on the vFire system:

- The vFire installation must support the RESTful Alemba API, which has been added in vFire version 9.7. The legacy API of older versions is not supported by the Greenbone connector.
- An Alemba API client with the correct session type (analyst/user) and password login must be enabled.
- The user account that should be used requires permissions to use the Alemba API.

⁶⁴ <https://alemba.com/>



18.5.2 Configuring an Alemba vFire Alert

To have the GSM automatically create tickets (called “calls”) in vFire, an alert must be set up as follows:

1. Select *Configuration > Alerts* in the menu bar.
2. Create a new alert by clicking .
3. Define the alert (see Fig. 18.13).

Tip: For the information to enter in the input boxes see Chapter 10.12 (page 305).

4. Choose *Alemba vFire* in the drop-down list *Method*.

The screenshot shows the 'New Alert' configuration window. The 'Method' dropdown is set to 'Alemba vFire'. The 'Call Description' section contains a note about events and conditions, followed by a note about ticket formats and report details. The 'Active' checkbox is checked ('Yes').

Fig. 18.13: Creating an alert with Alemba vFire

5. Click *Save*.

The following details of the alert can be defined:

Report Formats The report formats used for the attachments. Multiple report formats can be selected or the selection can be left empty if no attachments are wanted.

Base URL This is the URL of the Alemba instance including the server name and the virtual directory. For example, if the user interface is accessed via <https://alemba.example.com/vfire/core.aspx>, the base URL would be <https://alemba.example.com/vfire>.

Credential The user name and the password used for logging into Alemba vFire.

Session Type The type of session to use. It can be either “analyst” or “user”.

As an “analyst” it is possible to perform some actions not available to a “user”. The “user” requires special permissions for these actions and the number of concurrent logins may be limited.



Alemba Client ID This is the Alemba API client ID (see Chapter 18.5.1 (page 434)).

Partition The partition to create the ticket in. See the Alemba vFire help for more information about partitioning.

Call Description This is the template for the description text used for the newly created calls. The same placeholders as in the message input box of the e-mail alert method can be used (see Chapter 10.12 (page 305)).

Call Template The name of a call template to use for the calls created by the alert. A call template can be configured in vFire to fill in all the fields that cannot be specified directly in the alert.

Call Type The name of a call type to use for the calls created by the alert.

Impact The full name of an impact value.

Urgency The full name of an urgency value.

18.6 Using Splunk

The GSM can be configured to forward the scan results to a Splunk enterprise installation for further analysis and correlation.

Connecting a GSM to a Splunk solution is not part of the GSM core functionality. As an add-on, Greenbone Networks provides an app for the integration with Splunk Enterprise on-premise solutions. The app is currently available at <https://download.greenbone.net/tools/Greenbone-Splunk-App-1.0.1.tar.gz>.

Important: External links to the Greenbone download webpage are case-sensitive.

Note that upper cases, lower cases and special characters have to be entered exactly as they are written here.

Note: If there are problems with downloading or testing the app contact the Greenbone Networks Support.

In the following Splunk Enterprise version 8.5 is used. The installation of the app on Splunk Light is not supported. Connecting a GSM to Splunk Cloud is not supported.

18.6.1 Setting up the Greenbone-Splunk App

18.6.1.1 Installing the App

The Greenbone-Splunk app can be installed as follows:

1. Open Splunk Enterprise.
2. Click  in the left menu panel (see Fig. 18.14).
3. Click *Install app from file*.
4. Click *Browse*....
5. Select the TAR file of the Greenbone-Splunk app.
6. Click *Upload*.

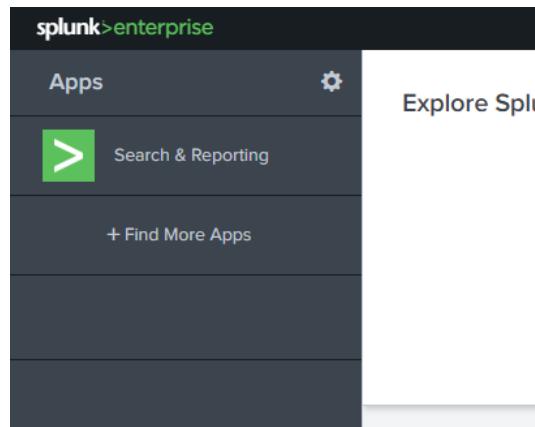


Fig. 18.14: Installing the Splunk app

18.6.1.2 Configuring the Greenbone-Splunk App

The port of the Greenbone-Splunk app is required for the configuration on the GSM.

Check the port of the Greenbone-Splunk app as follows:

1. Select the Greenbone-Splunk app in the left menu panel.
2. Select *Settings > Data inputs* in the menu bar.
3. Click *TCP* (see Fig. 18.15).

Note: The Greenbone-Splunk app sets up a data input on port 7680/tcp (default port) and tags the incoming data to *Greenbone Scan Results* and places it in the index *default*.

TCP port	Host Restriction	Source type	Status	Actions
7680	Greenbone Scan Results	Results	Enabled	Disable Delete Clone

Fig. 18.15: Checking the port of the Greenbone-Splunk app

To make the data more user-friendly, the field names can be replaced as follows:

1. Click in the left menu panel.
2. In the row of *Greenbone* click *View objects*.
3. Click *Greenbone Scan Results: FIELDAIAS-reportfields*.
4. Enter the field name aliases in the respective input boxes (see Fig. 18.16).



Greenbone Scan Results : FIELDALIAS-reportfields

Fields » Field aliases » Greenbone Scan Results : FIELDALIAS-reportfields

Field aliases	<code>result.description</code>	=	VulnerabilityResultDescription	Delete
	<code>result.host</code>	=	VulnerabilityResultHost	Delete
	<code>result.nvt.cert.cert_ref(@id)</code>	=	VulnerabilityResultNvtCertRef	Delete
	<code>result.nvt.cve</code>	=	VulnerabilityResultNvtCVE	Delete
	<code>result.nvt.cvss_base</code>	=	VulnerabilityResultNvtCVSS	Delete
	<code>result.nvt.family</code>	=	VulnerabilityResultNvtFamily	Delete
	<code>result.nvt.name</code>	=	VulnerabilityResultNvtName	Delete

Fig. 18.16: Changing the field name aliases

18.6.2 Configuring a Splunk Alert

The GSM transfers the scan results in the form of an XML report via an alert directly to the Splunk main server.

Note: The dashboard of the Greenbone-Splunk app only shows results from reports less than 7 days old.

If a report older than 7 days is sent, the dashboard will not display the results. However, the results are in the main index of the Splunk server.

18.6.2.1 Creating the Splunk Alert

The alert is created as follows:

1. Select *Configuration > Alerts* in the menu bar.
2. Create a new alert by clicking .
3. Define the alert (see Fig. 18.17).

Tip: For the information to enter in the input boxes see Chapter 10.12 (page 305).

4. Choose *Send to host* in the drop-down list *Method*.
5. Enter the IP address of the Splunk server in the input box *Send to host* and 7680 in the input box *on port*.

Note: The TCP port is 7680 by default.

This setting can be checked in the Greenbone-Splunk app as described in Chapter 18.6.1.2 (page 437).

6. Choose *XML* in the drop-down list *Report*.



The screenshot shows the 'New Alert' configuration dialog. The 'Event' section has 'New' selected under 'NVTs'. The 'Condition' section includes 'Severity at least 0.1' and 'Always'. The 'Report Content' section has 'Compose' selected. The 'Delta Report' section has 'None' selected. The 'Method' section has 'Send to host' selected. The 'Send to host' field contains '192.168.0.2' and the 'on port' field contains '7680'. The 'Report' section has 'XML' selected. The 'Active' section has 'Yes' selected. At the bottom are 'Cancel' and 'Save' buttons.

Fig. 18.17: Configuring the Splunk alert

7. Click **Save**.

18.6.2.2 Adding the Splunk Alert to a Task

The alert can now be selected when creating a new task (see Chapter 10.2.2 (page 251)) or be added to an existing task (see Chapter 10.12.2 (page 310)).

18.6.2.3 Testing the Splunk Alert

For testing purposes existing reports may be processed by the alert.

1. Select *Scans > Reports* in the menu bar.
2. Click on the date of a report.
3. Click \triangleright .
4. Select the alert in the drop-down list *Alert* (see Fig. 18.18).

The screenshot shows the 'Trigger Alert for Scan Report' dialog. It includes a 'Filter' field with 'apply_overrides=0 min_qod=70', 'Include' checkboxes for 'Notes' and 'Overrides', and an 'Alert' dropdown menu. The 'Splunk Connector' option is highlighted with a cursor. At the bottom are 'Cancel' and 'OK' buttons.

Fig. 18.18: Triggering the alert

5. Click **OK**.



18.6.3 Using the Greenbone-Splunk App

18.6.3.1 Accessing the Information in Splunk

To access the information in Splunk open the Greenbone dashboard as follows:

1. Open Splunk Enterprise.
2. Select the Greenbone-Splunk app in the left menu panel.
3. Select *Dashboards* in the menu bar.
4. Click *Greenbone Dashboard*.

Note: The dashboard of the Greenbone-Splunk app only shows results from reports less than 7 days old.

If a report older than 7 days is sent, the dashboard will not display the results. However, the results are in the main index of the Splunk server.

