

# cognitix Threat Defender

Manual

Release 20221013.1.0

November 22, 2022

© Copyright 2022 genua GmbH. All rights reserved.

genua GmbH  
Domagkstraße 7  
85551 Kirchheim, Germany  
Phone: +49 89-991950-0  
Fax: +49 89-991950-999

All trademarks and licenses indicated in the user manual are the property of their respective owners and are mentioned for information purposes only.

For the registered trademarks of genua GmbH see: <https://kunde.genua.de/en/imprint/trademark.html>

Please note that in accordance with current legal requirements, all owners of waste electrical and electronic equipment (WEEE) may not dispose of WEEE together with unsorted municipal waste. In addition, the following icon of a crossed out trash bin depicted on WEEE devices denotes the requirement to collect and dispose of all WEEE arising separately:



Fig. 1: Do not dispose of with municipal waste.

You as the end user bear the sole responsibility for deletion of all personal information from WEEE devices before their disposal. For disposal of WEEE devices, please contact genua as the manufacturer at +49 89-991950-0 with the reference “waste electrical and electronic devices”.

Kind regards

genua GmbH

# Table of Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	About this Manual . . . . .	2
1.1.1	Intended Audience . . . . .	2
1.1.2	Conventions . . . . .	2
1.1.3	Related Resources . . . . .	3
1.2	What's new in this version? . . . . .	4
1.2.1	Upgrade Compatibility . . . . .	4
1.2.2	New Features and Improvements . . . . .	4
1.2.3	Important Fixed Issues . . . . .	5
1.2.4	Known Issues . . . . .	5
1.2.5	Upgrade Instructions and Requirements . . . . .	5
<b>2</b>	<b>Installation and Setup</b>	<b>7</b>
2.1	System Environment . . . . .	8
2.1.1	System Requirements . . . . .	8
2.1.2	genua Hardware Systems . . . . .	10
2.1.3	Hardware Troubleshooting . . . . .	11
2.1.4	Virtual Environments . . . . .	14
2.2	Install cognitix Threat Defender . . . . .	24
2.2.1	Installation Preparation . . . . .	24
2.2.2	Installation via USB Installer Drive . . . . .	25
2.3	Sign In . . . . .	34
2.4	Change the Administrator Password . . . . .	35
2.5	Complete the Setup . . . . .	36
2.5.1	Introduction to the User Interface . . . . .	36
2.5.2	Add a License . . . . .	39
2.5.3	Change the Hostname and Time Settings . . . . .	40
2.5.4	Create New System Users . . . . .	41
2.5.5	Change the Management Interface . . . . .	42

2.5.6	Configure Proxy Settings . . . . .	43
2.5.7	Update cognitix Threat Defender . . . . .	43
2.5.8	Define Update Schedules . . . . .	44
2.5.9	Set up the User API for User Mapping . . . . .	45
2.5.10	Manage the Processing Interfaces . . . . .	46
2.5.11	Back up the Configuration . . . . .	50
<b>3</b>	<b>Monitor the Network</b>	<b>53</b>
3.1	Passive Monitoring . . . . .	54
3.1.1	Analyze Protocols and Destination Countries . . . . .	54
3.1.2	Find YouTube Users in the Last Hour . . . . .	56
3.1.3	Port Monitoring . . . . .	57
3.2	Monitor Network Assets . . . . .	60
3.2.1	Assets in cognitix Threat Defender . . . . .	60
3.2.2	Create a Network Inventory . . . . .	61
3.2.3	Handle Newly Discovered Assets . . . . .	62
3.3	Export Reporting Data to Elastic/ELK . . . . .	64
3.3.1	Export IPFIX Reporting Data to Filebeat . . . . .	64
3.3.2	Export JSONL Reporting Data to Logstash via an Encrypted Channel	68
<b>4</b>	<b>Secure the Network</b>	<b>71</b>
4.1	Active Network Integration . . . . .	72
4.1.1	Example 1: cognitix Threat Defender in Breakout Mode . . . . .	72
4.1.2	Example 2: cognitix Threat Defender in a DMZ . . . . .	73
4.2	Correlation in Threat Defender . . . . .	74
4.2.1	The Approach of Threat Defender . . . . .	74
4.2.2	Example Workflow . . . . .	75
4.3	Event Tracking Tables . . . . .	78
4.4	Define the Policy . . . . .	80
4.5	Policy Setup Examples . . . . .	83
4.5.1	Create Global Rules . . . . .	83
4.5.2	View the Content of Event Tracking Tables . . . . .	84
4.5.3	Restrict Access to Certain Websites . . . . .	85
4.6	Detect Threats . . . . .	94
4.6.1	Deploy cognitix Threat Defender as an IDS at the Network Perimeter	94
4.6.2	Detect ARP Spoofing Attacks . . . . .	96
4.6.3	Detect MITRE ATT&CK Techniques . . . . .	102

4.6.4	Time-based Baselining . . . . .	113
4.6.5	Adaptive Behavior-based Graylisting . . . . .	117
<b>5</b>	<b>Segment the Network</b>	<b>121</b>
5.1	Network Segmentation . . . . .	122
5.1.1	Example Workflow . . . . .	122
5.1.2	Static Network Objects . . . . .	125
5.1.3	Dynamic Network Objects . . . . .	125
5.2	Create Static Network Objects . . . . .	127
5.3	Create Dynamic Network Objects . . . . .	129
5.4	Use Network Segmentation . . . . .	131
5.4.1	Dynamic Network Segmentation for BYOD Clients . . . . .	131
5.4.2	Allow Internet Traffic via Internal Proxy Server Only . . . . .	133
5.4.3	Create a DMZ with Two Threat Defenders . . . . .	135
<b>6</b>	<b>Interface Reference</b>	<b>141</b>
6.1	Analytics . . . . .	142
6.1.1	Overview of the Analytics Dashboards . . . . .	142
6.1.2	Network . . . . .	143
6.1.3	Assets . . . . .	144
6.1.4	Policy . . . . .	144
6.2	Policy . . . . .	145
6.2.1	Rules . . . . .	145
6.2.2	Advanced Correlation . . . . .	153
6.2.3	Network Objects . . . . .	154
6.2.4	Schedules . . . . .	159
6.2.5	Event Tracking Tables . . . . .	160
6.3	Inventory . . . . .	163
6.3.1	Assets . . . . .	163
6.3.2	Asset Setting . . . . .	169
6.3.3	Users . . . . .	169
6.3.4	User API Setting . . . . .	174
6.3.5	Backup/Restore . . . . .	175
6.3.6	Data Export . . . . .	177
6.4	Threats . . . . .	178
6.4.1	Overview . . . . .	178
6.4.2	Incident Logs . . . . .	179

6.4.3	Intelligence Database . . . . .	180
6.5	Network . . . . .	186
6.5.1	Overview . . . . .	186
6.5.2	Manage Processing Interfaces . . . . .	187
6.6	Logging . . . . .	189
6.6.1	Audit Logs . . . . .	189
6.6.2	Audit Log Channels . . . . .	190
6.6.3	Report Channels . . . . .	194
6.6.4	Local Logs . . . . .	195
6.7	Settings . . . . .	197
6.7.1	General . . . . .	197
6.7.2	Monitoring . . . . .	200
6.7.3	System Users . . . . .	202
6.7.4	Updates . . . . .	203
6.7.5	Update Schedules . . . . .	204
6.7.6	License . . . . .	206
6.7.7	Configurations . . . . .	206
6.7.8	genucenter . . . . .	207
6.7.9	System Actions . . . . .	210
6.8	Diagnostics . . . . .	211
6.8.1	Overview . . . . .	211
6.8.2	System Health . . . . .	211
6.8.3	Troubleshooting . . . . .	211
6.8.4	Flow Table Reporting . . . . .	212
6.8.5	MAC Table Reporting . . . . .	213
<b>7</b>	<b>Appendix</b> . . . . .	<b>215</b>
7.1	Access Rights by User Roles . . . . .	216
7.2	JSON Lines Formatted Output . . . . .	223
7.3	IPFIX Specification . . . . .	226
7.3.1	IPFIX Setup . . . . .	226
7.3.2	IPFIX Records . . . . .	226
7.3.3	cognitix IPFIX Enterprise Elements . . . . .	226
7.3.4	cognitix Threat Defender IPFIX Events . . . . .	230
7.3.5	Common Event Fields . . . . .	230
7.3.6	Message Types . . . . .	231
7.4	syslog Specification . . . . .	233

7.4.1	syslog Setup . . . . .	233
7.4.2	syslog Messages in General . . . . .	233
7.4.3	Message Types . . . . .	233
7.4.4	syslog Fields . . . . .	234
7.4.5	cognitix Threat Defender syslog Message Types . . . . .	239
7.5	Flow Table Reports . . . . .	241
7.6	IPS Rule Definitions . . . . .	243
7.6.1	Rule Syntax . . . . .	243
7.6.2	Metadata Keywords . . . . .	246
7.6.3	Payload Keywords . . . . .	248
7.6.4	Flow Keywords . . . . .	257
7.6.5	DNS Keywords . . . . .	259
7.6.6	HTTP Keywords . . . . .	259
7.6.7	SSL/TLS Keywords . . . . .	267
7.6.8	JA3 Keywords . . . . .	269
7.6.9	SSH Keywords . . . . .	270
7.6.10	Thresholding Keywords . . . . .	271
7.7	FAQ . . . . .	274
7.7.1	Can I enable multiple conditions in a rule and how are they handled?	274
7.7.2	In what order does Threat Defender process rules? . . . . .	274
7.7.3	How does Threat Defender perform in active mode compared to passive mode? . . . . .	274
7.7.4	What can I do if Threat Defender doesn't boot? . . . . .	275
7.7.5	Why does the Threat Defender installer crash with minicom 2.8? . .	276

<b>8</b>	<b>Glossary</b>	<b>277</b>
----------	-----------------	------------

	<b>Index</b>	<b>287</b>
--	--------------	------------






| Chapter 1

# Introduction

## 1.1 About this Manual

This manual describes cognitix Threat Defender (or Threat Defender for short) build 20221013.1.0. For an overview of the most significant changes in this build, see [What's new in this version?](#) (page 4)

This manual is available in HTML and PDF format. To access the HTML version of this manual, click  Documentation in the Threat Defender user interface or go to <https://documentation.cognitix.de/>. In the HTML version, you can switch between the English and German manual by clicking the respective link at the top of each HTML page.

### 1.1.1 Intended Audience

This manual is for network administrators and technicians who are responsible for installing and configuring cognitix Threat Defender as well as defining the network policy.

To be able to use this manual effectively, a solid background knowledge and experience regarding networking concepts is required.

### 1.1.2 Conventions

The following typographic conventions and notations are used to represent information in this manual.

Elements of the graphical user interface are indicated as follows:

- Buttons, checkboxes, list names and other GUI items appear in **bold font**.
- List options and literal text appear in a `fixed-width font`.
- A sequence of menu commands is indicated as follows: **Policy > Network Objects > Static Network Objects**. In this case, go to the **Policy** menu, select **Network Objects** and open the **Static Network Objects** submenu.

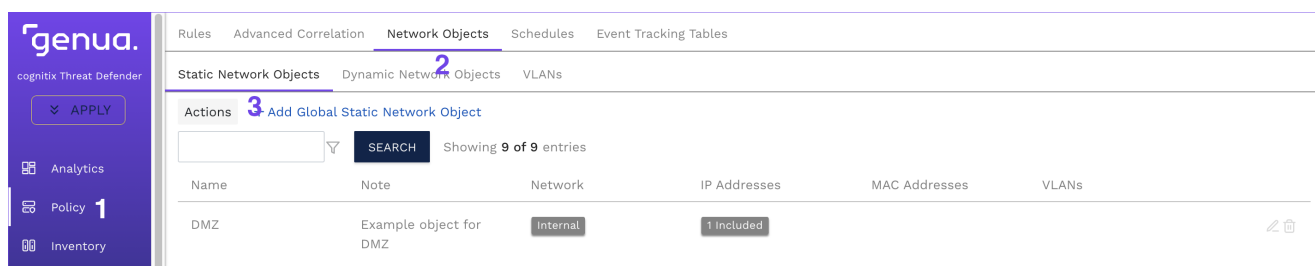


Fig. 1: Policy > Network Objects > Static Network Objects

Links appear as [violet text](#).

Glossary terms appear as **green** text. Click the term to jump to the respective section in the glossary.

The following types of notes are used to indicate additional information or call attention to a particular point:

**Tip:** This note contains useful tips that make your work easier.

**Note:** This note contains important information.



**Warning:** This note contains information that is very important to consider. If it is not observed, network security may be at risk.

### 1.1.3 Related Resources

Refer to the following resources for further information on Threat Defender:

- Release Notes provide information on each release. See [Previous Releases](#) in the HTML version for the release notes as of version 20200805.0.0.
- On the [customer website](#)<sup>1</sup> you will find information about new product releases, check-sums to verify the software integrity and so on. You can also submit feedback and open support requests.
- The [genua website](#)<sup>2</sup> contains valuable information about our products and solutions, as well as the latest company news.

---

<sup>1</sup> <https://kunde.genua.de/en.html>

<sup>2</sup> <https://www.genua.de>

## 1.2 What's new in this version?

cognitix Threat Defender build 20221013.1.0 rolls out a number of new features and improvements. Find out what's new below.

### 1.2.1 Upgrade Compatibility

The following previous builds are compatible with cognitix Threat Defender build 20221013.1.0:

- 20220711.0.0
- 20220729.0.0

To view the release notes of previous builds, see **Previous Releases** in the [HTML version of the manual](#)<sup>3</sup>.

cognitix Threat Defender build 20221013.1.0 is compatible with **genucenter 7.5** and **genucenter 8.0**.

### 1.2.2 New Features and Improvements

#### IDS/IPS Improvements

The traffic evaluation by the IDS/IPS engine is now more in-depth and therefore more thorough.

#### User Interface Improvements

- We implemented a first dark mode version for the cognitix Threat Defender UI. To switch to dark mode and back, click the toggle at the bottom of the main navigation.
- cognitix Threat Defender now shows a progress bar when the system is shut down or rebooted.
- We improved usability on small screens.
- We improved the style of chart lists in detailed views.
- The **Apply** button at the top of the main navigation has a new style so that it is now more noticeable when pending changes need to be applied.
- We improved the error message on the login screen.

#### Documentation Improvements

The PDF version of the manual now has an index to facilitate searching for content.

---

<sup>3</sup> <https://documentation.cognitix.de>

### 1.2.3 Important Fixed Issues

- We improved the handling of whitelisting and classification conditions in rules so that it is now more robust.
- In rare cases, a client/server mismatch could occur when assets were inserted into dynamic network objects. We fixed this potential problem with this release.
- We fixed the donut charts for different resolutions.

#### Patch 1

- We fixed a bug which led to missing matches of the policy engine when asset tags were used as source or destination conditions in rules.

### 1.2.4 Known Issues

- When the API is under high load, cognitix Threat Defender may display a misleading “Connection Issue” notification. It is also possible that some data is not completely displayed.
- The system may show a wrong genucenter connection state under **Settings > genucenter**. This may occur when you restore the genucenter configuration from a backup file without providing the required SSH key files or when you abort the configuration assistant and the configuration is incomplete. In this case, you need to set up the genucenter connection again.
- When IPS rules under **Threats > Intelligence Database > IPS Rules** are enabled or disabled, it may take a few seconds for the table to update.

### 1.2.5 Upgrade Instructions and Requirements

For information on the hardware requirements needed to install this build version, see the [system requirements](#) (page 8).

For instructions on how to install the new build version, see [Updating cognitix Threat Defender](#) (page 43).



| Chapter 2

# Installation and Setup

## 2.1 System Environment

genua provides dedicated hardware systems for cognitix Threat Defender. You can find their specifications under [genua Hardware Systems](#) (page 10).

cognitix Threat Defender is also available as a software-only solution that you can install on your own hardware. See [System Requirements](#) (page 8) for the requirements that your system has to meet.

While we do not officially support virtualization for cognitix Threat Defender, it is possible to install and run Threat Defender in a virtual environment for evaluation purposes. See [Virtual Environments](#) (page 14) for setup examples using virtualization.

### 2.1.1 System Requirements

To be able to use cognitix Threat Defender on your own hardware, your system has to meet the following hardware requirements.

#### 2.1.1.1 CPU

- Intel CPU with SSE 4.2
- Minimum of 4 threads, for example
  - 2 CPU cores with [hyper-threading](#)
  - 1 CPU with 4 cores
- Maximum of 512 threads
- Maximum of 8 [NUMA](#) nodes (CPU sockets)

#### 2.1.1.2 RAM

- Minimum of 8GB
- Recommended 16GB or more
- Recommended 2GB per CPU core
- Minimum of 8GB per NUMA node
- Equal amount of memory on all NUMA nodes

**Note:** Threat Defender uses [DPDK](#) to accelerate processing. DPDK can address a maximum of 512GB RAM. There may be problems if you use considerably larger amounts of RAM.



### 2.1.1.3 Network Interface Cards

- Minimum of 3 network interfaces in total
- Minimum of 2 network interfaces with Intel chipset. If you wish to use chipsets from other vendors, contact [support@genua.de](mailto:support@genua.de).

cognitix Threat Defender supports the following Intel chipsets:

- Intel 1G: 82575, 82576, 82580, I210, I211, I350, I354
  - Intel 2.5G: I225-LM, I225-V, I225-I, I225-K (Foxville)
  - Intel 10G: 82598, 82599, X540, X550, X552/X557 (Niantic)
  - Intel 10G/40G: X710 (Fortville)
- Maximum of 32 Ethernet ports
  - To achieve optimum performance on an Intel platform, use an Intel Xeon class server system such as Ivy Bridge, Haswell or newer.
  - Make sure each NIC has the latest version of NVM firmware.
  - Use PCIe Gen3 slots, such as Gen3 x8 or Gen3 x16, because PCIe Gen2 slots do not provide enough bandwidth for 2 x 10GbE and above.

### 2.1.1.4 Disk

- SSD recommended
- Minimum of 60GB
- Recommended 240GB

### 2.1.1.5 Installation

- Via bootable USB device
- The system has to support UEFI



**Warning:** To be able to get firmware and license updates, the management interface of Threat Defender has to be able to reach our servers via the Internet. If you do not want to connect Threat Defender to the Internet, you need to update it manually (see [Updates](#) (page 203)).

---

#### Additional References:

For information on the hardware provided by genua, see [genua Hardware Systems](#) (page 10).

## 2.1.2 genua Hardware Systems

genua provides dedicated hardware systems for cognitix Threat Defender.

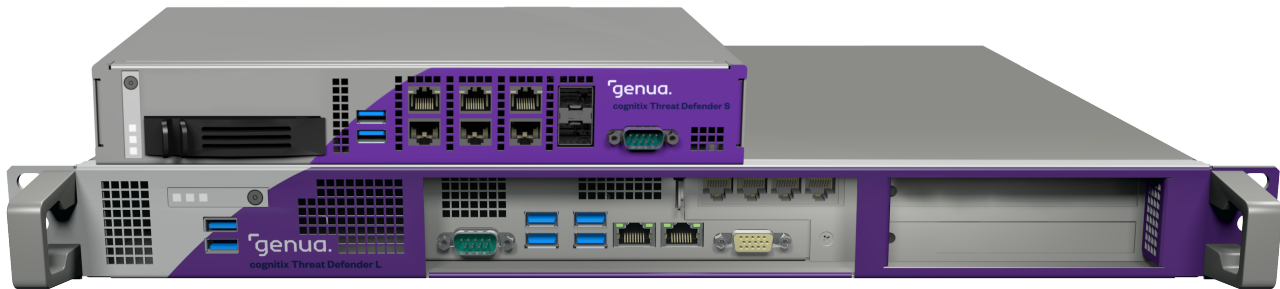


Fig. 1: cognitix Threat Defender S and M/L appliances

These systems have the following technical specifications:

System	Main-board	CPU	RAM	NICs (default)
Threat De-fender S	Super-micro A2SDi-TP8F	Intel Atom C3858 12C/12T - 2.0Ghz	4x 8GB DDR4 2400MHz ECC	4x 1GbE RJ45 (i350-AM4), 2x 10GbE RJ45 (X557-AT2), 2x 10GbE SFP+ (CS4227)
Threat De-fender M	Super-micro H12SSW-iN	AMD EPYC 7272 12C/24T - 2.9-3.2GHz	8x 16GB DDR4 3200MHz ECC	2x 1GbE RJ45 (BCM5720L), 4x 1GbE RJ45 (i350-T4)
Threat De-fender L	Super-micro H12SSW-iN	AMD EPYC 7402 24C/48T - 2.8-3.35GHz	8x 32GB DDR4 3200MHz ECC	2x 1GbE RJ45 (BCM5720L), 4x 1GbE RJ45 (i350-T4)

For additional information, see the [hardware datasheets](#)<sup>4</sup>.

### Additional References:

For information on the general hardware requirements, see [System Requirements](#) (page 8).

<sup>4</sup> <https://www.genua.de/fileadmin/Loesungen/Downloads/cognitix-threat-defender-hardware.pdf>

## 2.1.3 Hardware Troubleshooting

The following chapters assist you with issues related to the hardware.

### 2.1.3.1 Workaround: Detect Hardware Interfaces

On cognitix Threat Defender M and L systems it is possible that the system does not detect all network interfaces during a soft (re-)boot. If this problem occurs, proceed as follows:

1. Enter the BIOS (e.g. by pressing the DEL key) and adjust the following settings:

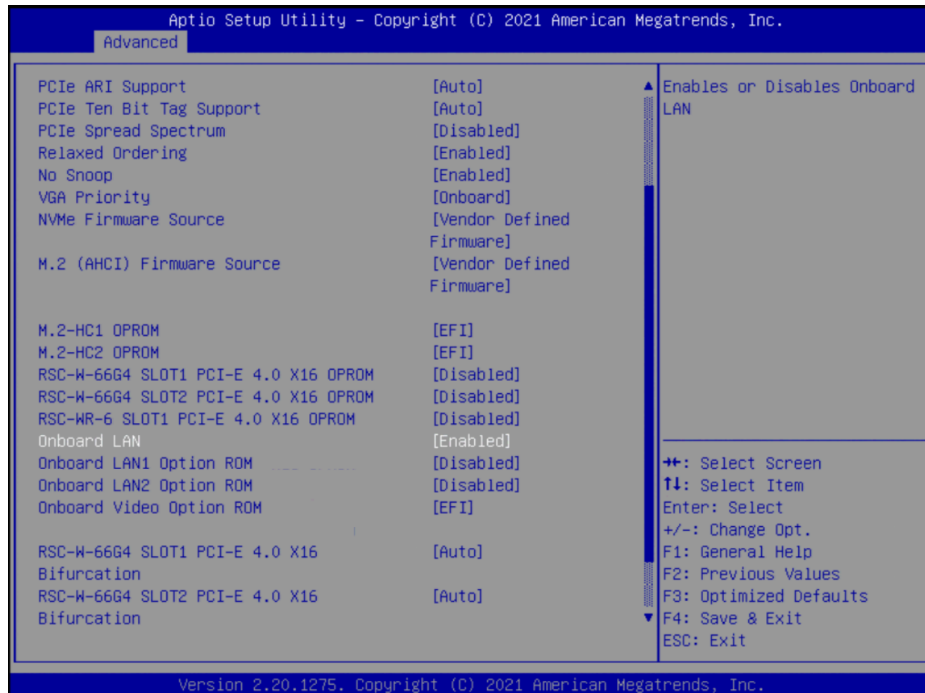
In the **Boot** menu:

- Set **Boot Mode Select** to UEFI.
- Set **LEGACY to EFI Support** to Disabled.



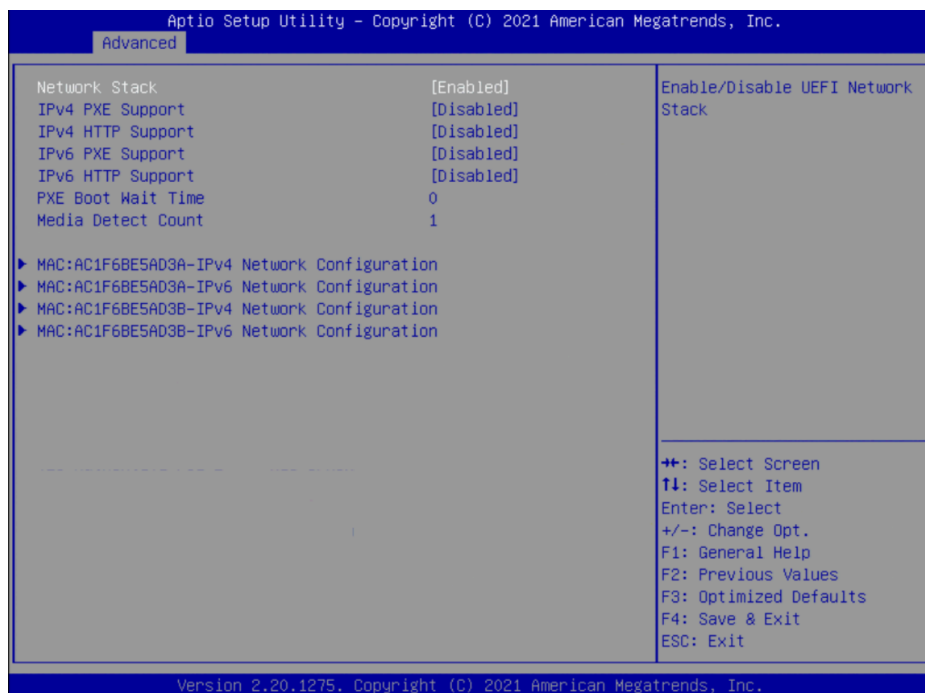
Under **Advanced > PCIe/PCI/PnP Configuration**:

- Set **Relaxed Ordering** to Enabled.
- Disable all **Option ROM (OPROM)** related to PCIe and LAN. The remaining OPROM options should be set to EFI.



Under Advanced > Network Configuration:

- Disable PXE Boot.



2. Disconnect cognitix Threat Defender from power for about 10 seconds. Re-connect it, then restart the system.

If the issue persists, please contact our support team at [support@genua.de](mailto:support@genua.de).

**Note:** This solution is only a workaround. To permanently solve the issue, an EFI update of the NICs is required, see [Update the NIC Firmware via EFI](#) (page 13).

### 2.1.3.2 Update the NIC Firmware via EFI

To permanently solve the issue of disappearing hardware interfaces, you need to update the firmware of the network interface cards.

**Warning:** If the firmware update is unsuccessful or faulty, it may destroy the NIC:



- The firmware update may fail if the update file is corrupted.
- Do not reboot or shut down the system while the update is in progress.
- Do not interrupt the update in any way.

This procedure may become necessary for the following Intel NIC types:

- 700 Series
- E810
- I210
- X550

Create an USB drive with the needed driver:

1. Download the [Intel driver package](#)<sup>5</sup>.
2. In the package, find the `NVMUpdatePackage` folder. It contains the NIC drivers.
3. Find the folder for the type of NIC you want to update.
4. You need the archive file with the ending `_EFI.zip`. Extract it to a FAT16 USB drive with at least 1GB capacity.
5. Connect the USB device to Threat Defender.

On cognitix Threat Defender proceed as follows:

1. Enable the EFI shell, if required.
2. Reboot Threat Defender into the EFI shell.
3. In the EFI shell, carry out the following steps:
  1. Access the USB device. You can check its name in the displayed mapping table. Usually, the USB device is `FS0`. In this case, enter the string `fs0:.`

<sup>5</sup> <https://www.intel.de/content/www/de/de/download/15084/intel-ethernet-adapter-complete-driver-pack.html>

2. You can check the content of the device by typing `ls`. This will show the folder and files on the USB device.
3. Access the folder.
4. Start the NVMUpdate utility by running the executable, i.e. type `nvmupdate64e.efi`. The update will require several reboots. Make sure to reboot to the EFI shell.
5. Select the network card to be updated from the table.
6. The system prompts you to create a backup of the running firmware. It will be saved to the USB device.

When the update is finished, you can restart cognitix Threat Defender from the EFI shell by typing `reset -c`.

**Note:** You will have to update every network card individually.

If you have any questions, please contact our support team at [support@genua.de](mailto:support@genua.de).

#### 2.1.4 Virtual Environments

We do not officially support virtual environments.

However, if the virtualization software is able to provide the necessary hardware requirements, it is possible to install and run cognitix Threat Defender in a virtual environment for testing purposes. This will slow its processing speed down, however.

cognitix Threat Defender can process up to 40Gbit/s and higher on suitable hardware and with the respective license volume. It achieves this high processing speed because it directly accesses the network hardware. Any layer added between Threat Defender and the network hardware, such as the operating system and drivers for virtual environments, causes additional latencies and slows the processing speed down.

**Note:** cognitix Threat Defender cannot be virtualized using Microsoft Azure or Microsoft Hyper-V due to incompatible drivers.

The following examples serve as illustrations on how to set up Threat Defender in a virtual environment for evaluation purposes. However, due to the wide variety of operating system environments we cannot guarantee that they will work in every case.

### 2.1.4.1 VirtualBox

The following sections illustrate how to install a virtual cognitix Threat Defender using Oracle VirtualBox and to set it up so that it can see all traffic in the host system. This way you can run cognitix Threat Defender on a notebook or desktop computer to evaluate it.

Depending on your operating system, you may have to adapt some of the settings.

#### System Requirements

The host system has to meet the following requirements:

- CPU:
  - CPU with SSE 4.2
  - Minimum of 4 threads, we recommend using 8 threads
- RAM:
  - Minimum of 8GB
  - 16GB recommended

#### Preparations

1. Install VirtualBox. For further information, see its [documentation](#)<sup>6</sup>.
2. Convert the cognitix Threat Defender installation image from `.img` to `.vdi` to make it readable for VirtualBox:
  - Download the installation image and store it in a dedicated folder.
  - Open a console window.
  - Enter the following command:

```
VBoxManage convertfromraw --format vdi cgntx_installer_VERSION.img cgntx_
↪installer_VERSION.vdi
```

Where `cgntx_installer_VERSION.img` and `cgntx_installer_VERSION.vdi` have to be replaced by the actual file names.

This command is identical for all operating systems as it calls the `VBoxManage` program.

---

<sup>6</sup> <https://www.virtualbox.org/manual/UserManual.html#installation>

## Creating a Virtual Machine for cognitix Threat Defender

1. Start VirtualBox.
2. Create a new virtual machine with the following settings:
  - Operating system type: Linux
  - Version: Other Linux (64-bit)
  - Memory size: 8192MB (8GB)
  - Hard disk: Create a virtual hard disk now
  - Hard disk file type: VDI
  - Storage on physical hard disk: dynamically allocated
  - File location and size: minimum 32GB (64GB recommended); if there is enough space, we recommend using 120GB or more
3. Configure the settings of the virtual machine as follows:
  - System:
    - Motherboard > Boot Order: disable floppy and optical
    - Motherboard > Extended Features: Enable EFI (special OSes only)
    - Processors: 4
  - Storage:
    - Under Controller: IDE add a hard disk.
    - Add the converted installation image in .vdi format to the new hard disk.
  - Network:
 

Enable adapters 1 to 3 with the following settings:

VM Settings	Adapter 1	Adapter 2	Adapter 3
Attached to	Host-only adapter	Bridged Adapter	Bridged Adapter
Name	vboxnet0	The (wireless) host network interface <sup>7</sup> .	The (wireless) host network interface <sup>8</sup> .
Adapter type	Paravirtualized network	Paravirtualized network	Paravirtualized network
Promiscuous mode		Allow for all VMs and the host	Allow for all VMs and the host

<sup>7</sup> Choose the network interface used for network connections of the host system.

<sup>8</sup> If there is a second network interface. Otherwise, it is not connected.



## Installing cognitix Threat Defender

1. [Install](#) (page 25) cognitix Threat Defender with the following settings:

- Management Interface: first interface, defined by the network settings of the virtual machine
- IP address: in the 192.168.56.0/24 network, defined by `vboxnet0`
- Gateway: empty
- DNS server: empty

2. Call the IP address assigned to cognitix Threat Defender in the browser.

cognitix Threat Defender can now see all the traffic in the host system.

### 2.1.4.2 QEMU/KVM

The following chapter illustrates how to set up cognitix Threat Defender in a virtual environment using QEMU/KVM.

Depending on your operating system, you may have to adapt some of the settings.

#### Preparations

You need the following tools:

- QEMU KVM
- libvirt
- virt-manager

Optionally, you can set up virtual bridges for every port of Threat Defender you want to implement. To do so, access the connection details of your virtual network in virt-manager.

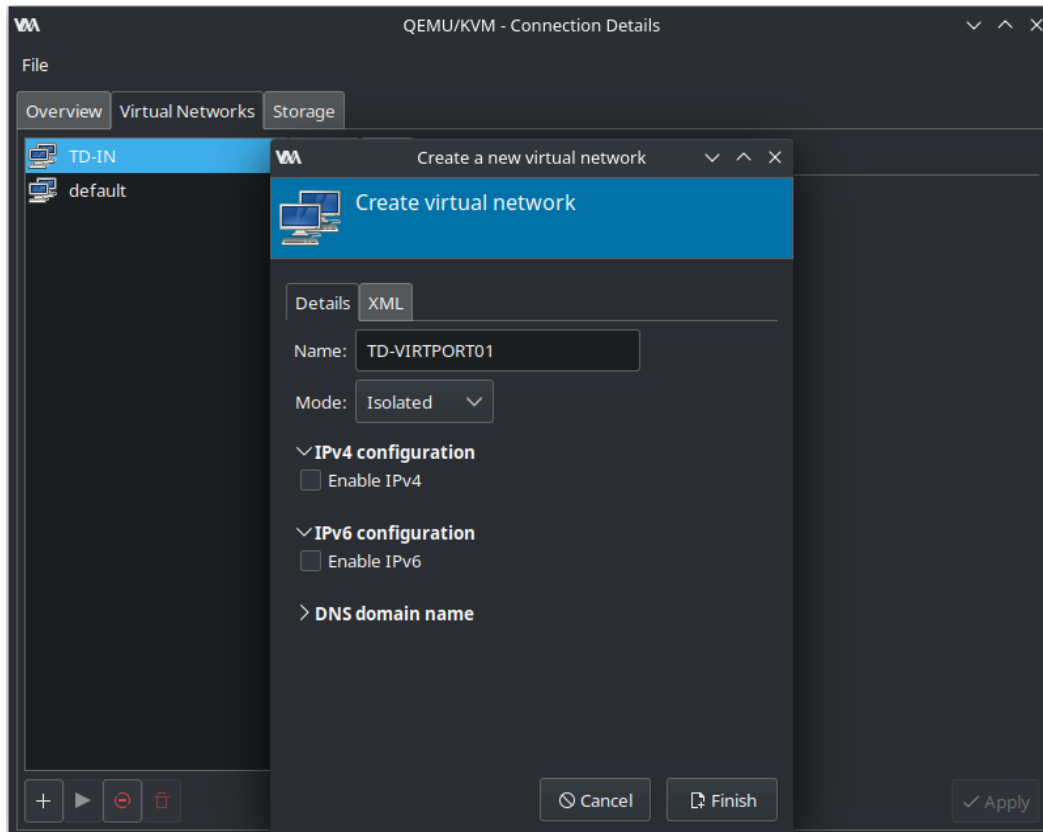


Fig. 2: Optional setup of virtual bridges.

### Creating a Virtual Machine for cognitix Threat Defender

1. Start virt-manager.
2. Create a new virtual machine. A wizard guides you through the setup process.
3. Select **Manual install**.
4. Set the following configuration:
  - Operating system: Red Hat Enterprise Linux 8.5
  - Memory: minimum of 8 GB RAM and 4 CPUs

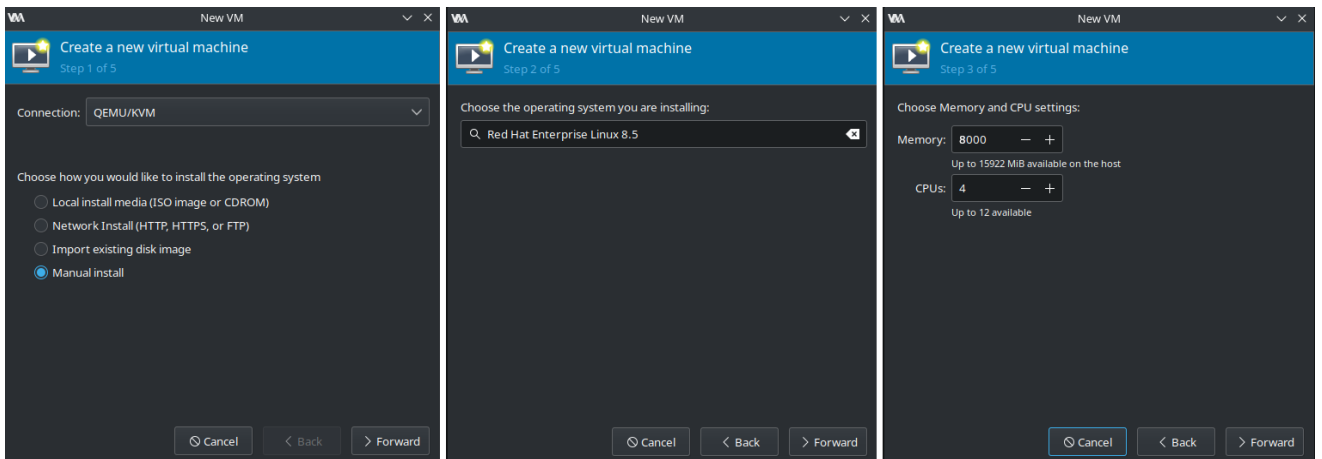


Fig. 3: VM setup steps 1 to 3.

- Disk image: 60 GB HDD
- Network selection: we recommend using the default NAT for the management interface
- Activate `Customize configuration before install`.

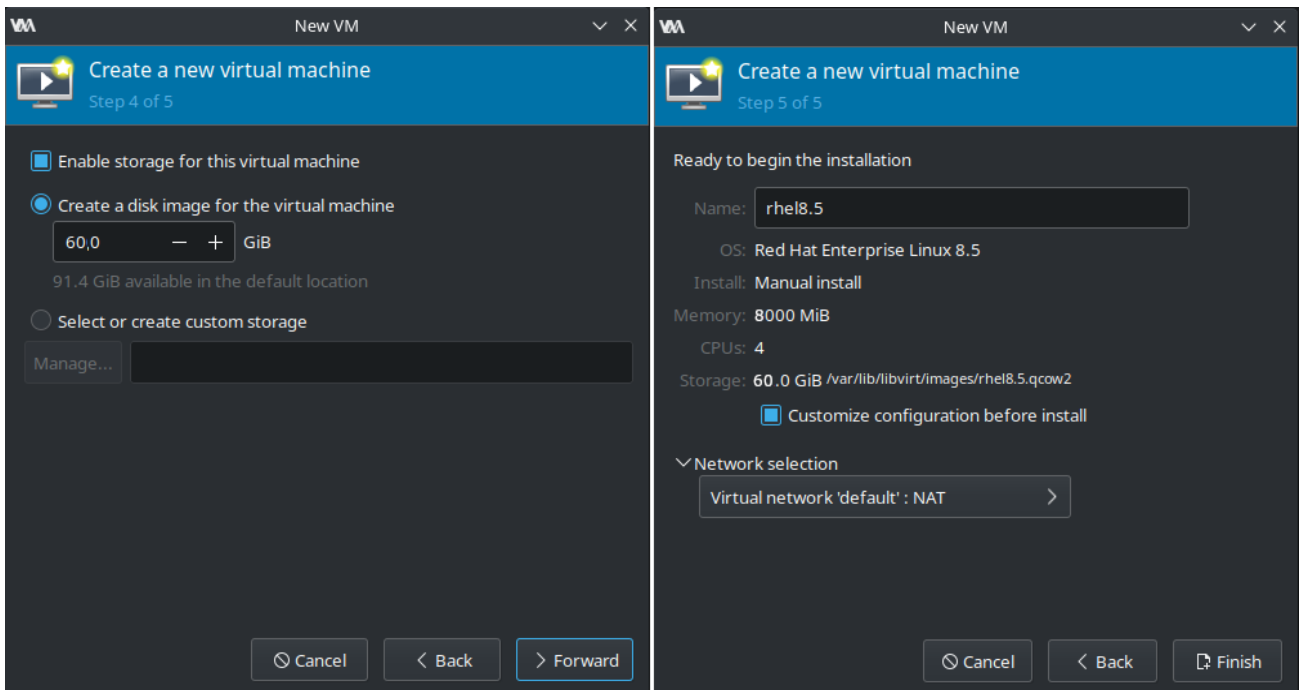


Fig. 4: VM setup steps 4 and 5.