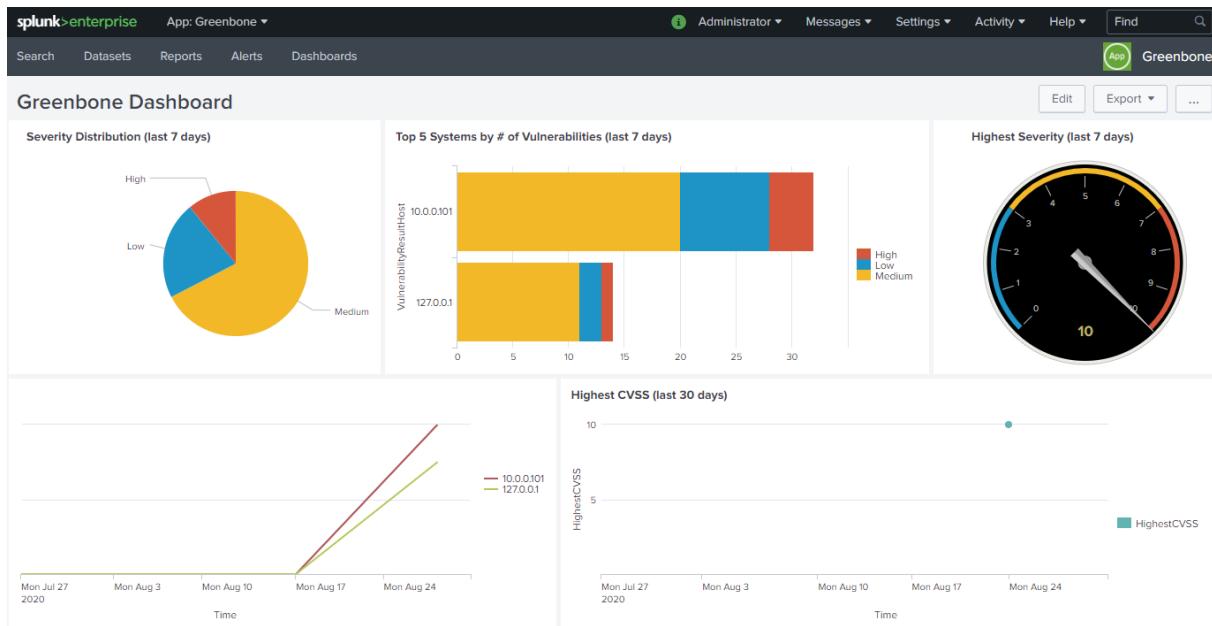


Fig. 18.19: Greenbone dashboard within the Greenbone-Splunk app

The input field *CVE-ID* below the dashboard can be used to display the number of hosts affected by a certain CVE over time.

Note: If the input box is left empty and `Enter` is pressed, the number of hosts affected by all CVEs is displayed.

18.6.3.2 Performing a Search

Since the information forwarded by the GSM is indexed by Splunk, the search view can be used to search for any data as follows:

1. Open Splunk Enterprise.



2. Select the Greenbone-Splunk app in the left menu panel.
3. Select *Search* in the menu bar.
4. Enter the index and the value that should be searched in the input box.
5. Select the time window in the drop-down list right of the input box.
6. Click .

Events (210) Patterns Statistics Visualization		
<input type="button" value="Format Timeline"/>	<input type="button" value="Zoom Out"/>	<input type="button" value="Zoom to Selection"/>
<input type="button" value="Deselect"/>		<input type="button" value="1 day per column"/>
<input type="button" value="List"/> <input checked="" type="checkbox"/> <input type="button" value="Format"/> <input type="button" value="20 Per Page"/> <input type="button" value="< Prev"/> <input type="button" value="1"/> <input type="button" value="2"/> <input type="button" value="3"/> <input type="button" value="4"/> <input type="button" value="5"/> <input type="button" value="6"/> <input type="button" value="7"/> <input type="button" value="8"/> ... <input type="button" value="Next >"/>		
< Hide Fields	☰ All Fields	i Time Event
SELECTED FIELDS		> 8/25/20 8:56:19.000 AM <result id='172d2fc4-65aa-4f3d-9eca-be77506bb6b4'><name>CPE Inventory</name><owner>sean</owner><creation_time>2020-08-25T08:56:19Z</creation_time><host>10.0.0.252<asset asset_id='854f4be9-b6ab-4c16-8c2a-25fe240594ce' 1.0.8'0002'><type>nvt</type><name>CPE Inventory</name><family>Service detection</family><cvss_base>0.0</cvss_base><cvss_temporal>0.0</cvss_temporal><cvss_vector>0.0</cvss_vector><description>Selected by other routines about CPE identities of operating systems, services and applications detected by this product. After a product got renamed or a specific vendor was acquired by another one it might have older CPE. lirsight= affected= impact= solution= vulnctact= solution_type=</tags><solution type=''/><script>can_nvt_version><threat>Log</threat><severity>0.0</severity><qod><value><></value></qod><se>pfsense 10.0.0.252 cpe:/a:php:php 10.0.0.252 cpe:/h:hp:jetdirect /</description><original_threat>host = 192.168.79.194 source = Greenbone Security Manager sourcetype = Greenbone Scan Results</original_threat>
INTERESTING FIELDS		> 8/25/20 8:56:19.000 AM <result id='b54d51bf-2765-49c7-808d-298773f2b7c'><name>Hostname Determination Reporting</name><owner>sean</owner><creation_time>2020-08-25T08:56:19Z</creation_time><host>10.0.0.252<asset asset_id='854f4be9-b6ab-4c16-8c2a-25fe240594ce' 1.3.6.1.4.1.25623.1.0.103449'><type>nvt</type><name>Hostname Determination Reporting</name><family>Host</family><summary>The script reports information on how the hostname of the target was determined. lirsizht=laff</summary>

Fig. 18.20: Carrying out a search in the Greenbone-Splunk app

Some supported indexes are:

- host
- source, sourcetype
- date_hour, date_minute, date_month, date_year, date_mdate, date_wday, date_zone
- VulnerabilityResultNvtCVE
- VulnerabilityResultNvtCVSS
- VulnerabilityResultQod
- VulnerabilityResultSeverity
- VulnerabilityResultThreat



18.6.3.3 Creating a Dashboard for the Top 5 Affected Hosts and for Incoming Reports

A new dashboard can be created to show the top 5 affected hosts of all time and the incoming reports from the GSM. The dashboard will show each time a new report comes in to the Splunk server for the past year.

1. Open Splunk Enterprise.
2. Select the Greenbone-Splunk app in the left menu panel.
3. Select *Dashboards* in the menu bar.
4. Click *Create New Dashboard*.
5. Enter a title in the input box *Title*, e.g., Greenbone incoming stats.
6. Click *Create Dashboard*.
7. Click *Source*.
8. Copy and paste the following into the input field (replacing all):

```
<dashboard>
    <label>Greenbone incoming stats</label>
    <row>
        <panel>
            <title>Top 5 all time</title>
            <chart>
                <search>
                    <query>sourcetype = "Greenbone Scan Results"
                    ↵VulnerabilityResultSeverity &gt; 0 | chart count over VulnerabilityResultHost by
                    ↵VulnerabilityResultThreat | fillnull High | fillnull Medium | fillnull Low | eval
                    ↵_count= High+Low+Medium | sort by _count desc | head 5</query>
                    <earliest>0</earliest>
                    <latest></latest>
                </search>
                <option name="charting.axisLabelsX.majorLabelStyle.overflowMode">
                    ↵ellipsisNone</option>
                    <option name="charting.axisLabelsX.majorLabelStyle.rotation">0</
                    ↵option>
                    <option name="charting.axisTitleX.visibility">visible</option>
                    <option name="charting.axisTitleY.visibility">visible</option>
                    <option name="charting.axisTitleY2.visibility">visible</option>
                    <option name="charting.axisX.scale">linear</option>
                    <option name="charting.axisY.scale">linear</option>
                    <option name="charting.axisY2.enabled">0</option>
                    <option name="charting.axisY2.scale">inherit</option>
                    <option name="charting.chart">bar</option>
                    <option name="charting.chart.bubbleMaximumSize">50</option>
                    <option name="charting.chart.bubbleMinimumSize">10</option>
                    <option name="charting.chart.bubbleSizeBy">area</option>
                    <option name="charting.chart.nullValueMode">gaps</option>
                    <option name="charting.chart.showDataLabels">none</option>
                    <option name="charting.chart.sliceCollapsingThreshold">0.01</option>
                    <option name="charting.chart.stackMode">stacked</option>
                    <option name="charting.chart.style">shiny</option>
                    <option name="charting.drilldown">all</option>
                    <option name="charting.fieldColors">{"High":0xD6563C, "Medium
                    ↵":0xF2B827, "Low":0x1E93C6}</option>
                    <option name="charting.layout.splitSeries">0</option>
                    <option name="charting.layout.splitSeries.allowIndependentYRanges">0
                    ↵</option>
                    <option name="charting.legend.labelStyle.overflowMode">
                    ↵ellipsisMiddle</option>
                </option>
            </chart>
        </panel>
    </row>

```

(continues on next page)



(continued from previous page)

```
<option name="charting.legend.placement">right</option>
<option name="refresh.display">progressbar</option>
</chart>
</panel>
</row>
<row>
<panel>
<chart>
<title>Incoming feed to Greenbone App</title>
<search>
<query>| tstats count where sourcetype = "Greenbone Scan Results" ↵
by sourcetype _time | timechart span=1d count by sourcetype</query>
<earliest>@y</earliest>
<latest>now</latest>
</search>
<option name="charting.chart">line</option>
<option name="refresh.display">progressbar</option>
</chart>
</panel>
</row>
</dashboard>
```

9. Click Save.

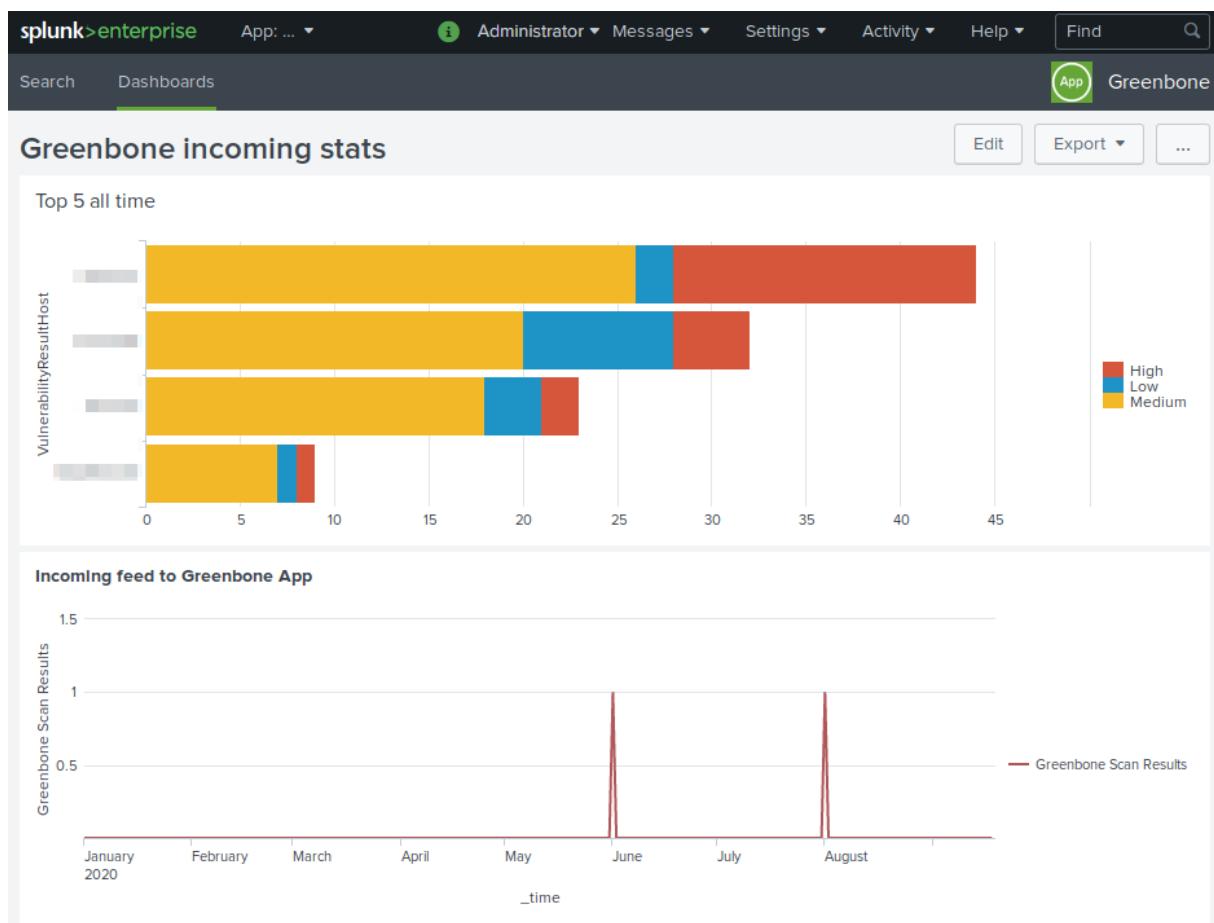


Fig. 18.21: Dashboard for the top 5 affected hosts and for incoming reports

CHAPTER 19

Architecture

19.1 GOS Architecture

The Greenbone Operating System (GOS) is the operating system of the Greenbone Security Manager. Here is an architecture overview for GOS 21.04.

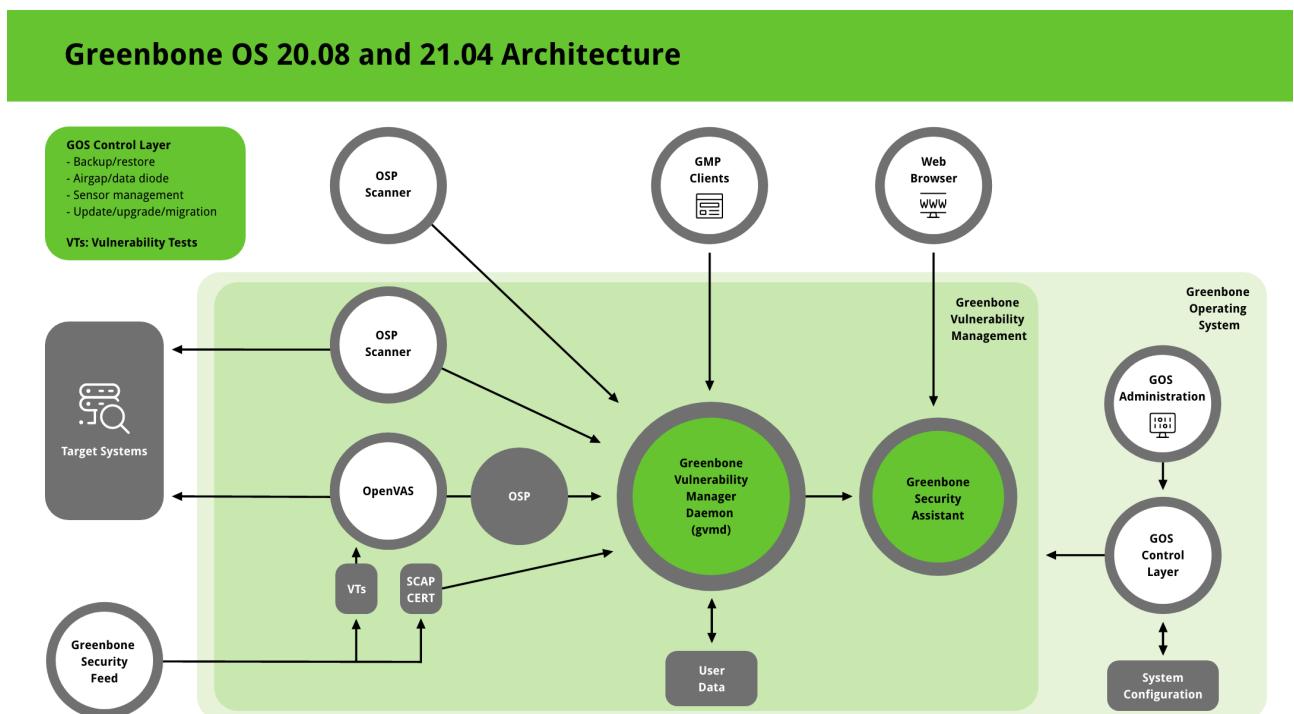


Fig. 19.1: GOS 21.04 architecture

The GOS control layer provides access to the administration of the Greenbone Operating System (GOS). Only a single system administrator account is supported. The system administrator cannot modify system files



directly but can instruct the system to change configurations.

GOS is managed using a menu-based graphical interface (GOS administration menu). The system administrator is not required to use the command line (shell) for configuration or maintenance tasks. Shell access is provided for support and troubleshooting purposes only.

Accessing the system level requires either console access (serial, hypervisor or monitor/keyboard) or a connection via SSH.

GOS allows users to configure, start, and stop all services of the Greenbone Vulnerability Management (GVM) framework.

Greenbone Vulnerability Management (GVM)

The Greenbone Vulnerability Management (GVM) is a framework originally built as a community project named “OpenVAS” and is primarily developed and forwarded by Greenbone Networks. It consists of the Greenbone Vulnerability Manager Daemon (gvmd), the Greenbone Security Assistant (GSA) with the Greenbone Security Assistant Daemon (gsad) and the executable scan application that runs vulnerability tests (VT) against target systems.

The GVM framework is released under Open Source licenses as the Greenbone Source Edition (GSE)⁶⁶. By using it, Linux distributions can create and provide GVM in the form of installation packages.

Greenbone Vulnerability Manager Daemon (gvmd)

The Greenbone Vulnerability Manager (gvmd)⁶⁷ is the central service that consolidates plain vulnerability scanning into a full vulnerability management solution. gvmd controls the OpenVAS Scanner via Open Scanner Protocol (OSP)⁶⁸.

The service itself offers the XML-based, stateless Greenbone Management Protocol (GMP)⁶⁹. gvmd also controls an SQL database (PostgreSQL) where all configuration and scan result data is centrally stored. Furthermore, gvmd also handles user management including permissions control with groups and roles. And finally, the service has an internal runtime system for scheduled tasks and other events.

Greenbone Security Assistant (GSA)

The Greenbone Security Assistant (GSA)⁷⁰ is the web interface of GVM that a user controls scans and accesses vulnerability information with. It the main contact point for a user with GVM. It connects to gvmd via the web server Greenbone Security Assistant Daemon (gsad) to provide a full-featured web application for vulnerability management. The communication occurs using the Greenbone Management Protocol (GMP) with which the user can also communicate directly by using different tools.

OpenVAS Scanner

The main scanner OpenVAS Scanner⁷¹ is a full-featured scan engine that executes vulnerability tests (VTs) against target systems. For this, it uses the daily updated and comprehensive feeds: the full-featured, extensive, commercial Greenbone Security Feed (GSF) or the free available Greenbone Community Feed (GCF)⁷².

The OpenVAS Scanner is controlled via OSP. The OSP Daemon for the OpenVAS Scanner (ospd-openvas) communicates with gvmd via OSP: VT data is collected, scans are started and stopped, and scan results are transferred to gvmd via ospd.

⁶⁶ <https://www.greenbone.net/en/product-comparison/>

⁶⁷ <https://github.com/greenbone/gvmd>

⁶⁸ <https://docs.greenbone.net/API/OSP/osp-21.04.html>

⁶⁹ <https://docs.greenbone.net/API/GMP/gmp-21.04.html>

⁷⁰ <https://github.com/greenbone/gsa>

⁷¹ <https://github.com/greenbone/openvas-scanner>

⁷² <https://www.greenbone.net/en/security-feed/>



OSP Scanner

Users can develop and connect their own OSP scanners using the generic ospd scanner framework. An (generic) OSP scanner example which can be used as an OSP scanner template can be found here⁷³.