5. When the you have finished the setup wizard for the VM, adjust its detailed settings:

- In the overview, set its firmware to `UEFI x86_64 without secure boot`.

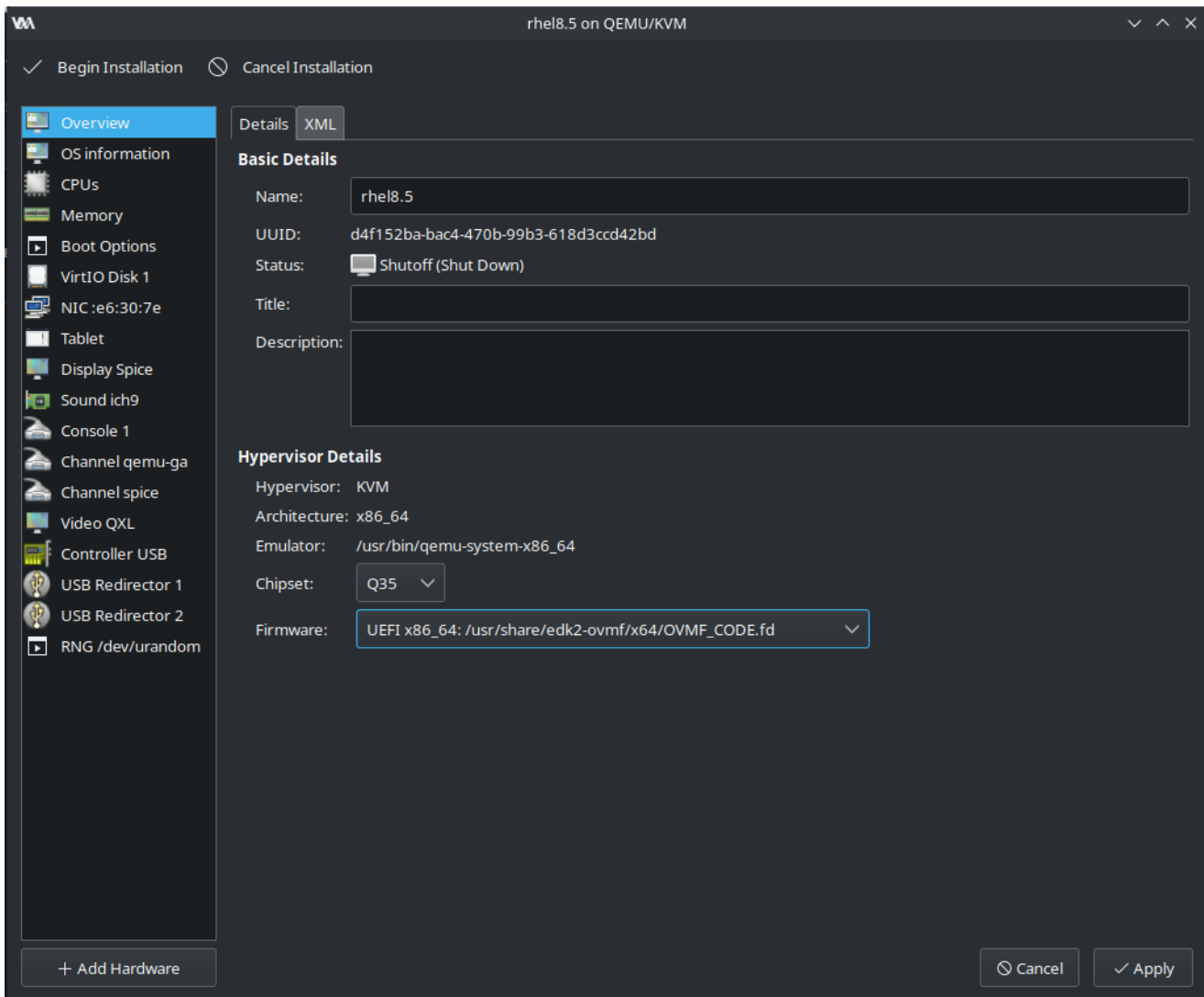


Fig. 5: Set up the firmware of the VM.

- Add new hardware to the VM.
- In the storage settings of the new hardware, select the installation image as custom storage.
- Set it up as USB disk device.

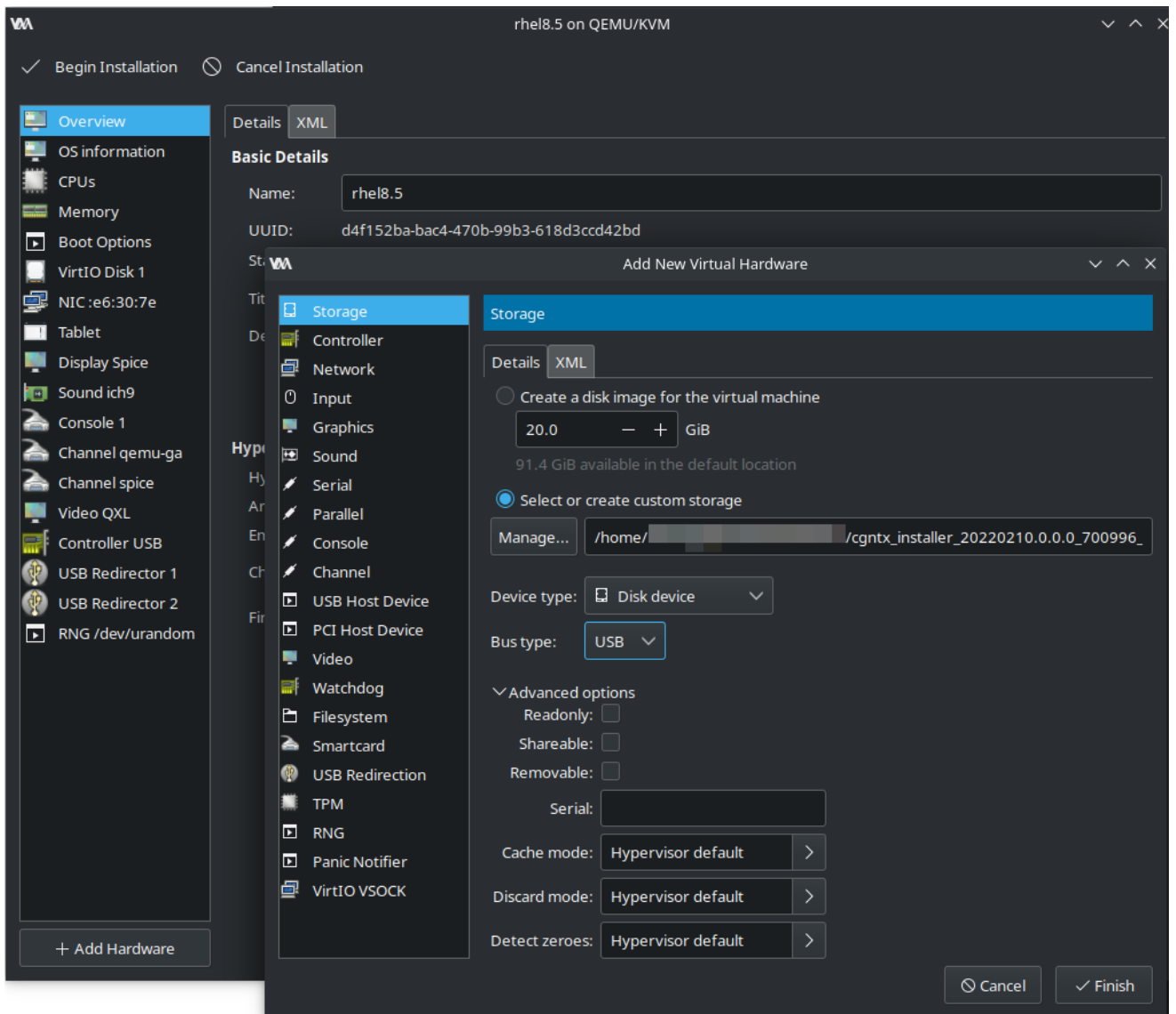


Fig. 6: Set up the installation image as a USB disk device.

- In the boot options, set the new USB disk as the first boot device.

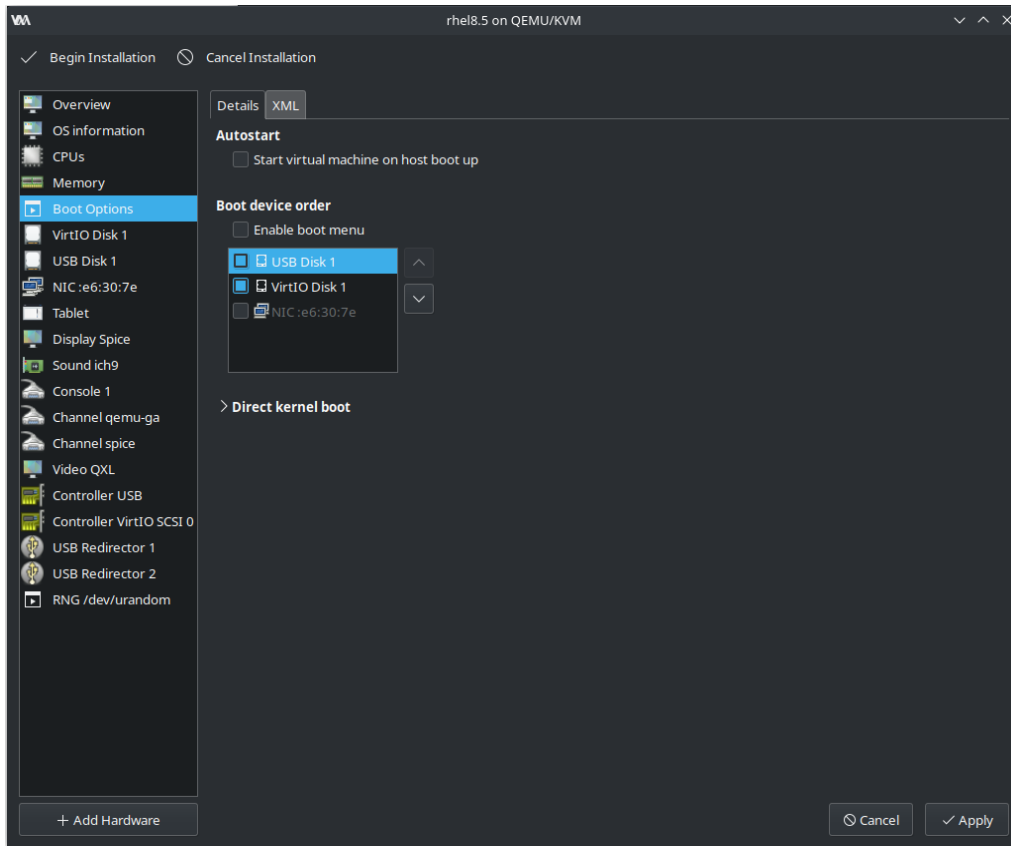


Fig. 7: Set up the boot order.

- Add new hardware to the VM for each Threat Defender port you want to implement plus at least one additional network interface.
- In the network settings of the new hardware, adjust the following:
  - Use the virtual bridges (see [Preparations](#) (page 17).)
  - Use macvtap as network source.

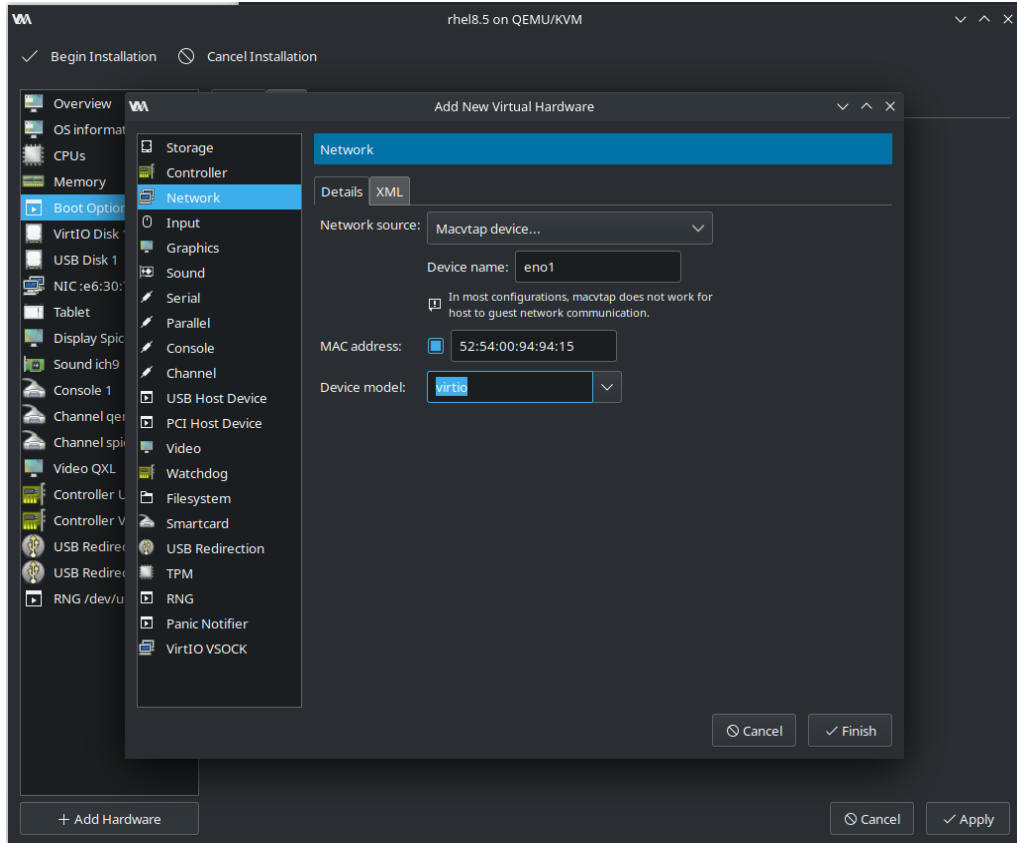


Fig. 8: Port setup.

6. Install the VM.

## Installing cognitix Threat Defender

1. [Install](#) (page 25) cognitix Threat Defender.
2. If you set **default NAT** for the management interface as recommended, use the following settings:
  - IP address: 192.168.122.10/24
  - Gateway: 192.168.122.1
3. Open the IP address of the management interface in the browser to access the Threat Defender user interface.

**Note:** If cognitix Threat Defender does not boot correctly, check that the CPU is using the host configuration. Also make sure that CPU sockets is set to 1 and that the cores/threads match your CPU.

## 2.2 Install cognitix Threat Defender

To install cognitix Threat Defender, you need an installable image of the software.

If you purchase Threat Defender with a genua hardware appliance, you also receive a ready-to-use USB installer drive. Otherwise, you may receive the installer image via e-mail or you can download it from the [genua customer website](#)<sup>9</sup>.

### 2.2.1 Installation Preparation

To install cognitix Threat Defender, you need an installable image of the software. You will either receive a USB installer drive with the software image or you may receive the only the image file. In that case you need to write it to a USB drive first.

#### 2.2.1.1 Verify the Software Integrity

To make sure that the cognitix Threat Defender software image is intact and was issued by genua, you can verify the installation image and update files using checksums.

On the cognitix Threat Defender page of the [genua customer website](#)<sup>10</sup> access the **Checksums** section. The SHA-256 checksums are listed by release version.

To verify the integrity of your software, generate a local checksum using a suitable tool. Under Linux, for example, you can use the following command:

```
sha256sum /path/to/file
```

Compare the local checksum to the checksum on the [genua customer website](#). If it is identical, the downloaded file is intact and authentic.

#### 2.2.1.2 Create a USB Installer Drive

**Tip:** If you purchased Threat Defender with a genua hardware appliance, you also received a USB installer drive and can skip the following steps.

If you downloaded the installation image or received it via e-mail, you need to write it to a USB flash drive (4GB or larger).



**Warning:** Any data stored on the USB flash drive will be deleted.

<sup>9</sup> <https://kunde.genua.de/en/overview/cognitix-threat-defender.html>

<sup>10</sup> <https://kunde.genua.de/en/overview/cognitix-threat-defender.html>



There are various tools for different operating systems for creating a bootable USB flash drive, such as [Etcher<sup>11</sup>](#) for Microsoft Windows, Apple macOS, and Linux. See the documentation of your selected tool on how to use it to write the image file to the USB flash drive.

Under Linux, you can also manually copy the image to the USB flash drive as follows:

1. Make sure that the USB drive is unmounted and you know the name of the device. In this example, the USB drive is `/dev/sdb`.
2. Access the command line interface and run the following command:

```
sudo cp cgntx_installer_latest.img /dev/sdb && sync
```

Alternatively, you can also use:

```
sudo dd if=cgntx_installer_latest.img of=/dev/sdb bs=1M && sync
```

Remember to replace `cgntx_installer_latest.img` with the actual file name of your installation file.

## 2.2.2 Installation via USB Installer Drive

To be able to install Threat Defender, you need a USB flash drive with the installation image (see [Installation Preparation](#) (page 24)).

**Tip:** If you install the software on a headless device using a serial console, there may be issues when using special characters. Try to avoid this by using an EN keyboard layout.

To make sure that Threat Defender will be able to get software and license updates, you will be asked to enter a reachable network [gateway](#) and [DNS](#) server for the management interface. You can also do this via the user interface when the installation is complete, see [Change the Management Interface](#) (page 42).

Depending on your hardware equipment, autonegotiation for the network ports may have to be disabled (best case: device AND switch). Otherwise, Threat Defender may configure the management interface before the network card has a proper IP state for the dedicated management LAN port, for example. Threat Defender may then start without having an [IP address](#).

---

<sup>11</sup> <https://etcher.io/>

### 2.2.2.1 Setup

To install Threat Defender, proceed as follows:

1. Insert the USB flash drive with the installation image into your appliance. The system checks for existing installations.
2. Select the **Threat Defender Installer** option. If there is no previous installation on the system, this option will be automatically selected after a few seconds.



Fig. 9: cognitix Threat Defender boot menu.

An installation wizard guides you through the installation process.

3. The installer displays an overview of your hardware information. Proceed with **OK**.
4. Select your keyboard layout.
5. Select **Yes** to confirm that the installer may delete your hard disk.

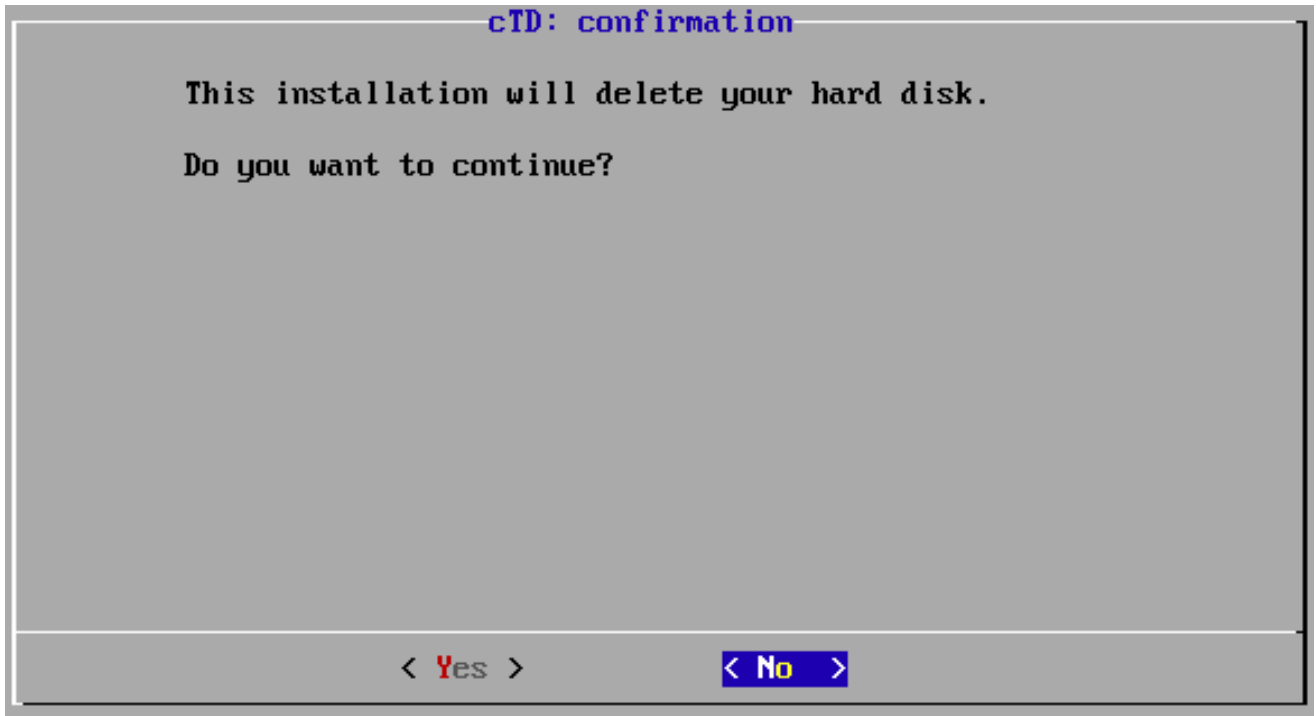


Fig. 10: Deletion confirmation.

6. Confirm the installation target.
7. Enter the hostname of the device.

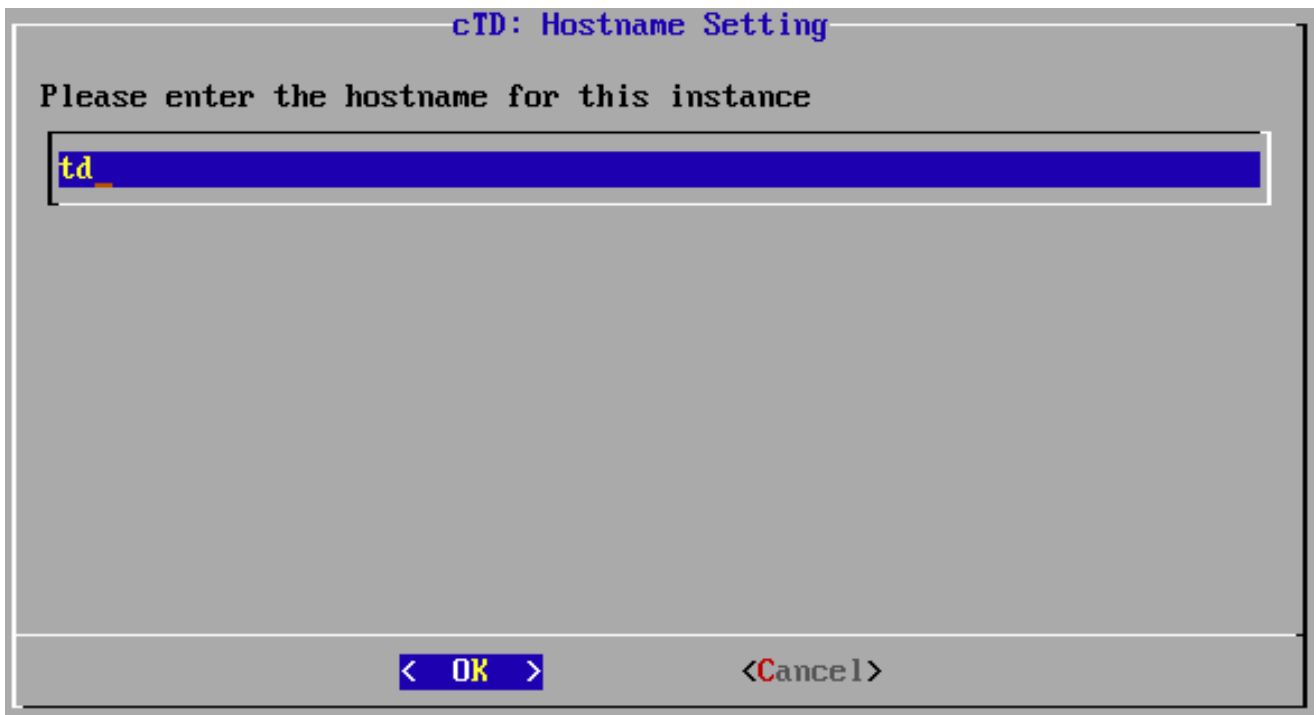


Fig. 11: Input of the hostname.

Confirm your settings with OK.

8. Select the interface you want to use for out-of-band management (i.e. the management interface).

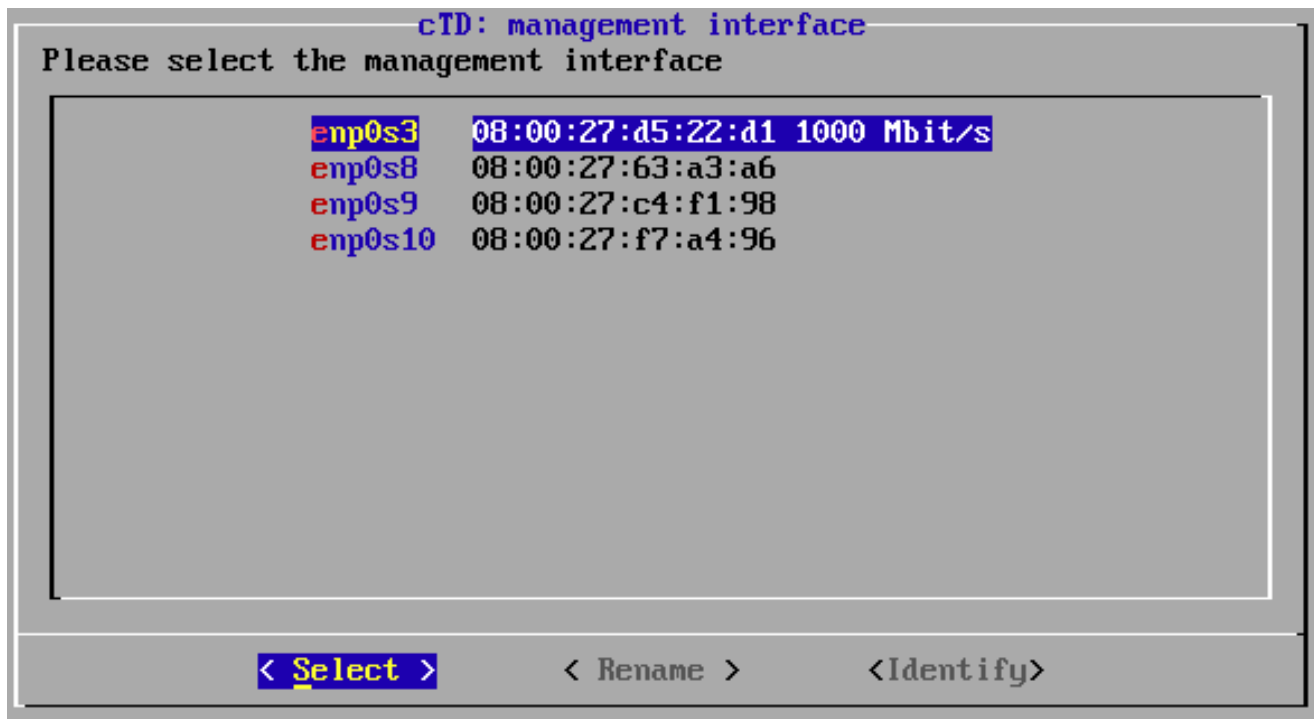


Fig. 12: List of interfaces.

The installer automatically detects usable network interfaces. If an interface is connected to a remote station (e.g. a switch or server) the connection speed is indicated after the **MAC address** of that interface.

To be able to access the GUI, the management interface has to be in “link up” state. Nevertheless, it is possible to configure an unconnected interface and activate the connection later.

Optional:

- To verify a selected interface, select **Identify**. This will cause the LEDs of the selected interface to flash.
- Select **Rename** if you wish to assign more convenient names to the interfaces, e.g. `management` for your management interface.

9. Enter the IP address of the management interface in **CIDR** format.

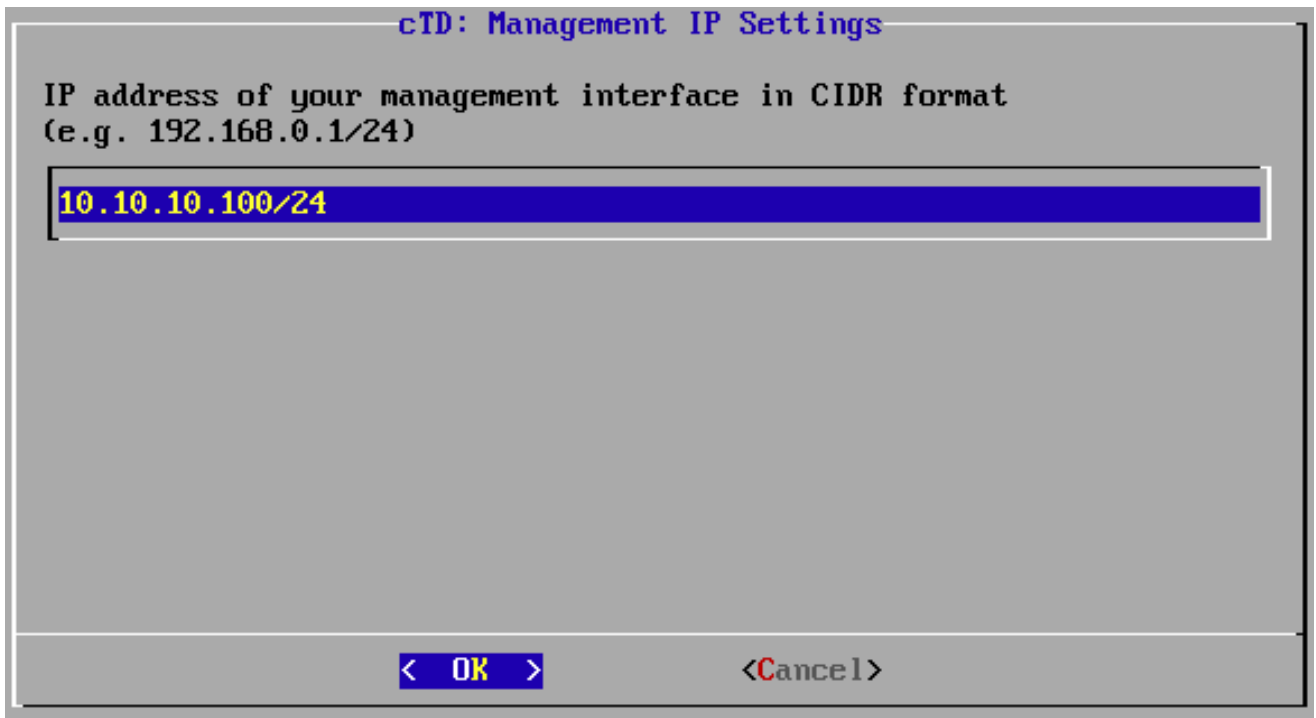


Fig. 13: IP address of the management interface.

Confirm your settings with **OK**. This IP address will be used to access the Threat Defender user interface.

10. If you want to receive software and signature updates via the Internet, enter your gateway and DNS server.

- Enter the IP address of your gateway, if applicable. Confirm your settings with **OK**.

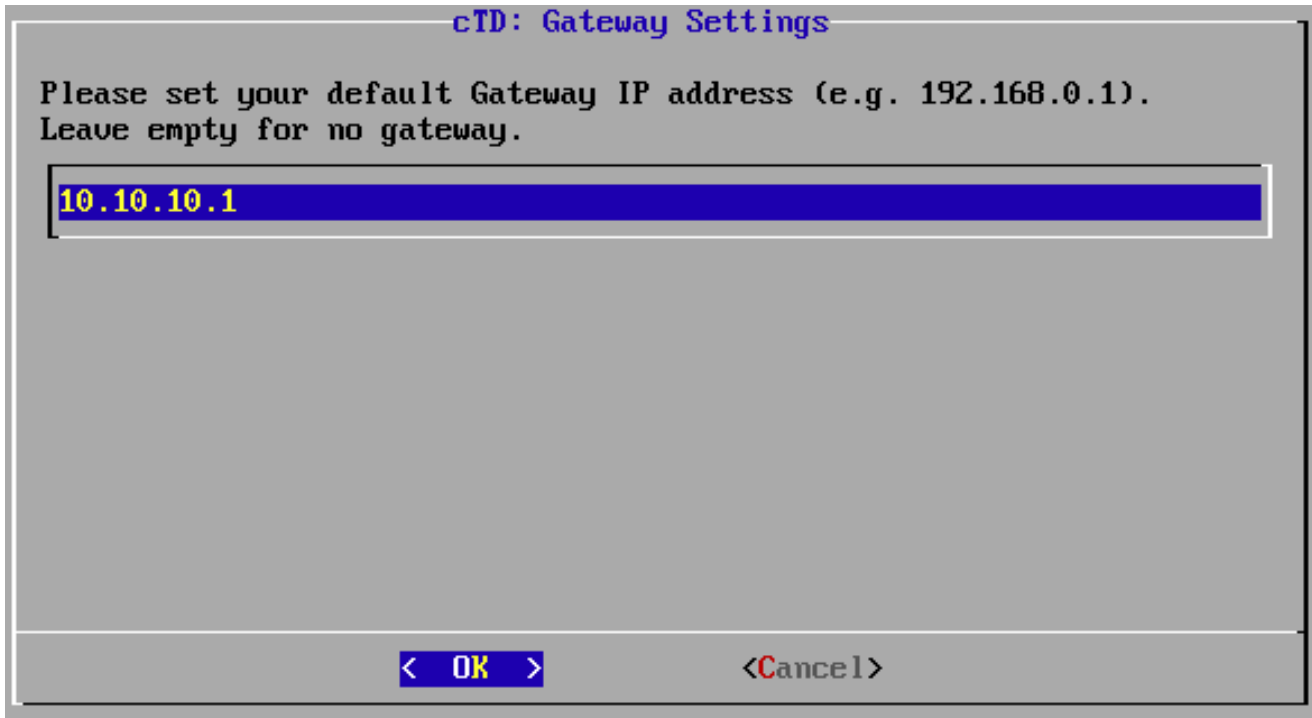


Fig. 14: IP address of the gateway.

- Enter the IP address of a reachable DNS server. Confirm your settings with OK.

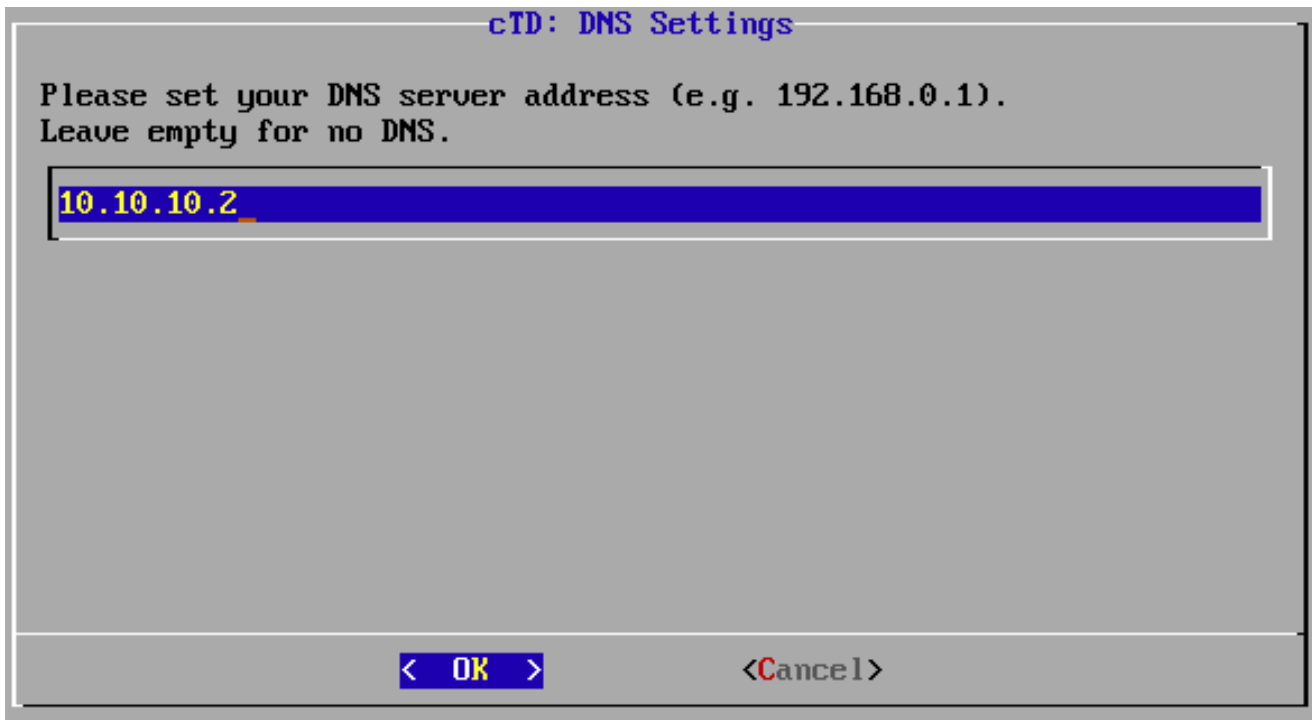


Fig. 15: IP address of the DNS server.



**Warning:** To be able to get firmware and license updates, Threat Defender has to be able to reach our servers via the Internet. If you do not want to connect Threat Defender to the Internet, you need to update it manually (see [Updates](#) (page 203)).

11. Select the time zone as required. Press OK to confirm the setting.

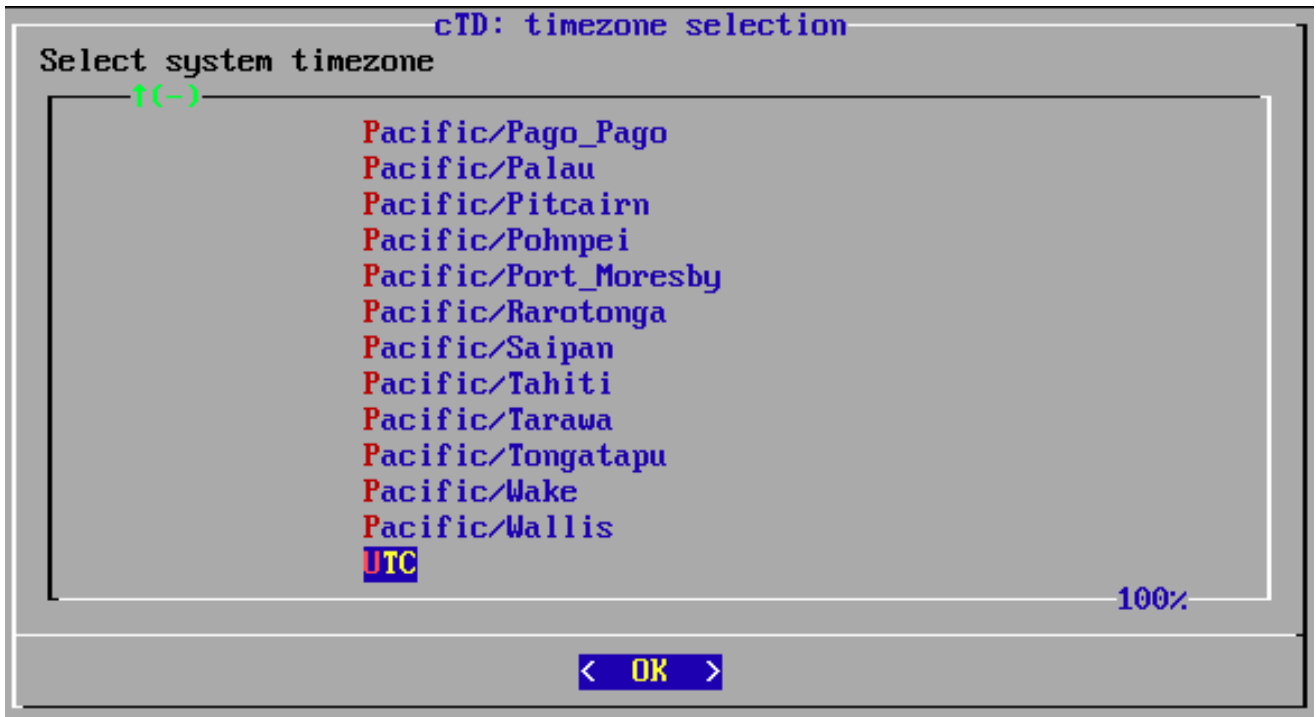


Fig. 16: Time zone selection.