GMP Clients

The Greenbone Vulnerability Management Tools (gvm-tools)⁷⁴ are a collection of tools that help with remote controlling a Greenbone Security Manager (GSM) appliance and its underlying Greenbone Vulnerability Manager Daemon (gvmd). The tools aid in accessing the communication protocols GMP (Greenbone Management Protocol) and OSP (Open Scanner Protocol).

This module is comprised of interactive and non-interactive clients. The programming language Python is supported directly for interactive scripting. But it is also possible to issue remote GMP/OSP commands without programming in Python.

19.2 Protocols

There are mandatory and optional protocols. Some protocols are only used in specific setups.

The GSM requires several protocols to fully function. These protocols provide the feed updates, Domain Name System (DNS) resolution, time, etc.

19.2.1 GSM as a Client

The following protocols are used by a stand-alone system or a GSM master to initiate connections as a client:

DNS – Name resolution

- Connecting to 53/udp and 53/tcp
- Mandatory
- Not encrypted
- May use internal DNS server

NTP – Time synchronization

- Connecting to 123/udp
- Mandatory
- Not encrypted
- May use internal NTP server

Feeds (see below)

- Direct
 - Connecting to 24/tcp or 443/tcp
 - Direct internet access required

⁷³ <https://github.com/greenbone/ospd-example-scanner>

⁷⁴ <https://github.com/greenbone/gvm-tools>



- Via proxy
 - Connecting to internal HTTP proxy supporting CONNECT method on configurable port
- Connecting to apt.greenbone.net and feed.greenbone.net
- Mandatory on stand-alone and master appliances
- Used protocol is SSH
- Encrypted and bidirectionally authenticated via SSH
 - Server: public key
 - Client: public key

DHCP

- Connecting to 67/udp and 68/udp
- Optional
- Not encrypted

LDAPS – User authentication

- Connecting to 636/tcp
- Optional
- Encrypted and authenticated via SSL/TLS
 - Server: certificate
 - Client: user name/password

Syslog – Remote logging and alerts

- Connecting to 514/udp or 514/tcp
- Optional
- Not encrypted

SNMP traps for alerts

- Connecting to 162/udp
- Optional
- Only SNMPv1
- Not encrypted

SMTP for e-mail alerts

- Connecting to 25/tcp by default, alternatively connecting to 587/tcp
- Optional
- Encrypted via STARTTLS, if possible
- Not encrypted, if encryption via STARTTLS is not possible

SSH for backup

- Connecting to 22/tcp
- Optional
- Encrypted and bidirectionally authenticated via SSH
 - Server: public key



- Client: public key

Cisco Firepower (Sourcefire) for IPS integration

- Connecting to 8307/tcp
- Optional
- Encrypted and bidirectionally authenticated via SSL/TLS
 - Server: certificate
 - Client: certificate

verinice.PRO

- Connecting to 443/tcp
- Optional
- Encrypted via SSL/TLS
 - Server: optional via certificate
 - Client: user name/password

TippingPoint SMS

- Connecting to 443/tcp
- Optional
- Encrypted via SSL/TLS
 - Server: certificate
 - Client: certificate, user name/password

Greenbone OS: GSM Acting as a Client

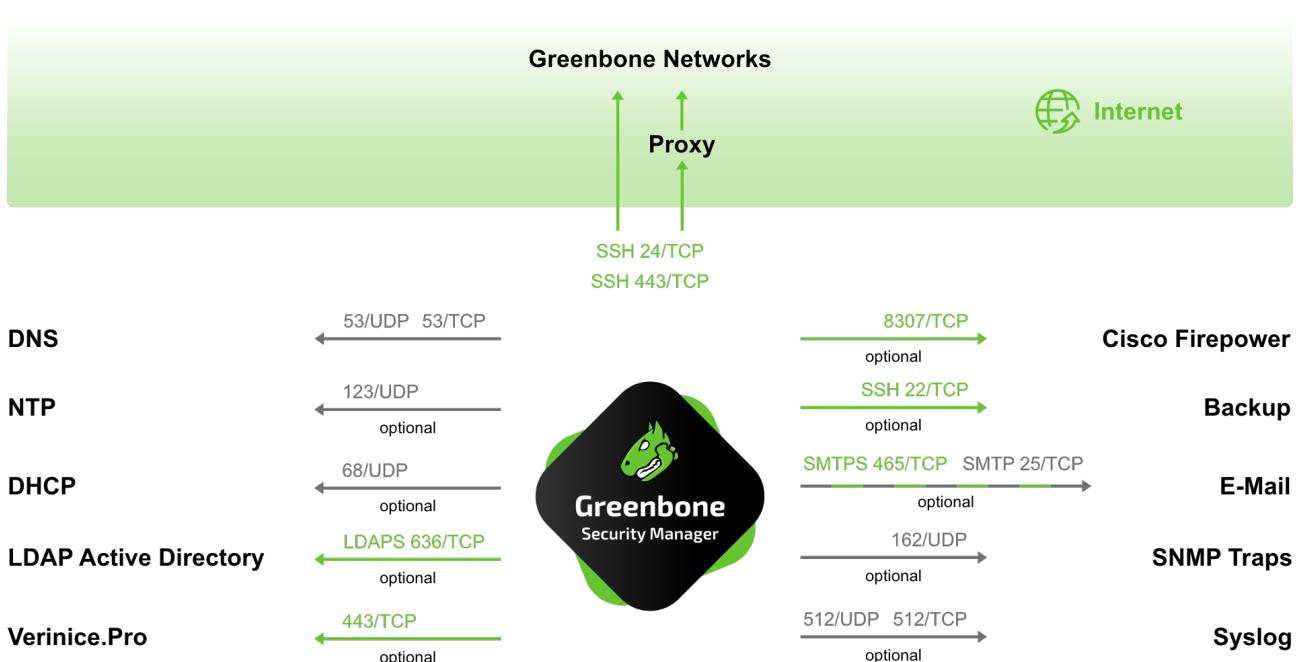


Fig. 19.2: GSM acting as a client



19.2.2 GSM as a Server

The following connections are supported by a GSM acting as a server:

HTTPS – Web interface

- 443/tcp
- Mandatory on stand-alone and master appliances
- Encrypted and authenticated via SSL/TLS
 - Server: optional via certificate
 - Client: user name/password

SSH – CLI access and GMP

- 22/tcp
- Optional
- Encrypted and authenticated via SSH
 - Server: public key
 - Client: user name/password

SNMP

- 161/udp
- Optional
- Optionally encrypted when using SNMPv3

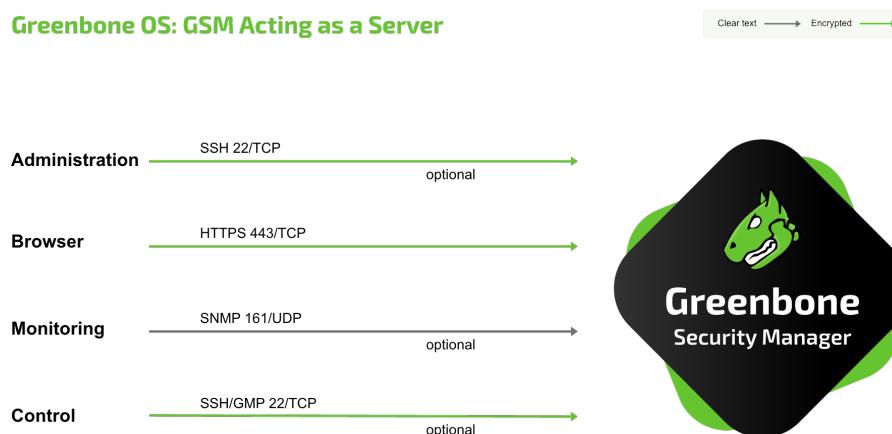


Fig. 19.3: GSM acting as a server



19.2.3 Master-Sensor Setup

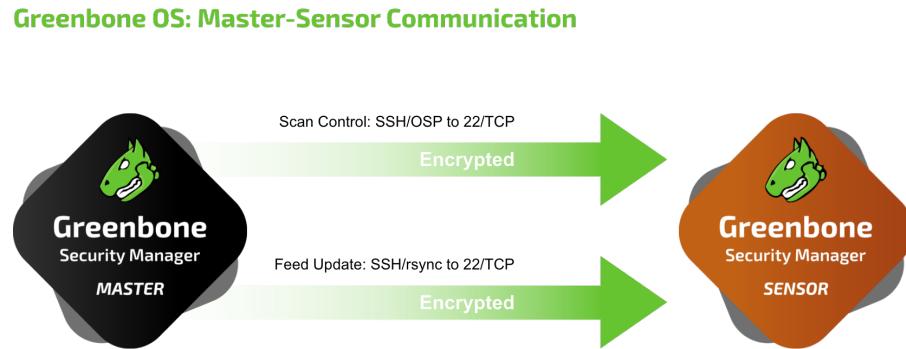


Fig. 19.4: GSM master and sensor

In a master-sensor setup the following additional requirements apply. The master (server) initiates up to three additional connections to the sensor (client):

SSH for GOS upgrades, feed updates, GMP and OSP

- 22/tcp
- Mandatory
- Encrypted and bidirectionally authenticated via SSH
 - Server: public key
 - Client: public key

19.3 Security Gateway Considerations

Many enterprises deploy security gateways to restrict the internet access. These security gateways can operate as packet filters or application layer gateways.

Some products support deep inspection and try to determine the actual protocol used in the communication channels. They may even try to decrypt and analyze any encrypted communication.

19.3.1 Stand-Alone/Master GSM

While many protocols used by the GSM are only used internally, some protocols require access to the internet. These protocols may be filtered by such a security gateway.

When deploying the GSM as a stand-alone appliance or as a master, the GSM needs to be able to access the Greenbone Security Feed. The Greenbone Security Feed can be accessed directly via port 24/tcp or 443/tcp or using a proxy.

Note: In all cases the used protocol is SSH, even when using the port 443/tcp or a HTTP proxy.

A deep inspection firewall may detect the usage of the SSH protocol running on port 443/tcp and drop or block the traffic.

If the security gateway tries to decrypt the traffic using man-in-the-middle techniques, the communication of the GSM and the feed server fails. The SSH protocol using bidirectional authentication based on public keys prevents any man-in-the-middle approaches by terminating the communication.



Additional protocols which need internet access are DNS and NTP. Both DNS and NTP can be configured to use internal DNS and NTP servers.

19.3.2 Sensor GSM

If security gateways are deployed between the master and the sensor, the security gateway must permit SSH (22/tcp) connections from the master to the sensor.

CHAPTER 20

Frequently Asked Questions

20.1 Why is the Scanning Process so Slow?

The performance of a scan depends on various aspects.

- Several port scanners were activated concurrently.
If an individual scan configuration is used, select only a single port scanner in the VT family *Port scanners* (see Chapter 10.9.2 (page 292)). The VT *Ping Host* can still be activated.
- Unused IP addresses are scanned very time-consuming.

As a first step, it is detected whether an active system is present or not for each IP address. In case it is not, this IP address will not be scanned. Firewalls and other systems can prevent a successful detection. The VT *Ping Host* (1.3.6.1.4.1.25623.1.0.100315) in the VT family *Port scanners* offers fine-tuning of the detection.

20.2 Why Is a Service/Product Not Detected?

- The target is not detected as online/reachable.

Solution(s):

- Fix the network setup/routing to the target.
- Update the criteria/test configuration to detect the target as alive (see Chapter 10.2.1 (page 248)).
- Verify and remove any network device (firewall, IDS/IPS, WAF, etc.) between the scanner and the target, or any security mechanisms on the target itself. Whitelist the scanner's IP address.

- The service/product is running on a specific port not included in the port list.

Solution(s):

- Create a suitable port list (see Chapter 10.7 (page 285)). This is especially important for UDP ports.



- There is a detection VT for an service/product available but the service/product is not found during a scan.

Solution(s):

- Fix the network setup/routing to the target.
- Update the criteria/test configuration to detect the target as alive (see Chapter 10.2.1 (page 248)).
- Verify and remove any network device (firewall, IDS/IPS, WAF, etc.) between the scanner and the target, or any security mechanisms on the target itself. Whitelist the scanner's IP address.
- Create a suitable port list (see Chapter 10.7 (page 285)). This is especially important for UDP ports.
- If the solutions above do not help, contact the Greenbone Networks Support (support@greenbone.net) and provide more information about the service/product (product name, specific version running, etc.).

- The target is not stable/responds slowly during a scan.

Solution(s):

- Lower the concurrently executed VTs (see Chapter 10.2.2 (page 251)).
- Update the service/product to a newer version (e.g., to fix triggered bugs).
- Assign more resources (CPU, RAM, etc.) to the target to make it more stable during scans.

20.3 Why Is a Vulnerability Not Detected?

- The affected service/product is not detected at all.

Solution(s):

- See Chapter 20.2 (page 452).

- The service/product was detected but the a version extraction was not possible.

Solution(s):

- Perform an authenticated scan (see Chapter 10.3 (page 253)).
- If the solutions above do not help, contact the Greenbone Networks Support (support@greenbone.net) and provide more information about the service/product (product name, specific version running, etc.).

- There is only a version check with a lower Quality of Detection (QoD) and the vulnerability is not displayed by default.

Solution(s):

- Change the QoD value in the results filter (see Chapter 11.2.1.3 (page 323)).
- Perform an authenticated scan (see Chapter 10.3 (page 253)).

- If an authenticated scan was carried out, the login has failed.

Solution(s):

- Check the correctness of the used credentials.
- Verify that the user is not blocked.
- Verify that the user is allowed to log in to the target.



- If the solutions above do not help, contact the Greenbone Networks Support (support@greenbone.net) and provide more information about the service/product (product name, specific version running, etc.).
- The service/product itself crashed or stopped to respond during the scan.

Solution(s):

- Lower the concurrently executed VTs (see Chapter 10.2.2 (page 251)).
- Update the service/product to a newer version (e.g., to fix triggered bugs).
- Assign more resources (CPU, RAM, etc.) to the target to make it more stable during scans.

- The vulnerability was only recently discovered and there is no VT for it yet.

Solution(s):

- Contact the Greenbone Networks Support (support@greenbone.net) and ask for a new VT or whether a VT is already planned.

- The specific detection became outdated.

Solution(s):

- Contact the Greenbone Networks Support (support@greenbone.net).

20.4 Why Is It Not Possible to Edit Scan Configurations, Port Lists, Compliance Policies, or Report Formats?

Scan configurations, port lists, compliance policies and report formats by Greenbone Networks (hereafter referred to as “objects”) are distributed via the feed. These objects must be owned by a user, the Feed Import Owner. The objects are downloaded and updated during a feed update, if a Feed Import Owner has been set.

The objects cannot be edited. This is by design to ensure that the objects function as intended by Greenbone Networks.

20.5 Why Is It Not Possible to Delete Scan Configurations, Port Lists, Compliance Policies, or Report Formats?

Scan configurations, port lists, compliance policies and report formats by Greenbone Networks (hereafter referred to as “objects”) are distributed via the feed. These objects must be owned by a user, the Feed Import Owner. The objects are downloaded and updated during a feed update, if a Feed Import Owner has been set.

Only the Feed Import Owner, a super administrator and users who obtained respective rights are able to delete objects.

If objects are deleted, they will be downloaded again during the next feed update. If no objects should be downloaded, the Feed Import Owner must be unset.

20.6 Why Does a VNC Dialog Appear on the Scanned Target System?

When testing port 5900 or configuring a VNC port, a window appears on the scanned target system asking the user to allow the connection. This was observed for UltraVNC Version 1.0.2.

Solution: exclude port 5900 or other configured VNC ports from the target specification. Alternatively, upgrading to a newer version of UltraVNC would help (UltraVNC 1.0.9.6.1 only uses balloons to inform users).



20.7 Why Does the Scan Trigger Alarms on Other Security Tools?

For many vulnerability tests the behaviour of real attacks is applied. Even though a real attack does not happen, some security tools will issue an alarm.

A known example is:

Symantec reports attacks regarding CVE-2009-3103 if the VT *Microsoft Windows SMB2 '_Smb2ValidateProviderCallback()' Remote Code Execution Vulnerability* (1.3.6.1.4.1.25623.1.0.100283) is executed. This VT is only executed if the radio button *No* is selected for *safe_checks* in the scanner preferences (see Fig. 20.1). Otherwise the target system can be affected.

Edit Scan Config Unnamed

Edit Scanner Preferences (20)

Name	New Value	Default Value
auto_enable_dependencies	<input checked="" type="radio"/> Yes <input type="radio"/> No	yes
cgi_path	/cgi-bin/scripts	/cgi-bin:/scripts
checks_read_timeout	5	5
drop_privileges	<input type="radio"/> Yes <input checked="" type="radio"/> No	no
expand_vhosts	yes	yes
max_sysload	25	25
min_free_mem	1024	1024
network_scan	<input type="radio"/> Yes <input checked="" type="radio"/> No	no
non_simult_ports	139, 445	139, 445, 3389, Services/irc
open_sock_max_attempts	5	5
optimize_test	<input checked="" type="radio"/> Yes <input type="radio"/> No	yes
plugins_timeout	320	320
report_host_details	<input checked="" type="radio"/> Yes <input type="radio"/> No	yes
safe_checks	<input type="radio"/> Yes <input checked="" type="radio"/> No	yes
scanner_plugins_timeout	36000	36000

Cancel Save

Fig. 20.1: Disabling the scanner preference *safe_checks*



20.8 How Can a Factory Reset of the GSM Be Performed?

A factory reset can be performed to erase user data securely from the GSM.

Note: Contact the Greenbone Networks Support via e-mail (support@greenbone.net) to receive detailed instructions on how to perform a factory reset.

20.9 Why Does Neither Feed Update nor GOS Upgrade Work After a Factory Reset?

A factory reset deletes the whole system including the Greenbone Security Feed (GSF) subscription key. The GSF subscription key is mandatory for feed updates and GOS upgrade.

1. Reactivate the GSF subscription key:

A backup key is delivered with each GSM appliance (see Chapter 7.1.1 (page 120)). Use this key to reactivate the GSM. The activation is described in the setup guide of the respective GSM model (see Chapter 5 (page 26)).

2. Update the system to the current version:

Depending on the GOS version, the respective upgrade procedure has to be executed.

20.10 How Can an Older, Newer or Unsupported Backup Be Restored?

Only backups created with the currently used GOS version or the previous GOS version can be restored. For GOS 6, only backups from GOS 5 or GOS 6 can be imported. If an older backup should be imported, e.g., from GOS 3 or GOS 4, an appliance with a matching GOS version has to be used.

Backups from GOS versions newer than the currently used GOS version are not supported as well. If a newer backup should be imported, an appliance with a matching GOS version has to be used.

If there are any questions, contact the Greenbone Networks Support via e-mail (support@greenbone.net).

20.11 What Can Be Done if the GOS Administration Menu Is not Displayed Correctly in PuTTY?

Check the settings in PuTTY by selecting *Window > Translation* in the left panel. *UTF-8* has to be selected in the drop-down list *Remote character set* (see Fig. 20.2).