**Tip:** You can also change the time zone via the GUI when the installation is complete (see [Change the Hostname and Time Settings](#) (page 40)).

12. The installer prompts you to change the system date and time. If the settings are correct, select **No** and proceed with checking the usable network cards. Otherwise, select **Yes** to manually change the system date and time.
13. Select how Threat Defender proceeds after the installation is complete. The **Fast Reboot** option will be automatically selected after 10 seconds.

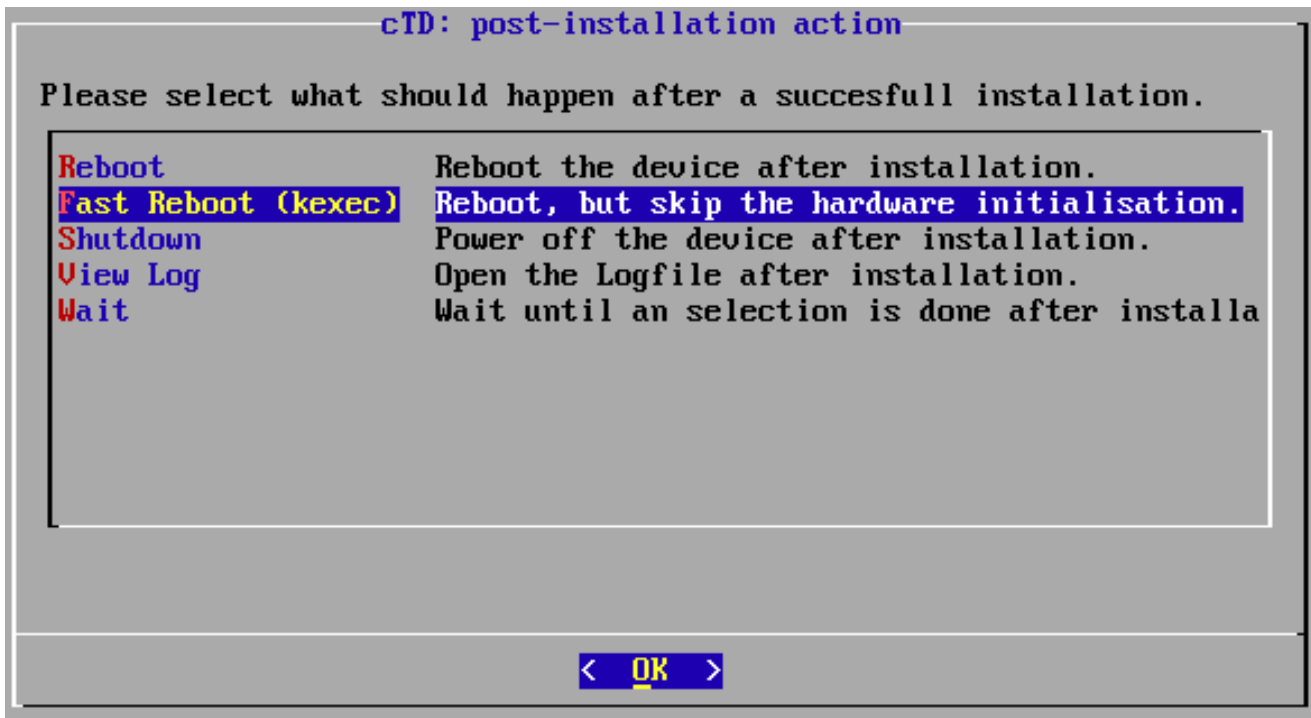


Fig. 17: List of post-installation options.

14. The installer then displays a summary of the settings and prompts you to confirm that they are correct.

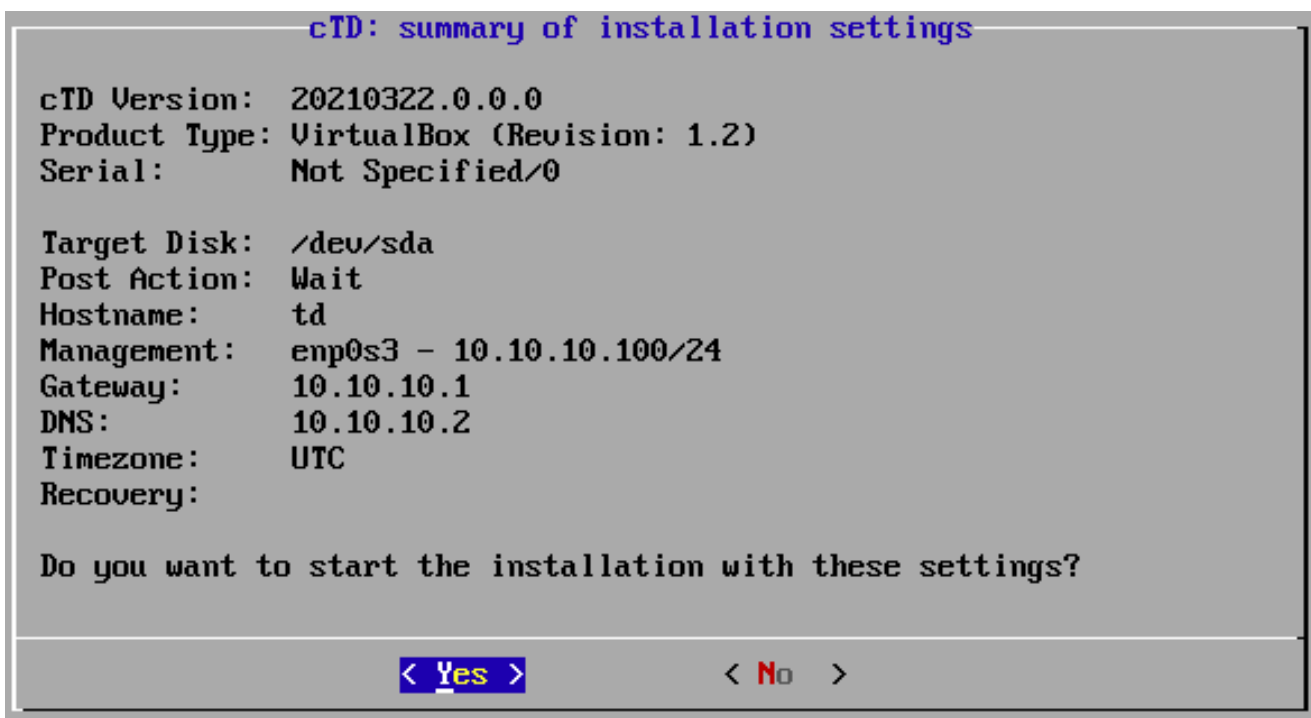


Fig. 18: Configuration summary.

15. Confirm them with Yes to proceed with the installation.



The installer creates a new file system. This may take a few minutes.

16. When the installation is complete, you can once more select how you want to proceed.

### 2.2.2.2 Result

After rebooting the appliance, you see a summary of your settings.

```
_____ cognitix TD _____
      https://www.genua.de
_____

cTD Version: 20210322.0.0.0
Product Type: Software Only
Product Serial: -----

          time: 10:40:23 Tue Mar 23 2021
        host name: td
management IP address: 10.10.10.100
              IPv6: fe80::f5a:64d5:f5aa:ecf
        terminal: tty1 38400

Please open https://10.10.10.100 for graphical configuration interface.
Any terminal login attempt will void your warranty.

td login:
```

Fig. 19: Complete Threat Defender installation.

The installation of Threat Defender is now complete.

To proceed with its configuration, open the IP address of the management interface in your browser. We recommend using Google Chrome.

---

#### Additional References:

- For information on how to log in, see [Sign In](#) (page 34).
- To read more about completing the setup of Threat Defender, see [Complete the Setup](#) (page 36).


## 2.3 Sign In

1. Start your web browser. We recommend using Google Chrome.
2. In the address bar, enter the cognitix Threat Defender IP address which you entered when you installed the software (see [Installation via USB Installer Drive](#) (page 25)).
3. Since cognitix Threat Defender uses a self-signed certificate, most browsers will return a warning. Confirm that you want to proceed.
4. cognitix Threat Defender prompts you to sign in. Enter the default credentials:
  - **Username:** admin
  - **Password:** cognitixOptional: Click **Show Password** if you want to display the password in plaintext.
5. Click **SIGN IN**.

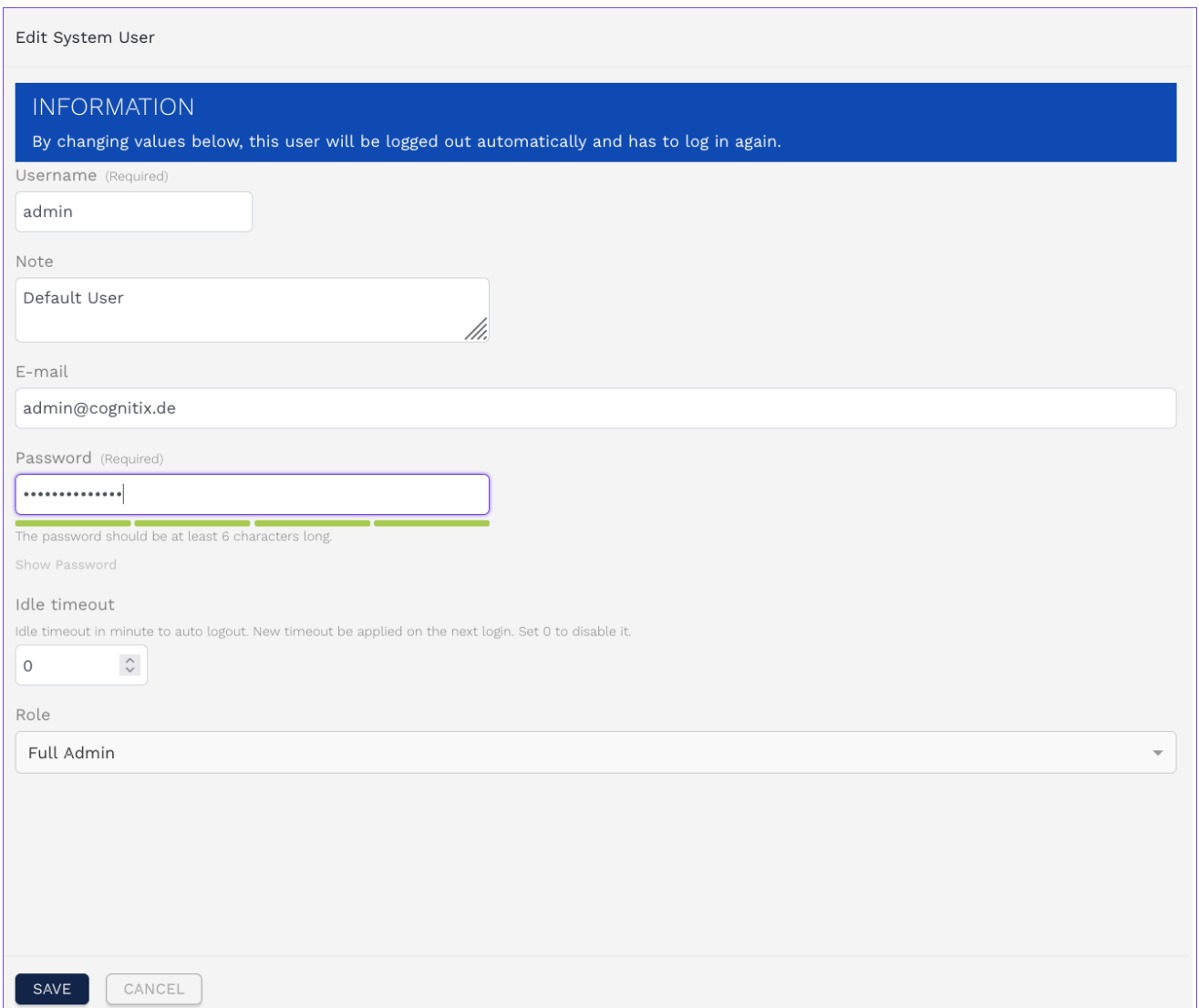
**Tip:** If you need any help, contact our support team by clicking the **SUPPORT** button in the bottom left corner of the screen.

**Note:** If you log in to Threat Defender for the first time, the system prompts you to change your password.

## 2.4 Change the Administrator Password

1. Navigate to **Settings > System Users**.
2. From the list of system users, select the default `admin` user.
3. Click the  icon in the last column of the table. The settings screen opens.
4. Enter a new **Password**. Optional: Click **Show Password** if you want to display the password in plaintext.

**Note:** The maximum password length is 72 characters. It should consist of at least eight alphanumeric characters and special characters.



Edit System User

**INFORMATION**  
By changing values below, this user will be logged out automatically and has to log in again.

Username (Required)  
admin

Note  
Default User

E-mail  
admin@cognitix.de

Password (Required)  
.....  
The password should be at least 6 characters long.

Show Password

Idle timeout  
Idle timeout in minute to auto logout. New timeout be applied on the next login. Set 0 to disable it.  
0

Role  
Full Admin

SAVE CANCEL

Fig. 20: User settings screen.

5. Click **SAVE** to store the new administrator password.

## 2.5 Complete the Setup

The following sections assist you in completing the setup of Threat Defender.

### 2.5.1 Introduction to the User Interface

The following chapters contain general information on the components and handling of the graphical user interface of cognitix Threat Defender.

**Note:** We recommend using Google Chrome to access the user interface.

#### 2.5.1.1 User Interface Components

This chapter describes the main components of the cognitix Threat Defender user interface.

**Note:** Depending on your user role, you may not have access to all menus and screens. Refer to [Access Rights by User Roles](#) (page 216) for further information.

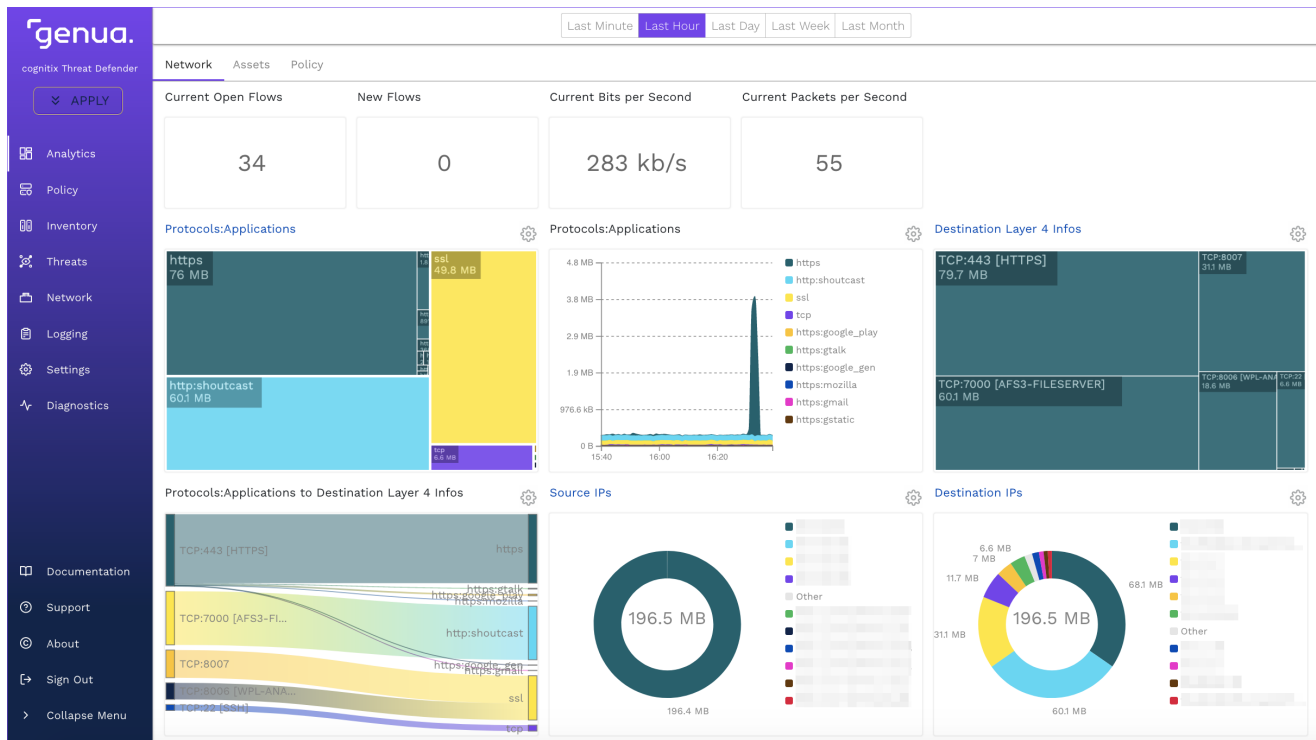



Fig. 21: Overview of the GUI.

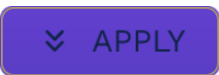
The user interface consists of two main areas: the main navigation on the left side of the screen and the content area.







## The Main Navigation

The main navigation contains the following elements from top to bottom:

- The **APPLY/APPLY CHANGES** button at the top of the main navigation allows you to activate the current configuration. If you change the Threat Defender configuration, the changes have to be applied before they take effect.

-  - This button indicates pending changes. When it is clicked, the button disappears to indicate that the configuration is being applied. Do not shut down Threat Defender during the apply process.

-  - This button is displayed when the configuration does not contain pending changes.

- The main navigation grants access to the available menus on the top navigation level.
- Click  **Documentation** to open the Threat Defender documentation in a new browser tab.
- Click  **Support** to access our customer website.
- Under  **About**, you find details about your hardware and software.
- Click  **Sign out** to log off from Threat Defender.
- In expanded view, the main navigation shows the icons and the titles of the corresponding menus and elements. To increase the space of the content area, click  **Collapse Menu** to only display the icons. To expand the main navigation, click  again.
- With the toggle at the bottom of the navigation you can switch the GUI to dark mode and back.

## The Content Area

The content area takes up the main part of the screen. The information displayed here depends on the selected menu item. At the top of the content area, you see the available sub-levels of navigation for the selected menu item.
















### 2.5.1.2 Handle the User Interface

This chapter contains general information on using the user interface screens.











**Note:** Changes to the configuration of Threat Defender will only take effect when you click the **APPLY CHANGES** button at the top of the main navigation.

## Icons

The following icons are used in the main navigation:











Icon	Description
	Indicates that configuration changes have to be applied.
	Indicates that no configuration changes are pending.
	Access the <b>Analytics</b> menu.
	Access the <b>Policy</b> menu.
	Access the <b>Inventory</b> menu.
	Access the <b>Threats</b> menu.
	Access the <b>Network</b> menu.
	Access the <b>Logging</b> menu.
	Access the <b>Settings</b> menu.
	Access the <b>Diagnostics</b> menu.
	Open the cognitix Threat Defender manual in a new browser tab.
	Open the customer website in a new browser tab.
	View details about your hardware and software.
	Sign out of cognitix Threat Defender.
	Expand/collapse the main navigation.

The following icons are used throughout the content area of the user interface:

Icon	Description
	The element is enabled.
	The element is disabled.
	View details of the corresponding element.
	Edit the corresponding element.
	Copy the corresponding element.
	Delete the corresponding element.
	Download the corresponding element.
	Create a PDF report.
	Access chart type options.
	Include the element in the filtered results.



continues on next page



Table 2 – continued from previous page

Icon	Description
	This icon can have two meanings: <ul style="list-style-type: none"> <li>• Exclude the element from the filtered results.</li> <li>• Remove the filter.</li> </ul>
	Investigate outbound traffic under <b>Analytics</b> .
	Investigate inbound traffic under <b>Analytics</b> .
	Ascending sort order.
	Descending sort order.
	Yes.
	No.
	Show more information.
	Show less information.
	View the event belonging to the selected attribute.

## Handle Tables

Many screens of the cognitix Threat Defender user interface contain tables.

You can filter tables using the  filter field above the respective table. Type a search string in the input field and click **SEARCH**. Threat Defender then only displays the matching table entries. Filters are case-insensitive. To remove the filter and display all table entries, click  next to the input field.

You can sort most tables by one of the table columns in ascending or descending order. To do so, click the header in the desired table column. An  or  icon indicates the sort order. Click the header again to reverse the sort order.

### 2.5.2 Add a License

**Note:** Make sure that the date and time are set correctly (see [Change the Hostname and Time Settings](#) (page 40)). Otherwise, installing the license may fail with an “invalid license” message.

To apply a license to your cognitix Threat Defender installation, proceed as follows:

1. Navigate to **Settings > License**.
2. Click **Add**. The license upload screen opens.

3. Paste the license token into the **License token** field.

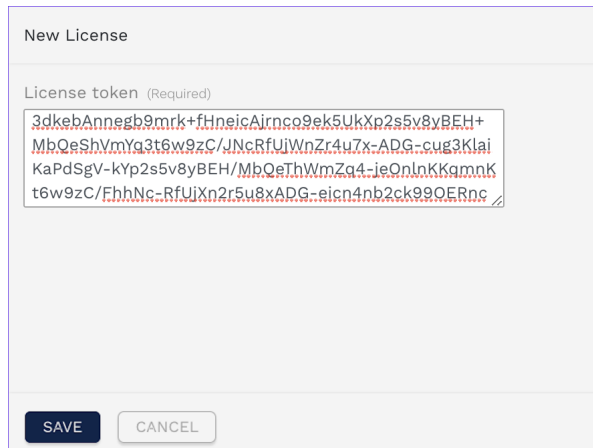


Fig. 22: License token field.

4. Click **SAVE** to store the license and close the upload screen. The license information is displayed as an entry in the overview table.



Actions		+ Add				
Enabled	Title	Contract ID	Version	Valid From	Valid Until	Max Assets
<input type="checkbox"/>	manual	TD-65	1	2018-08-16 - 11:17:43	2024-08-16 - 11:17:43	1000000
<input checked="" type="checkbox"/>	manual	[REDACTED]	7	2020-08-03 - 16:22:33	2021-11-04 - 15:22:33	1000

Fig. 23: License overview table

**Note:** Only one license may be enabled at a time. When you add a new license, it is enabled by default and any previously active license is automatically disabled.

### 2.5.3 Change the Hostname and Time Settings

In order to install a license, the time settings have to be correct. Carry out the following steps to change the hostname and time settings:

1. Navigate to **Settings > General**.
2. Click the  icon in the overview table under **General**. A settings screen is displayed.
3. Enter the **Hostname**.
4. Click **SAVE** to store your settings.
5. Next, click the  icon in the table under **Time**. A settings screen is displayed.



6. Select your **Time Zone** from the drop-down list.

To manually set the date and time, proceed as follows:

1. Make sure that the **NTP** toggle is set to .
2. Click **MANUALLY SET CURRENT TIME**.
3. Use the date picker to set the date.
4. Enter the time in the 24-hour format.

If you want to use an NTP server, proceed as follows:

1. Set the **NTP** toggle to .
2. Enter an NTP server in the **NTP Servers** input field. If you enter multiple NTP servers, they have to be separated by commas.

**Note:** To be able to use an NTP server, make sure that a **gateway** and a **DNS** server are set up for the management interface.

3. Click **SAVE** to store your settings.

When you have finished adjusting the settings, click **APPLY CHANGES** at the top of the main navigation to activate the new configuration.

## 2.5.4 Create New System Users

The following example shows how to add a new user to the system.

1. Navigate to **Settings > System Users**.
2. Click **Add** to create a new user.
3. Enter a **Username**.

**Note:** This username also serves as login name (case-sensitive). It may consist of alphanumeric characters and special characters. It may not contain blank spaces.


4. Optional: Enter a **Note** to describe the new user.
5. Optional: Enter the **E-mail** address of the user.
6. Enter a **Password** for the user. Passwords should be at least 8 characters long and contain upper- and lowercase alphanumeric characters as well as special characters. Optional: Click **Show Password** if you want to display the password in plaintext.

7. Set the **Idle timeout** after which the user will be automatically logged out.
8. Assign a **Role** to the user. See [Access Rights by User Roles](#) (page 216) for information on the available roles.
9. Click **SAVE** to store the new user. The new user is now added to the list of available system users.

### 2.5.5 Change the Management Interface

You can change the default management interface to access the Threat Defender web interface at a different IP address.

To change the management interface, proceed as follows:

1. Navigate to **Settings > General**.
2. The **Management Interface** table displays the current management interface configuration. Click the  icon in the last column of the table or double-click on the table row. The settings screen opens.
3. Under **Address**, enter the IP address you want to use to access the Threat Defender web interface in **CIDR** notation (IP address followed by a slash and the number of bits set in the **subnet** mask).
4. Enter the **Gateway** to be used for the management interface.
5. Optional: Under **DNS Addresses**, enter the IP addresses of the domain name servers that resolve host and domain name requests. The IP addresses have to be separated by commas.
6. Click **SAVE** to store your changes.

When you have finished adjusting the settings in the web interface, click **APPLY CHANGES** in the upper left corner to activate the new configuration.



**Warning:** After your configuration changes are applied, the web interface will no longer respond at the previous address. To access the web interface after changing the IP address of the management interface, open a new browser tab and enter the new IP address in the address bar.


---

#### Additional References:

For further information on the settings options, see [General](#) (page 197).

## 2.5.6 Configure Proxy Settings

Proceed as follows to configure Threat Defender for proxy server access:

1. Navigate to **Settings > General**.
2. In the **Proxy** table, click  to edit the proxy settings.
3. Under **Proxy**, enter the URI of the proxy server e.g. `http://proxy.example.com:8080`. If you also want to specify a username and password for the proxy, use the following format: `http://username:password@proxy.example.com:8080`

**Tip:** When using domains in the username, avoid the backslash by using `%5C` instead.

4. Optional: Enter a **Note** to describe the proxy configuration.
5. Click **SAVE** to store the changed proxy configuration.

## 2.5.7 Update cognitix Threat Defender

To make sure that cognitix Threat Defender runs the latest firmware, check for available updates and install them after deploying Threat Defender for the first time.

If Threat Defender is connected to the Internet, it automatically checks for available updates once per hour. You can also launch the update check manually:

1. Updates can only be installed if there are no pending configuration changes. Click the **APPLY CHANGES** button to save any pending changes.
2. Navigate to **Settings > Updates**.
3. Click **CHECK FOR UPDATES**. Threat Defender checks our servers for available updates and displays them in the updates table.

Type	Product	Current Version	Update Version	Description	Size	Downloaded / Added	
firmware	cognitix Threat Defender firmware	20220711.0.0.0	20220729.0.0.0	The firmware package of the cognitix Threat Defender containing all subsystems	1.20 GB	2022-08-08 - 10:58:31	<b>INSTALL AND REBOOT NOW</b>
ips	cognitix IPS signatures	20220518.0.0.1652877880	20220714.0.17:1659665022	The signature package of cognitix' Intrusion Prevention System	2.23 MB	2022-08-08 - 10:59:12	<b>INSTALL NOW</b>

Fig. 24: Updates table.

4. Select the latest firmware update. Click **INSTALL AND REBOOT NOW** in the last table column. Threat Defender installs the update and reboots automatically.

**Note:** IPS and IoC updates are sometimes included in a firmware update. For this reason, it is recommended to install firmware updates first. Any smaller updates they contain will disappear from the updates table when the firmware update is complete.

When Threat Defender has completed the reboot, check the updates table again to see if there are any more updates to be installed.

## 2.5.8 Define Update Schedules

Using update schedules, you can plan updates in a way that they do not interfere with normal operation. If update schedules are enabled, Threat Defender automatically checks for the respective updates at the preset times. If an update is available, it is automatically installed.

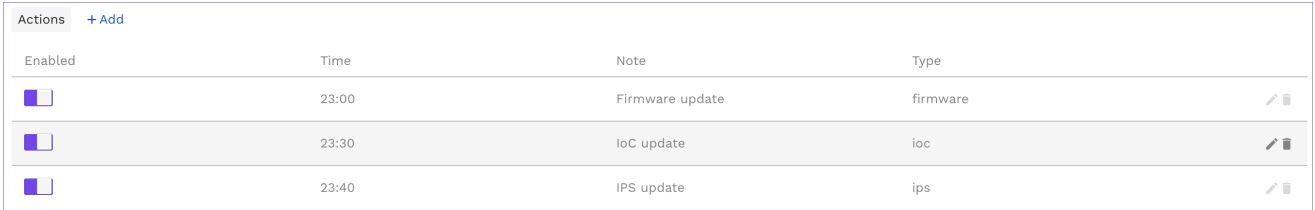
**Note:** Updates can only be installed if there are no pending configuration changes. Otherwise, Threat Defender aborts the installation and tries to install the update again at the next scheduled time. Threat Defender also creates a [syslog](#) message on the failed installation attempt.

Proceed as follows to set up an update schedule for Threat Defender:

1. Navigate to **Settings > Update Schedules**.
2. Click **Add** to set up a new update schedule.
3. Enter the **Time** when the update is to be installed in the 24-hour format.
4. Optional: Enter a **Note** to describe the update schedule.
5. Select the **Type** of update you want schedule. You can only select one update type per schedule.

**Tip:** If you schedule a firmware update, Threat Defender will automatically reboot to complete the update installation. This will take a few minutes and you should time the following update accordingly.

6. Click **SAVE** to store the new update schedule. The new schedule is added to the list of update schedules. New schedules are enabled by default.



Enabled	Time	Note	Type
<input checked="" type="checkbox"/>	23:00	Firmware update	firmware
<input checked="" type="checkbox"/>	23:30	IoC update	ioc
<input checked="" type="checkbox"/>	23:40	IPS update	ips

Fig. 25: List of update schedules.

## 2.5.9 Set up the User API for User Mapping

Threat Defender can be set up to track the usernames and IP addresses of users who connect to the network.

However, Threat Defender cannot independently detect users. Users can either be created manually (see [Users](#) (page 169)) in Threat Defender or this information can be transmitted by the network clients or servers. We recommend setting up the servers since this is more efficient.

### 2.5.9.1 Prepare Threat Defender

Set up Threat Defender to receive user tracking information:

1. Navigate to **Inventory > User Api Setting**.
2. Make sure the toggle is set to  Enabled.
3. Specify a **Secret Key** that servers will use to login in to Threat Defender.
4. Click **SAVE** to store the settings.

**Tip:** Optionally, you can define exceptions that will not be logged.

### 2.5.9.2 Prepare the Network

Set up the servers to contact Threat Defender using the specified **Secret Key** and to transmit the IP addresses and usernames of users connecting to the network. For example, this can be done using [curl](#)<sup>12</sup>:

<sup>12</sup> <https://curl.haxx.se/>

```
curl -skL "https://$TARGET/userapi/registration?action=login&clientIP=${IP}&username=${USER}&secretKey=password"
```

Where the \$TARGET variable is the DNS name or IP address of Threat Defender.

### 2.5.9.3 Result

Threat Defender displays the login and logout events generated by the users in the user API log and reporting.

## 2.5.10 Manage the Processing Interfaces

Navigate to **Network > Manage Processing Interfaces** to manage the processing interfaces. You can freely assign VLAN ranges to individual interfaces and group them in bridges as required.

By default, all interfaces of Threat Defender belong to a single bridge. This default configuration provides a working fallback you can activate, if required.

**Note:** When setting up your own configuration, keep the following in mind:

- Threat Defender does not manipulate any packets.
- Packets cannot be transmitted from the same interface they were received on.

Depending on the number of assigned interfaces, there are the following bridge configurations:

- **1 interface:** The bridge is in SPAN mode, i.e. the received packets cannot be transmitted. This configuration can be used for an interface that is connected to a switch via mirror port. It serves analysis purposes, there is no traffic interception, and VLAN tags remain untouched.
- **2 interfaces:** The bridge is in VirtualWire mode, i.e. packets received on one interface are transmitted on the other. VLAN tags remain untouched, but traffic can now be intercepted and the policy can be enforced.
- **3 or more interfaces:** The bridge is in simple switch mode. This means Threat Defender forwards traffic to the target ports as required and acts like an unmanaged switch (VLAN tags still remain untouched).

The following chapters contain example configurations using VLAN tagging:

### 2.5.10.1 Use a Switch as Port Extender for Threat Defender (Breakout Mode)

Using a VLAN-capable switch as port extender, you can connect Threat Defender to your LAN and intercept the network traffic, i.e. apply policies to the traffic.

**Tip:** This approach differs from setting up a mirror port where Threat Defender only sees copies of the packets but cannot intercept them.

#### On the Switch

1. Assign VLAN tags 301-348 to each port of the switch. We recommend mapping VLAN tag 301 to port 1 and so on. Refer to the documentation of your switch for further information.
2. Set up one port as trunk port that contains all tagged VLANs.
3. Connect the trunk port of the switch to Threat Defender. In this example, we connect the trunk port to interface `enp4s0`.

**Note:** With this setup, the switch cannot transmit any other VLAN-tagged traffic.

#### On cognitix Threat Defender

1. Navigate to **Network > Manage Processing Interfaces**.
2. Click **Add** to create a new bridge.
3. Under **Port**, select the interface connected to the trunk port of the switch, i.e. `enp4s0`.
4. Enter the used **VLAN Range**, i.e. 301-348.
5. Save the bridge.

New Processing Interface Group

Bridge  
br0

Port  
enp4s0 x ▾

VLAN Range  
301-348

SAVE CANCEL

Fig. 26: Example interface setup.

6. Disable the default interface configuration, i.e. set the toggle to .
7. Click the **APPLY CHANGES** button in the header to activate your configuration changes.

## Result

All the physical ports of the switch are now bridged via their VLANs on the selected interface. Threat Defender can now intercept the communication going through the switch via the assigned VLAN tags.



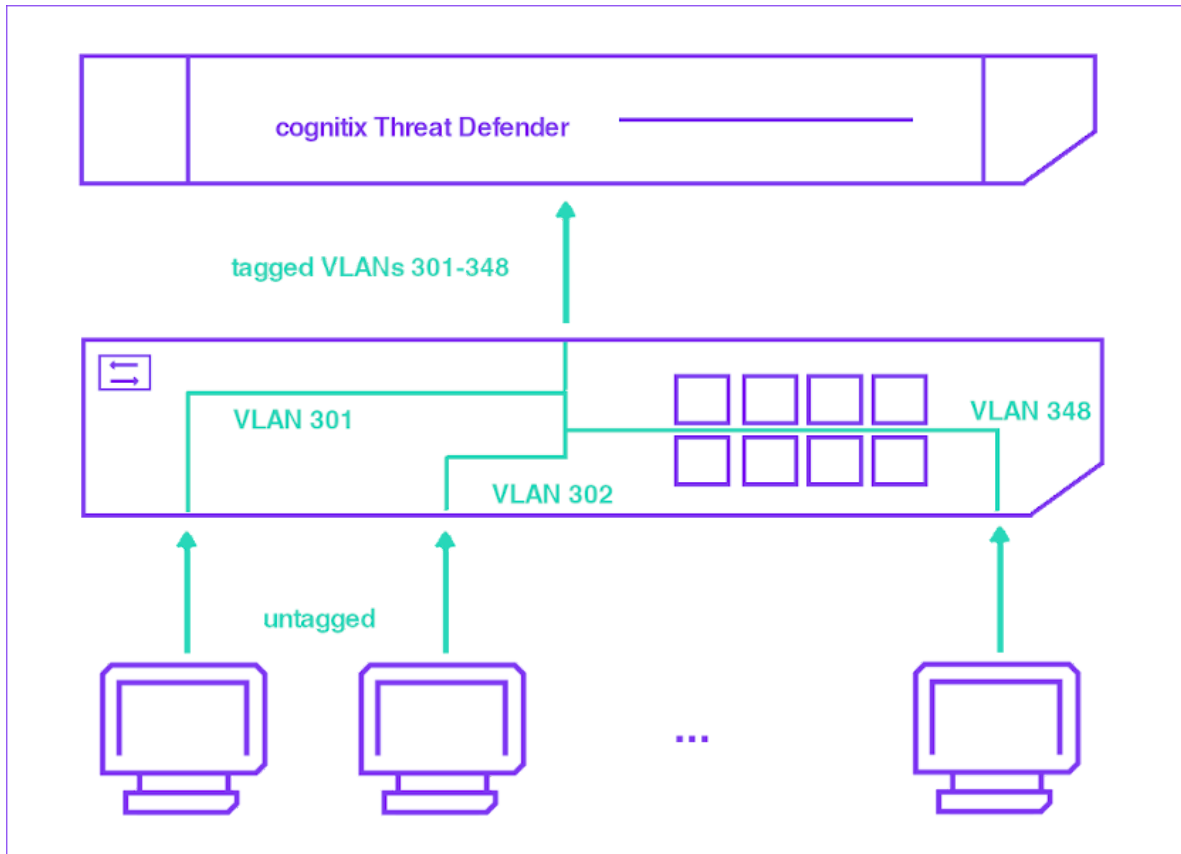


Fig. 27: The switch handles VLAN traffic.

### 2.5.10.2 Configure VLAN Trunking

In order to connect multiple VLANs to networks, you need to set up VLAN trunking. The following example illustrates the setup for cognitix Threat Defender assuming that:

- port `enp3s0` is connected to VLAN10 untagged,
- port `enp4s0` is connected to VLAN20 untagged,
- port `enp5s0` is the trunk port for VLAN10 and VLAN20.

Under **Network > Manage Processing Interfaces**, configure the following setup:

Bridge	Port ID	VLAN Range
VLAN10	<code>enp3s0</code>	
VLAN10	<code>enp5s0</code>	10
VLAN20	<code>enp4s0</code>	
VLAN20	<code>enp5s0</code>	20

Disable the default interface configuration, i.e. set the toggle to . Otherwise, your configuration will not take effect.

Click the **APPLY CHANGES** button in the header to activate your configuration changes.

## 2.5.11 Back up the Configuration


We recommend creating backups of the cognitix Threat Defender configuration at regular intervals.

**Tip:** Threat Defender creates an automatic backup whenever you apply configuration changes. However, Threat Defender stores only one automatically generated configuration file. Older files are overwritten when a new file is auto-generated.

### 2.5.11.1 Create Configuration Files

1. Navigate to **Settings > Configurations**.
2. Click **Add** to create a new backup file of the current system configuration.

**Note:** The backup file only contains the activated configuration. Pending changes are not backed up.

3. Optional: Enter a descriptive note.
4. Click **SAVE** to store the configuration file.
5. If you wish to download the file, click the  icon in the overview table.


### 2.5.11.2 Restore Configuration Files

Under **Settings > Configurations**, you can restore the configuration files listed in the overview table.