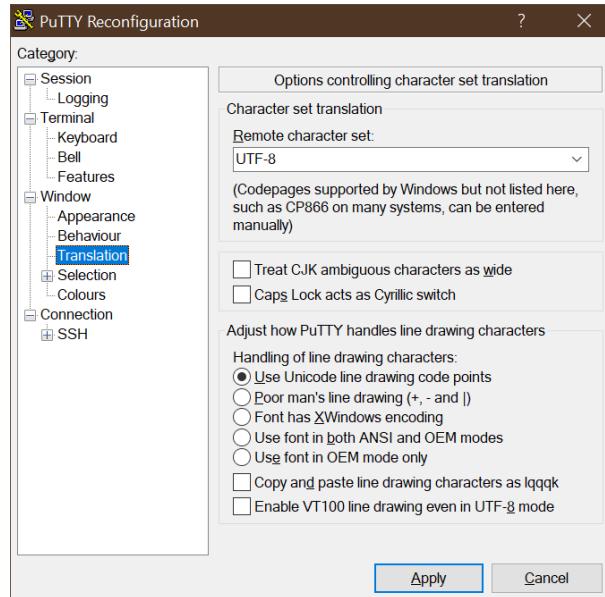


Fig. 20.2: Selecting the remote character set

20.12 How Can the GMP Status Be Checked Without Using Credentials?

1. Build an SSH connection to the GSM via command line using the GMP user:

```
ssh gmp@<gsm>
```

Replace <gsm> with the IP address or DNS name of the GSM appliance.

Note: No input prompt is displayed but the command can be entered nevertheless.

2. Enter <get_version/>.

→ If GMP is activated, the output should look like <get_version_response status="200" status_text="OK"><version>8.0</version></get_version_response>.

CHAPTER 21

Glossary

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

21.1 Alert

An alert is an action which can be triggered by certain events. In most cases, this means the output of a notification, e.g., an e-mail in case of new found vulnerabilities.

21.2 Asset

Assets are discovered on the network during a vulnerability scan or entered manually by the user. Currently, assets include hosts and operating systems.

21.3 CERT-Bund Advisory

An advisory published by CERT-Bund. See <https://www.cert-bund.de/about> for more information.

21.4 Compliance Audit

A compliance audit is a scan task with the flag *audit* and used to check the fulfillment of compliances.

21.5 Compliance Policy

A compliance policy is a scan configuration with the flag *policy* and used to check the fulfillment of compliances.



21.6 CPE

Common Platform Enumeration (CPE) is a structured naming scheme for information technology systems, platforms and packages. Based on the generic syntax for Uniform Resource Identifiers (URI), CPE includes a formal name format, a language for describing complex platforms, a method for checking names against a system and a description format for binding text and tests to a name.

A CPE name starts with “cpe:/”, followed by up to seven components separated by colons:

- Part (“h” for hardware, “o” for operating system or “a” for application)
- Vendor
- Product
- Version
- Update
- Edition
- Language

Example: cpe:/o:linux:kernel:2.6.0

21.7 CVE

Common Vulnerabilities and Exposures (CVE) is a dictionary of publicly known information security vulnerabilities and exposures.

21.8 CVSS

The Common Vulnerability Scoring System (CVSS) is an open framework to characterize vulnerabilities.

21.9 DFN-CERT Advisory

An advisory published by DFN-CERT. See <https://www.dfn-cert.de/> for more information.

21.10 Filter

A filter describes how to select a certain subset from a group of resources.

21.11 Group

A group is a collection of users.



21.12 Host

A host is a single system that is connected to a computer network and that can be scanned. One or many hosts form the basis of a scan target.

A host is also an asset type. Any scanned or discovered host can be recorded in the asset database.

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

In the asset database the identification is independent of the actual network address, which however is used as the default identification.

21.13 Note

A note is a textual comment associated with a VT. Notes show up in reports, below the results generated by the VT. A note can be applied to a particular result, task, severity, port and/or host, so that the note appears only in certain reports.

21.14 Vulnerability Test (VT)

A Vulnerability Test (VT) is a routine that checks a target system for the presence of a specific known or potential security problem.

VTs are grouped into families of similar VTs. The selection of families and/or single VTs is part of a scan configuration.

21.15 OVAL Definition

An OVAL definition is a definition as specified by the OVAL (Open Vulnerability and Assessment Language), version 5.10.1. It can be used for different classes of security data like vulnerabilities, patches or compliance policies.

21.16 Override

An override is a rule to change the severity of items within one or many report(s).

Overrides are especially useful to mark report items as False Positives (e.g., an incorrect or expected finding) or emphasize items that are of higher severity in the observed scenario.

21.17 Permission

A permission grants a user, role or group the right to perform a specific action.

21.18 Port List

A port list is a list of ports. Each target is associated with a port list. This determines which ports are scanned during a scan of the target.



21.19 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.

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 %		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.



The value of 70 % is the default minimum used for filtering the displayed results in the reports.

21.20 Remediation Ticket

Remediation tickets are used to resolve the findings of vulnerabilities. Tickets can be assigned to the current user or other users. All valuable information to understand and resolve the problem is directly cross-linked and available for the assigned user.

All tickets have a specific status (e.g., open, fixed) to track the progress.

Additionally, alerts can be assigned for certain events considering tickets, e.g., a status change of an assigned ticket.

The ticket management system is capable of considering the repetition of scans automatically in order to verify that the problem has been solved.

21.21 Report

A report is the result of a scan and contains a summary of what the selected VTs detected for each of the target hosts.

A report is always associated with a task. The scan configuration that determines the extent of the report is part of the associated task and cannot be modified. Therefore, for any report it is ensured that its execution configuration is preserved and available.

21.22 Report Format

A format in which a report can be downloaded.

An example is TXT which has the content type “text/plain”, meaning that the report is a plain text document.

21.23 Result

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

21.24 Role

A role defines a set of permissions that can be applied to a user or a group.

21.25 Scan

A scan is a task in progress. For each task only one scan can be active. The result of a scan is a report.

The status of all active scans can be seen on the page *Tasks*.

The progress is shown as a percentage of total number of tests to be executed. The duration of a scan is determined by the number of targets and the complexity of the scan configuration and ranges from minutes to many hours or even days.



The page *Tasks* offers an option to stop a scan.

If a stopped or interrupted scan is resumed, all unfinished hosts are scanned completely anew. The data of hosts that were already fully scanned is kept.

21.26 Scanner

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

21.27 Scan Configuration

A scan configuration covers the selection of VTs as well as general and very specific (expert) parameters for the scan server and for some of the VTs.

Not covered by a scan configuration is the selection of targets.

21.28 Schedule

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

21.29 Severity

The severity is a value between 0.0 (no severity) and 10.0 (highest severity) and expresses also a severity class (*Log*, *Low*, *Medium* or *High*).

This concept is based on CVSS but is applied in case no full CVSS Base Vector is available as well. 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 *High* are defined by sub-ranges of the main range 0.0 – 10.0. Users can select to use different classifications. The default is the NVD classification which is the most commonly used one.

Scan results are assigned a severity while achieved. The severity of the related VT may change over time though. If *Dynamic Severity* is selected in the user settings the system always uses the most current severities of VTs for the results.

21.30 Solution Type

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

- ⓘ Workaround: Information about a configuration or specific deployment scenario that can be used to avoid exposure to the vulnerability is available. There can be none, one or more workarounds available. This is usually the “first line of defense” against a new vulnerability before a mitigation or vendor fix has been issued or even discovered.



- ↳ Mitigation: Information about a configuration or deployment scenario that helps to reduce the risk of the vulnerability is available but that does not resolve the vulnerability on the affected product. Mitigations may include using devices or access controls external to the affected product. Mitigations may or may not be issued by the original author of the affected product and they may or may not be officially sanctioned by the document producer.
- ↳ Vendor fix: Information is available about an official fix that is issued by the original author of the affected product. Unless otherwise noted, it is assumed that this fix fully resolves the vulnerability.
- ∅ No fix available: Currently there is no fix available. Information should contain details about why there is no fix.
- ✗ Will not fix: There is no fix for the vulnerability and there never will be one. This is often the case when a product has been orphaned, is no longer maintained or otherwise deprecated. Information should contain details about why there will be no fix issued.

21.31 Tag

A tag is a short data package consisting of a name and a value that is attached to a resource of any kind and contains user defined information on this resource.

21.32 Target

A target defines a set of systems (hosts) that is scanned. The systems are identified either by their IP addresses, by their host names or with CIDR network notation.

21.33 Task

A task is initially formed by a target and a scan configuration. Executing a task initiates a scan. Each scan produces a report. As a result, a task collects a series of reports.

A task's target and scan configuration are static. Thus, the resulting sequence of reports describes the change of security status over time. However, a task can be marked as alterable when there are no reports present. For such a task the target and scan configuration can be changed at any time which may be convenient in certain situations.

A container task is a task with the function to hold imported reports. Running a container task is not possible.

21.34 TLS Certificate

A TLS (Transport Layer Security) certificate is a certificate used for authentication when establishing a connection secured by TLS.

The scan report contains all TLS certificates collected during a vulnerability scan.

Index

A

Access roles, 130
Accessing web interface, 220
Adding dashboard displays, 203
Adding report formats, 318
Administrative access, 141
Administrator, 126, 225
Administrator password, 124
Advanced, 193
Advanced task wizard, 246
Advisory, 396, 397, 458, 459
Airgap, 166
Airgap FTP server, 167
Airgap master, 166
Airgap sensor, 166
Airgap USB stick, 166
Alarm on another security tool, 454
Alemba vFire, 305, 434
Alemba vFire alert, 434
Alert, 305, 422, 458
Alert for reports, 325
Alert for tickets, 333
Alert method, 306
Alert via Alemba vFire, 434
Alert via e-mail, 422
Alert via HTTP, 422
Alert via SNMP trap, 422
Alert via sourcefire connector, 433
Alert via Splunk, 438
Alert via Syslog, 422
Alive scanner, 117
Alive test, 248, 313
Appliance performance, 417
Architecture, 444
ARF, 316
Asset, 377, 458
Asset management, 377
Asset Reporting Format, 316
Assigning alerts, 310
Assigning roles, 228
Audit, 351, 458

Authenticated scan, 253
Authentication algorithm, 255
Auto-FP, 118
Auto-generated password, 255
Automatic e-mails, 171
Automatic False Positives, 118
Automatic logout, 220
Automatic result forwarding, 422

B

Backup, 158, 179, 180
Backup on USB stick, 181
Basic system setup, 42
Beaming, 183
Boreas alive scanner, 117
BPM, 341
BSI, 345, 372–374
BSI TR-02102, 374
BSI TR-02102-4, 374
BSI TR-03116, 373
BSI TR-03116-4, 373
Business Process Map, 341

C

Calculating severity scores, 116, 391
Central password storage, 240
Central user management, 240
CERT-Bund advisory, 383, 396, 458
CERT-Bund Short Information, 396
Certificate, 148, 149
Certificate authority, 150
Changes, 122
Changes of default behavior, 116
Changes to GMP, 399
Changing administrator password, 124
Changing password, 128
Changing scanner preferences, 295
Changing severity, 338
Changing ticket status, 332
Changing user password, 128
Changing VT preferences, 297
Checking file checksums, 363



- Checking file checksums for Microsoft Windows, **365**
 Checking file content, **357**
 Checking IT-Grundschutz, **372**
 Checking registry content, **360**
 Checking standard policies, **372**
 Ciphers, **147**
 Cisco Firepower Management Center, **422, 431**
 Cleanup, **165**
 Client certificate, **255**
 Client for gvm-cli, **402**
 Cloning roles, **226**
 COBIT, **345**
 Command gvm-cli, **402**
 Command gvm-pyshell, **404**
 Command permission, **231**
 Committing changes, **122**
 Common Platform Enumeration, **367, 383, 389, 458**
 Common Vulnerabilities and Exposures, **383, 387, 459**
 Common Vulnerability Scoring System, **116, 391, 459**
 Compliance audit, **351, 458**
 Compliance policies, **130, 454**
 Compliance policy, **347, 458**
 Compliance scans, **345**
 Composing scan report content, **324**
 Computer Emergency Response Team for Federal Agencies, **396, 458**
 Configuring master-sensor setup, **410**
 Configuring scans, **248**
 Connecting master and sensor, **410**
 Console, **121**
 Container task, **282**
 Content composer, **324**
 Control Objectives for Information and Related Technology, **345**
 Copyright file, **198**
 CPE, **367, 383, 389, 458**
 CPE-based check, **367**
 CPU usage, **417**
 Creating alerts, **305**
 Creating audits, **352**
 Creating Business Process Maps, **341**
 Creating container tasks, **282**
 Creating groups, **229**
 Creating guest login, **225**
 Creating hosts, **378**
 Creating notes, **335**
 Creating overrides, **338**
 Creating permissions, **231**
 Creating policies, **347**
 Creating port lists, **285**
 Creating roles, **226**
 Creating scan configurations, **292**
 Creating scan user account, **413**
 Creating scanners, **303**
 Creating schedules, **301**
 Creating super administrator, **127, 229**
 Creating super permissions, **234**
 Creating targets, **248, 380**
 Creating tasks, **251**
 Creating tickets, **331**
 Creating users, **222**
 Creating web administrator, **126**
 Credential, **253, 255**
 CVE, **383, 387, 459**
 CVE scanner, **280, 303**
 CVSS, **116, 391, 459**
- ## D
- Dashboard displays, **203**
 Dashboards, **203**
 Data Objects, **130, 454**
 Default behavior, **116**
 Default settings, **218**
 Deleted objects, **216**
 Deleting dashboard displays, **203**
 Deleting the GSF subscription key, **165**
 Deleting user account, **128**
 Deleting user data, **456**
 Deploying sensors, **414**
 Deploying the appliance, **78, 90, 101**
 Details page, **200**
 Detecting absence of important products, **369**
 Detecting problematic products, **367**
 Deutsches Forschungsnetz, **397, 459**
 DFN, **397, 459**
 DFN-CERT advisories, **397**
 DFN-CERT advisory, **383, 459**
 DHCP, **135**
 Differences between GOS 20.08 and GOS 21.04, **116**
 Disabling feed synchronization, **163**
 Disabling overrides, **341**
 Displays, **203**
 Distributed data objects, **130, 454**
 Distributed scan system, **408**
 DNS, **139**
 DNS server, **139**
 Domain name, **140**
 Domain Name System, **139**
 Downloading reports, **116**
- ## E
- E-Mail alert, **422**
 E-Mail server, **171**
 E-Mail size, **173**
 E-Mails, **171**



- Editing scanner preferences, 295
 Editing VT preferences, 297
 Enabling feed synchronization, 163
 Enabling overrides, 341
 Enterprise Class, 18
 Entry Class, 23
 eth0, 134
 EulerOS, 278
 Exporting reports, 116, 315, 324
- F**
- Factory reset, 456
 False positive, 322, 338
 Family of VTs, 290
 FAQ, 451
 Federal Office for Information Security, 345, 372–374
 Feed, 120, 161, 189
 Feed Import Owner, 130, 454
 Feed status, 218
 Feed synchronization, 161, 177
 Feed time, 177
 Feed update, 189
 Feed update after factory reset, 456
 Feed update on sensors, 189
 Feed version, 199
 File checksums, 363
 File checksums for Microsoft Windows, 365
 File content, 357
 Filter, 207, 459
 Filtering reports, 323
 Firepower, 431
 First setup wizard, 42
 First system setup, 42
 Flash partition, 114, 190
 Frequently Asked Questions, 451
- G**
- GaussDB, 279
 GCF, 444
 General preferences, 295
 General system setup, 26, 40, 42, 53, 66, 78, 90, 101
 Generic policy scan, 357
 German Federal Office for Information Security, 345, 372–374
 German Research Network, 397, 459
 get_users, 236
 Global gateway, 140
 GMP, 119, 120, 145, 153, 398, 422, 444, 457
 GMP changes, 399
 GMP scanner, 118
 GMP status, 457
 GMP status code, 407
 GOS administration menu, 119–122, 456
- GOS upgrade, 188
 GOS upgrade after factory reset, 456
 GOS upgrade on sensors, 188
 GOS version, 199
 Granting read access, 236
 Greenbone Community Feed, 444
 Greenbone Executive Report, 316
 Greenbone Feed Service, 120, 161
 Greenbone Management Protocol, 119, 120, 145, 153, 398, 422, 444, 457
 Greenbone Operating System, 119
 Greenbone Security Assistant, 26, 40, 53, 78, 101, 120, 199, 444
 Greenbone Security Assistant Daemon, 444
 Greenbone Security Feed, 120, 161, 384, 444
 Greenbone Security Report, 316
 Greenbone Update Service, 120, 161
 Greenbone Vulnerability Management, 444
 Greenbone Vulnerability Management Daemon, 444
 Greenbone Vulnerability Management Tools, 444
 Greenbone Vulnerability Management tools, 400
 Greenbone Vulnerability Manager, 444
 Greenbone-Splunk app, 436
 Group, 229, 459
 GSA, 26, 40, 53, 78, 101, 120, 199, 444
 gsad, 444
 GSF, 120, 161, 444
 GSF subscription key, 120, 162, 165, 198, 199
 GSM 150, 19
 GSM 25V, 22
 GSM 35, 20
 GSM 400, 19
 GSM 450, 19
 GSM 5400, 18
 GSM 600, 19
 GSM 650, 19
 GSM 6500, 18
 GSM as client, 446
 GSM as server, 449
 GSM DECA, 22
 GSM EXA, 22
 GSM model, 199
 GSM models, 17
 GSM ONE, 23
 GSM overview, 17
 GSM PETA, 22
 GSM TERA, 22
 GSR, 316
 Guest, 225
 Guest login, 225
 Guest user, 126
 GVM, 444
 gvm-cli, 402



gvm-cli client, 402
gvm-cli.exe, 400
gvm-pyshell, 404
gvm-pyshell.exe, 404
gvm-tools, 400, 444
gvm-tools scripts, 407
gvmd, 444
GXR, 316

H

Hardware appliances, 117
High severity, 322
Host, 378, 459
Host name, 140
Host-input-API, 432
HTPPS, 146
HTTP Get, 305
HTTPS, 145
HTTPS certificate, 148
HTTPS certificates for logging, 175
HTTPS ciphers, 147
HTTPS fingerprints, 152
HTTPS timeout, 146
Huawei VRP, 274
Hypervisor, 78, 90, 101

I

IANA, 419
Importing reports, 324
Importing scan configurations, 294
Info, 225
Information, 199
Information Systems Audit and Control Association, 345
Installing the appliance, 26, 40, 53, 66
Interface, 134
Interface routes, 138
International Organization for Standardization, 345
Internet Assigned Numbers Authority, 419
IP address, 142
IP address of web interface, 199
IPS, 431
IPv6, 136
ISACA, 345
ISMS, 424
ISO 27001, 424
ISO 27005, 424
IT security, 383
IT security management, 424
IT-Grundschutz, 316, 372
IT-Grundschutz compendium, 372
ITG, 316

K

Keyboard layout, 170

Kryptographische Verfahren:
Empfehlungen und Schlüssellängen, 374
Kryptographische Vorgaben für Projekte der Bundesregierung, 373