To upload configuration files, proceed as follows:

1. Click the **Upload** button above the overview table.
2. In the upload screen, click **SELECT** to access the file system.
3. Select the desired configuration file (.pc format).
4. Click the **Upload** button at the bottom of the screen. The configuration file is now displayed in the overview table.

To restore a configuration file, proceed as follows:

1. Click the  icon in the overview table to access the details view of the respective file.

2. The buttons below the table allow you to select which part of the configuration you want to restore: the entire configuration, the network configuration, the policy configuration, or the asset configuration.
  3. Click **INSTALL** to restore the selected configuration. Do not shut down Threat Defender during the restoration of the configuration.
- 

**Additional References:**

For information on how to install Threat Defender, refer to [Installation Preparation](#) (page 24) and [Installation via USB Installer Drive](#) (page 25).



| Chapter 3

# Monitor the Network

### 3.1 Passive Monitoring

cognitix Threat Defender monitors the network to increase transparency. Using rules, it tracks assets, communication flows, and so on. These rules can generate log messages if unexpected or anomalous behavior is detected.

This provides clear visibility of the network traffic and active assets. Using the intuitive drill-down reporting system of Threat Defender you can analyze this information.

To passively monitor the network traffic without intercepting it, connect cognitix Threat Defender to the mirror port of a switch (mirroring or switch monitoring). You need to configure the switch to send copies of all packets to the mirror port. For further information, see the documentation of your switch.

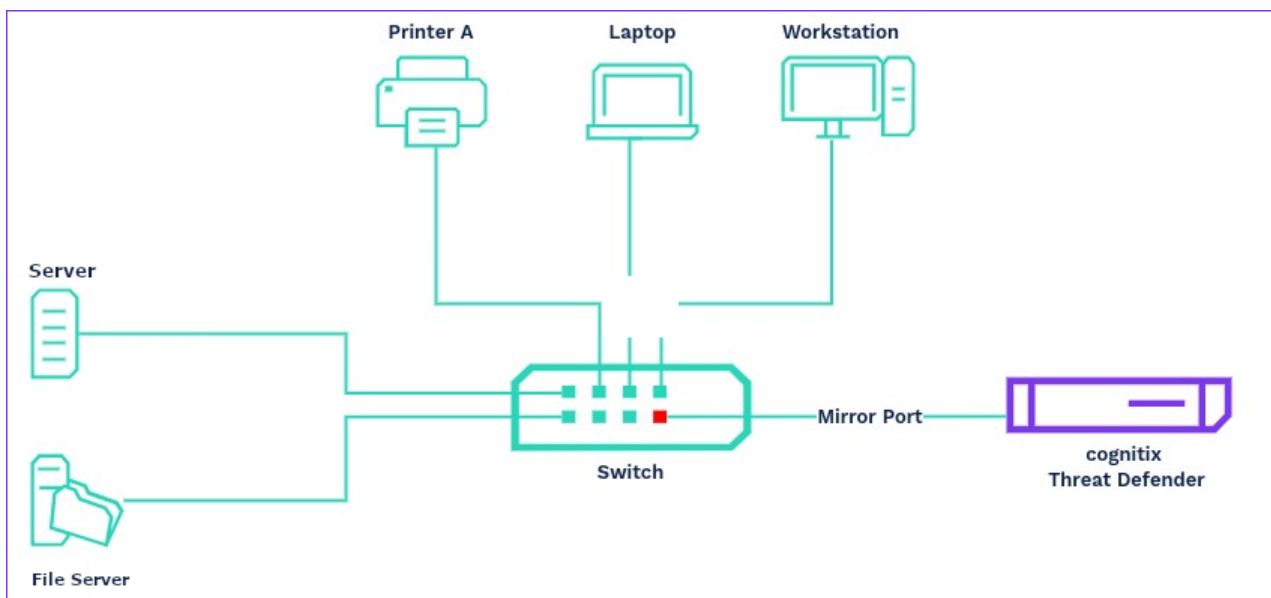


Fig. 1: cognitix Threat Defender connected to the mirror port of the network switch.

In this mode, cognitix Threat Defender aggregates reporting data and logs on the network traffic seen at the mirror port. The traffic is not intercepted and VLAN tags remain untouched.

The reporting system of Threat Defender allows you to analyze the traffic. Drill down from the high-level dashboards to detailed analysis screens.

The following chapters provide a starting point for your network analysis:

#### 3.1.1 Analyze Protocols and Destination Countries

Starting from the **Network** dashboard, you can analyze what protocols communicate with a specific destination country.

1. Navigate to **Analytics > Network**. Here, you see the total traffic distribution by destination countries among other things.

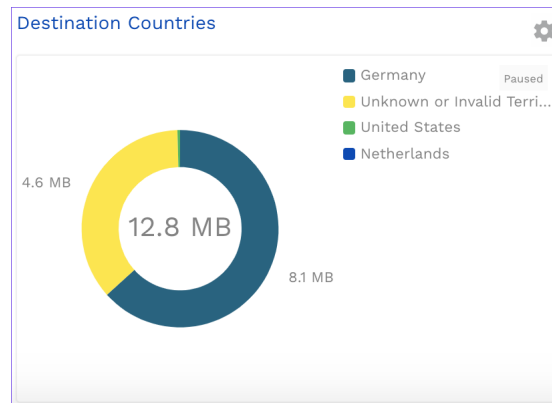



Fig. 2: Total traffic distribution by destination countries.

**Tip:** You can change the chart type by clicking the  icon in the upper right corner and selecting a type from the drop-down list.

2. In the chart, click the country you want to analyze further. The link takes you to a detailed view of the traffic directed to this destination country.
3. The **Protocols:Applications** chart displays the protocols and applications that communicate with the selected country.

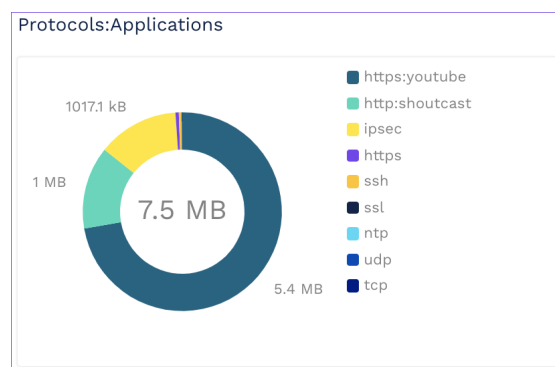


Fig. 3: Traffic distribution by protocols/applications.

4. Click one of the protocols in the chart to analyze it further. This takes you to an overview page for this protocol. It displays the source and destination IP addresses and assets that use this protocol, other source and destination countries this protocol talks to, the users who use this protocol and more.

From here, you can continue to analyze the traffic by clicking the respective sections in the charts. For example, you can investigate individual devices under source assets.

**Additional References:**

For further information on the analytics screens, see [Analytics](#) (page 142).

### 3.1.2 Find YouTube Users in the Last Hour

Starting from the **Network** dashboard, you can display the top ten clients that accessed YouTube in the past 24 hours.

1. Navigate to **Analytics > Network**. Here, you see the total traffic distribution by protocols and applications.

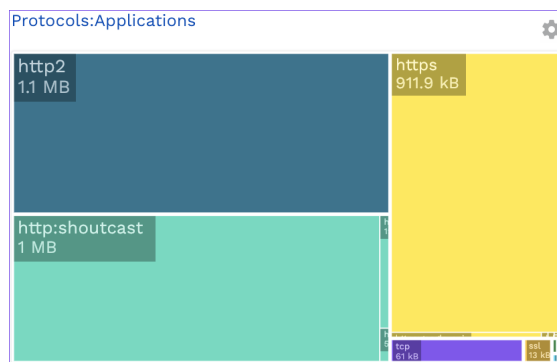




Fig. 4: Total traffic distribution by protocols and applications.

**Tip:** You can change the chart type by clicking the  icon in the upper right corner and selecting a type from the drop-down list.

2. Click the header of the chart. The link takes you to the **Protocols:Applications** subpage.
3. In the table, enter `youtube` into the  filter field. Click **SEARCH**. The table filters the entries to display only entries that contain the search string in their **Name**.
4. Click the desired entry. The link takes you to the overview page, which displays the users who accessed YouTube, in addition to other data.
5. Using the default settings, the charts display the entries in the last day. Change the default settings via the buttons at the top of the screen. The charts are automatically updated to reflect the changed settings.
6. You can now click an individual user to analyze them further. Among others, you can see the destination IPs and URLs this user accessed.

**Additional References:**

For further information on the analytics screens, see [Analytics](#) (page 142).



### 3.1.3 Port Monitoring

Using policy rules cognitix Threat Defender can monitor individual ports and generate log entries when it sees unexpected traffic.

In the following example, Threat Defender monitors port 443, the default port for HTTPS traffic. If other traffic, such as SSH or VPN, is rerouted to port 443 this may indicate attempts to circumvent network restrictions.

cognitix Threat Defender logs warnings for any traffic other than HTTPS on port 443.

#### 3.1.3.1 Create the Rule

Create the following global rule:

Source Networks	Destination Networks	Conditions
Any	Any	Layer 4 Port Destinations Ports: 443 Classification Excl

For detailed instructions on how to create a rule, refer to [Create Global Rules](#) (page 83).

With the above rule, Threat Defender will generate incident log entries for all traffic via port 443, other than HTTPS. But it will not intercept the traffic.

**Tip:** You can expand this rule as required. For example, if you want to avoid creating incident log entries for certain protocols or traffic from specific sources, you can exclude them as well.

#### 3.1.3.2 Result

You can see the rule hits in the reporting.

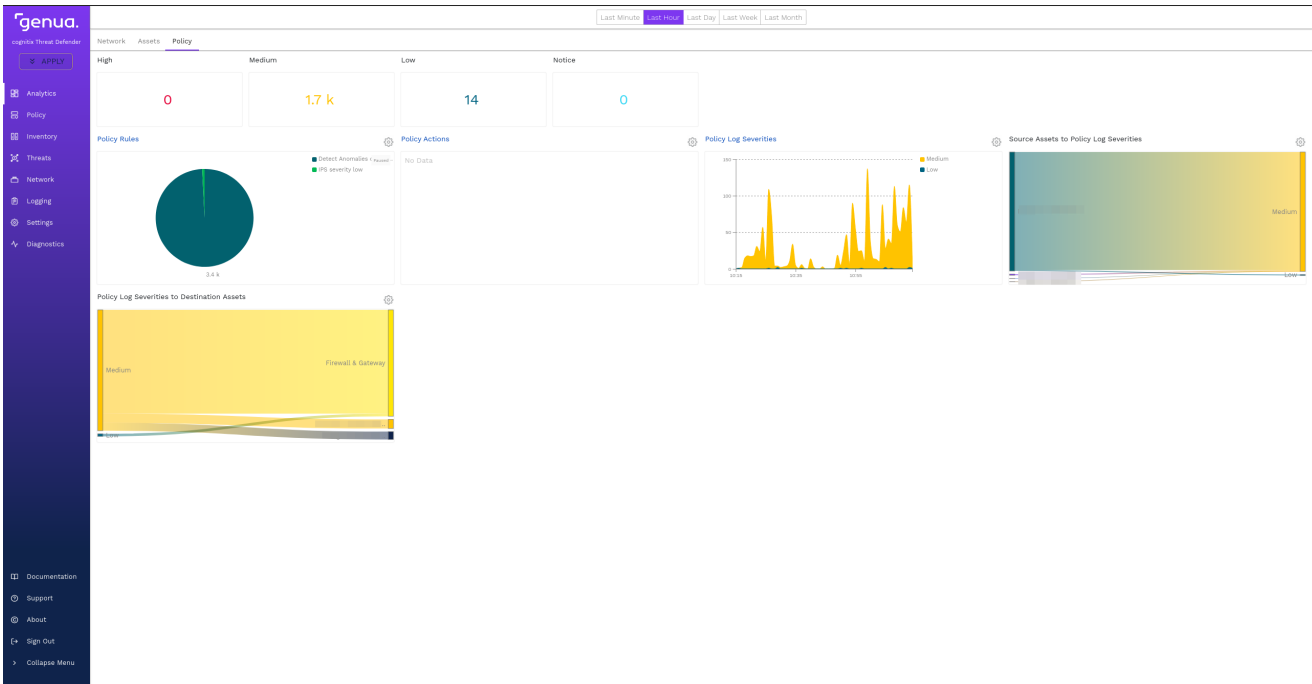


Fig. 5: The rule hits seen under Analytics > Policy.

The incidents logs show warnings with severity **Medium** for all traffic on port 443 that is not HTTPS.

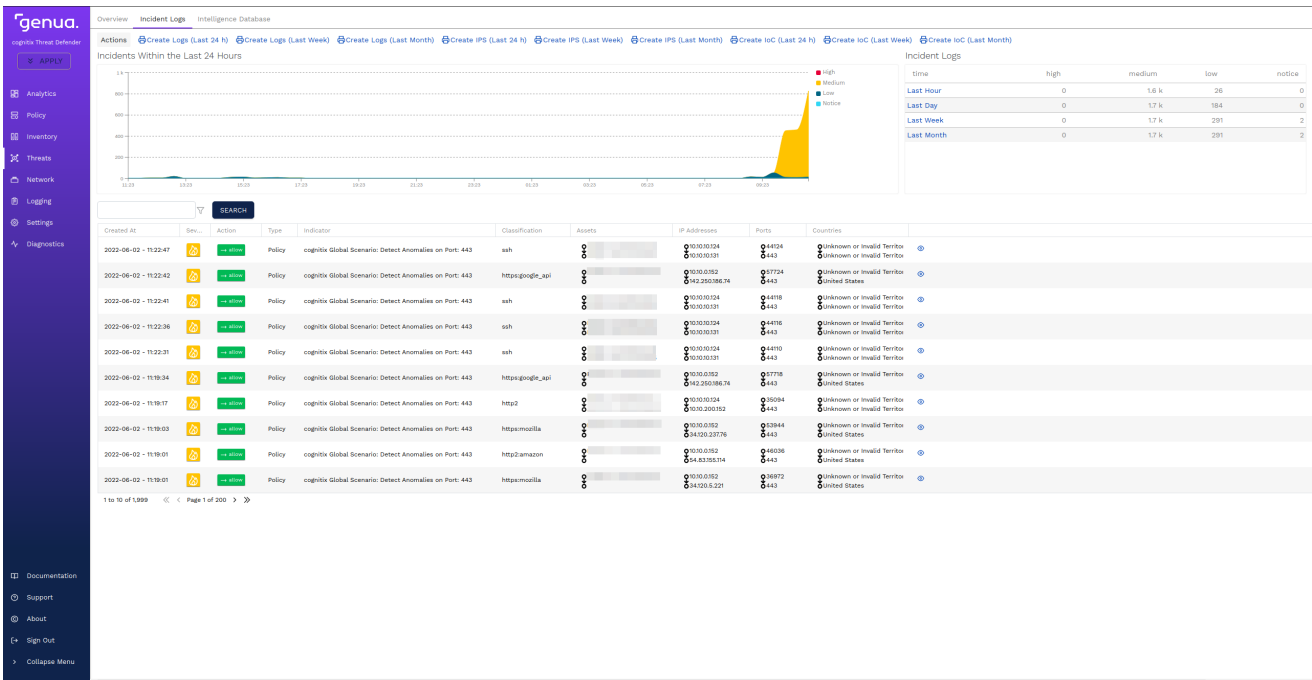


Fig. 6: The incidents log entries under Threats > Incident Logs created by the rule.

Starting at these screens, you can further analyze the anomalous traffic via port 443. If cognitix Threat Defender is **active** (page 72) in the network, you can then create additional rules to actively block unwanted traffic.

**Additional References:**

For information on the incidents logs, see [Incident Logs](#) (page 179).

## 3.2 Monitor Network Assets

cognitix Threat Defender monitors the behavior of network assets and users.

When you first activate Threat Defender in your network, the automatic discovery of assets (see [Asset Setting](#) (page 169)) is enabled by default. This means, Threat Defender automatically learns the MAC addresses of the detected devices in the network and creates individual assets for them in the internal database. While automatic asset discovery is active, Threat Defender creates a new database entry whenever it sees an unknown MAC address in the network.

**Note:** Asset tracking requires an active license. The maximum number of tracked assets depends on the selected license.

The following examples show you how to maintain your asset database and how to restrict access for newly discovered assets.

### 3.2.1 Assets in cognitix Threat Defender

cognitix Threat Defender maps the IP and MAC addresses of network devices to track network assets.

Each asset is identified by its unique ID, a human readable name and a list of MAC addresses and/or IP addresses. In addition, Threat Defender tracks related, passively aggregated values for every MAC address:

- assigned user ID
- assigned tags
- a gateway indicator
- creation timestamp
- last update timestamp
- every IP address seen for this MAC
- MAC address vendor

Furthermore, the following **Last Seen** information is updated every time an asset is active in the network:

- timestamp
- VLAN tag
- IPv4 address

- IPv6 address
- hostname requested via DHCP
- hostname offered via DHCP
- bridge name
- interface name
- user ID
- time to live value (based on IPv4 TTL field or IPv6 hop limit field)

Assets can be used in [network objects](#) (page 122) to segment the network. They can also be used in [policies](#) (page 74) and event tracking tables to create policies for individual assets or groups of assets.

**Note:** Asset tracking requires an active license. The maximum number of tracked assets depends on the selected license.

---


#### Additional References:

- Threat Defender can track assets automatically, see [Asset Setting](#) (page 169).
- Assets can also be managed manually via the GUI under **Inventory > Assets**. See [Create a Network Inventory](#) (page 61) and [Inventory](#) (page 163).

### 3.2.2 Create a Network Inventory


If you have devices with more than one interface and therefore more than one MAC address, Threat Defender creates individual asset database entries for each MAC address. You will have to check your assets database and consolidate them manually. This requires some initial effort but once the database is set up, you can gain valuable insights into your network.

Proceed as follows to consolidate multiple MAC addresses that belong to one asset:

1. Navigate to **Inventory > Assets**. The screen displays an overview of all assets Threat Defender created.
2. Select the automatically created assets from the list that belong to the device with several MAC addresses. Use the  filter field to find it more quickly.
3. Tick their checkboxes in the first table column.
4. Click **Operations** above the table. The asset operations screen opens.

5. Click **Merge Assets**.
6. Click into the **Primary Asset** field and select the asset you want to keep in the database.
7. Click **SAVE**.

Threat Defender now merges the selected assets into the primary asset. The other automatically created assets are deleted from the database. You can see on the asset overview that the number of current assets decreases accordingly.

Click the  icon in the last table column to analyze the source traffic of the new asset under **Analytics > Network** and to see its behavior in the network.

**Tip:** Once you have finished creating the network inventory, we recommend creating a [backup of the asset database](#) (page 175).

### 3.2.3 Handle Newly Discovered Assets

When the automatic discovery of assets (see [Asset Setting](#) (page 169)) is enabled, cognitix Threat Defender assigns predefined tags to assets that connect to the network for the first time. Using these tags, you can set up rules that will be applied to these new assets.

The following example shows how to configure a simple rule that denies unknown (i.e. newly discovered) assets access to the internal resources until an administrator explicitly grants it by removing the predefined `AutoDiscovered` tag.

1. Navigate to **Inventory > Asset Setting** to configure the tag that will be assigned to newly discovered assets.
2. Under **Add this Tag to Auto Discovered Assets**, the preset `AutoDiscovered` tag is already provided. You can enter your own tags that you want to assign to newly discovered assets, however.
3. Navigate to **Policy > Rules**.
4. Click **Add Global Rule** to create a new rule with the following settings:
  - Enter a descriptive **Name** for the rule and an optional **Note**.
  - In the **Source & Destination** section, set **Destination Networks** to `Internal`.
  - In the **Conditions** section, enable **Assets** by clicking the toggle.
  - Under **Source Tags**, select the `AutoDiscovered` tag. With these settings, the rule matches all traffic that originates from assets with the `AutoDiscovered` tag and is targeted at internal network resources.
  - In the **Actions** section, enable **Final Action** by clicking the toggle.

- Select **Drop Traffic and Stop Processing**.
5. Click **SAVE** to store this rule.
  6. Click the **APPLY CHANGES** button at the top of the main navigation to activate your configuration changes.
- 

**Additional References:**

For further information on the **Inventory** menu, see [Inventory](#) (page 163).

## 3.3 Export Reporting Data to Elastic/ELK

The **flow** data collected by one or multiple Threat Defender installations can be aggregated via Logstash or Filebeat and written to one or multiple Elasticsearch instances. They are then evaluated with Kibana.

To quickly start an Elastic stack, have a look at this [example using docker](#)<sup>13</sup>.

### 3.3.1 Export IPFIX Reporting Data to Filebeat

#### 3.3.1.1 Objective

The **flow** data collected by one or multiple Threat Defender installations can be collected in a single Elasticsearch instance and evaluated with Kibana.

#### 3.3.1.2 Set up Filebeat

Set up [Filebeat](#)<sup>14</sup> to handle the flow data provided by Threat Defender.

1. In the Filebeat directory, add a new file called `genua_ipfix.yml` with the custom definitions of our **PEN**:

```
45480:
  10:
    - :uint16
    - :dpiProtocol
  11:
    - :uint16
    - :dpiApplication
  12:
    - :uint16
    - :dpiSrcOS
  13:
    - :uint32
    - :dpiClassification
  14:
    - :uint32
```

(continues on next page)

<sup>13</sup> <https://www.github.com/deviantony/docker-elk>

<sup>14</sup> <https://www.elastic.co/de/downloads/beats/filebeat>



(continued from previous page)

```
- :dpiInSslClassification
20:
- :string
- :countrySource
21:
- :string
- :countryDestination
30:
- :string
- :policyRuleId
31:
- :uint32
- :iPSRuleId
32:
- :string
- :policyRuleName
33:
- :uint8
- :policyRuleAction
34:
- :string
- :policyId
35:
- :string
- :policyName
36:
- :uint8
- :logSeverity
37:
- :uint8
- :cognitixScenarioHit
50:
- :string
- :url
51:
```

(continues on next page)

(continued from previous page)

```
- :uint16
- :urlCategory
52:
- :uint16
- :urlReputation
60:
- :string
- :fileTransferFilename
70:
- :uint16
- :iocFeedId
71:
- :uint32
- :iocIpv4
72:
- :string
- :iocDomain
73:
- :uint64
- :iocUrl
74:
- :string
- :iocFeedName
75:
- :uint8
- :iocValueType
76:
- :string
- :iocValue
80:
- :uint8
- :srcLocation
81:
- :uint8
- :dstLocation
```

(continues on next page)

(continued from previous page)

```
90:
- :string
- :srcAssetId
91:
- :string
- :dstAssetId
92:
- :string
- :userId
```

2. Edit the `filebeat.yml` to contain the following element:

```
filebeat.inputs:
- type: netflow
  host: "0.0.0.0:2055"
  protocols: [ ipfix ]
  max_message_size: 50KiB
  custom_definitions:
    - <absolute path to genua_ipfix.yml created above>
```

3. Run Filebeat.

### 3.3.1.3 Set up Threat Defender

Configure Threat Defender to send IPFIX data to Filebeat:

1. Go to **Logging > Report Channels**.
2. Click **Add** to create a new reporting channel.
3. On the settings screen, configure the following:
  - **Report Type:** IPFIX
  - **Message Type:** Select **Flow Reports**. You can select additional types as required.
  - **Observation Domain Id:** can be 0 if you use only one Threat Defender. Otherwise, set a different value for each Threat Defender to be able to distinguish the reporting sources.
  - **Update Interval:** 30 seconds
  - **Endpoint:** UDP

- **IP Address:** enter the IP address of your Filebeat installation
- **Port:** 2055 (the port of your Filebeat installation as defined in the `filebeat.yml` above)
- **Reconnection Delay:** 15 seconds

4. Click **SAVE** to store your settings and close the settings screen. The new IPFIX channel is displayed in the list of configured reporting channels.

Click the **APPLY CHANGES** button at the top of the main navigation to activate your configuration changes.

As a result, the state of the newly configured IPFIX channel should change to `connected` and show a rising number of transmitted events.

#### 3.3.1.4 Check Kibana

Open the Kibana interface in your browser (see the [Kibana documentation](#)<sup>15</sup> for more detailed information). In the Dashboard section, select the `Netflow Overview` dashboard to get a quick overview of some of the possibilities. You can also use the SIEM section to take a look into some predefined statistics; or start discovering on your own with the Discover section. You can preselect the netflow events by using `input.type: netflow` as a search filter.

### 3.3.2 Export JSONL Reporting Data to Logstash via an Encrypted Channel

#### 3.3.2.1 Objective

The `flow` data collected by one or multiple Threat Defender installations can be collected by a Logstash instance and written to one or multiple Elasticsearch instances and evaluated with Kibana.

#### 3.3.2.2 Requirements

To enable encryption via TLS you need the following:

- a certificate authority in `.pem` format that is self-signed or signed by a trusted CA,
- a certificate issued by this certificate authority, and
- a private key belonging to that certificate.

Make sure that these are present in the Logstash pipeline directory.

<sup>15</sup> <https://www.elastic.co/guide/en/kibana/index.html>

### 3.3.2.3 Set up Logstash

In the Logstash pipeline directory, edit `logstash.conf` to define your inputs, processing and outputs:

```
input {
  tcp {
    port => 5000
    ssl_enable => true
    ssl_verify => true
    ssl_cert => "/path/to/your/server/certificate.pem"
    ssl_key => "/path/to/your/server/key.pem"
    ssl_extra_chain_certs => ["/path/to/your/server/certificate-authority-
↪pem"]
    ssl_certificate_authorities => ["/path/to/your/cTD/certificate-
↪authority.pem"]
    codec => json_lines {
      ecs_compatibility => v1
    }
  }
}

## Add your filters / logstash plugins configuration here

output {
  elasticsearch {
    hosts => "elasticsearch:9200"
    user => "logstash_internal"
    password => "${LOGSTASH_INTERNAL_PASSWORD}"
  }
}
```

### 3.3.2.4 Set up Threat Defender

Configure Threat Defender to send JSONL data to Logstash:

1. Go to **Logging > Report Channels**.
2. Click **Add** to create a new reporting channel.

3. On the settings screen, configure the following:

- **Report Type:** JSONL
- **Message Type:** Select Flow Reports. You can select additional types as required.
- **Endpoint:** TLS encryption
- **Hostname:** enter the hostname of your Logstash installation. Ensure the hostname matches the common name specified in the Logstash certificate.
- **Port:** 5000 (the port of your Logstash installation as defined in the `logstash.conf` above)
- **Reconnection Delay:** 15 seconds
- **Remote certificate authority:** Select the remote CA specified in the Logstash configuration.

4. Click **SAVE** to store your settings and close the settings screen. The new JSONL channel is displayed in the list of configured reporting channels.

Click the **APPLY CHANGES** button at the top of the main navigation to activate your configuration changes.

As a result, the state of the newly configured JSONL channel should change to `connected` and show a rising number of transmitted events.

### 3.3.2.5 Check Kibana

Open the Kibana interface in your browser (see the [Kibana documentation](#)<sup>16</sup> for more detailed information). You can use the SIEM section to take a look into some predefined statistics; or start discovering on your own with the Discover section.

---

#### Additional References:

- For the IPFIX specification of Threat Defender, see [IPFIX Specification](#) (page 226).
- For information on the JSONL events generated by Threat Defender, see [JSON Lines Formatted Output](#) (page 223).

---

<sup>16</sup> <https://www.elastic.co/guide/en/kibana/index.html>

| Chapter 4

# Secure the Network

## 4.1 Active Network Integration

When cognitix Threat Defender is active in the network, it can intercept the network traffic. This allows it to detect complex attacks and to initiate countermeasures.

When using cognitix Threat Defender in your switched network, keep in mind that only traffic that passes Threat Defender can be analyzed.

Threat Defender operates on **layer 2** of the **OSI** model, i.e. the data link layer. It is transparent to the network so that it can be integrated into the network at any point - not just between network segments.

Due to its **network switch** characteristics only the sending and receiving ports can see the traffic. For this reason, place Threat Defender in front of the switch to protect the network behind it.

If you want to secure parts of your network, make sure that all packets pass Threat Defender. You can use a separate switch for the critical network part and connect Threat Defender between.

**Tip:** Integrating Threat Defender actively into the network does not impact performance because the policy is always evaluated. This means even when Threat Defender is used for port mirroring, the policy is evaluated for analytics purposes.

The following examples illustrate how cognitix Threat Defender can be used inside the network.

### 4.1.1 Example 1: cognitix Threat Defender in Breakout Mode

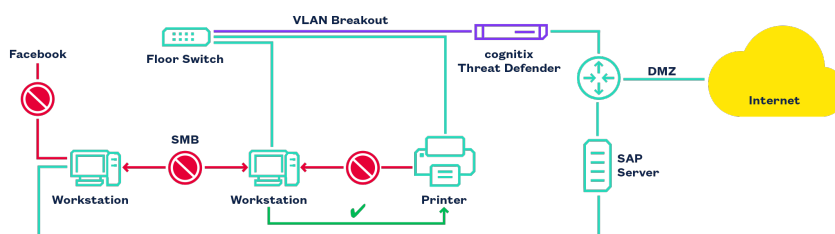


Fig. 1: cognitix Threat Defender in VLAN breakout mode.

In this setup, Threat Defender acts as a switch with security functionality. It monitors the traffic and enforces the security policy:



- Clients may access the SAP server.
- Clients accessing the SAP server must not access Facebook at the same time.
- Clients must not share files among each other to stop lateral movement of attackers.
- Clients may access the printer but the printer must not access clients.

See also [Use a Switch as Port Extender for Threat Defender \(Breakout Mode\)](#) (page 47).

#### 4.1.2 Example 2: cognitix Threat Defender in a DMZ

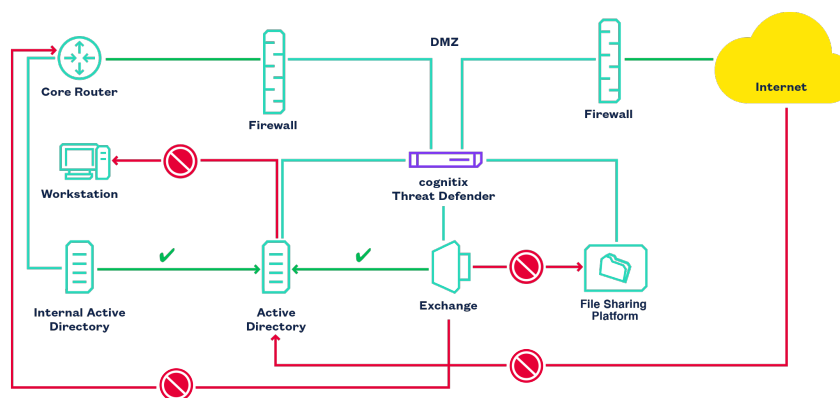


Fig. 2: cognitix Threat Defender isolates services in a DMZ.

This DMZ setup adds additional prevention of DoS attacks on public services. It also prevents lateral movement of attackers within the DMZ and into internal networks. cognitix Threat Defender isolates the services inside the DMZ from each other and allows only the necessary communication:

- Exchange may communicate with Active Directory.
- But Exchange must not communicate with the file sharing platform.
- Exchange must not access the internal network.
- Active Directory must not contact any clients.
- An internal Active Directory is allowed to access Active Directory in the DMZ.

## 4.2 Correlation in Threat Defender

Attacks are often hard to detect as attackers hide in seemingly harmless communication to prevent detection by network security systems, such as next-generation firewalls. The only way to detect such threats is to analyze the behavior of the network to spot subtle changes in the communication. Once relationships between seemingly unrelated events are discovered, they can be analyzed further to determine if they contain any threats or abnormal behavior which may indicate that the network is under attack.

### 4.2.1 The Approach of Threat Defender

Threat Defender uses **behavior-based correlation** to analyze traffic and correlate events across multiple traffic flows. The **single-pass** correlation and policy engine correlates current traffic flows with historical information from previous flows. This means correlation takes place inline, inside the policy engine. Data is correlated in real time, i.e. the moment it is generated. Reactions to any identified threats are immediate and applied to the flow that triggered them.

Threat Defender expands the policy language to track attributes of communication events. Based on the detected behavior, granular multi-level **policy** rules can be created and dynamically executed.

To achieve meaningful behavior-based correlation, the policy and correlation engine enriches each flow with relevant information extracted from the data, such as basic layer 2-4 attributes but also information on **layer 7** protocols and applications, IPS events and **IoC/IoA** events.

The behavior-based correlation of Threat Defender is implemented using an in-memory database. This database contains **Event Tracking Tables** (page 78), which store combinations of attributes and track the properties of communication events across traffic flows and over time. The expanded policy engine queries these tables and inserts entries. The entries in event tracking tables have individual retention times that are specified by the administrator. They are removed automatically when this timeout expires. This enables event tracking tables to track changes in the behavior of assets/users over time.

Using behavior-based correlation via event tracking tables requires at least two rules:

1. One rule adds a pair of flow attributes (such as IP/MAC addresses, URLs, **IDS** hits, etc.) to the table.
2. Another rule evaluates the table:
  - A counting condition counts the number of entries with the same attribute.

- A distinct counting condition counts entries with a particular timestamp.
- Rules can also query if a specific attribute pair is contained in the table; based on the result rule actions are carried out or not.

With behavior-based correlation, Threat Defender gives you the tools to build complex scenarios of multi-staged policies to detect similar or related events in all network flows, both in real time and historically (limited to the retention time of the event tracking tables). All scenarios are evaluated for each network flow and no traffic can pass Threat Defender without being handled by the correlation engine.

### 4.2.2 Example Workflow

The following shows a simplified example workflow using behavior-based correlation:

- Threat Defender tracks the network traffic using event tracking tables. You can specify what kind of traffic will be tracked by the indicating traffic source and destination, used protocols and applications, etc.

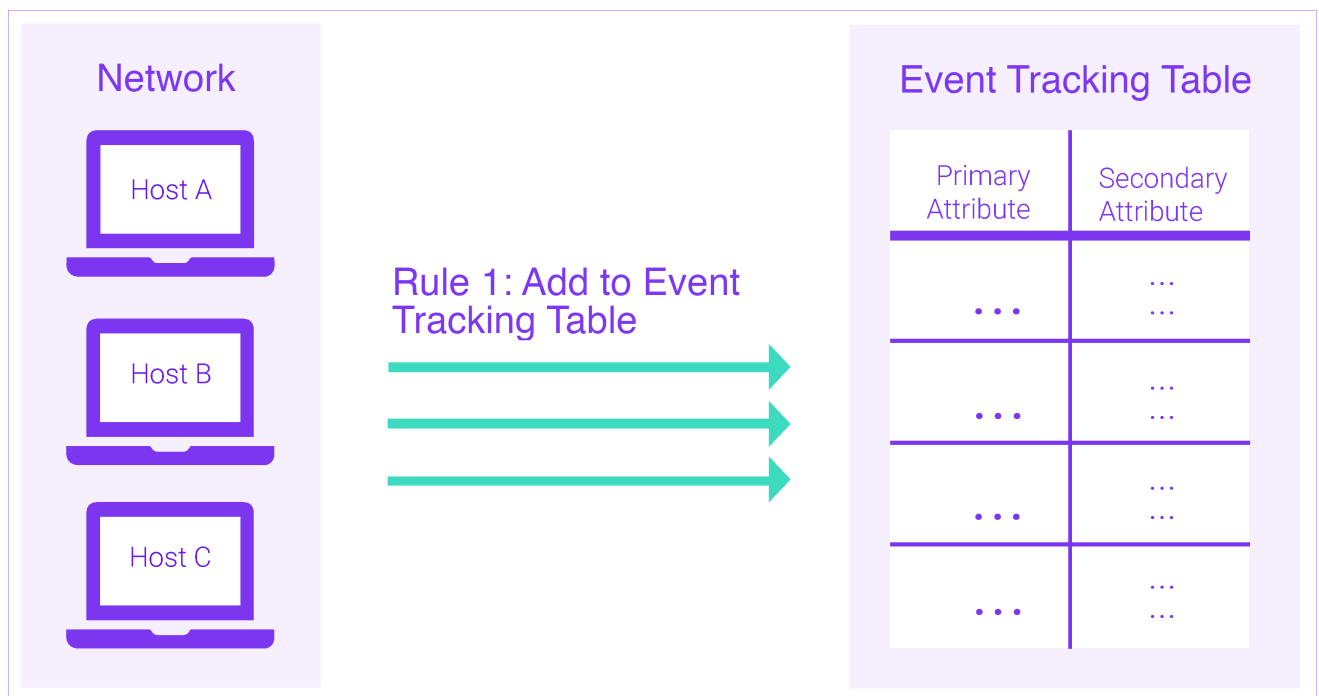


Fig. 3: Threat Defender records traffic in an event tracking table.

- Threat Defender evaluates the entries in the event tracking table by comparing traffic to the events (an event is a combination of one primary attribute and its secondary attributes) stored in the table or by counting the number of events and/or attributes.

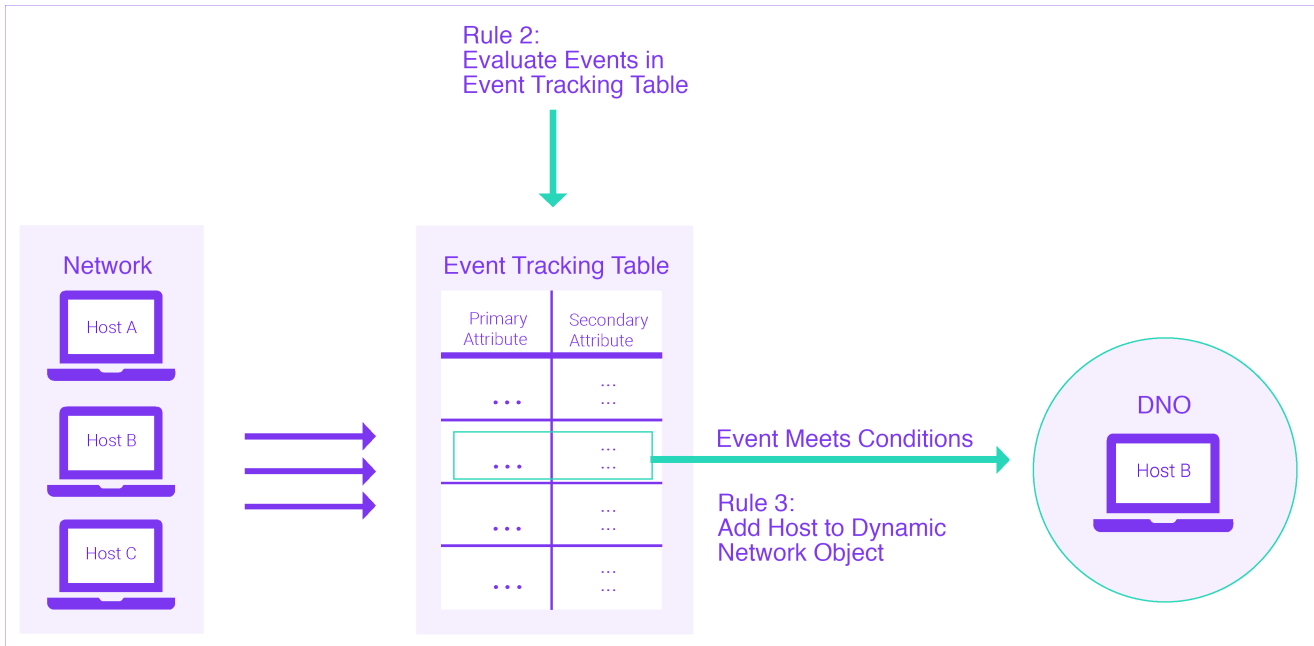


Fig. 4: Threat Defender evaluates the entries in the event tracking table. It adds any hosts that display the specified behavior to a dynamic network object.