L

Language, 170, 218
LaTeX, 316
LDAP, 240
LDAP with SSL/TLS, 241
List page, 200
Local security checks, 253
Log, 322
Log files, 193
Logging, 173, 175
Logging in, 220
Logging in as a guest, 225
Logging into the web interface, 38, 51, 64, 89, 111, 200
Logging server, 174
Login, 26, 38, 40, 51, 53, 64, 78, 89, 101, 111, 121, 200, 221
Login information, 121
Logout, 220
Low severity, 322

M

MAC address, 142
Mail server, 171
Mail server authentication, 172
Mail size, 173
Mailhub, 171
Maintenance, 178
Maintenance time, 177
Management access, 141
Management IP address, 141
Managing users, 124
Managing web users, 125
Master, 408, 450
Master-sensor setup, 408, 450
Maximum Transmission Unit, 136
Medium severity, 322
Midrange Class, 19, 22
Midrange class, 117
Migration, 112
Mitigation, 321, 328, 463
MITRE, 387, 389, 390
Modify task wizard, 247
Monitoring performance, 417
MTU, 136
My settings, 218

N

Nagios, 422, 428
Namespace, 132



NASL wrapper, 297
National Institute of Standards and Technology, 386
National Vulnerability Database, 386
Network interface, 134
Network Intrusion Detection System, 431
Network routes, 142
Network settings, 132
Network Time Protocol, 169
Network Vulnerability Test, 383, 384, 460
NIDS, 431
NIST, 383, 386
Nmap, 297, 419
Nmap NASL preferences, 297
No solution, 321, 328, 463
Note, 335, 460
NTP, 169
NTP server, 169
NVD, 383, 386
NVT, 383, 384, 460

O

Observer, 225, 290
Obstacles, 313
Open Scanner Protocol, 153, 422, 423, 444
Open Scanner Protocol Daemon, 444
Open Vulnerability and Assessment Language, 390, 460
OpenVAS, 444
OpenVAS scanner, 303, 444
OpenVPN, 143
Operating system, 119, 381
OSP, 153, 422, 423, 444
OSP scanner, 422, 423
ospd, 444
ospd-openvas, 444
OVAL definition, 383, 390, 460
Override, 338, 460
Overview, 17
Overview dashboard, 204

P

Page content, 207
Passphrase, 255
Password, 121, 128, 218, 255
Password policy, 129
Performance, 416
Performing a backup, 179
Performing a backup on USB stick, 181
Performing a general system setup, 26, 40, 53, 66, 78, 90, 101
Performing scans, 244
Periodic backups, 158
Permission, 231, 460
Permission get_users, 236
Permissions for a task, 290

PGP encryption key, 255
Physical Enterprise Class, 18
Physical Midrange Class, 19
Physical sensor, 20
Physical SME Class, 19
Ping, 297
Ping preferences, 297
Planned scan, 301
Policy, 347, 458
Policy scan, 357
Port, 419
Port list, 285, 419, 460
Port lists, 130, 454
Powerfilter, 207
Privacy algorithm, 255
Privacy password, 255
Problems, 313
Processes, 417
Prognosis scan, 280
PuTTY, 26, 40, 53, 66, 456

Q

QoD, 320, 328, 329, 460
QoD types, 460
Quality of Detection, 320, 328, 329, 460

R

RADIUS, 243
Read access, 236
Reading reports, 320
Reboot, 191
Rebooting, 191
Registry Content, 360
ReHash, 365
Remediation Ticket, 462
Remote character set, 456
Remote scanner, 408, 415
Removing user data, 456
Report, 116, 314, 320, 462
Report alert, 325
Report content composer, 324
Report format, 116, 315, 422, 462
Report format plug-in, 315
Report formats, 130, 454
Report plug-in, 315
Resolving vulnerabilities, 331
Restoring a backup, 180
Restoring a backup from USB stick, 181
Result, 321, 328, 462
Result forwarding, 422
RFP, 315
Role, 225, 462
Router advertisement, 136
Routes, 138, 142



S

S/MIME certificate, 255
 Saving changes, 122
 Scan, 244, 248, 462
 Scan administrator, 125
 Scan configuration, 290, 420, 463
 Scan configurations, 130, 454
 Scan duration, 419, 452
 Scan performance, 419
 Scan problems, 313
 Scan queueing, 422
 Scan report content composer, 324
 Scan target, 248, 464
 Scan user account, 413
 Scanner, 303, 463
 Scanner preferences, 295
 Scanning, 244
 Scanning order, 421
 Scanning with sensors, 415
 SCAP, 383, 386
 Schedule, 301, 463
 Scheduled scan, 301, 463
 SCP, 305
 Scripts for gvm-tools, 407
 SecInfo, 218, 383
 SecInfo portal, 383
 Secure networks, 414
 Secure shell, 122
 Security Content Automation Protocol, 386
 Security gateway considerations, 450
 Selecting port lists, 420
 Selecting scan configuration, 420
 Selecting scanning order, 421
 Self-check, 178
 Sending reports, 325
 Sensor, 20, 22, 199, 408, 450, 451
 Sensor as remote scanner, 415
 Sensor type, 118
 Serial console, 121
 Serial port, 26, 40, 53, 66
 Services, 145
 Setting up the GSM, 25
 Settings, 218
 Setup, 123
 Setup checklist, 25
 Setup guide, 25
 Setup guide for GSM 150, 53
 Setup guide for GSM 25V, 90
 Setup guide for GSM 35, 66
 Setup guide for GSM 400/450/600/650, 40
 Setup guide for GSM 5400/6500, 26
 Setup guide for GSM
 CENO/DECA/TERA/PETA/EXA, 78
 Setup guide for GSM ONE, 101
 Setup requirements, 78, 90, 101
 Severity, 321, 322, 328, 329, 463
 Severity change, 338
 Severity class, 118, 463
 Sharing resources, 236
 Shell, 122, 197
 Shutdown, 192
 Shutting down, 191
 Simple CPE-based check, 367
 Simple scan, 248
 Simultaneous login, 225
 Simultaneous scanning via multiple IP address, 118
 Slow scan, 419, 452
 Smart host, 171
 SMB, 305
 SME Class, 19
 SMTP, 172
 SMTP authentication, 172
 SNMP, 145, 156, 255, 305, 422
 SNMP trap alert, 422
 Solution type, 321, 328, 463
 Sourcefire, 431
 Sourcefire connector, 305
 Sourcefire connector alert, 433
 Sourcefire Intrusion Prevention System, 431
 Splunk, 436
 Splunk alert, 438
 SSH, 122, 145, 153
 SSH fingerprints, 156
 SSH key, 255
 Standard policies, 372
 Starting scans with gvm-cli, 402
 Starting scans with gvm-pyshell, 404
 Starting task, 253
 Starting the appliance, 26, 28, 40, 41, 53, 54, 66, 67
 Static IP address, 135
 Status bar, 287
 Status Code, 407
 Status of a ticket, 332
 Status of GMP, 457
 Subscription key, 120, 162, 165, 198, 199
 Super administrator, 127, 225, 229
 Super permission, 231, 234
 Superuser, 193
 Support, 193
 Support package, 195
 Swap usage, 417
 Synchronization port, 163
 Synchronization proxy, 164
 Synchronization time, 177
 Syslog, 173, 422
 Syslog alert, 422
 System administrator, 121, 122, 124
 System level access, 121



System load, 417

System operations, 199

System status, 199

T

Tag, 214, 464

Target, 248, 284, 464

Task, 251, 287, 464

Task wizard, 245, 246

TCP port, 419

Temporary HTTP server, 158

Ticket, 331, 462

Ticket alert, 333

Ticket status, 332

Time synchronization, 169

Timeout, 220

Timezone, 218

TLS, 376

TLS certificate, 382, 464

TLS-Map scan, 376

TR-02102, 374

TR-02102-4, 374

TR-03116, 373

TR-03116-4, 373

Transmission Control Protocol port, 419

Transport Layer Security, 376

Trashcan, 216

Trend, 330

Triggering alerts for reports, 325

U

UDP port, 419

Updating feed after factory reset, 456

Updating sensors, 189

Updating the feed, 189

Updating the feed on sensors, 189

Upgrading from GOS 20.08 to GOS 21.04, 112

Upgrading GOS, 112, 114, 188, 190

Upgrading GOS after factory reset, 456

Upgrading GOS on sensors, 188

Upgrading sensors, 188

Upgrading the flash partition, 114, 190

Upgrading the GSM, 112

User, 125, 221, 225

User Datagram Protocol port, 419

User level access, 120

User management, 124, 221

User manual, 220

User name, 121, 255

User password, 128

User settings, 218

Utilizing the serial port, 26, 40, 53, 66

V

Vendor fix, 321, 328, 463

Verinice, 316, 422, 424

Verinice ISM, 424

Verinice ITSM system, 422

Verinice.PRO, 305

Verinice.PRO connector, 305

vFire, 305, 434

vFire alert, 434

vhost, 314

Virtual Midrange Class, 22

Virtual Private Network, 143

Virtual sensor, 22

VirtualBox, 101

VLAN, 137

VMware ESXi, 22, 23, 78, 90

VNC dialog, 454

VPN, 143

VT, 290, 383, 384, 460

VT families, 290

VT preferences, 297

Vulnerability, 321, 329, 330

Vulnerability Report HTML, 316

Vulnerability Report PDF, 316

Vulnerability Test, 383, 384, 460

W

Web administrator, 125, 126

Web interface, 26, 40, 53, 78, 101, 120, 199, 220

Web interface access, 220

Web interface timeout, 146

Web user, 125, 221

Will not fix, 321, 328, 463

Wizard, 245–247

Workaround, 321, 328, 463