- If Threat Defender identifies the specific behavior that is described by the correlation scenario, it performs the defined actions, such as adding the concerned hosts to a dynamic network object.

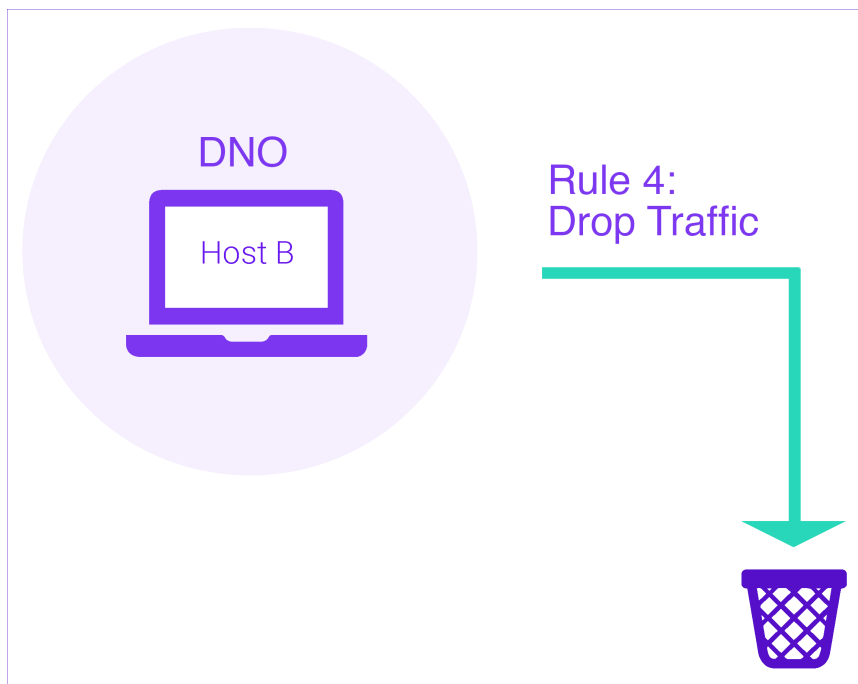


Fig. 5: Threat Defender carries out specified actions on the identified communication event.

- You can then enforce further rules on the hosts in the dynamic network object. For

example, you can block their traffic, limit their bandwidth, isolate them from the remaining network, etc.

---

**Additional References:**

- For a detailed step-by-step instruction on how to set up a correlation scenario, see [Block TCP Port Scanners \(T1046\)](#) (page 102).
- For more complex examples illustrating possible usage scenarios of correlation, see [Define the Policy](#) (page 80).
- For information on the correlation screens and settings options, see [Advanced Correlation](#) (page 153).

## 4.3 Event Tracking Tables

Event tracking tables (ETTs) are data buffers that store combinations of attributes. They track traffic properties in order to enable [Correlation in Threat Defender](#) (page 74). Rules can be applied based on whether and how often certain properties were encountered.

ETTs track pairs of attributes of communication events across multiple traffic flows. A communication event consists of a combination of one primary attribute and several secondary attributes. Rules enter these events into the event tracking tables. Every entry in an ETT has an individual timeout. Therefore, changes can be tracked over time and the entries can be automatically removed once the timeout has elapsed. Rules can query the tables to check if certain attributes are present or count the number of attributes. Based on whether the evaluation condition is met, further rules are applied to the flow.

For example, you can check how many times a certain host was added to an ETT for [TCP](#) connection ports. If it was added 100 times to the ETT within a minute, the traffic of this host is dropped. Otherwise, it may operate without restrictions. See [Block TCP Port Scanners \(T1046\)](#) (page 102) for further information. This way, attributes seen in earlier communication flows determine how later flows are handled.

Event tracking tables can track and correlate any combination of flow attribute pairs. The following attribute types are available:

- Assets
- Classification applications and/or protocols
- HTTP domain names
- HTTP URLs
- Interfaces
- IDS hits
- IP addresses
- Layer 4 ports
- MAC addresses
- None (used to track only one attribute instead of attribute pairs)
- Timestamps
- Users
- VLAN tags

The table shows useful example combinations of attributes:

Primary Attribute Type	Secondary Attribute Type	Use
IP Address	Layer 4 port	Stores a list of ports per IP address.
MAC Address	Timestamp	Counts how often a MAC address was added to an ETT.
User	HTTP URL	Shows what URLs users visited by storing a list of accessed URLs per user.
Asset	IDS Hit	Stores a list of IDS hits per asset. You can use this event tracking table to set up rules that isolate devices, which exceed a certain number of IDS hits.
User	None	This ETT tracks users. You can use it to create policy rules that are based on the behavior of users.
None	Assets	You can use this ETT to count the number of assets in your system and set up rules that are triggered if a certain value is exceeded.

---

#### Additional References:

- For step-by-step instructions on how to create an event tracking table, see [Create an Event Tracking Table](#) (page 103).
- For instructions on how to view or delete the contents of an event tracking table, see [View the Content of Event Tracking Tables](#) (page 84).
- For further information on the settings options, see [Event Tracking Tables](#) (page 160) in the interface reference.

## 4.4 Define the Policy

The policy in cognitix Threat Defender consists of global rules and [correlation](#) (page 74) scenarios.

Navigate to **Policy > Rules** to see the current policy. Global rules are placed at the top of the policy table. Rules used in correlation scenarios are grouped by scenario.

These rules and scenarios are processed from top to bottom.

cognitix Threat Defender checks for each rule if the current traffic flow meets its conditions. If yes, it carries out the specified rule actions. If not, it checks the traffic against the next rule.

**Note:** cognitix Threat Defender has a blacklisting approach to rule processing. This means if the policy contains no rules or if a specific traffic flow matches no rules, its traffic is allowed by default.

Flows are evaluated against the policy for each new packet that updates the flow. This means a traffic flow practically continues to cycle through the policy until it ceases.

The following image illustrates the policy processing of Threat Defender.



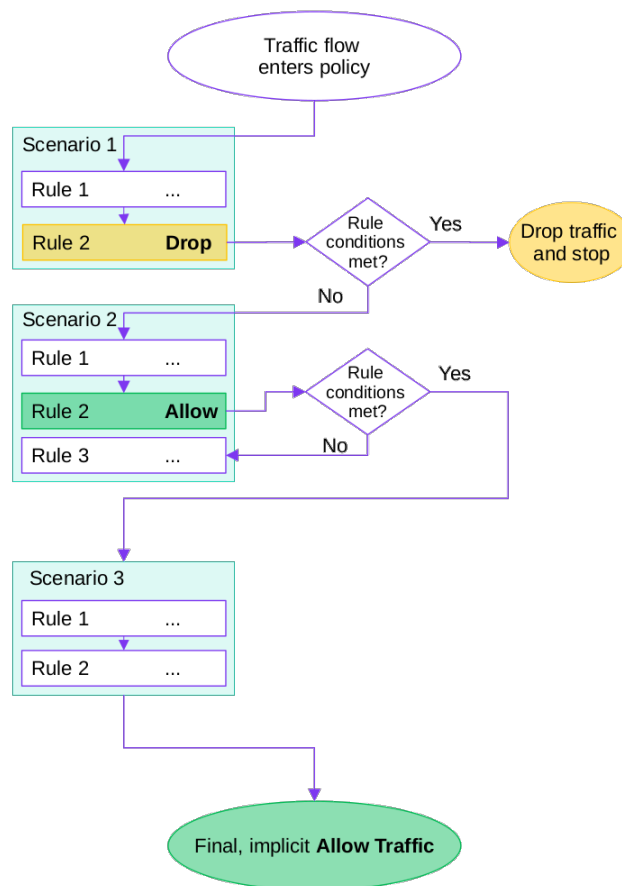


Fig. 6: Example processing sequence.

Rule actions are performed on the traffic flow, if a rule matches. When no action is selected, Threat Defender will evaluate the traffic flow against the next rule in the policy.

Final actions define how Threat Defender will continue to process the traffic flow. There are the following final rule actions:

- **Allow Traffic and Skip to Next Scenario**

Traffic matching this rule is not intercepted. This means that cognitix Threat Defender exits the current scenario for this traffic flow and continues to correlate it with the next scenario in the policy.

- **Drop Traffic and Stop Processing**

Traffic matching this rule is silently dropped, i.e. the packets are silently discarded. Rule processing for this traffic flow ceases.

- **Reject Traffic and Stop Processing**

Traffic matching this rule is actively rejected, i.e. all parties are notified by TCP reset (if possible) that the packets are discarded. Rule processing for this traffic flow ceases.

**Additional References:**

- For information on behavior-based correlation in general, see [Correlation in Threat Defender](#) (page 74).
- If you want to look up the settings options for rules and correlation scenarios, refer to [Policy](#) (page 145) in the interface reference.

## 4.5 Policy Setup Examples

The following examples illustrate how to define policy rules and scenarios.

The first two examples help you familiarize yourself with cognitix Threat Defender. They explain how to set up a global rule and how to handle an event tracking table.

The remaining examples are more complex and show how to set up correlation scenarios, including network objects and event tracking tables. They are primarily for users who are already familiar with the Threat Defender user interface.

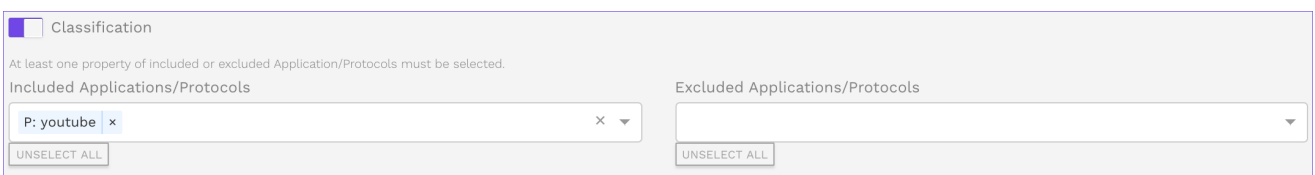
### 4.5.1 Create Global Rules

Rules manage network traffic. They can be used in specific correlation scenarios or applied globally to all network traffic.

The following example shows how to create a global rule to block YouTube traffic. For this purpose, you need to specify a rule condition and a rule action.

**Tip:** Refer to [Rules](#) (page 145) in the interface reference chapter to see what other conditions and actions are available for rules.

1. Navigate to **Policy > Rules**.
2. Click **Add Global Rule** to create a new global rule.
3. Enter general information on the rule:
  - Assign a **Name**, e.g. Block YouTube.
  - Optional: Add a **Note**.
4. Specify what traffic the rule will match:
  - In the **Source & Destination** section, set **Source Networks** and **Destination Networks** to **Any** to include all traffic sources and destinations.
  - In the **Conditions** section, narrow down the scope of the rule:
    - Enable **Classification** by clicking the toggle.
    - Under **Included Applications/Protocols**, enter `youtube` into the input field. This way, the action of this rule is only applied to YouTube traffic.



Classification

At least one property of included or excluded Application/Protocols must be selected.

Included Applications/Protocols

P: youtube x

UNSELECT ALL

Excluded Applications/Protocols

UNSELECT ALL

Fig. 7: Traffic classification by application.

5. In the **Actions** section, specify how traffic that matches the rule will be handled:
  - Enable **Final Action** by clicking the toggle.
  - Select **Reject Traffic and Stop Processing**.

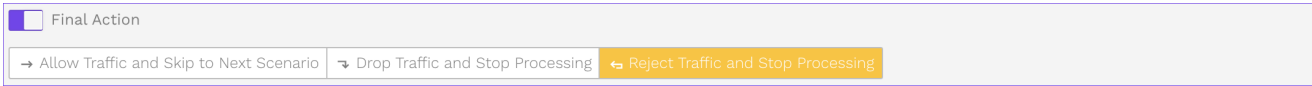


Fig. 8: Reject matching traffic.

6. Click **SAVE** to store this rule.
7. Click the **APPLY CHANGES** button at the top of the main navigation to activate your configuration changes.

When this rule is enabled, Threat Defender rejects all YouTube traffic.

**Note:** The difference between the “Drop” and “Reject” rule action is that dropping traffic does not take the sender into account. Dropping therefore silently discards the packets. Reject, however, notifies all parties by sending a **TCP reset** (if possible) that the packets are discarded.

---

#### Additional References:

For further information on the settings options, see [Rules](#) (page 145).

### 4.5.2 View the Content of Event Tracking Tables

**Note:** [Event Tracking Tables](#) (page 78) can only be used within [correlation scenarios](#) (page 74). You can add a new event tracking table only while setting up a scenario.

Under **Policy > Event Tracking Tables**, you see an overview of the existing tables in active correlation scenarios.

Here, you can click on the number in the **Counts** column to see the content of the respective event tracking table.


Name	Note	Timeout (in Secon...	Primary Attribute	Secondary Attribute	Counts
<b>Port scan protection</b> ^					
Ports per host		300	IP Address - max. count 10000	Layer 4 port - max. count 76	24 
<b>Threat Intelligence Logging Severity</b> ^					
No entries added yet.					

Fig. 9: Overview of event tracking tables in correlation scenarios.

A content view opens. Note that the maximum number of displayed entries is 64.

## Ports per host

Glimpse information

Inserted At	Recent	Primary	Secondary
2021-09-21 - 09:59	true	vlan(301)/i	5353
2021-09-21 - 09:59	true	vlan(301)/	5353
2021-09-21 - 09:58	true	vlan(301)/	1900
2021-09-21 - 09:58	true	vlan(301)/	137
2021-09-21 - 09:58	true	vlan(301)/	57621
2021-09-21 - 09:59	true	vlan(302)/	443
2021-09-21 - 09:57	true	vlan(302)/	8007

Fig. 10: Content of an event tracking table that records layer 4 ports per IP address.

If you want to delete the content of the event tracking table, click **RESET STATE** in this view.

#### Additional References:

- For general information on the concept of event tracking tables, see [Event Tracking Tables](#) (page 78).
- For step-by-step instructions on how to create an event tracking table, see [Create an Event Tracking Table](#) (page 103).
- For further information on the settings options, see [Event Tracking Tables](#) (page 160).

### 4.5.3 Restrict Access to Certain Websites

You can set up Threat Defender to restrict access to certain websites for a certain time. The following examples illustrate how to implement these access restrictions based on the behavior of assets or users.

Restricting website access for certain assets is useful if you do not track users in your network.

Restricting access for users is independent of the devices used. This means the restrictions will remain in place if the respective user switches to another computer or a mobile phone, for example.

#### 4.5.3.1 Restrict YouTube Access Based on Asset Behavior

You can set up Threat Defender to restrict access to certain websites for a certain time. This example shows how to use the following concepts:

- [Behavior-based correlation](#) for assets
- Dynamic network objects
- Schedules

#### Objective

Outside office hours, YouTube access is permitted without restrictions. During office hours, however, YouTube access is restricted to 5 minutes. Afterwards, YouTube is blocked for an hour.

In this example, the restriction is implemented by tracking the behavior of assets. This means if a new user logs in on a device that is blocked for Youtube, this new user will also be blocked for YouTube until the blocking period expires. If you want to see how to restrict access for specific users independently of the devices they use, refer to [Restrict YouTube Access Based on User Behavior](#) (page 90).

To implement this, you need to set up a correlation scenario with two dynamic network objects and a dedicated rule set.

**Tip:** To define the office hours, the predefined `Office hours` schedule is used in this example. You can modify this schedule to your needs under **Policy > Schedules**.

#### Create the Correlation Scenario

First, navigate to **Policy > Advanced Correlation**. Set up a new correlation scenario that will contain the rules and dynamic network objects.

## Create the Dynamic Network Objects

In the correlation scenario, open the **Dynamic Network Objects** tab. Create two dynamic network objects. One stores assets for 5 minutes, the other stores assets for one hour. This way, two lists with assets accessing YouTube are created.

The following table shows the required settings of the dynamic network objects:

Name	Network	Size	Timeout
5 min list	Internal	1000	300
1 hour list	Internal	1000	3600

For detailed instructions on how to create a dynamic network object in a correlation scenario, refer to [Create a Dynamic Network Object](#) (page 105).

## Create the Rule Set

Set up a rule set of six rules in the correlation scenario:

- **Rule 1** allows all traffic except YouTube.
- **Rule 2** allows YouTube access for assets on the five minutes list during office hours.
- **Rule 3** rejects YouTube access for assets on the one hour list during office hours.
- **Rule 4** adds assets to the five minutes list if they started a new YouTube connection and were neither on the five minutes nor on the one hour list.
- **Rule 5** adds assets generating YouTube traffic to the one hour list.
- **Rule 6** allows all YouTube traffic. Since it is at the bottom of the rules table, it is processed last. Inside office hours, this rule is only applied to assets that meet the following conditions:
  - They did not use YouTube in the past hour.
  - They are new on the 5 minutes list.
  - They are new on the 1 hour list.

The following table shows the required rule settings:

Rule	Schedule	Source	Destination	Condition	Actions
1.		Any	Any	Classification Excluded Applications/ Protocols: youtube	Final Action: Allow Traffic and Skip to Next Scenario
2.	Include Office hours	5 min list	Any	Classification Included Applications/ Protocols: youtube	Final Action: Allow Traffic and Skip to Next Scenario
3.	Include Office hours	1 hour list	Any	Classification Included Applications/ Protocols: youtube	Final Action: Reject Traffic and Stop Processing
4.	Include Office hours	Any	Any	Classification Included Applications/ Protocols: youtube	Dynamic Network Object Operation: Add Host Identifier: Asset Who: Client Target Dynamic Network Object: 5 min list

continues on next page



Table 1 – continued from previous page

Rule	Schedule	Source	Destination	Condition	Actions
5.	Include Office hours	Any	Any	Classi- fication Included Ap- plications/ Protocols: youtube	Dynamic Network Object Op- eration: Add Host Identifier: Asset Who: Client Tar- get Dynamic Network Object: 1 hour list
6.		Any	Any	Classi- fication Included Ap- plications/ Protocols: youtube	Final Action: Allow Traffic and Skip to Next Scenario

For detailed instructions on how to create a rule in a correlation scenario, refer to [Create Rules in a Correlation Scenario](#) (page 105).

Click the **APPLY CHANGES** button at the top of the main navigation to activate your configuration changes.

## Result

The system processes the specified rule set in a top-down approach.

Inside office hours this means:

1. The system allows all traffic but YouTube.
2. For YouTube traffic, the system checks if the requesting asset is in any of the dynamic network objects.
  - If yes, it carries out the respective action.
  - If no, it adds the asset to the dynamic network objects and proceeds to the last rule, i.e. allows YouTube access.

Outside office hours this means:

1. The system allows all traffic but YouTube.
2. The system allows YouTube traffic (rules 2 to 5 only apply during office hours).

#### 4.5.3.2 Restrict YouTube Access Based on User Behavior

You can set up Threat Defender to restrict access to certain websites for a certain time.

This example shows how to use the following concepts:

- [Behavior-based correlation](#) for users
- Event tracking tables

#### Objective

YouTube access is restricted to 5 minutes. Afterwards, YouTube is blocked for an hour.

In this example, the restriction is based on the behavior of users independently of the devices they use. If you do not track users and want to see how to restrict access based on devices, refer to [Restrict YouTube Access Based on Asset Behavior](#) (page 86).

To implement this, you need to set up a correlation scenario with two event tracking tables and a dedicated rule set.

#### Create the Correlation Scenario

First, navigate to **Policy > Advanced Correlation**. Set up a new correlation scenario that will contain the rules and event tracking tables.

#### Create the Event Tracking Tables

In the correlation scenario, open the **Event Tracking Tables** tab. Create two event tracking tables. One stores users for 5 minutes, the other stores users for one hour. This way, two lists with YouTube users are created.

Event tracking tables track the users. Since you only want to track the primary attribute, i.e. the `User`, select `None` as secondary attribute. This is important as Threat Defender would compare the attribute pairs if a secondary attribute was selected. In that case, the rules would not match.

The following table shows the required settings of the event tracking tables:

Name	Retention Time	Primary Attribute Type	Max. No. Primary	Secondary Attribute Type	Max. No. Secondary per Primary
1 hour users	3600	User	100	None	1
5 min users	300	User	100	None	1

**Note:** Under **Maximum Number of Primary Attributes**, make sure that both tables are large enough to fit the number of users in your network.

For detailed instructions on how to create an event tracking table, refer to [Create an Event Tracking Table](#) (page 103).

### Create the Rule Set

Set up a rule set of five rules in the correlation scenario:

- **Rule 1** allows all traffic except YouTube.
- **Rule 2** allows YouTube access for users on the five minutes list.
- **Rule 3** rejects YouTube access for users on the one hour list.
- **Rule 4** adds users to the five minutes list who started a new YouTube connection.
- **Rule 5** adds users generating YouTube traffic to the one hour list.

The following table shows the required rule settings:

Rule	Source	Destination	Condition	Actions
1.	Any	Any	Classification Excluded Applications/ Protocols: youtube	Final Action: Allow Traffic and Skip to Next Scenario

continues on next page

Table 2 – continued from previous page

Rule	Source	Destination	Condition	Actions
2.	Any	Any	<b>Classification</b> Included Applications/ Protocols: youtube Advanced Correlation Condition: <b>Event in Event Tracking Table</b> Event Tracking Table: 5 min users	<b>Final Action:</b> Allow Traffic and Skip to Next Scenario
3.	Any	Any	<b>Classification</b> Included Applications/ Protocols: youtube Advanced Correlation Condition: <b>Event in Event Tracking Table</b> Event Tracking Table: 1 hour users	<b>Final Action:</b> Reject Traffic and Stop Processing
4.	Any	Any	<b>Classification</b> Included Applications/ Protocols: youtube	<b>Add to Event Tracking Table</b> Event Tracking Table: 5 min users Primary Attribute: User Secondary Attribute: None

continues on next page

Table 2 – continued from previous page

Rule	Source	Destination	Condition	Actions
5.	Any	Any	Classification Included Applications/ Protocols: youtube	Add to Event Tracking Table Event Tracking Table: 1 hour users Primary Attribute: User Secondary Attribute: None

For detailed instructions on how to create a rule in a correlation scenario, refer to [Create Rules in a Correlation Scenario](#) (page 105).

Click the **APPLY CHANGES** button at the top of the main navigation to activate your configuration changes.

## Result

The system processes the specified rule set in a top-down approach:

1. The system allows all traffic but YouTube.
2. For YouTube traffic the system checks if the requesting user is in any of the event tracking tables:
  - If the user is on the 5 min users list, Threat Defender allows YouTube access and skips to the next correlation scenario.
  - If the user is not on the 5 min users list but on the 1 hour users list, Threat Defender rejects YouTube access and skips to the next correlation scenario.
  - If the user is on none of the two lists, Threat Defender adds the user to both event tracking tables.

## 4.6 Detect Threats

The following chapters are intended to give you some ideas on how you can detect threats to your network using cognitix Threat Defender.

**Tip:** A freshly installed Threat Defender comes with several preset behavior-based correlation scenarios, static network objects, etc. for various use cases that you can enable or adapt to your requirements.

### 4.6.1 Deploy cognitix Threat Defender as an IDS at the Network Perimeter

The following setup illustrates how cognitix Threat Defender can be deployed as an IDS at the network perimeter. In this setup, it extends a high availability P-A-P stack consisting of genugates and genuscreens.

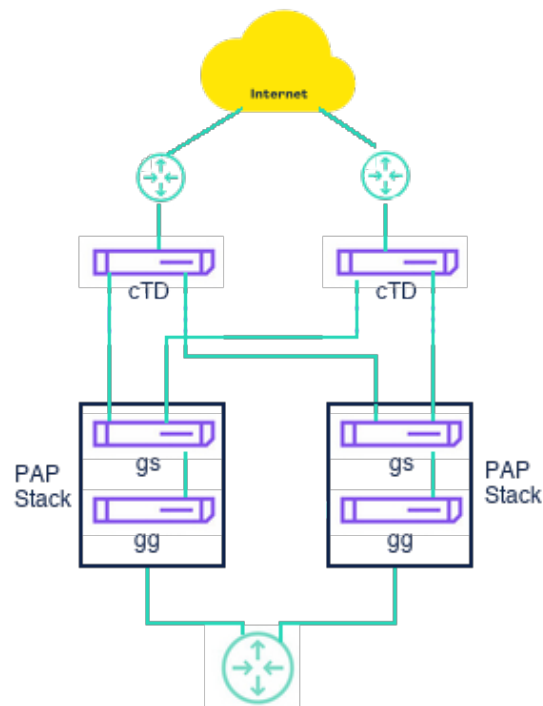


Fig. 11: cognitix Threat Defender used as an IDS at the network perimeter.

**Tip:** The P-A-P concept is recommended by the BSI (German Federal Office for Security in Information Technology). A packet filter, an application level gateway, and a second packet filter are combined so that all traffic has to pass through all three components. This type of 3-tier firewall architecture is used primarily to separate two networks that differ significantly in terms of trust level, e.g. to separate the internet from an intranet.

In this setup, cognitix Threat Defender is connected to the network-facing switch, for example via mirror port. This places it at the perimeter between the external network and the first packet filter. Here, Threat Defender can see and analyze all incoming external traffic as well as all outgoing traffic.

To ensure high availability, each Threat Defender is connected to the genuscreen appliances in both legs of the P-A-P. This way, traffic information is shared between the two instances of Threat Defender. This avoids loss of information in case one component fails and the active P-A-P leg is switched.

Used as a perimeter IDS, cognitix Threat Defender complements the P-A-P system in the following ways:

- Analysis of tunneled and encrypted communication.
- Additional monitoring of services that cannot be sufficiently controlled, such as protocols for which application gateways are not available.
- Detection and monitoring of external access that is not routed through the firewall e.g. via modems.
- Threat Defender can also be used to check whether the firewall is working according to its specifications.

cognitix Threat Defender compares the network traffic to a bundle of IDS/IPS feeds from multiple sources (see [Intelligence Database](#) (page 180)). If a threat indicator is discovered, the policy engine can be used to log the event and/or intercept the concerned traffic.

Under **Threats > Incident Logs** the detected IDS hits are shown over time and by severity. You can filter the incident logs and create PDF reports see [Incident Logs](#) (page 179).

By creating custom IPS rule sets, you can control in detail what traffic is to be logged and/or blocked. See [IPS Settings](#) (page 184).

This setup can quickly be adapted to actively integrate cognitix Threat Defender and use it as an IPS. The only required change is that cognitix Threat Defender cannot be connected to a mirror port but has to be able to intercept the traffic and enforce the policy.

## 4.6.2 Detect ARP Spoofing Attacks

### 4.6.2.1 Objective

Threat Defender can be set up to detect ARP spoofing inside the network and block the ARP spoofing device.

Attackers may use manipulated address resolution protocol (ARP) messages to redirect traffic to another device, e.g. the attackers' computer. The attacker's MAC address is linked to the IP addresses of legitimate devices in the network. Attackers can then log or manipulate the redirected data. For example, they can see what domains the victim requests or replace a download file with a trojan.

ARP spoofing attacks can be detected by monitoring the relations between IP and MAC addresses. An IP address can only be related to one MAC address at a time. If an IP address frequently changes its MAC address relation in a short time, an ARP spoofing attack may be underway. If multiple IP addresses change their MAC address relations to the same MAC address, an ARP spoofing attack is very likely.

Threat Defender can detect this behavior and interrupt the ARP spoofing attack using two event tracking tables and a dynamic network object.

### 4.6.2.2 Create a Correlation Scenario

First, navigate to **Policy > Advanced Correlation**. Create a correlation scenario that provides the framework for the required event tracking tables, dynamic network object and rule set.

### 4.6.2.3 Create the Event Tracking Tables

In the correlation scenario, open the **Event Tracking Tables** tab. Create two event tracking tables. One table stores MAC addresses per IP address, the other table stores IP addresses per MAC address.

The following table shows the required settings of the event tracking tables:



Name	Retention Time	Primary Attribute Type	Max. No. Primary	Secondary Attribute Type	Max. No. Secondary per Primary
ETT 1 - MACs per IP	3600	IP Address	5000	MAC Address	500
ETT 2 - IPs per MAC	3600	MAC Address	5000	IP Address	500

**Note:** Under **Maximum Number of Primary Attributes**, make sure that both tables are large enough to fit your network.

For detailed instructions on how to create an event tracking table, refer to [Create an Event Tracking Table](#) (page 103).

#### 4.6.2.4 Create a Dynamic Network Object

Create a dynamic network object in the correlation scenario. It stores the MAC addresses of the suspected ARP spoofing devices.

The following table shows the required settings of the dynamic network object:

Name	Network	Size	Timeout
ARP spoofing devices	External	100	0

For detailed instructions on how to create a dynamic network object in a correlation scenario, refer to [Create a Dynamic Network Object](#) (page 105).

**Tip:** A timeout of 0 means that the entries are not removed automatically.

**Note:** If your network contains special configurations, such as a computer with two network cards in the same **subnet**, define exceptions for these devices by excluding their MAC addresses in the dynamic network object.

#### 4.6.2.5 Create the Rule Set

To monitor IP/MAC address relations and drop traffic from possible attackers, the following four rules are needed in the correlation scenario:

- **Rule 1** silently drops all traffic from devices stored in the ARP spoofing devices network object. This way, identified ARP spoofing devices are blocked.
- **Rule 2** enters all client IP and MAC addresses into the ETT 1 - MACs per IP event tracking table.
- **Rule 3** counts the entries in the ETT 1 - MACs per IP event tracking table. If a client IP has more than two MAC addresses, this indicates that an ARP spoofing attack may be underway. All clients with more than one entry are then added to the ETT 2 - IPs per MAC event tracking table.
- **Rule 4** counts the entries in the ETT 2 - IPs per MAC event tracking table to identify which device is the originator of the ARP spoofing attack. If a MAC address has more than two IP addresses, it is added to the ARP spoofing devices dynamic network object. This way, the source of the ARP spoofing attack is identified and isolated.

The following table shows the required rule settings:

Rule	Source	Destination	Condition	Actions
1.	ARP spoofing devices	Any		<b>Final Action:</b> Drop Traffic and Stop Processing
2.	Any	Any		<b>Add to Event Tracking Table</b> Event Tracking Table: ETT 1 - MACs per IP Primary Attribute: Client Address Secondary Attribute: Client MAC Address

continues on next page

Table 3 – continued from previous page

Rule	Source	Destination	Condition	Actions
3.	Any	Any	Advanced Correlation Condition: Number of Similar Events in Event Tracking Table Event Tracking Table: ETT 1 - MACs per IP Count entries equal to: Client Address Minimum number of entries: 2	Add to Event Tracking Table Event Tracking Table: ETT 2 - IPs per MAC Primary Attribute: Client MAC Address Secondary Attribute: Client Address
4.	Any	Any	Advanced Correlation Condition: Number of Similar Events in Event Tracking Table Event Tracking Table: ETT - IPs per MAC Count entries equal to: Client MAC Address Minimum number of entries: 3	Dynamic Network Object Operation: Add Host Identifier: MAC Address Who: Client Target Dynamic Network Object: ARP spoofing devices

For detailed instructions on how to create a rule in a correlation scenario, refer to [Create Rules in a Correlation Scenario](#) (page 105).

Click the **APPLY CHANGES** button at the top of the main navigation to activate your configuration changes.

#### 4.6.2.6 Result

Threat Defender monitors the IP/MAC address relations of all devices in the network. If it detects client IP addresses that are assigned more than two MAC addresses, this indicates that an ARP spoofing attack may be underway. There may be other reasons for this behavior, however.

ETT 1 - IPs per MAC (Enabled)		
<input type="button" value="RESET STATE"/>		
Primary Attribute	Secondary Attribute	
10.10.10.148	F4:4D:30:67:8F:A6	Mar 22, 2018 - 10:48 AM
10.10.0.109	F4:4D:30:67:8F:A6 B8:AE:ED:78:D3:64	Mar 22, 2018 - 10:45 AM Mar 22, 2018 - 10:48 AM
10.10.0.185	F4:4D:30:67:8F:A6 00:24:67:30:DD:13	Mar 22, 2018 - 10:45 AM Mar 22, 2018 - 10:48 AM
10.10.0.174	B8:AE:ED:7F:46:B9	Mar 22, 2018 - 10:48 AM
10.10.0.156	F4:4D:30:67:8F:A6 B8:AE:ED:EB:6C:7C	Mar 22, 2018 - 10:45 AM Mar 22, 2018 - 10:48 AM
192.168.0.1	D4:6E:0E:6D:4E:EA	Mar 22, 2018 - 10:48 AM
10.10.10.180	F4:4D:30:67:8F:A6 B8:AE:ED:78:D1:08	Mar 22, 2018 - 10:45 AM Mar 22, 2018 - 10:48 AM
fe80::baae:edff:fe78:d108	B8:AE:ED:78:D1:08	Mar 22, 2018 - 10:48 AM
fe80::ec4:7aff:fedd:5851	0C:C4:7A:DD:58:51	Mar 22, 2018 - 10:48 AM
10.10.10.145	F4:4D:30:6E:50:3E F4:4D:30:67:8F:A6	Mar 22, 2018 - 10:48 AM Mar 22, 2018 - 10:45 AM
fe80::f64d:30ff:fe6e:503e	F4:4D:30:6E:50:3E	Mar 22, 2018 - 10:48 AM
10.10.0.184	F4:4D:30:67:8F:A6 8C:85:90:82:81:BD	Mar 22, 2018 - 10:45 AM Mar 22, 2018 - 10:48 AM
10.10.111.112	F4:4D:30:6E:4F:33 F4:4D:30:67:8F:A6	Mar 22, 2018 - 10:48 AM Mar 22, 2018 - 10:45 AM
10.10.10.125	F4:4D:30:67:8F:A6 F4:4D:30:67:69:2A	Mar 22, 2018 - 10:45 AM Mar 22, 2018 - 10:48 AM
10.10.10.142	F4:4D:30:67:8F:A6 98:01:A7:A3:24:07	Mar 22, 2018 - 10:45 AM Mar 22, 2018 - 10:47 AM
fe80::f2de:f1ff:fe76:6182	F0:DE:F1:76:61:82	Mar 22, 2018 - 10:47 AM

Fig. 12: Content of ETT 1, indicating that an ARP spoofing attack is underway.

To confirm if an ARP spoofing attack is being carried out, Threat Defender cross-checks the MAC/IP address relations. If multiple IP addresses are related to the same MAC address, this confirms that an ARP spoofing attack is indeed underway.

ETT 2 - Macs per IP (Enabled)

Primary Attribute	Secondary Attribute	
38:C9:86:3F:38:5D	10.10.10.177	Mar 22, 2018 - 10:49 AM
00:28:F8:73:BC:25	10.10.10.146	Mar 22, 2018 - 10:49 AM
98:01:A7:B6:45:9D	10.10.10.186	Mar 22, 2018 - 10:48 AM
A4:D1:8C:CE:7A:66	10.10.10.199	Mar 22, 2018 - 10:48 AM
98:01:A7:A3:24:07	10.10.10.142	Mar 22, 2018 - 10:48 AM
70:56:81:C4:27:A3	10.10.10.193	Mar 22, 2018 - 10:48 AM
F4:4D:30:6E:50:3E	10.10.10.145	Mar 22, 2018 - 10:48 AM
B8:AE:ED:78:D1:08	10.10.10.180	Mar 22, 2018 - 10:48 AM
80:FA:5B:43:56:F4	10.10.10.152	Mar 22, 2018 - 10:48 AM
B8:AE:ED:78:D3:64	10.10.0.109	Mar 22, 2018 - 10:48 AM
F4:4D:30:67:69:2A	10.10.10.125	Mar 22, 2018 - 10:48 AM
F4:4D:30:6E:4F:33	10.10.111.112	Mar 22, 2018 - 10:48 AM
00:17:C8:26:21:20	10.10.0.202	Mar 22, 2018 - 10:48 AM
8C:85:90:84:17:7D	10.10.0.186	Mar 22, 2018 - 10:48 AM
00:10:74:33:13:2F	10.10.200.60	Mar 22, 2018 - 10:48 AM
78:7B:8A:AC:8E:F8	10.10.0.125	Mar 22, 2018 - 10:48 AM
B8:AE:ED:7B:AB:1F	10.10.10.196	Mar 22, 2018 - 10:48 AM
B8:AE:ED:78:D3:D3	10.10.0.242	Mar 22, 2018 - 10:48 AM
3C:F8:62:33:EB:B3	10.10.10.169	Mar 22, 2018 - 10:48 AM
F0:DE:F1:76:61:82	10.10.10.147	Mar 22, 2018 - 10:48 AM
B8:AE:ED:78:DA:A5	10.10.0.195	Mar 22, 2018 - 10:48 AM
B8:AE:ED:EB:6C:7C	10.10.0.156	Mar 22, 2018 - 10:48 AM
00:24:67:30:DD:13	10.10.0.185	Mar 22, 2018 - 10:48 AM
8C:85:90:82:81:BD	10.10.0.184	Mar 22, 2018 - 10:48 AM
F4:4D:30:67:8F:A6	10.10.10.145	Mar 22, 2018 - 10:45 AM
	10.10.111.112	Mar 22, 2018 - 10:45 AM
	10.10.10.199	Mar 22, 2018 - 10:45 AM
	10.10.10.196	Mar 22, 2018 - 10:45 AM
	10.10.0.242	Mar 22, 2018 - 10:45 AM
	10.10.0.186	Mar 22, 2018 - 10:45 AM

Fig. 13: Content of ETT 2, identifying the source of the ARP spoofing attack.

The originator of the ARP spoofing attack is identified. Threat Defender adds it to the dynamic network object to isolate it. Traffic from hosts in this network object is blocked. ARP spoofing attacks run by these hosts are stopped.

**Note:** Once the suspected ARP spoofing situation is remedied, you need to flush the content of the dynamic network object. To do so, click the **RESET STATE** button in the correlation scenario.

### 4.6.3 Detect MITRE ATT&CK Techniques

The [MITRE ATT&CK Matrix](#)<sup>17</sup> is a knowledge base for adversary tactics and techniques. **ATT&CK** is also used as a common language for threat hunters around the globe.

The following examples illustrate possibilities to detect some of the network-based techniques from the MITRE **ATT&CK** Matrix using cognitix Threat Defender.

**Tip:** For additional examples see the following:

- [Handle Newly Discovered Assets](#) (page 62) shows how the automatic discovery of assets can be used to prevent attackers from introducing their own hardware into the network ([T1200](#)<sup>18</sup>)
- Enabling the predefined DDoS protection scenario detects and blocks the **ATT&CK** technique [T1499](#)<sup>19</sup>.

<sup>18</sup> <https://attack.mitre.org/techniques/T1200/>

<sup>19</sup> <https://attack.mitre.org/techniques/T1499/>

#### 4.6.3.1 Block TCP Port Scanners (T1046)

This predefined correlation scenario detects network service scanning ([T1046](#)<sup>20</sup>).

Threat Defender uses **behavior-based correlation** to analyze traffic and correlate events across multiple traffic flows.

The following example shows how to set up a correlation scenario with Threat Defender that contains an event tracking table (**ETT**), a dynamic network object (**DNO**) and rules.

For further information on the various setting options of correlation scenarios, refer to [Advanced Correlation](#) (page 153).

**Tip:** Threat Defender provides several preset correlation scenarios that you can enable and adapt to suit your network and requirements. You will find the Port scan protection scenario under **Policy > Advanced Correlation**.

<sup>17</sup> <https://attack.mitre.org/matrices/enterprise/>

<sup>20</sup> <https://attack.mitre.org/techniques/T1046/>

## Objective

With this example setup, Threat Defender detects and blocks port scanners by dropping their connection attempts.

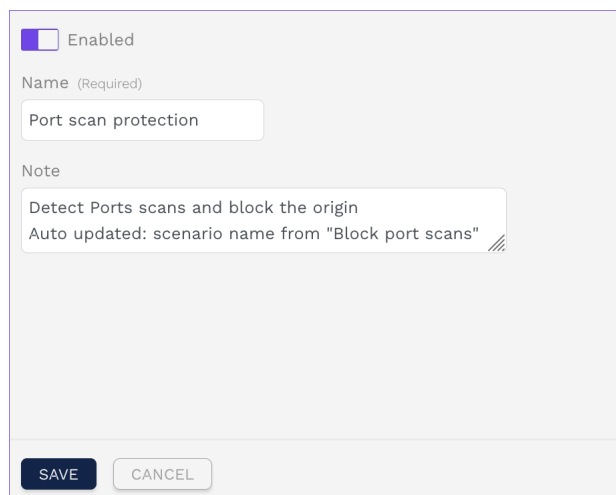
Attackers use port scans to detect vulnerable services in the network. By interrupting such a scan, an attack can be stopped in its first stage. Port scan attacks can be identified by a large number of connections to different **TCP** ports established by the same client IP. Normally, clients only connect to a small set of different server ports.

Using the Threat Defender correlation engine, you can track the destination ports of all traffic flows per client. If clients initiate more than 100 TCP connections to different ports within one minute, this behavior is classified as a port scan. To stop the port scan, traffic from these clients is dropped.

## Create an Advanced Correlation Scenario

First, create a correlation scenario that provides the framework for the required event tracking table, dynamic network object and rule set.

1. In the GUI, navigate to **Policy > Advanced Correlation**.
2. Click **Add** to create a new scenario.
3. Enter a **Name** and an optional **Note**.
4. Click **SAVE**.



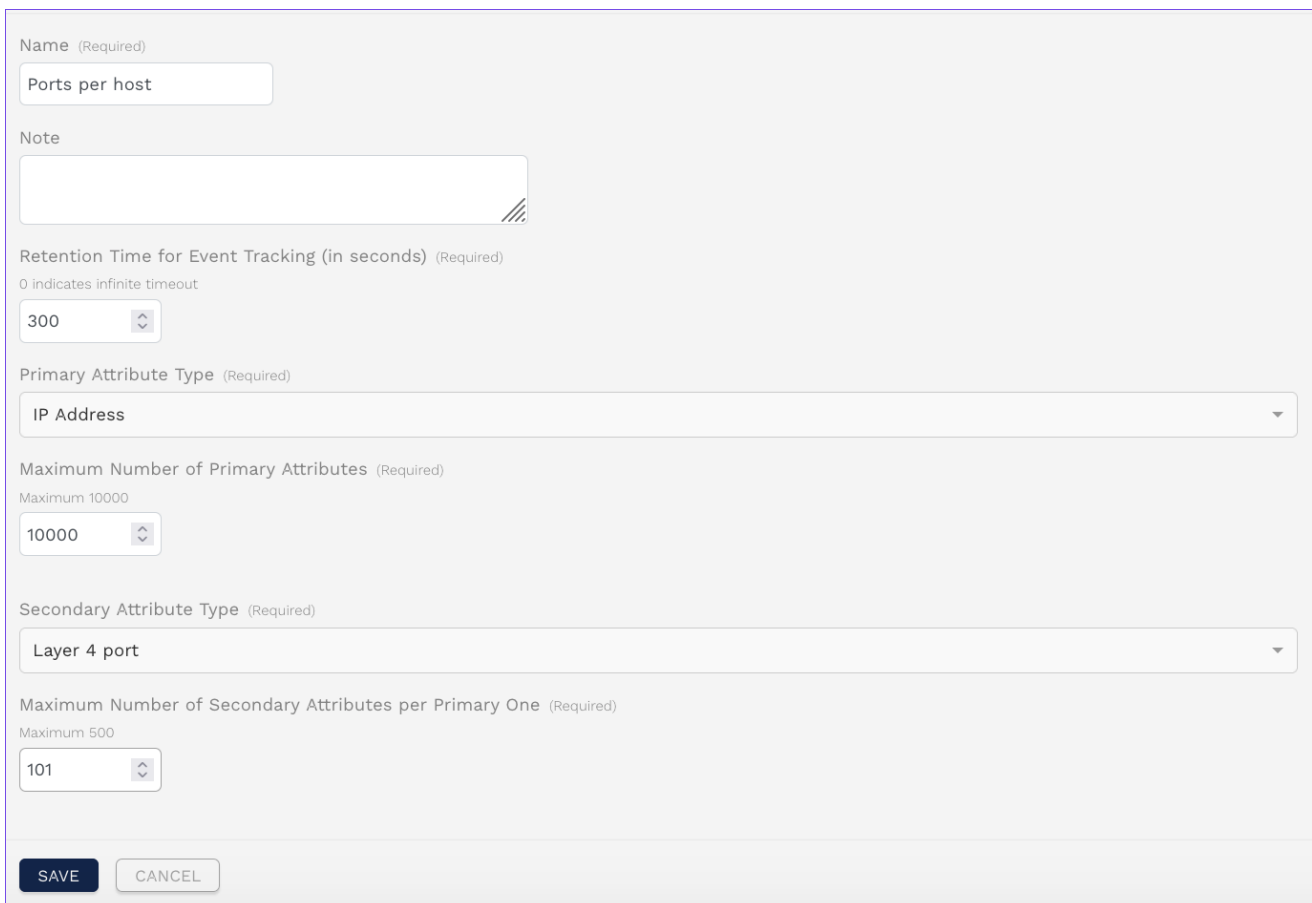
The screenshot shows a configuration dialog box for an advanced correlation scenario. At the top, there is a checkbox labeled "Enabled" which is currently unchecked. Below this is a "Name (Required)" field containing the text "Port scan protection". Underneath is a "Note" field containing the text "Detect Ports scans and block the origin" and "Auto updated: scenario name from 'Block port scans'". At the bottom of the dialog, there are two buttons: "SAVE" and "CANCEL".

Fig. 14: Basic settings of the advanced correlation scenario.

## Create an Event Tracking Table

Create an event tracking table that stores the number of contacted destination ports per source IP address.

1. In the scenario, open the **Event Tracking Tables** tab.
2. Click **Add**.
3. Assign a **Name** to the table, e.g. **Ports per host**.
4. Configure the following settings:
  - Set the **Retention Time for Event Tracking** to 300 in order to track all connections within a 300 second window.
  - Set the **Primary Attribute Type** to **IP Address**.
  - Set the **Maximum Number of Primary Attributes** to 1000.
  - Set the **Secondary Attribute Type** to **Layer 4 port**.
  - Set the **Maximum Number of Secondary Attributes per Primary One** to 101.
5. Click **SAVE**.



The screenshot shows a configuration form for an event tracking table. The form is titled "Name (Required)" and contains a text input field with the value "Ports per host". Below this is a "Note" field, which is currently empty. The next section is "Retention Time for Event Tracking (in seconds) (Required)", with a sub-note "0 indicates infinite timeout" and a dropdown menu set to "300". The "Primary Attribute Type (Required)" is a dropdown menu set to "IP Address". The "Maximum Number of Primary Attributes (Required)" section has a sub-note "Maximum 10000" and a dropdown menu set to "10000". The "Secondary Attribute Type (Required)" is a dropdown menu set to "Layer 4 port". The "Maximum Number of Secondary Attributes per Primary One (Required)" section has a sub-note "Maximum 500" and a dropdown menu set to "101". At the bottom of the form are two buttons: "SAVE" and "CANCEL".

Fig. 15: Configuration of the event tracking table.

This event tracking table tracks a maximum of 1000 IP addresses with 101 ports each. That means, the data structure may contain up to 101000 entries in total.



## Create a Dynamic Network Object

Create a dynamic network object in the advanced correlation scenario. It collects the IP addresses of all hosts that have more than 100 port entries in the event tracking table, i.e. contact more than 100 ports per minute.

1. In the correlation scenario, open the **Dynamic Network Objects** tab.
2. Click **Add**.
3. Assign a **Name**, e.g. `Port scanner hosts`.
4. Configure the following settings:
  - Under **Network**, select **External**.
  - Set the **Size** to 100.
  - Set the **Timeout** to 300.

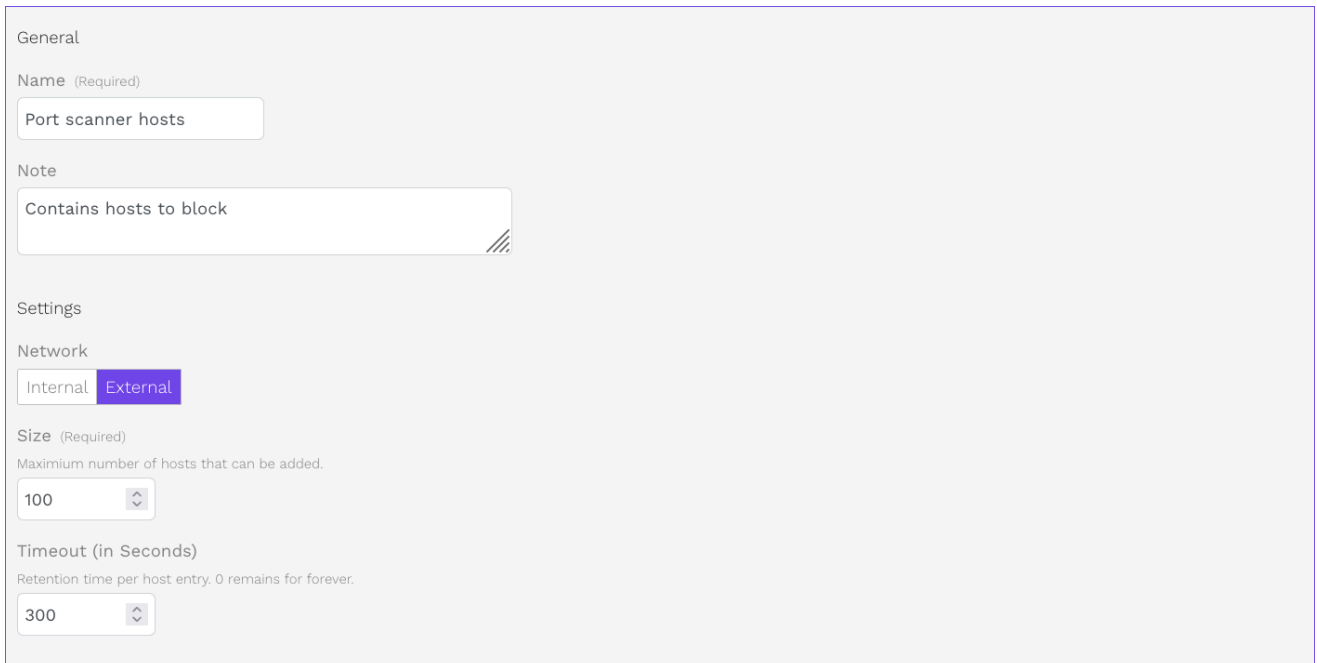


Fig. 16: Configuration of the dynamic network object.

5. Click **SAVE** to store the dynamic network object.

## Create Rules in a Correlation Scenario

To evaluate the traffic, the following three rules are needed in this correlation scenario:

- **Rule 1** rejects the traffic from IPs stored in the dynamic network object.
- **Rule 2** enters the combinations of source IP and destination port of all clients into the event tracking table.

- **Rule 3** counts the port entries stored in the event tracking table for each client IP. If a client IP has more than 100 port entries, i.e. connections to ports, it is added to the dynamic network object.

To set up a rule in the correlation scenario, proceed as follows:

1. In the correlation scenario, open the **Rules** tab.
2. Click **Add** to create a new rule for the scenario.
3. Assign a **Name**.
4. Optional: Add a **Note**.
5. Configure the following settings:
  - In the **Source & Destination** section, set **Source Networks** to `D: Port Scanner Hosts`.
  - Set **Destination Networks** to `Any`.
  - In the **Actions** section, set **Final Action** to **Reject Traffic and Stop Processing**.
6. Click **SAVE** to store this rule.

Create the remaining two rules in a similar fashion.

The following table shows the required settings for all three rules:

Rule	Source	Destination	Condition	Actions
1.	D: Port Scanner Hosts	Any		<b>Final Action:</b> Reject Traffic and Stop Processing
2.	Any	Any		<b>Add to Event Tracking Table</b> Event Tracking Table: Ports per host Primary Attribute: Client Address Secondary Attribute Server Layer 4 port

continues on next page

Table 4 – continued from previous page

Rule	Source	Destination	Condition	Actions
2.	Any	Any	Advanced Correlation Condition: Number of Similar Events in Event Tracking Table Event Tracking Table: Ports per host Count entries equal to: Client Address Minimum number of entries: 40	Dynamic Network Object Operation: Add Host Identifier: IP Address Who: Client Target Dynamic Network Object: D: Port Scanner Hosts

Click the **APPLY CHANGES** button at the top of the main navigation to activate your configuration changes.

### Result

Traffic from all hosts that establish 100 or more TCP connections to different ports per minute is dropped for 5 minutes. Port scans performed by these hosts are stopped. When the timeout expires, the hosts are automatically removed from the dynamic network object and may establish new connections with the network.

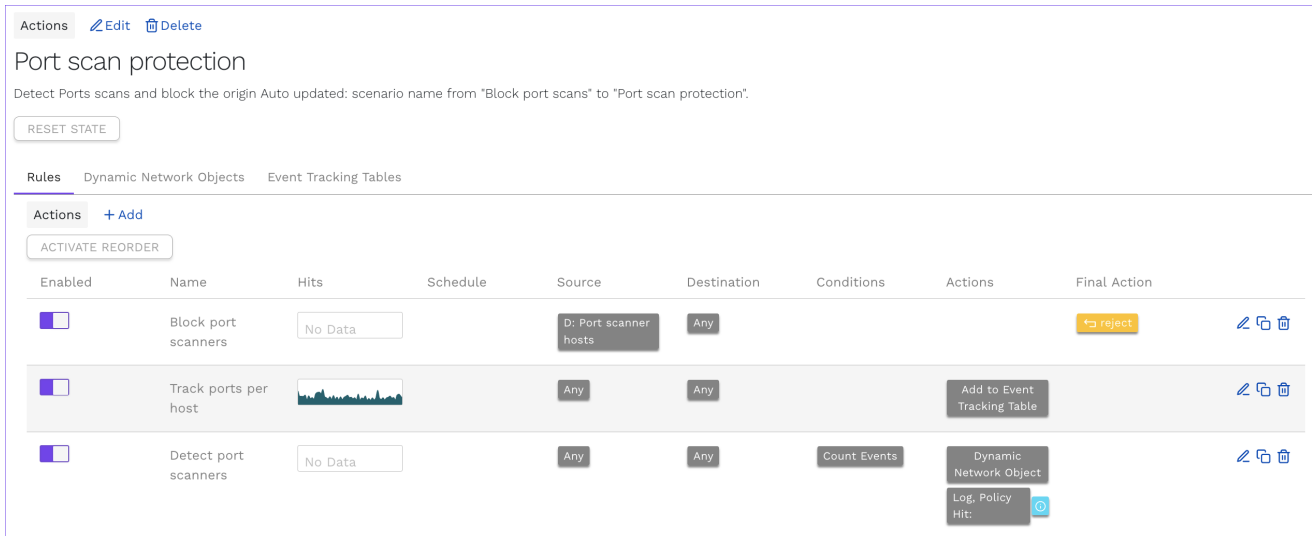


Fig. 17: Rule set of the correlation scenario.

#### Additional References:

- For further information on the settings options for correlation scenarios, see [Advanced Correlation](#) (page 153).
- For further information on the settings options for event tracking tables, see [Event Tracking Tables](#) (page 160).
- For further information on the settings options for dynamic network objects, see [Dynamic Network Objects](#) (page 156).
- For further information on the settings options for rules, see [Rules](#) (page 145).

#### 4.6.3.2 Detect SSH Brute Force (T1110)

##### Objective

Attackers may gain credential access by using brute force techniques ([T1110<sup>21</sup>](#)). If these techniques are used via the network, Threat Defender can detect and block them.

Using event tracking tables and dynamic network segmentation, all SSH connections inside an internal company network are tracked and brute force attempts are detected. The access to internal resources of suspected brute force attackers is blocked.

##### Create a Correlation Scenario

First, navigate to **Policy > Advanced Correlation**. Create a correlation scenario that provides the framework for the required event tracking tables, dynamic network object and rule set.

<sup>21</sup> <https://attack.mitre.org/techniques/T1110/>

## Create the Event Tracking Tables

In the correlation scenario, open the **Event Tracking Tables** tab. Create an event tracking table that stores source ports per IP address.

The following table shows the required settings of the event tracking table:

Name	Retention Time	Primary Attribute Type	Max. No. Primary	Secondary Attribute Type	Max. No. Secondary Primary	Sec-per
ETT SSH - Ports per IP	10	IP Address	5000	Source Port	100	

**Note:** Under **Maximum Number of Primary Attributes**, make sure that the table is large enough to fit your network.

For detailed instructions on how to create an event tracking table, refer to [Create an Event Tracking Table](#) (page 103).

## Create the Dynamic Network Object

Create a dynamic network object in the correlation scenario that stores the SSH brute forcing clients.

The following table shows the required settings of the dynamic network object:

Name	Network	Size	Timeout
SSH Brute Forcers	External	10000	0

For detailed instructions on how to create a dynamic network object in a correlation scenario, refer to [Create a Dynamic Network Object](#) (page 105).

**Note:** Make sure that the size of the dynamic network object is large enough to store all device entries.

**Tip:** A timeout of 0 means that the entries are not removed automatically.

### Create the Rule Set

To monitor SSH connections and drop traffic from possible attackers, the following three rules are needed in the correlation scenario:

- **Rule 1** silently drops all traffic from devices stored in the SSH Brute Forcers network object. This way, identified brute forcing devices are blocked.
- **Rule 2** enters all client IP addresses and source ports of SSH connections into the ETT SSH - Ports per IP event tracking table.
- **Rule 3** counts the entries in the ETT SSH - Ports per IP event tracking table. If a client IP has more than 20 source ports within ten seconds, this indicates that an SSH brute force attack may be underway. Therefore, all clients with more than 20 entries are added to the SSH Brute Forcers dynamic network object.

The following table shows the required rule settings:

Rule	Source	Destination	Condition	Actions
1.	SSH Brute Forcers	Any		<b>Final Action:</b> Drop Traffic and Stop Processing
2.	Any	Any		<b>Add to Event Tracking Table</b> Event Tracking Table: ETT SSH - Ports per IP Primary Attribute: Client Address Secondary Attribute: Client Port

continues on next page

Table 5 – continued from previous page

Rule	Source	Destination	Condition	Actions
3.	Any	Any	Advanced Correlation Condition: Number of Similar Events in Event Tracking Table Event Tracking Table: ETT SSH - Ports per IP Count entries equal to: Client Address Minimum number of entries: 20	Dynamic Network Object Operation: Add Host Identifier: IP Address Who: Client Target Dynamic Network Object: SSH Brute Forcers

For detailed instructions on how to create a rule in a correlation scenario, refer to [Create Rules in a Correlation Scenario](#) (page 105).

Click the **APPLY CHANGES** button at the top of the main navigation to activate your configuration changes.

### Result

Threat Defender monitors all SSH connections and counts the source ports of each client IP address. If it detects client IP addresses that used more than 20 different source ports within ten seconds, this indicates that an SSH brute force attack may be underway.

The originator of the SSH brute force attack is identified. Threat Defender adds it to the dynamic network object to isolate it. Traffic from hosts in this network object is blocked. SSH brute force attacks run by these hosts are stopped.

**Note:** Once the suspected brute force attack is remedied, you need to flush the content of the dynamic network object. To do so, click the **RESET STATE** button in the correlation scenario.

### 4.6.3.3 Detect Data Obfuscation: Protocol Impersonation (T1001:003)

#### Objective

Attackers may try to impersonate a legitimate protocol in order to disguise C&C communication and bypass network filtering (T1001:003<sup>22</sup>).

Using the protocol classification, this global rule blocks all traffic that has a mismatch between the HTTP protocol and its standard destination port 80.

**Note:** Similar rules can also be created for other protocols such as HTTPS, SSH, etc.

#### Create the Rule

Configure a global rule that drops all non-HTTP traffic to destination port 80 and generates a warning.

The following table shows the required rule settings:

Rule	Source	Destination	Conditions	Actions
1.	Any	Any	Classification Excluded Applications/Protocols: http Layer 4 Port Destination Ports: 80	Log: Medium Final Action: Reject Traffic and Stop Processing

For detailed instructions on how to create a rule, refer to [Create Global Rules](#) (page 83).

Click the **APPLY CHANGES** button at the top of the main navigation to activate your configuration changes.

#### Result

HTTP impersonation attempts are discovered and blocked.

#### Additional References:

<sup>22</sup> <https://attack.mitre.org/techniques/T1001/003/>



- If you want to look up the settings options for network objects, refer to [Network Objects](#) (page 154) in the interface reference.
- If you want to look up the settings options for correlation scenarios, refer to [Advanced Correlation](#) (page 153) in the interface reference.

## 4.6.4 Time-based Baselineing

### 4.6.4.1 Objective

Threat Defender can be set up to learn what behavior is normal during a fixed period of time, the learning phase. When this learning phase is over, Threat Defender enforces the learned behavior, allowing only the learned communication and rejecting everything else.

The learning phase is established using a [schedule](#) (page 159). During this phase, Threat Defender operates like a normal switch but gathers data about the devices in the network and their communication paths. Once this learning phase is completed, Threat Defender can use this behavior data to make filtering decisions to allow learned traffic patterns and reject unknown traffic.

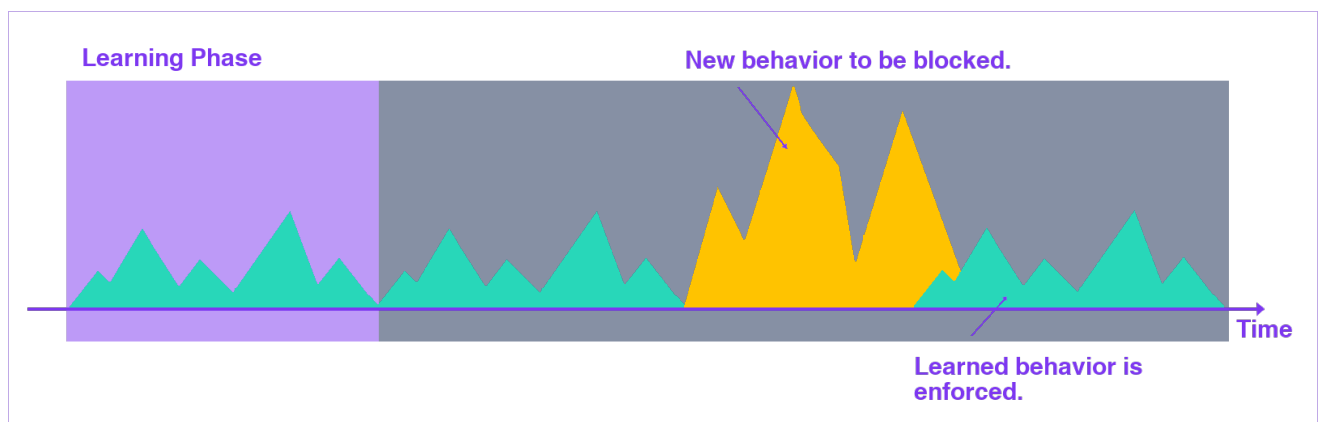


Fig. 18: Time-based baselining.

**Note:** This scenario demonstrates the ability to allow dedicated connections (e.g. IP/IP, MAC address/MAC address, MAC address/port, etc.) between clients and servers. This can only be done using an **event tracking table (ETT)** because dynamic network objects do not store the client/server relationship.

### 4.6.4.2 Create the “Learning Phase” Schedule

Set up a schedule that defines the learning phase.

1. Navigate to **Policy > Schedules**.
2. Click **Add** to add a new schedule.
3. Enter a **Name**, e.g. Learning Phase.
4. Optional: Enter a **Note**.
5. Enter the validity period using the date pickers under **Valid from** and **Valid until**.
6. Click **Add Time Range** to set a time during which the schedule is applied. You can add multiple time ranges.
7. Under **Repeat**, specify how often the learning phase is to be repeated automatically.
8. Click **SAVE** to store the schedule

#### 4.6.4.3 Create the Correlation Scenario

Navigate to **Policy > Advanced Correlation**. Create a new correlation scenario that provides the framework for the required event tracking table and rule set.

#### 4.6.4.4 Create the Event Tracking Table

In the correlation scenario, open the **Event Tracking Tables** tab. Create an event tracking table that stores the combinations of source (client) and destination (server) MAC address.

The following table shows the required settings of the event tracking tables:

Name	Retention Time	Primary Attribute Type	Max. No. Primary	Secondary Attribute Type	Max. No. Secondary Primary	Sec- per
Learned Communication	604800	MAC Address	5000	MAC Address	500	

**Note:**

- Under **Maximum Number of Primary Attributes**, make sure that the table is large enough to fit your network.
- Adapt the **Retention Time for Event Tracking** to the desired repetition intervals of the learning phase. Set it to 0 if you want to store the entries indefinitely.

For detailed instructions on how to create an event tracking table, refer to [Create an Event Tracking Table](#) (page 103).

#### 4.6.4.5 Create the Rule Set

In the correlation scenario, the following rules are needed for Threat Defender to learn traffic patterns and filter out any unknown traffic.

- **Rule 1** is only applied during the learning phase. It tracks the source and destination of the traffic in the event tracking table. Outside the learning phase, this rule is ignored.
- **Rule 2** is only applied outside the learning phase. If the source and destination of the detected traffic are contained in the event tracking table, the traffic is allowed. No further rules in this correlation scenario are processed for the respective traffic flows.
- **Rule 3** is only applied outside the learning phase. It blocks all remaining traffic, i.e. traffic that does not match the learned communication paths.

Rule	Schedule	Source	Destination	Condition	Actions
1.	Include Learning Phase	Any	Any		<b>Add to Event Tracking Table</b> Learned Communication Primary: Client MAC Address Secondary: Server MAC Address

continues on next page

Table 7 – continued from previous page

Rule	Schedule	Source	Destination	Condition	Actions
2.	Exclude Learning Phase	Any	Any	Advanced Correlation Conditions: Event in Event Tracking Table Learned Communication Compare Primary: Client MAC Address Compare Secondary: Server MAC Address	Final Action: Allow Traffic and Skip to Next Scenario
3.	Exclude Learning Phase	Any	Any		Final Action: Drop Traffic and Stop Processing

For detailed instructions on how to create a rule in a correlation scenario, refer to [Create Rules in a Correlation Scenario](#) (page 105).

Click the **APPLY CHANGES** button at the top of the main navigation to activate your configuration changes.

#### 4.6.4.6 Result

During the learning phase, Threat Defender learns which source and destination hosts are permitted to establish connections with each other. When the learning phase is completed, Threat Defender investigates all traffic and only allows the connections it identified during the learning phase.

## 4.6.5 Adaptive Behavior-based Graylisting

### 4.6.5.1 Objective

Threat Defender can be set up to continuously learn (and forget) normal behavior to create an adaptive baseline. When suspicious behavior is detected, traffic from the respective client is graylisted. It is then compared to the learned behavior so that unknown behavior is blocked and only the learned normal behavior is allowed. This way the system stays operational while threats are stopped and cannot spread.

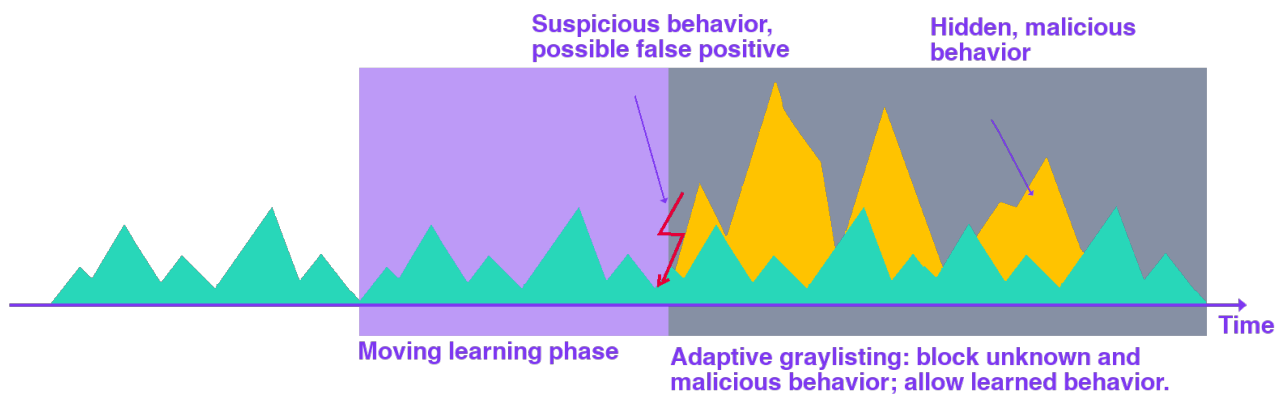


Fig. 19: Adaptive behavior-based graylisting.

A dynamic network object stores the MAC addresses of suspicious clients for an hour. An event tracking table stores the learned communication paths for 24 hours, creating a moving time window for baseline learning.

### 4.6.5.2 Create the Correlation Scenario

First, navigate to **Policy > Advanced Correlation**. Create a new correlation scenario that provides the framework for the required dynamic network object, event tracking table and rule set.

### 4.6.5.3 Create the Dynamic Network Object

In the correlation scenario, open the **Dynamic Network Objects** tab. Create a dynamic network object that stores the client MAC addresses of suspicious clients for one hour.

The following table shows the required settings of the dynamic network object:

Name	Network	Size	Timeout
Suspicious Clients	Internal	200	3600

For detailed instructions on how to create a dynamic network object in a correlation scenario, refer to [Create a Dynamic Network Object](#) (page 105).

#### 4.6.5.4 Create the Event Tracking Table

In the correlation scenario, create an event tracking table. It stores the source (client) MAC addresses per destination (server) IP address.

The following table shows the required settings of the event tracking table:

Name	Retention Time	Primary Attribute Type	Max. No. Primary	Secondary Attribute Type	Max. No. Secondary Primary
Learned Communication	86400	IP Address	5000	MAC Address	200

**Note:** Under **Maximum Number of Primary Attributes**, make sure that the table is large enough to fit your network traffic.

For detailed instructions on how to create an event tracking table, refer to [Create an Event Tracking Table](#) (page 103).

#### 4.6.5.5 Create the Rule Set

The following rules are needed for Threat Defender to learn traffic patterns and reject suspicious or unknown traffic.

- **Rule 1** adds clients that trigger an incident to the dynamic network object `Suspicious Clients`.
- **Rule 2** checks the communication destinations of clients in `Suspicious Clients`. If the communication destination is stored in the event tracking table `Learned Communication`, the traffic is allowed. Otherwise, Threat Defender continues processing the next rule.
- **Rule 3** drops traffic from clients in `Suspicious Clients`, because this is unknown traffic.
- **Rule 4** tracks the source and destination for all clients that are not in `Suspicious Clients` in the event tracking table `Learned Communication`. This allows Threat Defender to learn normal communication.

Rule	Source	Destination	Condition	Actions
1.	Any	Any	Threats Indicators Severity Tags: High, Medium	Dynamic Network Object: Operation: Add Host Identifier: MAC Address Who: Client Target Dynamic Network Object: Suspicious Clients
2.	Suspicious Clients	Any	Advanced Correlation Conditions: Event in Event Tracking Table Learned Communication Compare Primary: Server Address Compare Secondary: Client MAC Address	Final Action: Allow Traffic and Skip to Next Scenario
3.	Suspicious Clients	Any		Final Action: Drop Traffic and Stop Processing
4.	Any	Any		Add to Event Tracking Table Learned Communication Primary: Server Address Secondary: Client MAC Address

For detailed instructions on how to create a rule in a correlation scenario, refer to [Create Rules in a Correlation Scenario](#) (page 105).

Click the **APPLY CHANGES** button at the top of the main navigation to activate your configuration changes.

#### 4.6.5.6 Result

Threat Defender continuously adapts its baseline of normal behavior. The number of false-positives is reduced with this graylisting approach.

---

#### Additional References:

- For information on how to activate IPS rule sets in Threat Defender, see [IPS Settings](#) (page 184).
- See [IPS Rule Definitions](#) (page 243) on how to create custom IPS rule sets.



| Chapter 5

# Segment the Network

## 5.1 Network Segmentation

Threat Defender uses a concept of enriched network objects to apply **policy** rules specifically to traffic initiated from and/or directed to specific assets and groups of assets in the network. Using **static network objects** (page 125) (SNOs) and **dynamic network objects** (page 125) (DNOs), Threat Defender provides a virtual overlay security network with a dynamically changing topology on top of the physical network. These network objects are used to adapt the **network segmentation** dynamically and at runtime based on asset/user behavior without requiring a change in the existing network topology.

Network objects can be used in multiple rules simultaneously. This means it is possible to apply a set of rules to a group of assets without redefining the group for each rule. If an asset is part of several network objects, multiple policy rules can be layered and applied to that asset.

### 5.1.1 Example Workflow

The following simplified example workflow illustrates how network segmentation using static and dynamic network objects can be effected:

- Static network objects (SNOs) segment the network based on the purpose of the assets. Dynamic network objects (DNOs) segment the network based on the asset behavior.
- In this example, the DNO called “RC” is used to contain clients that are remotely accessed. This way, specific rules can be applied to them, e.g. to deny them access to the internal servers.

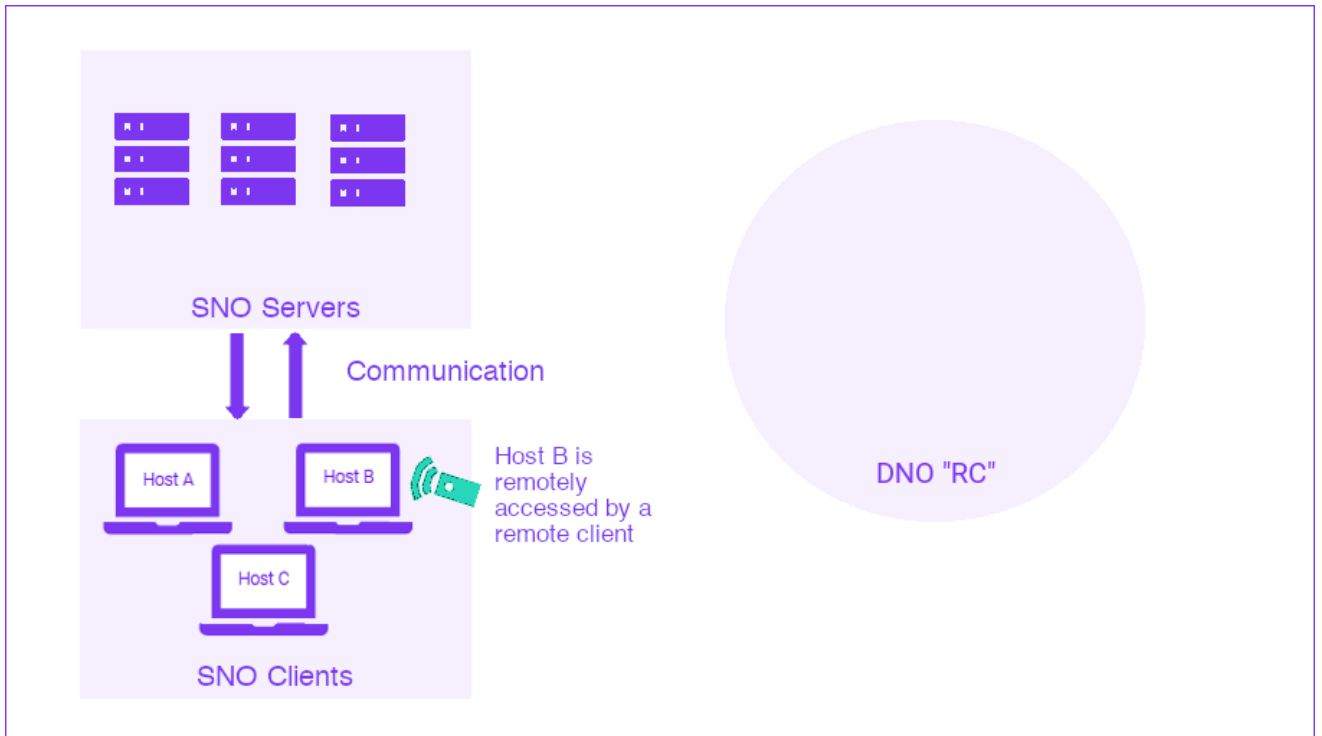


Fig. 1: Network segmentation using static and dynamic network objects.

- Using rules, Threat Defender monitors the communication behavior in the network.
- If suspicious or unwanted behavior is detected, a rule adds the respective client to dynamic network objects.
- In this example, client B is remotely accessed. Therefore, it is added to the DNO "RC".

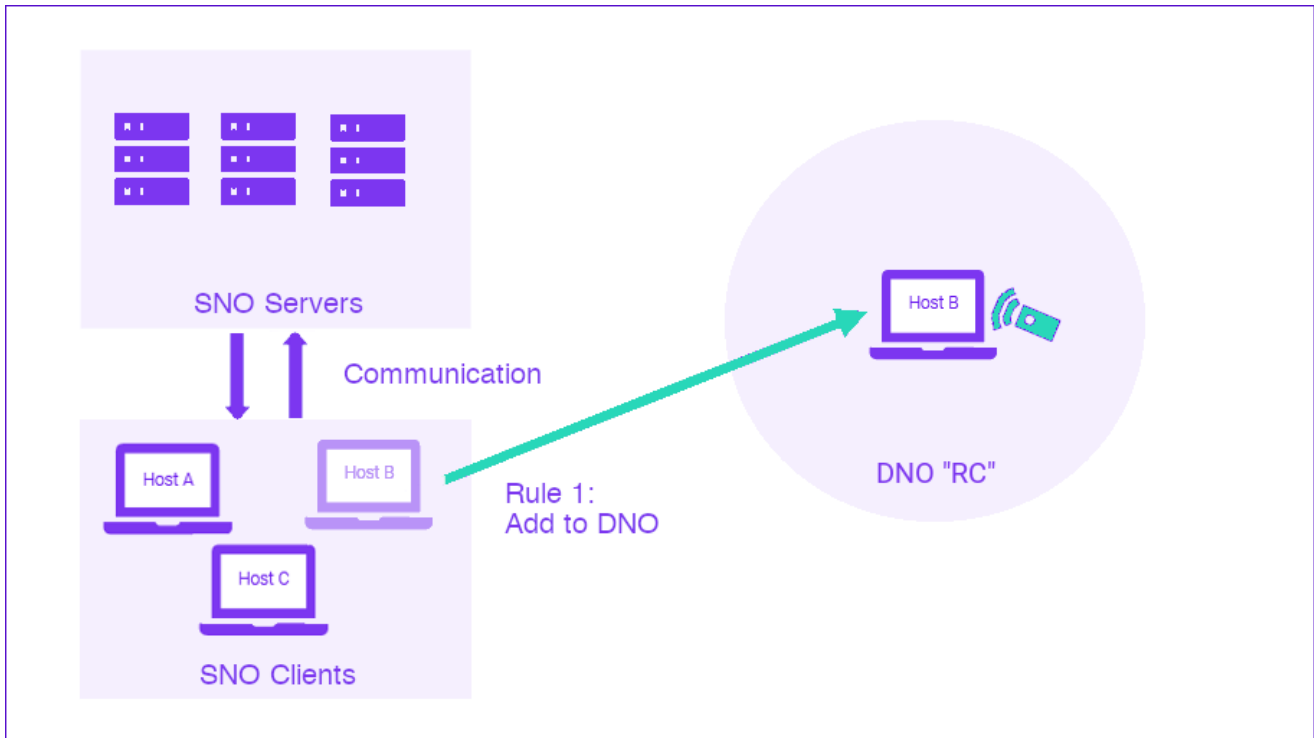


Fig. 2: A rule adds the concerned host to the dynamic network object.

- Another rule rejects all communication from clients in this dynamic network object to the internal servers.

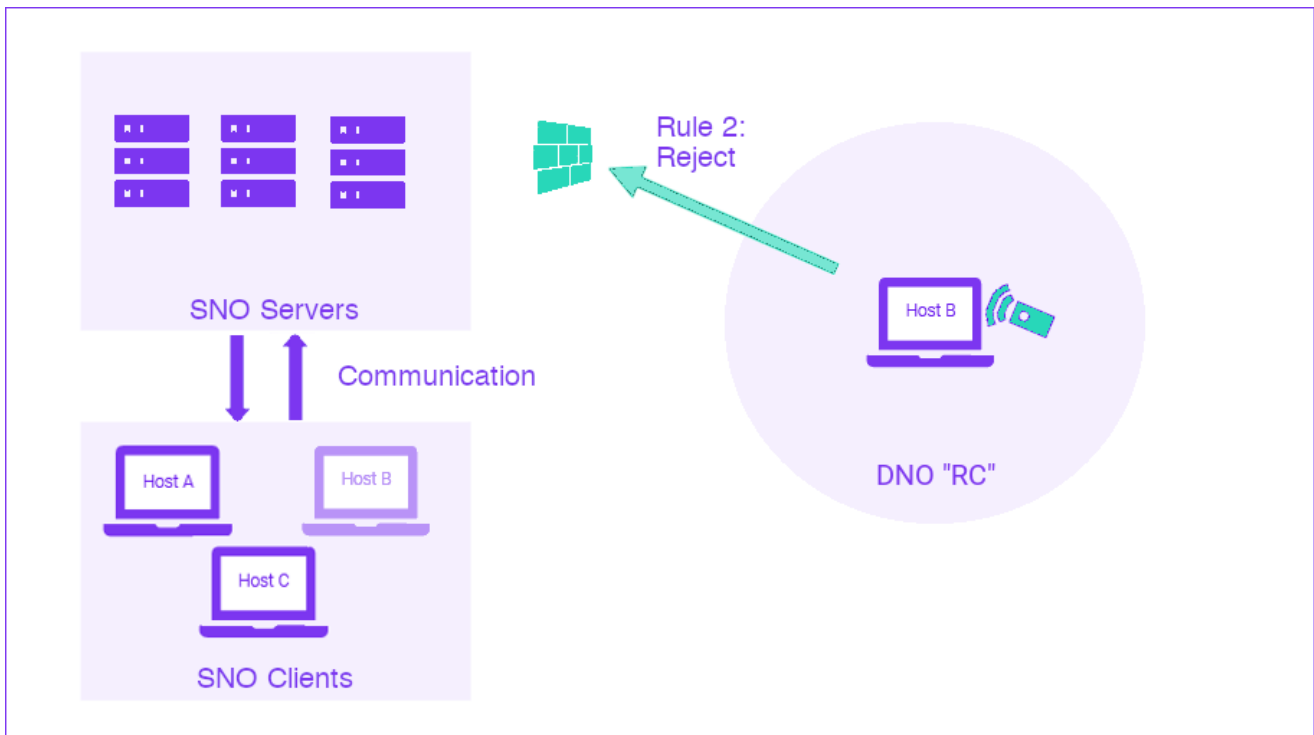


Fig. 3: Traffic from hosts in the dynamic network object to the internal servers is rejected.

### 5.1.2 Static Network Objects

Static network objects are used to group hosts and devices. They are used globally, meaning they are available for all rules. The following attributes can be used to assign devices to a static network object:

- Inclusion and exclusion of individual IP addresses and networks in **CIDR** notation, both in **IPv6** and **IPv4**
- Inclusion and exclusion of individual MAC addresses and MAC address ranges
- VLAN tags

You can define static network objects using just one or any combination of these attributes. For example, it is possible to have a network object that matches all devices in VLAN 21. But you can also have very specific conditions, e.g. only devices with IP network 10.10.10.0/27 in VLAN 5 match.

See [Create Static Network Objects](#) (page 127) for further information.

### 5.1.3 Dynamic Network Objects

Dynamic network objects are used to track the state of hosts and create host groups with common behavior on the fly. The hosts of the group share a specific characteristic or property that is not static but depends on events happening dynamically in the running system. Based on this behavior, a specific set of policy rules is applied to them. This allows the policy engine to adapt to changing situations. It dynamically controls what rules are applied to different groups of hosts in real time.

Dynamic network objects are lists of individual IPv6/IPv4 addresses and/or MAC addresses. IP and MAC addresses can be added dynamically and are removed either by an explicit rule action or automatic timeout.

cognitix Threat Defender adds a new type of action to the policy rule language to add the source or destination IP/MAC address of a flow to a dynamic network object. These dynamic network objects can then be used to match the source and destination of flows in other rules to dynamically apply policy rules to all traffic of a device depending on the behavior of that device. This allows for automatically safeguarding the network without the need to manually maintain long, unordered network object lists.

In combination with the [Correlation in Threat Defender](#) (page 74) engine, the dynamic network objects allow you to react to changing, unwanted or suspicious behavior by enforcing policy rules that are applied to all the flows generated by certain hosts and not just to individual flows.

Dynamic network objects can be global (available for all rules) or be defined and used within a correlation scenario for individual hosts or groups of hosts.

Using dynamic network objects, you can for example:

- Define a policy that automatically adds all source hosts in the network that trigger a certain number of incidents to a dynamic network object. You can then implement various access restriction policy rules for that object.
- Using the timeout feature of dynamic network objects, you can block hosts for a certain amount of time.

---

#### Additional References:

- For step-by-step instructions on creating network objects, see [Create Static Network Objects](#) (page 127) and [Create Dynamic Network Objects](#) (page 129).
- For information on the settings options of network objects, see [Network Objects](#) (page 154).
- For examples on segmenting your network using Threat Defender, see [Use Network Segmentation](#) (page 131).

## 5.2 Create Static Network Objects

Static network objects group hosts and devices. They are used globally, meaning they are available for all rules. Several attributes can be used to assign hosts and devices to a static network object: IP addresses, MAC addresses, VLAN tags.

The following chapter shows how to set up a static network object for a printer. In this example, the device is identified by its MAC address.

1. Navigate to **Policy > Network Objects**.
2. On the **Static Network Objects** tab, click **Add Global Static Network Object** to create a new object.
3. Enter general information on the static network object:
  - Enter a **Name** for the object, e.g. Printer, 1st floor.
  - Optional: Enter a **Note** to describe the object.
4. Under **Network Definition**, specify what devices will belong to this network object:
  - Under **Network**, make sure that **Internal** is selected.

**Tip:** The **Internal** and **External** networks are basically superordinate network objects, i.e. they contain the network objects assigned to them. They can be used as traffic source and destination in rules like other network objects. The **Internal** network refers to the part of the network that Threat Defender can see, while the **External** network is the part that is not monitored by Threat Defender.

- Under **MAC Addresses**, enter the MAC address of the printer in the **Included** field, e.g. 00:17:c8:26:21:20.

New Static Network Object

Internal External

IP Addresses  
Comma separated list of IP addresses. IPv4 or IPv6 in CIDR notation (e.g. 20.20.20.200/16, 2001:1620:28::116/32)

Included Excluded

MAC Addresses  
Comma separated list of MAC addresses (e.g. AA:BB:CC:DD:EE:FF). Masked bytes (12:;::; 12:34:56:7:;) are allowed.

Included Excluded

00:17:c8:21:26:20

VLANs  
If no VLAN is set, it will match all.

SELECT ALL UNSELECT ALL

ADD VLAN

SAVE CANCEL

Fig. 4: Network settings.

5. Click **SAVE** to store the new static network object.
6. Click the **APPLY CHANGES** button at the top of the main navigation to activate your configuration changes.

---

#### Additional References:

For further information on the settings options, see [Static Network Objects](#) (page 155).



## 5.3 Create Dynamic Network Objects

Dynamic network objects track the state of hosts and create host groups with common behavior on the fly (see also [Network Segmentation](#) (page 122)). Rules add hosts to dynamic network objects. Hosts that belong to a dynamic network object are removed from them by rules or by timeout.

Dynamic network objects can be global (available for all rules) or defined and used within a [correlation scenario](#) (page 74).

The following example shows how to create a global dynamic network object for test clients in the network.

1. Navigate to **Policy > Network Objects**.
2. Open **Dynamic Network Objects**.
3. Click **Add Global Dynamic Network Object** to create a new dynamic network object.
4. Enter general information for the object:
  - Enter a **Name**, e.g. All Test Clients.
  - Optional: Enter a **Note** to describe the object.
5. Specify the **Settings** of the dynamic network object:
  - Under **Network**, select **Internal**.

**Tip:** The **Internal** and **External** networks are basically superordinate network objects, i.e. they contain the network objects assigned to them. They can be used as traffic source and destination in rules like other network objects. The **Internal** network refers to the part of the network that Threat Defender can see, while the **External** network is the part that is not monitored by Threat Defender.

- Specify the maximum **Size** of the object list (e.g. 100 entries).
  - Set a **Timeout** after which the entries will be removed automatically (e.g. 60s x 60 x 24 x 7 = 604800 seconds = 1 week).
6. Optional: If there are hosts you want to include in the list right away, enter their IP addresses under **Forced Includes**. These entries will be handled as any other host on the list. They will be removed by timeout or by a rule with the delete action for dynamic network objects. You can also explicitly exclude IP and/or MAC addresses from the dynamic network object.

New Dynamic Network Object

General

Name (Required)  
All test clients

Note  
All clients in the test network

Settings

Network  
Internal External

Size (Required)  
Maximum number of hosts that can be added.  
100

Timeout (in Seconds)  
Retention time per host entry. 0 remains for forever.  
604800

Fig. 5: Example dynamic network object for test clients.

7. Click **SAVE** to store the new global dynamic network object.
8. Click the **APPLY CHANGES** button at the top of the main navigation to activate your configuration changes.

---

**Additional References:**

For further information on the settings options, see [Dynamic Network Objects](#) (page 156).

## 5.4 Use Network Segmentation

The following examples illustrate possibilities of segmenting your network using cognitix Threat Defender.

### 5.4.1 Dynamic Network Segmentation for BYOD Clients

#### 5.4.1.1 Objective

Using dynamic network segmentation, all **BYOD** (bring your own device) clients inside an internal company network are tracked. Their access to company-critical resources, for example an internal file server, is restricted.

Employees and visitors connect their own private devices to the company network. Since these devices are not covered by company security policies, they should not be trusted and may be used to compromise the security of the company network.

BYOD clients are identifiable by their behavior in the network. In this example, we assume that WhatsApp is not allowed on internal devices. Therefore, any device generating WhatsApp traffic is classified as a BYOD.

The internal file server is contained in a dedicated static network object. A dynamic network object tracks BYOD clients by storing their MAC addresses. Because of the persistent nature of MAC addresses, there is no need to specify a timeout and devices can be tracked as BYOD for an unlimited amount of time. The maximum size of the dynamic network object has to be set sufficiently large to store all device entries.

#### 5.4.1.2 Create the Static Network Object for the File Server

Create a static network object that characterizes your internal file server.

The following table shows the required settings of the static network object:

Name	Network	IP Addresses	MAC Addresses
File Server	Internal		Included: MAC address of the internal file server

#### 5.4.1.3 Create the Dynamic Network Object for BYOD Clients

Create a dynamic network object that stores the BYOD clients.

The following table shows the required settings of the dynamic network object:

Name	Network	Size	Timeout
BYOD Hosts	External	10000	0

For detailed instructions on how to create a global dynamic network object, refer to [Create Dynamic Network Objects](#) (page 129).

**Note:** Make sure that the size of the dynamic network object is large enough to store all device entries.

**Tip:** A timeout of 0 means that the entries are not removed automatically.

#### 5.4.1.4 Create the Rule Set

Configure two global rules:

- **Rule 1** enters the MAC addresses of all hosts that generate WhatsApp traffic into the dynamic network object.
- **Rule 2** blocks all traffic from hosts in the dynamic network object to the internal file server.

The following table shows the required rule settings:

Rule	Source	Destination	Condition	Actions
1.	Any	Any	Classification Included Applications/Protocols: WhatsApp	Dynamic Network Object Operation: Add Host Identifier: MAC Address Who: Client Target Dynamic Network Object: BYOD Hosts
2.	BYOD Hosts	File Server		Final Action: Reject Traffic and Stop Processing

For detailed instructions on how to create a rule, refer to [Create Global Rules](#) (page 83). Click the **APPLY CHANGES** button at the top of the main navigation to activate your configuration changes.

#### 5.4.1.5 Result

BYOD clients in the company network are tracked and denied access to the internal file server. At the same time, they are still able to use the company network for other purposes, such as connecting to the Internet.

### 5.4.2 Allow Internet Traffic via Internal Proxy Server Only

#### 5.4.2.1 Objective

In a company there is a **proxy server** with detailed URL-based rule sets. Therefore, all **HTTP/HTTPS** traffic which is not handled by the proxy server should be blocked.

This requires the following:

- a static network object for the proxy server,
- a rule that handles the allowed traffic, and
- a rule that blocks all other traffic.

**Note:** This example configuration only handles HTTP/HTTPS communication. Other protocols, such as **QUIC**, are not blocked.

#### 5.4.2.2 Create the Static Network Object for the Proxy Server

Create a static network object that characterizes your proxy server.

The following table shows the required settings of the static network object:

Name	Network	MAC Addresses
Proxy Server	Internal	Included: MAC address of the internal proxy server

For detailed instructions on how to create a static network object, refer to [Create Static Network Objects](#) (page 127).

### 5.4.2.3 Create the Rule Set

Configure a rule set consisting of two global rules:

- **Rule 1** allows all HTTP/HTTPS traffic to the proxy server.
- **Rule 2** rejects all HTTP/HTTPS traffic in the network that is not directed at the proxy server.

The following table shows the required rule settings:

Rule	Source	Destination	Condition	Actions
1.	Any	Proxy Server	Classification Included Applications/Protocols: HTTP, SSL	Final Action: Allow Traffic and Skip to Next Scenario
2.	Any	Any	Classification Included Applications/Protocols: HTTP, SSL	Final Action: Reject Traffic and Stop Pro- cessing

For detailed instructions on how to create a rule, refer to [Create Global Rules](#) (page 83).

Click the **APPLY CHANGES** button at the top of the main navigation to activate your configuration changes.

### 5.4.2.4 Result

Threat Defender processes the rule set in a top-down approach, resulting in the workflows detailed below.

Network clients (web browsers) with a configured proxy server:

1. Network packages sent via HTTP (or HTTPS) to the network address of the proxy server (handles the website request) hit **rule 1**.
2. The network packages match the rule settings. Therefore, they are allowed to pass.

Network clients (web browsers) with no configured proxy server try to access the company intranet:

1. Network packages sent via HTTP (or HTTPS) to the webserver hosting the company intranet hit **rule 1**.

2. The network packages do not meet the rule criteria because their destination is not the proxy server. Therefore, the rule is skipped.
3. Threat Defender checks the network packages against the next rule, rule 2.
4. The packages match the rule settings and are rejected.
5. The client application is notified that the web server cannot be reached.

### 5.4.3 Create a DMZ with Two Threat Defenders

#### 5.4.3.1 Objective

The following use case illustrates how two installations of Threat Defender can be set up to create a demilitarized zone (DMZ).

A medium-sized example company has headquarters,

several subsidiaries and employees in the field, such as travelling sales people. The company hosts its database servers at the headquarters. The subsidiaries and field employees need to remotely access the database servers at the headquarters.

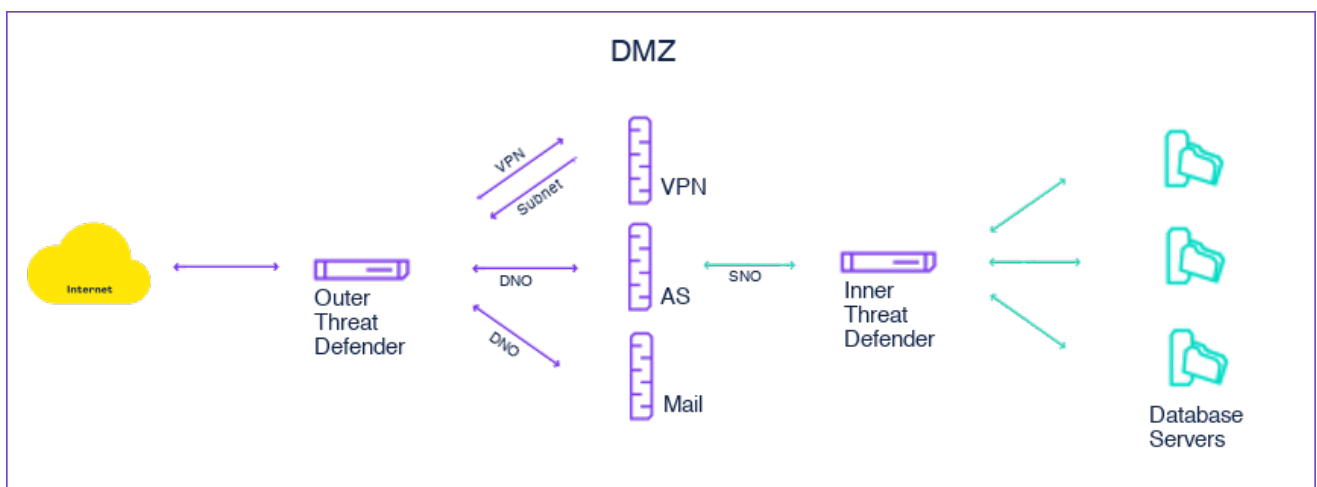


Fig. 6: A DMZ is created by two instances of Threat Defender.

To protect the database servers from external threats, a DMZ is created using two instances of Threat Defender. The DMZ separates sensitive network parts from publicly available services.

Remote access is granted via VPN. The outer Threat Defender manages VPN access from the Internet to the DMZ; the inner Threat Defender manages the connections between the DMZ and the database servers.

**Note:** Note that this example only shows how Threat Defender can be configured to create a DMZ. It does not include behavior-based traffic management. This has to be set up separately.

### 5.4.3.2 Set up VPN Access to the DMZ

The outer Threat Defender manages VPN access to the DMZ.



**Warning:** In this scenario, Threat Defender replaces the **network switch**. This means the various subnets have to be connected to Threat Defender with separate physical wiring. Otherwise, Threat Defender will not be able to see the traffic inside the DMZ.

Threat Defender has to be configured in a way that only the required VPN protocols are directly connected to the VPN server (VPN concentrator). The VPN server then authenticates the VPN clients and assigns them an IP address in the VPN clients **subnet**.

The network is segmented using static and dynamic network objects. The VPN, mail and application servers are assigned to separate static network objects. The incoming VPN clients are automatically assigned to a dynamic network object.

A dedicated rule set manages the network traffic. The clients stored in the dynamic network object may access the mail and application servers in the DMZ. Only the servers handle the data. This way, no external threats can enter the internal network.

#### Create the Static Network Objects

Create static network objects to segment the network. The VPN, mail and application servers are all assigned to separate static network objects. This adds transparency and allows for detailed analyses of the network traffic under **Analytics** (page 142).

Note that in this context, the company network is defined as the internal network, including the DMZ. Everything outside the company network is considered external.

The following table shows the required settings of the static network objects.

**Note:** The table contains example IP addresses by way of illustration.



Name	Network	IP Addresses
Application Servers	Internal	10.10.20.0/27
Mail Servers	Internal	10.10.30.0/29
VPN Server	Internal	10.10.10.0/29
VPN Clients	Internal	192.168.0.0/20

For detailed instructions on how to create a static network object, refer to [Create Static Network Objects](#) (page 127).

### Create a Dynamic Network Object

Create a dynamic network object that stores the IP and MAC addresses of the VPN clients that connect to the DMZ. This way, Threat Defender creates a dedicated VPN network with a limited retention time. Due to the timeout, inactive connections are automatically terminated after the timeout expires.

Storing both IP and MAC addresses allows for detailed analyses of who connects to the network using the Threat Defender [Analytics](#) (page 142) feature.

The following table shows the required settings of the dynamic network object:

Name	Network	Size	Timeout
VPN Clients	Internal	4000	600

For detailed instructions on how to create a global dynamic network object, refer to [Create Dynamic Network Objects](#) (page 129).

### Create the Rule Set

To configure Threat Defender to handle VPN access to the DMZ, you need to set up the following rule set comprising six global rules. The **Log** action is enabled in all rules. This provides valuable information on the network traffic that can be analyzed in the **Analytics** section of Threat Defender.

- **Rule 1** allows incoming VPN connections to the VPN server.
- **Rule 2** adds the IP and MAC addresses of all VPN clients to the `VPN Clients` dynamic network object.
- **Rule 3** grants the VPN clients access to **DNS** servers. Note that the `DNS Servers` static network object is preset on Threat Defender. If necessary, adapt it to your requirements.

- Rule 4 allows the VPN clients to access the mail servers.
- Rule 5 allows the VPN clients to access the application servers.
- Rule 6 rejects all remaining traffic.

Rule	Source	Destination	Condition	Actions
1.	External	VPN Server	Classification Included Applications / Protocols: openvpn	Log: Notice Final Action: Allow Traffic and Skip to Next Scenario
2.	VPN Clients	Any		Log: Notice Dynamic Network Object Operation: Add Host Identifier: Both Who: Client Target Dynamic Network Object: VPN Clients
3.	VPN Clients	DNS Servers		Log: Notice Final Action: Allow Traffic and Skip to Next Scenario
4.	VPN Clients	Mail Servers	Classification Included Applications / Protocols: imap, smtp, pop3	Log: Notice Final Action: Allow Traffic and Skip to Next Scenario
5.	VPN Clients	Application Servers	Classification Included Applications / Protocols: http	Log: Notice Final Action: Allow Traffic and Skip to Next Scenario

continues on next page

Table 2 – continued from previous page

Rule	Source	Destination	Condition	Actions
6.	Any	Any		Log: Medium Final Action: Drop Traffic and Stop Processing

For detailed instructions on how to create a rule, refer to [Create Global Rules](#) (page 83). Click the **APPLY CHANGES** button at the top of the main navigation to activate your configuration changes.

With this rule set, Threat Defender allows VPN connections to access the DMZ while rejecting all other traffic.

#### 5.4.3.3 Handle Traffic between the DMZ and the Internal Network

The inner Threat Defender is located between the DMZ with the VPN, mail and application servers and the internal network with the database servers. It isolates the two network parts from each other and handles communication between them.

##### Create the Static Network Objects

Create a static network object for the application servers in the DMZ and another one for the database servers in the internal network.

The following table shows the required settings of the static network objects.

**Note:** The table contains example IP addresses by way of illustration.

Name	Network	IP Addresses
Application Servers	Internal	10.10.20.0/27
Database Servers	Internal	10.10.100.0/26

For detailed instructions on how to create a static network object, refer to [Create Static Network Objects](#) (page 127).

##### Create the Rule

Create a rule that allows the application servers to access the database servers for database queries. This example assumes that the database servers run a SQL database.

Rule	Source	Destination	Condition	Actions
1.	Application Servers	Database Servers	Classification Included Applications / Protocols: mysql	Log: Notice Final Action: Allow Traffic and Skip to Next Scenario

With this rule, the application servers can contact the database servers which can answer their queries. However, the database servers cannot actively contact the DMZ.

#### 5.4.3.4 Result

Two installations of Threat Defender create a DMZ that contains the VPN, mail and application servers. The database servers of the company are located behind the DMZ. This grants them a second level of protection from external threats.

If suitable policies for behavior-based traffic management are implemented, Threat Defender can detect threats and react to them. These policies have to be configured in addition to the rule sets described above.

---

#### Additional References:

- For information on network segmentation in general, see [Network Segmentation](#) (page 122).
- If you want to look up the settings options for network objects, refer to [Network Objects](#) (page 154) in the interface reference.


| Chapter 6

# Interface Reference

## 6.1 Analytics

Threat Defender visualizes network information and relationships using interactive reports and charts as well as multiple levels of drill-down reporting via dashboards that provide multiple angles for traffic examination. The analysis feature includes more than 600 reporting combinations, graphs and matrixes.

### 6.1.1 Overview of the Analytics Dashboards

The  Analytics menu is your starting point for traffic analysis. It contains three dashboards that provide a quick overview of the network:

- [Network](#) (page 143)
- [Assets](#) (page 144)
- [Policy](#) (page 144)

**Note:** cognitix Threat Defender stores reporting data of up to the last 30 days (in 6-hour resolution).

The dashboards provide the most important information at a glance and allow you to drill down deeper into the reporting.

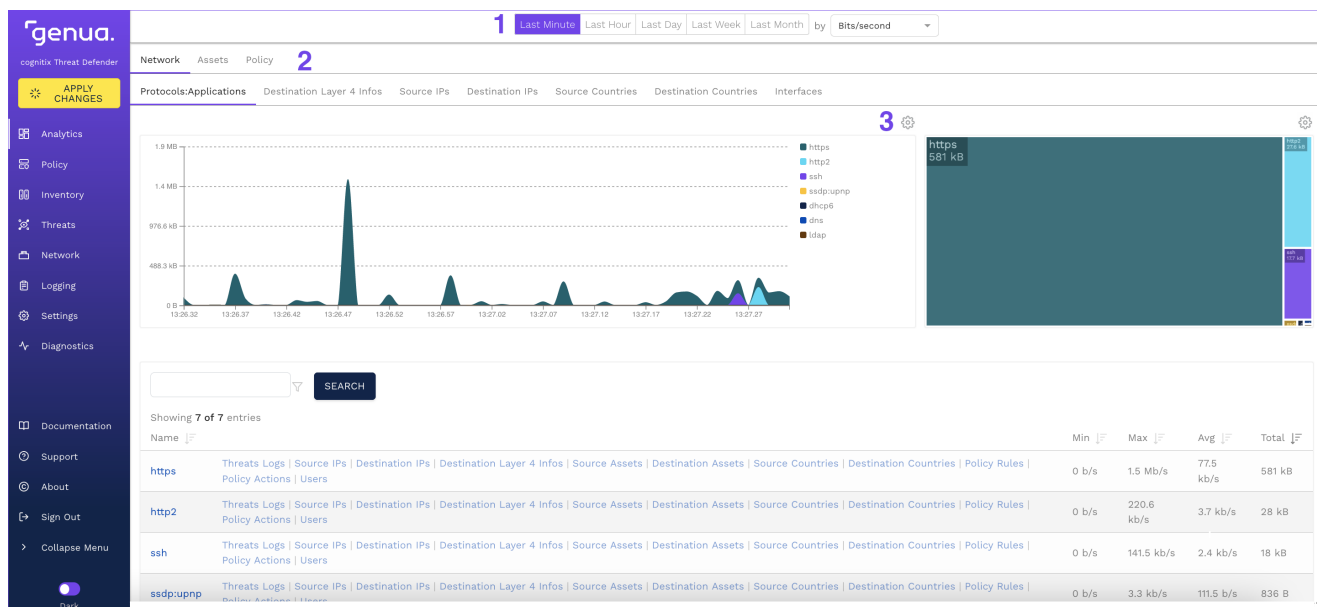



Fig. 1: Drilling into the Network screen.

The Analytics screens contain the following control elements:

1. With the buttons at the top of the content area, you can select the reporting period to be displayed in the charts. When you drill into deeper reporting levels, you can also select the metric from a drop-down list. These settings are automatically applied to all charts under **Analytics**. There are up to five reporting periods with individual resolutions:
  - **Last Minute** in 1-second resolution (live view)
  - **Last Hour** in 1-minute resolution
  - **Last Day** in 15-minute resolution
  - **Last Week** in 3-hour resolution
  - **Last Month** in 6-hour resolution
2. If you drill deeper into the reporting, a menu cascade above the charts displays the reporting levels you navigated.
3. The  icon at the top of the charts allows you to change the chart type by selecting a new type from the drop-down list.

In most charts, you can hover the mouse over a section to see the represented value in a tooltip.

**Tip:** If you hover the mouse over a chart, it pauses and is no longer updated. This gives you time to analyze the chart. This is particularly helpful in live view.

Many chart headings are links. They take you to a deeper level of analysis, where you see time and quantity-based charts as well as a table view of the entries. You can also directly click a section of a chart or a table entry to navigate to the relevant reporting screen.

### 6.1.2 Network

Navigate to **Analytics > Network** to see information related to the behavior of the network. The information fields at the top of this dashboard show the amount of traffic passing through Threat Defender.

The charts display the traffic distribution by protocols and applications, destination [layer 4](#) information, source and destination IP addresses and countries, and interfaces.

**Note:** Information on **Source Countries** and **Destination Countries** is based on GeoIP values. If you use a private IP range, the source and/or destination country is displayed as **Unknown** or **invalid territory**.

From here, you can drill down into deeper reporting levels to further analyze the network traffic. For example, you can check which source or destination IP consumes the most bandwidth.

---

#### Additional References:

For examples on using the network analytics dashboard, see [Analyze Protocols and Destination Countries](#) (page 54) and [Find YouTube Users in the Last Hour](#) (page 56).

### 6.1.3 Assets

Navigate to **Analytics > Assets** to see information related to asset and user behavior in the network.

The information fields at the top of this dashboard show the number of assets managed in Threat Defender with respect to the selected reporting period.

The charts display the traffic distribution by source and destination assets, and which assets talk to each other. They also show triggered incidents by source and destination assets. Furthermore, the traffic distribution by users and by URLs is shown.

From here, you can drill down into deeper reporting levels to begin a more detailed analysis of asset and user behavior in the network.

### 6.1.4 Policy

Navigate to **Analytics > Policy** to see information related to the network [policy](#).


The information fields at the top of this dashboard show the rule hits logged in the selected reporting period by severity.

The **Policy Rules** chart shows which policy rules were hit. The **Policy Actions** chart shows the number of times Threat Defender performed the drop traffic action (`blocked`) and the reject traffic action (`teardown`) of a policy on the network traffic. The logged policy hits are also displayed by severity and source/destination assets.

From here, you can further investigate the network traffic.





## | 6.2 Policy

In the  Policy menu, you can manage your traffic by setting up rules and correlation scenarios. You can segment your network by configuring network objects. Furthermore, you can set up time schedules and event tracking tables.

### 6.2.1 Rules

Navigate to **Policy > Rules** to see an overview of all rules currently configured in the system. Rules are flow-specific, i.e. they are only applied to traffic flows matching the conditions specified in the rule.

The overview table displays the rules that are defined in the system and gives a summary of their configuration (for further information, see [Rules Settings](#) (page 146)). The toggle in the first column allows you to enable () or disable () the respective rule. The icons in last column allow you to edit, copy or delete the rule.

**Tip:** You can hover the mouse on the entries in the table to see a tooltip displaying the defined options, where applicable.

Global rules, which are applied to all traffic, are placed at the top of the table. Rules used in correlation scenarios are grouped by scenario (see [Advanced Correlation](#) (page 153)).

**Note:** cognitix Threat Defender processes rules from top to bottom. Therefore, place more specific rules at the top of the table and rules that apply to a broader range of traffic at the bottom.

To reorder global rules, click the **ACTIVATE GLOBAL RULES REORDER** button above the table. Move the rules to the desired positions using drag and drop. Correlation scenarios can be reordered under **Policy > Advanced Correlation**.


To add a new global rule to the system, click the **Add Global Rule** button above the overview table.

Note that global rules cannot be added to advanced correlation scenarios. To create rules for Advanced Correlation scenarios, you need to create them directly in the respective scenario. Click the name of the scenario to access its settings screen (see [Advanced Correlation Scenario Settings](#) (page 153)). In the **Rules** tab, click **Add**.


### 6.2.1.1 Rules Settings

When you add a new rule or edit an existing one, the settings screen is displayed.

The **General** section provides the following options:

Field	Description
	The toggle indicates whether rule is enabled or disabled.
<b>Name</b>	Enter the name of the rule.
<b>Note</b>	Optional: Add a short description of the rule.
<b>Statistics</b>	This section displays the number of hits per second of this rule in a time chart. By mouseover you can see the individual values in a tooltip.

In the **Schedule** section, you can specify a time frame during which the rule is active:

Field	Description
 <b>Schedule</b>	Click the toggle to enable a time schedule for the rule.
<b>Include</b>	Click this button if you want the rule to be active during the selected period of time. Outside of this time period, the rule is inactive.
<b>Exclude</b>	Click this button if you want the rule to be inactive during the selected period of time. Outside of this time period, the rule is active.
<b>Schedule</b>	From the drop-down list, select the schedule you want to activate for the rule. You can only select one schedule at a time.
<b>ADD SCHEDULE</b>	Click this button to open the schedule settings screen and create a new time schedule (see <a href="#">Schedules</a> (page 159)).

The **Source & Destination** section provides the following options:

Field	Description
<b>Source Networks</b>	Specify the source networks of the traffic flows to which the rule is to be applied. The default setting is <i>Any</i> , i.e. the rule matches traffic from all source networks. You can select static network objects (preceded by <i>S:</i> ) and dynamic network objects (preceded by <i>D:</i> ) here. You can also type in the input field to narrow down the list to the sources whose names contain the characters you are typing. Click <b>X</b> next to an element to remove individual networks from the selection.
<b>Destination Networks</b>	Specify the destination networks of the traffic flows to which the rule is to be applied. The default setting is <i>Any</i> , i.e. the rule matches traffic directed to all destination networks. You can select static network objects (preceded by <i>S:</i> ) and dynamic network objects (preceded by <i>D:</i> ) here. You can also type in the input field to narrow down the list to the destinations whose names contain the characters you are typing. Click <b>X</b> next to an element to remove individual networks from the selection.
<b>ADD DYNAMIC NETWORK OBJECT</b>	Click this button to open the dynamic network objects settings screen and create a new dynamic network object (see <a href="#">Dynamic Network Objects</a> (page 156)). If you click this button in a global rule, you create a global dynamic network object. If the rule belongs to an advanced correlation scenario, the dynamic network object will be created inside the scenario.
<b>ADD STATIC NETWORK OBJECT</b>	Click this button to open the static network objects settings screen and create a new static network object (see <a href="#">Static Network Objects</a> (page 155)).

The **Advanced Correlation Conditions** section is only available for rules that are created in advanced correlation scenarios. It contains the following elements:

Field	Description
<b>Event in Event Tracking Table</b>	Enable this option to compare the traffic to the events in an event tracking table. From the drop-down list, select the <b>Event Tracking Table</b> you want to use for comparison. Click <b>ADD EVENT TRACKING TABLE</b> to open the event tracking tables settings screen and create a new table (see <a href="#">Event Tracking Tables</a> (page 160)). Select the elements you want to compare to the primary and secondary attributes of the events from the respective drop-down lists. The rule only matches the traffic if the comparison is successful.
<b>Number of Similar Events in Event Tracking Table</b>	Enable this option to count the number of events in an event tracking table. From the drop-down list, select the <b>Event Tracking Table</b> you want to count the events in. Click <b>ADD EVENT TRACKING TABLE</b> to open the event tracking tables settings screen and create a new table (see <a href="#">Event Tracking Tables</a> (page 160)). Under <b>Count all Entries with Primary Attribute equal to</b> , specify which entries you want to count. Under <b>Minimum Number of Entries</b> , specify the minimum number of entries that have to be counted for the rule to match.

In the **Conditions** section, click the toggles to enable the conditions you want to activate for the rule.

**Note:** You can enable any number of rule conditions. Conditions are **AND**-connected. This means, if you activate multiple conditions in a rule, the rule only matches if the traffic fulfills **all** active conditions. If you select multiple elements within a condition, those elements are **OR**-connected.

When you enable a condition, dedicated input fields are displayed for this condition:

Field	Description
<b>Assets</b>	Enable this option to apply the rule to traffic generated by specific assets. Select the asset tags that you want to use as source and/or destination in the rule. You can create new tags by entering them in the fields. Click <b>X</b> next to an element to remove individual tags from the selection.
<b>Users</b>	Enable this option to apply the rule to traffic generated by specific users. Click into the field and select the respective users from the list. You can also type in the input field to narrow down the list to the users whose names contain the characters you are typing. Click <b>X</b> next to an element to remove individual elements from the selection.
<b>GeoIP</b>	Enable this option to check the traffic by <b>Source Countries</b> and/or <b>Destination Countries</b> . Click into the field and select the required countries from the list. You can also type in the input field to narrow down the list to the countries whose names contain the characters you are typing. Click <b>X</b> next to an element to remove individual countries from the selection. If you enable <b>Include</b> , the rule matches the selected countries. If you enable <b>Exclude</b> , the rule matches all but the selected countries.
<b>Layer 4 Protocol</b>	Enable this option to check the traffic by layer 4 protocols used. Click into the field and select the required protocols from the list. You can also type in the input field to narrow down the list to the protocols whose names contain the characters you are typing. Click <b>X</b> next to an element to remove individual elements from the selection.
<b>Layer 4 Port</b>	Enable this option to check the traffic by layer 4 ports used. Enter the <b>Source Ports</b> and/or <b>Destination Ports</b> into the fields. The port numbers have to be separated by commas.

continues on next page

Table 5 – continued from previous page

Field	Description
<p><b>Classification</b></p>	<p>Enable this option to explicitly include or exclude applications and protocols in/from the rule. Click into the respective field and select the applications (preceded by A:) and protocols (preceded by P:) from the list. You can also type in the input fields to narrow down the list to the applications and protocols whose names contain the characters you are typing. Click <b>X</b> next to an element to remove individual elements from the selection. Threat Defender also provides groups of applications and protocols (preceded by G:).</p>
<p><b>Threats Indicators</b></p>	<p>Enable this option to select threats indicators to include in the rule. Select the tags you want to include by clicking into the respective field and selecting the tags from the list. You can also type in the input fields to narrow down the list to the tags whose names contain the characters you are typing. Click <b>X</b> next to an element to remove individual elements from the selection.</p>
<p><b>Intrusion Prevention System</b></p>	<p>Enable this option to specify the IPS rules to include in the rule. Click into the field and select the IPS tags from the list. You can also type in the input field to narrow down the list to the tags whose names contain the characters you are typing. Click <b>X</b> next to an element to remove individual elements from the selection.</p>

In the **Actions** section, click the toggles to activate the actions you want to apply to traffic matching the rule:

Field	Description
Log	<p>Enable this option to log rule hits to syslog, IPFIX and the reporting. There the following additional logging options:</p> <ul style="list-style-type: none"> <li>• Enable the <b>Late Log</b> option to log additional data when the flow has stopped. This way, the entire flow can be analyzed.</li> <li>• Enable the <b>Policy Hit</b> option to flag rule hits as incidents in the <a href="#">policy reporting</a> (page 144). They are also shown in the <b>Incident Logs</b>.</li> </ul> <p>Select the severity of the event in the logs by clicking the respective button. You can assign high, medium or low severity or log the event as notice.</p>
Final Action	<p>Enable this option to specify how traffic matching this rule is to be handled. You can select one of the following options:</p> <ul style="list-style-type: none"> <li>• <b>Allow Traffic and Skip to Next Scenario</b> - Traffic matching this rule is permitted and processing continues with the next scenario.</li> <li>• <b>Drop Traffic and Stop Processing</b> - Traffic matching this rule is silently dropped and rule processing for this traffic ceases.</li> <li>• <b>Reject Traffic and Stop Processing</b> - Traffic matching this rule is actively rejected and rule processing for this traffic ceases.</li> </ul>
Asset Tag	<p>Enable this option to tag or untag assets that match the rule conditions:</p> <ul style="list-style-type: none"> <li>• Select the <b>Operation</b> you want to perform, i.e. add or delete a tag.</li> <li>• Select the <b>Tag</b> you want to assign or remove. You can also enter a new asset tag.</li> <li>• Under <b>Who</b>, select which communication participant will be tagged or untagged.</li> </ul>

continues on next page

Table 6 – continued from previous page

Field	Description
<p><b>Dynamic Network Object</b></p>	<p>Enable this option to specify an action to be carried out for dynamic network objects:</p> <ul style="list-style-type: none"> <li>• Select the <b>Operation</b> you want to perform, i.e. add entries to or delete them from the <b>Target Dynamic Network Object</b>.</li> <li>• Under <b>Host Identifier</b>, specify what information is to be handled by the dynamic network object (IP addresses, MAC addresses, assets or all).</li> <li>• From the drop-down list, select <b>Who</b> the action is to be performed on.</li> <li>• Specify the <b>Target Dynamic Network Object</b> that is the target of the operation. Click <b>ADD DYNAMIC NETWORK OBJECT</b> to create a new dynamic network object.</li> </ul> <p>For further information, see <a href="#">Dynamic Network Objects</a> (page 156).</p>
<p><b>Shape Traffic</b></p>	<p>Enable this option to activate traffic shaping. Select the desired <b>Scope</b> from the drop-down list:</p> <ul style="list-style-type: none"> <li>• Select <b>Global</b> to shape all traffic matching the rule.</li> <li>• Select <b>Host Inbound/Outbound</b> to individually shape the inbound and outbound host traffic.</li> <li>• Select <b>Host Aggregated</b> to shape all host traffic.</li> </ul> <p>Enter the desired <b>Bandwidth</b>. Note that inbound and outbound bandwidth is seen from the perspective of Threat Defender.</p>
<p><b>Add to Event Tracking Table</b></p>	<p>Only available for rules in advanced correlation scenarios: Enable this option to add entries to an event tracking table. From the drop-down list, select the <b>Event Tracking Table</b> you want to add entries to. Specify what elements you want to add to the primary and secondary attributes of the new event in the respective drop-down lists.</p>

The buttons at the bottom of the screen allow you to store your changes (**SAVE**) or to discard them (**CANCEL**).




## 6.2.2 Advanced Correlation

Threat Defender uses [Correlation in Threat Defender](#) (page 74), also called advanced correlation, to analyze the network traffic and detect threats.

Threat Defender correlates current and historical traffic flows in real time. It uses event tracking tables to store combinations of attributes and track the properties of communication events across the traffic flows and over time. Threat Defender uses rules to add entries to the tables and to query them. No traffic passes Threat Defender without being handled by the correlation engine.

Navigate to **Policy > Advanced Correlation** to see an overview of all advanced correlation scenarios defined in the system. Threat Defender provides several predefined scenarios for the most common tasks.

The table displays the correlation scenarios with their **Name** and a **Note**. The toggle in the first column indicates whether a scenario is active () or inactive (). The icons in last column allow you to view the details of a scenario, edit its general settings or delete it from the system.


**Tip:** Using the  icon you can only edit the **Name** and **Note** of a scenario. To edit its security settings, double-click on the respective row in the overview table.


**Note:** cognitix Threat Defender processes the scenarios from top to bottom. Therefore, place more specific scenarios at the top of the table and scenarios that apply to a broader range of traffic at the bottom.

To reorder scenarios, click the **ACTIVATE REORDER** button above the table. Move the scenarios to the desired positions using drag and drop.

To add a new scenario to the system, click **Add** above the overview table.

### 6.2.2.1 Advanced Correlation Scenario Settings

After clicking **Add** or the  icon, you can change the general settings of the correlation scenario:

Field	Description
	The toggle indicates whether the scenario is enabled or disabled.
<b>Name</b>	Enter the name of the scenario.
<b>Note</b>	Optional: Add a short description of the scenario.

The buttons at the bottom of the screen allow you to store your changes (**SAVE**) or to discard them (**CANCEL**).

After saving the general settings of a correlation scenario or double-clicking on its row in the overview table, you can configure its security settings.

To reset the state of a correlation scenario, click **RESET STATE**. This will delete the content of all dynamic network objects and event tracking tables used in the scenario. The system prompts you to confirm the reset action.

For the security settings of the scenario, the following tabs are available:

- The **Rules** tab displays the rules included in the scenario. Click **Add** to add a new rule to the scenario. For further information, see [Rules](#) (page 145).
- The **Dynamic Network Objects** tab displays the dynamic network objects included in the scenario. Click **Add** to add a new dynamic network object to the scenario. For further information, see [Dynamic Network Objects](#) (page 156).
- The **Event Tracking Tables** tab displays the event tracking tables associated with this scenario. Click **Add** to add a new event tracking table to the scenario. For further information, see [Event Tracking Tables](#) (page 160).

Any changes you configure in these tabs are stored for the correlation scenario when you click **SAVE** in the respective tab.

**Additional References:**

- See also the concept description of [Correlation in Threat Defender](#) (page 74).
- For examples illustrating the usage of the Threat Defender correlation engine, see [Define the Policy](#) (page 80).

### 6.2.3 Network Objects

Navigate to **Policy > Network Objects** to segment your network by dividing it into logical segments using network objects. You can set up static and dynamic network objects, and configure VLANs.

Using network objects, you can apply **policy** rules to the traffic initiated from and sent to specific hosts in the network. You can use network objects in multiple rules and do not need to define them individually for every rule. If you assign a host to several network objects at once, you can layer multiple rules and apply them to that host.

### 6.2.3.1 Static Network Objects

Use static network objects to statically group hosts and devices.

Under **Static Network Objects**, the table displays the static network objects that are defined in the system and gives a summary of their configuration. For further information, see [Static Network Objects Settings](#) (page 155).

The icons in last column allow you to edit or delete the respective object.

**Tip:** The **IP Addresses** and **MAC Addresses** columns display the number of addresses that are defined as included or excluded for the static network object. Hover the mouse on the entries to display the individual addresses in a tooltip.

To add a new static network object to the system, click the **Add Global Static Network Object** button above the overview table.

#### Static Network Objects Settings

When you add a new static network object or edit an existing one, the settings screen is displayed.

The **General** section provides the following options:

Field	Description
<b>Name</b>	Enter the name of the object.
<b>Note</b>	Optional: Add a short description of the object.

The **Network Definition** section provides the following options:

Field	Description
<b>Network</b>	Allocate the network object to the <b>internal</b> or <b>external</b> network. Note that Threat Defender does not create asset database entries for hosts located in the <b>External</b> network.

continues on next page

Table 9 – continued from previous page

Field	Description
IP Addresses	Specify the IP addresses to be <b>Included</b> in the static network object. To define exceptions, specify the IP addresses to be <b>Excluded</b> from the static network object. Enter IP addresses in <b>CIDR</b> notation. The IP addresses have to be separated by commas.
MAC Addresses	Specify the MAC addresses of devices to be <b>Included</b> in the static network object. To define exceptions, specify the MAC addresses to be <b>Excluded</b> from the static network object. The MAC addresses have to be separated by commas. To indicate MAC address ranges, leave out pairs of characters while preserving the separating colons starting at the end of the MAC address. For example: 12:34:56:7::, 12::::.
VLANs	Click into the field and select the VLANs you want to assign to the network object from the list. If you do not select any VLAN, all available VLANs are included. Click <b>ADD VLAN</b> to open the VLAN settings screen and create a new VLAN (see <a href="#">VLANs</a> (page 158)).

The buttons at the bottom of the screen allow you to store your changes (**SAVE**) or to discard them (**CANCEL**).

### 6.2.3.2 Dynamic Network Objects

Dynamic network objects are dynamic lists of IP or MAC addresses. They are dynamically modified by policy [rules](#) (page 145).

Dynamic network objects track the state of hosts and create host groups with common behavior on the fly. The hosts of the group share a specific characteristic or property that is not static but depends on events happening dynamically in the running system. Based on this behavior, a specific set of rules is applied to them. This allows the policy engine to adapt to changing situations. It dynamically controls what rules are applied to different groups of hosts in real time.

Under **Dynamic Network Objects**, the table displays the dynamic network objects that are defined in the system and gives a summary of their configuration. For further information, see [Dynamic Network Objects Settings](#) (page 157).

The icons in last table column allow you to edit or delete the respective object.

**Tip:** Click the number in the **Counts** column to see the entries that the dynamic network object currently contains. If you want to delete the content of the dynamic network object, click **RESET STATE** in this view.

Global dynamic network objects are placed at the top of the table. Objects used in correlation scenarios are grouped by scenario. To add a new global dynamic network object to the system, click the **Add Global Dynamic Network Object** button above the overview table.

**Note:** To create dynamic network objects for correlation scenarios, you need to create them directly in the respective scenario. Click the name of the scenario to access its settings screen (see [Advanced Correlation Scenario Settings](#) (page 153)). In the **Dynamic Network Objects** tab, click **Add**.

### Dynamic Network Objects Settings

When you add a new dynamic network object or edit an existing one, the settings screen is displayed.

The **General** section provides the following options:

Field	Description
<b>Name</b>	Enter the name of the object.
<b>Note</b>	Optional: Add a short description of the object.

The **Settings** section provides the following options:

Field	Description
<b>Network</b>	Allocate the network object to the <b>internal</b> or <b>external</b> network. Note that Threat Defender does not create asset database entries for hosts located in the <b>External</b> network.
<b>Size</b>	Enter the maximum number of assets that can be added to the dynamic network object.

continues on next page

Table 11 – continued from previous page

Field	Description
Timeout	Specify in seconds for how long entries remain in the dynamic network object. When the set time expires, the entries are automatically removed from the dynamic network object. If you set the timeout to 0, entries are not removed automatically.
Forced Includes	Prefill the network object with hosts for the time specified in <b>Timeout</b> . Enter their IP addresses separated by commas.
Excluded IP Addresses	To define exceptions, specify IP addresses to be excluded from the dynamic network object. Enter the IP addresses separated by commas.
MAC Addresses	To define exceptions, specify MAC addresses to be <b>Excluded</b> from the dynamic network object. The MAC addresses have to be separated by commas. To indicate MAC address ranges, leave out pairs of characters while preserving the separating colons starting at the end of the MAC address. For example: 12:34:56:7::, 12:::..

The buttons at the bottom of the screen allow you to store your changes (**SAVE**) or to discard them (**CANCEL**).

**Note:** Rule evaluation is executed per **flow**, not per **packet**. When setting short timeouts, this means for longer-lasting flows that the timeout may expire while the flow still continues. In that case the dynamic network object will not be refreshed for that flow.

### 6.2.3.3 VLANs

Under **VLANs**, the table displays the VLANs that are defined in the system. The icons in the last column allow you to edit or delete the respective **VLAN**.

To add a new VLAN to the system, click the **Add** button above the overview table.

#### VLAN Settings

When you add a new VLAN or edit an existing one, the settings screen is displayed with the following options:

Field	Description
Name	Enter the name of the VLAN.
Note	Optional: Add a short description of the VLAN.
VLAN ID	Assign an ID to the VLAN by entering an integer from 0 to 4095. VLAN ID 0 matches all untagged networks.

The buttons at the bottom of the screen allow you to store your changes (**SAVE**) or to discard them (**CANCEL**).

#### Additional References:

- See also the concept of [Network Segmentation](#) (page 122).
- For examples that illustrate the usage of network objects, see [Use Network Segmentation](#) (page 131).

## 6.2.4 Schedules

You can set up custom time schedules to specify at what dates and times rules are applied to the network traffic.

Navigate to **Policy > Schedules** to see an overview of the time schedules currently defined in the system and a summary of their configuration. The icons in last column allow you to edit or delete the respective schedule.

**Tip:** Hover the mouse on the entries in the **Repeat** column to display the repetition details of the schedule in a tooltip.

To add a new schedule to the system, click the **Add** button above the overview table.

### 6.2.4.1 Schedules Settings

When you add a new time schedule or edit an existing one, the settings screen is displayed with the following options:

Field	Description
Name	Enter the name of the schedule.
Note	Optional: Add a short description of the schedule.

continues on next page

Table 13 – continued from previous page

Field	Description
Valid from/Valid until	Set a start and end date for the validity of the time schedule.
Repeat	<p>From the drop-down list, specify on what basis the time schedule should be repeated:</p> <ul style="list-style-type: none"> <li>• If you repeat the schedule on a <b>Weekly</b> basis, click into the <b>Valid Days of Week</b> field and specify on which days of the week it is active.</li> <li>• If you repeat the schedule on a <b>Monthly</b> basis, click into the <b>Valid Days of Month</b> field and specify on which days of the month it is active.</li> <li>• If you repeat the schedule on a <b>Yearly</b> basis, specify the dates on which it is active.</li> </ul>
Time Ranges	Optional: Click the <b>Add Time Range</b> button and specify a start and end time in HH:MM format if you want to limit the schedule to a specific time of the day. You can add multiple time ranges.

The buttons at the bottom of the screen allow you to store your changes (**SAVE**) or to discard them (**CANCEL**).

### 6.2.5 Event Tracking Tables

Event tracking tables are buffers that store combinations of attributes with timeouts for each entry. They track the properties of communication events across several traffic flows. Using individual timeouts for the entries, changes can be tracked over time and the entries can be automatically removed once the timeout has elapsed.

Navigate to **Policy > Event Tracking Tables** to see an overview of the event tracking tables currently defined in active correlation scenarios. The tables are grouped by scenario.

**Tip:** Click the number in the **Counts** column to see the entries that the event tracking table currently contains. If you want to delete the content of the event tracking table, click **RESET STATE** in this view.

To edit the settings of an existing event tracking table, click  in the last table column.



**Note:** New event tracking tables can only be created in correlation scenarios. Navigate to **Policy > Advanced Correlation**. Select the required scenario and double-click its name to access its **settings** (page 153). In the **Event Tracking Tables** tab, click **Add**.

### 6.2.5.1 Event Tracking Table Settings

When you configure an event tracking table, the settings screen is displayed with the following options:

Field	Description
<b>Name</b>	Enter the name of the event tracking table.
<b>Note</b>	Optional: Add a short description of the event tracking table.
<b>Retention Time for Event Tracking</b>	Specify in seconds for how long events will be stored in the event tracking table. The retention time expires individually for all entries. If you set the retention time to 0, events are stored permanently.
<b>Primary Attribute Type</b>	From the drop-down list, select the type of the primary attribute to be stored in the event tracking table. You can select any combination of the available attribute types.
<b>Maximum Number of Primary Attributes</b>	Enter the maximum number of primary attributes that may be stored in the event tracking table.
<b>Secondary Attribute Type</b>	From the drop-down list, select the type of the secondary attribute to be stored in the event tracking table. You can select any combination of the available attribute types.
<b>Maximum Number of Secondary Attributes per Primary One</b>	Enter the maximum number of secondary attributes that may be stored per primary attribute in the event tracking table.

The buttons at the bottom of the screen allow you to store your changes (**SAVE**) or to discard them (**CANCEL**).

**Note:** As long as an event tracking table is used in rules, it is not possible to change its **Primary Attribute Type** and **Secondary Attribute Type**.


#### Additional References:

- For general information on the concept of event tracking tables, see [Event Tracking Tables](#) (page 78).
- For instructions on how to view or delete the contents of an event tracking table, see [View the Content of Event Tracking Tables](#) (page 84).

## | 6.3 Inventory

cognitix Threat Defender maps the IP and MAC addresses of network devices to track [network assets](#) (page 60). Tracked assets are enriched with metadata such as last seen IP address, etc. Threat Defender also maps users to assets and logs user events.

**Note:** Asset tracking requires an active license. The maximum number of tracked assets depends on the selected license.

In the  **Inventory** menu, you can display overviews of the network assets and users as well as the asset and user information collected by Threat Defender. You can also edit the tracking settings for assets and users, create and restore backups of the assets and users databases, and create data exports on individual assets and users.

### 6.3.1 Assets

Under **Inventory > Assets**, you see the [network assets](#) (page 60) currently tracked by Threat Defender.

**Note:** Asset tracking requires an active license. The maximum number of tracked assets depends on the selected license.

If [automatic asset tracking](#) (page 169) is enabled, Threat Defender automatically learns the MAC addresses of the devices in the network and creates individual assets for them in the database. If your network contains devices with multiple MAC addresses, Threat Defender creates an individual entry for each MAC address. You have to consolidate them manually (see [Create a Network Inventory](#) (page 61)).

To manually add a new asset to be tracked by Threat Defender, e.g. for devices that are located in subnets, click the **Add** button above the information fields (see [Asset Settings](#) (page 168)).

Click **Create Report** if you wish to create a downloadable PDF report on the asset database. The report contains the entire assets table.




The information fields show the total number of assets by category:

- **Current** - the total number of assets currently stored in the database of Threat Defender.
- **Created** - the number of assets created in the past day.



- **Updated** - the number of assets updated in the past day.
- **Seen** - the number of assets that were active in the network in the past day.

The table displays the assets in the network. To manage multiple assets at once, mark their checkboxes in the first table column. Click **SELECT ALL** to select all visible assets.


You can then perform the following **List Actions**:

-  **Operations**: Add tags to the selected assets or remove tags from them. You can also merge several assets into one **Primary Asset**.
-  **Delete**: Delete the selected assets from the database.
-  **Reset Last Seen**: Delete the metadata currently stored in the **Last Seen** section of the selected assets.

The **Last Seen** column of the table shows the metadata collected for the asset when Threat Defender last saw it in the network. This means it will be empty if there is no outgoing traffic from this asset. Click **+** to show additional information and **-** to show less information.

The icons in the last table column allow you to directly access the reporting section under **Analytics** for the outbound () and inbound () traffic of the asset. You can also view the [asset details](#) (page 164) and edit the [asset settings](#) (page 168) or delete the asset.

### 6.3.1.1 Asset Details

To see further details on an asset, click  in the overview table or double-click its row. The details page displays the available information on the asset in several tabs.

The buttons at the top of the page allow you to edit or delete the asset. Click **Create Full Report** or **Create Summary Report** if you wish to create a downloadable PDF report on the asset. The full report contains all information displayed in the details page, including the charts. The summary report contains only the data tables.

### Summary

The **Summary** tab displays the configuration of the asset, information on the asset users as well as dynamically collected information.

The **Asset Config** table shows the configuration of the asset:

Field	Description
Tags	The tags assigned to the asset.

continues on next page

Table 15 – continued from previous page

Field	Description
Gateway	This field indicates whether the asset is a gateway (☑) or not (☐). For gateways, the IP addresses are not tracked.
Note	A short description of the asset, if available.
Created At	The date the asset was created in Threat Defender.
Updated At	The date the asset was last updated in Threat Defender.
IP Addresses	The IP addresses tracked for the asset.
MAC Addresses	The MAC addresses tracked for the asset.

The **Assigned Asset User** table shows information on the latest user who was manually assigned to this asset:


Field	Description
Name	The displayed name of the user.
Username	The internal login name of the user.
Domain	The domain assigned to the user.
Last Login At	The date when the user last logged in to the network.
Last Login From	The IP address used when the user last logged in to the network.
Last Logout At	The date when the user last logged out of the network.
Last Logout From	The IP address used when the user last logged out of the network.
Seen At	The date and time when the user was last active in the network.
Created At	The date and time when the user was created in Threat Defender.
Updated At	The date and time when the user was last updated in Threat Defender.

The **Last Seen** table displays information collected on the asset when it was last active in the network. If Threat Defender did not see any outgoing traffic from this asset, this table will be empty.

Field	Description
Seen	The date when Threat Defender last saw the asset in the network.
VLAN	The VLAN the asset belongs to.
IPv4 Addresses	The IPv4 addresses last used by the asset.
IPv6 Addresses	The IPv6 addresses last used by the asset.
MAC Vendors	The vendor and/or manufacturer of the asset.
DHCP Request Name	Hostname requested via DHCP.
DHCP Offer Name	Hostname offered via DHCP.
Bridge	The name of the bridge via that the asset communicates.
Interface	The interface of Threat Defender that sees the asset.

The Last Seen Asset User table shows information on the latest user who was dynamically mapped to this asset:

Field	Description
Name	The displayed name of the user.
Username	The internal login name of the user.
Domain	The domain assigned to the user.
Last Login At	The date when the user last logged in to the network.
Last Login From	The IP address used when the user last logged in to the network.
Last Logout At	The date when the user last logged out of the network.
Last Logout From	The IP address used when the user last logged out of the network.
Seen At	The date and time when the user was last active in the network.
Created At	The date and time when the user was created in Threat Defender.
Updated At	The date and time when the user was last updated in Threat Defender.

Click  RESET DATA to reset all tracking information Threat Defender gathered dynamically for this asset.


The Outbound Analytics and Inbound Analytics sections show charts that visualize the traffic information available for the asset. They are grouped in tabs by reporting period (last day,

last week, last month).

## Incidents

The **Incidents** tab displays an extract from the incidents log that contains the incidents involving the asset:

Field	Description
Created At	The date and time the incident was created in Threat Defender.
Severity	The severity logged for the incident.
Action	The rule action logged for the incident. Actions are allow, reject and drop.
Type	The type of the reported incident; IPS, IOC, or Policy hit.
Indicator	The detected threat indicator.
Classification	The applications and/or protocols involved in the event.
Assets	The source and destination assets involved in the incident.
IP Addresses	The source and destination IP addresses involved in the incident.
Ports	The source and destination ports involved in the incident.
Countries	The source and destination countries of the flow involved in the incident. If a private IP range is used, the country is displayed as Unknown or invalid territory.

Click the  in the last table column to go to the log entry under **Threats > Incident Logs**.

## Events

The **Events** tab displays log events involving the asset and asset users in separate tables:

Field	Description
Created At	The date and time the event was created in Threat Defender.
State	The state of the logged event, i.e. whether it was successful or failed.
Tag	The tag assigns the event to a certain log.
Action	The logged action.

continues on next page




Table 20 – continued from previous page

Field	Description
Message	A message describing the event.
Username	The login name of the user involved in the event.
User IP Address	The IP address of the user involved in the event.

Click the  in the last table column to go to the log entry of the respective event.

### 6.3.1.2 Asset Settings

When you manually add a new asset to be tracked or edit an existing one, the settings screen is displayed with the following options:

Field	Description
Name	Enter the name of the asset.
Note	Optional: Add a short description of the asset.
	The toggle indicates whether the asset is a gateway or not. For gateways, the IP addresses are not tracked.
User	Optional: Assign a static user to the asset. You can only map one user per asset. Click into the field and select the user from the list. You can also type in the input field to narrow down the list to the users whose names contain the characters you are typing.
Tags	Optional: Select the tags you want to assign to the asset or enter a new tag.
MAC Addresses	Enter the MAC addresses you want to assign to the asset into the input field and click <b>ADD</b> . Assigned MAC addresses are listed under <b>Value</b> . Click  to remove an address.
IP Addresses	Enter the IP addresses you want to assign to the asset into the input field and click <b>ADD</b> . Assigned IP addresses are listed under <b>Value</b> . Click  to remove an address.
Last Seen	The metadata collected for the asset when Threat Defender last saw it. Empty if there is no outgoing traffic from this asset.

The buttons at the bottom of the screen allow you to store your changes (**SAVE**) or to discard them (**CANCEL**).

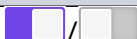


**Note:** Any changes of the asset settings will only be applied to future logging data. Any existing datasets in the database remain unchanged.

### 6.3.2 Asset Setting

Navigate to **Inventory > Asset Setting** to disable or enable automatic asset tracking as well as to define exceptions that will not be tracked.

The automatic discovery of assets is enabled by default. Threat Defender automatically creates a new asset database entry whenever an unknown MAC address is detected in the network. If automatic asset discovery is disabled, Threat Defender does not create new entries for new devices. In this case, they have to be added manually to be tracked.

Field	Description
	The toggle indicates whether automatic tracking of assets is enabled or disabled.
<b>Add this Tag to Auto Discovered Assets</b>	Optional: Enter a tag you want to automatically assign to newly discovered assets.
<b>Auto Discovery Limitation</b>	Specify a maximum value of how many assets Threat Defender discovers automatically. Irrespective of this value, license limitations remain in effect.
<b>MAC Addresses Excluded from Auto Discovery</b>	Optional: Define exceptions by adding MAC addresses you do not want to track automatically. You can enter multiple MAC addresses separated by commas. To exclude complete MAC prefixes, leave out pairs of characters while preserving the separating colons starting at the end of the MAC address. For example: 08:00:27::: for VirtualBox.
<b>Note</b>	Optional: Add a short description of the asset settings.

The buttons at the bottom of the screen allow you to store your changes (**SAVE**) or to discard them (**CANCEL**).

### 6.3.3 Users

Under **Inventory > Users**, you see the users currently tracked in the network.


Users can only be tracked if they are allocated to an asset. If the [user API](#) (page 174) is enabled, Threat Defender automatically maps users and assets. Otherwise, the allocation has to be done manually.

To manually add a new user to be tracked by Threat Defender, click the **Add** button above the information fields (see [User Settings](#) (page 174)).


Click **Create Report** if you wish to create a downloadable PDF report on the users database. The report contains the entire users table.

The information fields show the total number of users by category:

- **Current** - the total number of users currently stored in the database of Threat Defender.
- **Created** - the number of users created in the past day.
- **Updated** - the number of users updated in the past day.
- **Seen** - the number of users seen by Threat Defender in the past day.

The table displays an overview of the available user information. The  icon in last column allows you to directly access the reporting section under **Analytics** for the respective user. You can also view the [user details](#) (page 170), edit the [user settings](#) (page 174) or delete the user.

### 6.3.3.1 User Details

To see further details about a user, click  in the overview table or double-click its row. The details page displays the available information on the user in several tabs.

The buttons at the top of the page allow you to edit or delete the user. Click **Create Full Report** or **Create Summary Report** if you wish to create a downloadable PDF report on the user. The full report contains all information displayed in the details page, including the charts. The summary report contains only the data tables.

#### User

The **User** tab displays all information collected about the users when Threat Defender last saw them:

Field	Description
Name	The displayed name of the user.
Username	The internal login name of the user.
Domain	The domain assigned to the user.

continues on next page




Table 23 – continued from previous page

Field	Description
Last Login At	The date when the user last logged in to the network.
Last Login From	The IP address used when the user last logged in to the network.
Last Logout At	The date when the user last logged out of the network.
Last Logout From	The IP address used when the user last logged out of the network.
Seen At	The date and time when the user was last active in the network.
Created At	The date and time when the user was created in Threat Defender.
Updated At	The date and time when the user was last updated in Threat Defender.

## Assets

The Assets tab shows the assets associated with the user.

To manage multiple assets at once, mark their checkboxes in the first table column or click **SELECT ALL** to select all visible assets. You can then perform the following **List Actions**:



-  **Operations**: Add tags to the selected assets or remove tags from them. You can also merge several assets into one **Primary Asset**.
-  **Delete**: Delete the selected assets from the database.
-  **Reset Last Seen**: Delete the metadata currently stored in the **Last Seen** section of the selected assets.



The **Static Assets** table displays the assets that were manually assigned to this user:

Field	Description
Created At	The date when the asset was created in Threat Defender.
Name	The name of the asset.
User	The user associated to the asset.
Gateway	The icon in this column indicates whether the asset is a gateway (☑) or not (☹). For gateways, the IP addresses are not tracked.
Tags	The tags assigned to the asset.

continues on next page

Table 24 – continued from previous page

Field	Description
MAC Addresses	The MAC addresses tracked for the asset.
IP Addresses	The IP addresses tracked for the asset.
Last Seen	The metadata collected for the asset when Threat Defender last saw it. Click  to show additional information and  to show less information.

The icons in last table column allow you to view, edit or delete the respective asset. You can also access the reporting sections for its outbound () and inbound () traffic under **Analytics** by clicking the respective icon.

The **Auto connected assets via last seen** table displays the assets automatically allocated to this user.


Field	Description
Last Seen	The date and time when Threat Defender last saw the asset.
Name	The name of the asset.

The  icon in the last table column allows you to delete the asset.

### IP Addresses

The **IP Addresses** tab displays the IP addresses automatically allocated to this user at login.


Field	Description
Last Seen	The date and time when Threat Defender last saw the IP address.
IP Address	The assigned IP address.

The  icon in the last table column allows you to delete the IP address.

### Incidents

The **Incidents** tab displays an extract from the incident logs that contains the incidents involving the user:


Field	Description
Created At	The date and time the incident was created in Threat Defender.
Severity	The severity logged for the incident.
Action	The rule action logged for the incident. Actions are allow, reject and drop.
Type	The type of the reported incident; IPS, IOC, or Policy hit.
Indicator	The detected threat indicator.
Classification	The applications and/or protocols involved in the event.
Assets	The source and destination assets involved in the incident.
IP Addresses	The source and destination IP addresses involved in the incident.
Ports	The source and destination ports involved in the incident.
Countries	The source and destination countries of the flow involved in the incident. If a private IP range is used, the country is displayed as Unknown or invalid territory.

Click the  in the last table column to go to the log entry under **Threats > Incident Logs**.

## Events

The **Events** tab displays log events involving the user:

Field	Description
Created At	The date and time the event was created in Threat Defender.
State	The state of the logged event, i.e. whether it was successful or failed.
Tag	The tag assigns the event to a certain log.
Action	The logged action.
Message	A message describing the event.
Username	The login name of the user involved in the event.
User IP Address	The IP address of the user involved in the event.

If you click  in the last table column or double-click a log entry, you will be taken directly to the respective page in the [Audit Logs](#) (page 189).

## Analytics

The **Analytics** tab shows charts that visualize the traffic information available for the user. They are grouped in tabs by reporting period (last day, last week, last month).

### 6.3.3.2 User Settings

When you manually add a new user to be tracked or edit an existing one, the settings screen is displayed with the following options:

Field	Description
Associated Asset	If applicable, the assets associated to this user are displayed with their names and a link to their details pages.
Name	Enter the name to be displayed for the user.
Username	Enter the login name of the user.
Domain	Optional: Assign a domain to the user.
Note	Optional: Add a short description of the user.


The buttons at the bottom of the screen allow you to store your changes (**SAVE**) or to discard them (**CANCEL**).

### 6.3.4 User API Setting

Navigate to **Inventory > User Api Setting** to edit the user **API** settings of Threat Defender.

If the user API is enabled, Threat Defender automatically tracks users and maps their user-names to IP addresses.

The user API settings screen contains the following elements:

Field	Description
	The toggle indicates whether the user API is enabled or disabled.
Note	Optional: Add a short description of the API settings.
Secret Key	Enter the password for user API connections. Click <b>Show Password</b> if you want to display the password in plaintext.
Do Not Log These User-names	To define logging exceptions, enter the usernames of users you do not want to log events for. You can enter multiple usernames separated by commas.

continues on next page

Table 30 – continued from previous page

Field	Description
<b>Do Not Log These IP Addresses</b>	To define logging exceptions, enter the IP addresses you do not want to log user events for. You can enter multiple IP addresses separated by commas.
<b>Limit Access to These IP Addresses</b>	Create a whitelist of IP addresses you want to log user events for. If this field contains IP addresses, Threat Defender will only log events for the IP addresses in this list. Events generated by other IP addresses will not be logged. You can enter multiple IP addresses separated by commas.
<b>Auto-Expire Learned IP Addresses</b>	Specify after how many days Threat Defender will forget the learned user/IP address mappings. If you set this value to 0, the mappings are stored permanently.

The buttons at the bottom of the screen allow you to store your changes (**SAVE**) or to discard them (**CANCEL**).

### 6.3.5 Backup/Restore

Navigate to **Inventory > Backup/Restore** to create and restore backups of your assets and users databases.

We recommend creating backups as soon as you have created a clean inventory of your network assets and users. In addition to securing the databases, this allows you to transfer the databases from one Threat Defender to another.

#### 6.3.5.1 Assets


Navigate to **Inventory > Backup/Restore > Assets** to create and restore backups of your assets database.

#### Backup

Under **Backup**, the **Generate Downloadable Assets** button allows you to create a new backup file of the assets currently tracked by Threat Defender.

The table displays the latest assets backup file with its creation date, an automatically generated file name, and the file size.

**Note:** Older assets backup files are overwritten when a new file is created.

With the  icon in the last column, you can save the backup file to your file system.

## Restore

Under **Restore**, you can upload an assets backup file created earlier. This will replace your current assets database.

**Note:** Restoring assets works best from an empty database to avoid duplicate entries. Make sure that asset auto discovery is disabled under [Asset Setting](#) (page 169). Then clear the assets database before restoring the assets backup file.

Click **SELECT** to access the file system where you can choose the desired assets backup file (.json format).

To restore the backup file, click the **Upload** button at the bottom of the screen. If you do not want to upload the file, click **CANCEL**.

Restoring large asset databases may take a while depending on your hardware and the size of the assets backup file. Do not shut down Threat Defender during the restoration process. You can see how the restoration progresses by keeping an eye on the **Current** counter under **Inventory > Assets**.

### 6.3.5.2 Users


Navigate to **Inventory > Backup/Restore > Users** to create and restore backups of your users database.

## Backup

Under **Backup**, the **Generate Downloadable Users** button allows you to create a new backup file of the users currently tracked by Threat Defender.

The table displays the latest users backup file with its creation date, an automatically generated file name, and the file size.

**Note:** Older users backup files are overwritten when a new file is created.

With the  icon in the last column, you can save the backup file to your file system.



## Restore

Under **Restore**, you can upload a users backup file created earlier. This will replace your current users database.

Click **SELECT** to access the file system where you can choose the desired users backup file (.json format).

To restore the backup file, click the **Upload** button at the bottom of the screen. If you do not want to upload the file, click **CANCEL**.

Restoring large user databases may take a while depending on your hardware and the size of the users backup file. Do not shut down Threat Defender during the restoration process. You can see how the restoration progresses by keeping an eye on the **Current** counter under **Inventory > Users**.

## 6.3.6 Data Export

Navigate to **Inventory > Data Export** to create reports that contain all data collected on a selected asset or user in compliance with the with right of access as stipulated by the GDPR.

### 6.3.6.1 Assets

Click **Add** to create a new data export report. You can then select the asset whose data you want to export. You can also type in the input field to narrow down the list to the assets whose names contain the characters you are typing.

The table displays the available data exports with their respective update time, automatically generated file name, and the creation status.

The buttons in the last column allow you to download and delete the data export.


### 6.3.6.2 Users

Click **Add** to create a new data export report. You can then select the user whose data you want to export. You can also type in the input field to narrow down the list to the users whose names contain the characters you are typing.

The table displays the available data exports with their respective update time, automatically generated file name, and the creation status.

The buttons in the last column allow you to download and delete the data export.

## 6.4 Threats

In the  Threats menu, you can see charts of the security incidents logged in your network, view incident logs and search the intelligence database of Threat Defender.

Threat Defender integrates a continuously active threats subsystem that is designed to handle an optimized data structure and therefore causes no performance losses. It provides a bundle of feeds from multiple sources. These feeds contain various types of data, such as information on downloads of ransomware, C&C server domains and so on.

Threat Defender compares all network traffic flows to these feeds in real time. If a threat indicator is discovered, the policy engine can be used to log the event and/or intercept the concerned traffic.

### 6.4.1 Overview

Navigate to **Threats > Overview** to display incidents logged in your network.

With the buttons at the top of the content area, you can select the reporting period. In the information fields and in the **Logs Severities** charts, the incidents logged in the selected reporting period are displayed by level of severity.

There are four levels of severity:

- High
- Medium
- Low
- Notice

The other charts on this dashboard display the countries, assets, and internal IP addresses involved in the logged incidents. The **IPS**, **MISP**, and policy events detected by Threat Defender are also displayed.

**Note:** Information on **Source Countries** and **Destination Countries** is based on **GeoIP** values. If you use a private IP range, the source and/or destination country is displayed as **Unknown** or **invalid territory**.




From here, you can drill down into deeper reporting levels to further investigate any suspicious traffic.

## 6.4.2 Incident Logs

Navigate to **Threats > Incident Logs** to view the incident logs created by Threat Defender.


By default, the log displays all incidents contained in the database. You can create nine different downloadable PDF reports of the incident logs that vary with respect to the reporting period and the reported data by clicking the respective button at the top of the screen.

The chart and the **Incident Logs** table next to it display the incidents logged in the previous 24 hours over time and by severity. If you click a section of the chart or the table, the log is automatically filtered accordingly.

You can also filter the log entries using the  filter field above the log table. Alternatively, you can filter the log table by hovering the mouse over one of the cells and clicking  to include or  to exclude matching elements in the filtered results.

Filtered views display the active filters. Click  to remove the respective filter option.

### 6.4.2.1 Incident Details

To see further details on a log entry, click  in the last table column or double-click its row. The details page displays the available information on the logged TI incident in several tabs.


Click **Create Full Report** or **Create Summary Report** at the top of the screen if you wish to create a downloadable PDF report on the incident. The full report contains all information from all tabs displayed in the details page. The summary report contains only the information on the **Event** tab.

The **Event** tab provides an overview of the logged incident:

Field	Description
<b>Created At</b>	The date and time the incident was logged.
<b>Severity</b>	The severity of the detected incident.
<b>Action</b>	The rule action logged for the incident. Actions are allow, reject and drop.
<b>Type</b>	The type of the reported incident; IPS, IOC, or Policy hit.
<b>Policy</b>	The policy involved. Click the policy to directly access the correlation scenario under <a href="#">Advanced Correlation</a> (page 153).
<b>Rule</b>	The name of rule that logged the incident. Click the rule to directly access the relevant section in <a href="#">Analytics</a> (page 142).

continues on next page

Table 31 – continued from previous page

Field	Description
Indicator Value	The value of the detected indicator.
IPS Rule	The IPS rule that was triggered. Click the rule to access its entry in the intelligence database of Threat Defender.
Classification	Under classification, you see the application and/or protocol involved in the incident. Click the entry to directly access the relevant section in <a href="#">Analytics</a> (page 142).
User	Click the  icon and/or the name of the user involved in the incident to access the relevant section in <a href="#">Analytics</a> (page 142).
Transport	The transport protocol used.
VLAN	The VLAN ID of the flow involved of the incident.
Flow Id	The ID of the flow involved in the incident.
URL	The URL involved in the incident.
Source/Destination	This table displays source and destination information on the traffic flow involved in the incident: interfaces, assets, MAC and IP addresses, locations, ports and countries. Many of the entries are links that take you to the relevant sections in <a href="#">Analytics</a> (page 142).

In addition to information on the incident itself, the details page also aggregates the following data, where available:

- The **Related Indicators** tab shows information on any indicators related to the incident.
- The **Source Asset** and **Destination Asset** tabs display excerpts from the assets database with information on the source and destination assets involved in the incident. See [Asset Details](#) (page 164) for further information on the data tables.
- The **User** tab provides information on the user of the source asset from the users database. See [User Details](#) (page 170) for further information on the data tables.

### 6.4.3 Intelligence Database

Navigate to **Threats > Intelligence Database** to view all static information contained in the intelligence database of Threat Defender. Here, you can also upload custom IPS rule sets.

### 6.4.3.1 Summary

The **Summary** presents the total number of events and attributes assigned to them as well as the total number of IPS rules supported by Threat Defender.


The tables display the events and IPS rules most recently added to the database. Click one of the entries to directly access its details page.

For further information, see the following sections.

### 6.4.3.2 Events

The **Events** table displays an overview of the events contained in the intelligence database of Threat Defender.

**Tip:** Hover the mouse on the number in the **Tags** column to display the tags in a tooltip.

To see further details on an event, click  in the last table column or double-click its row.


#### Event Details

The details page displays the name of the event and the following details:

Field	Description
Threat Level	The threat level assigned to the event in the database. There are four threat levels: high, medium, low and unknown.
Analysis	The status of the community analysis of the event.
Created	The date and time the event was created.
Updated	The date and time when the event was last updated in the intelligence database.

The **Tags** section shows the tags assigned to the event in the database.

The **Related Events** section displays a list of events linked to the current event. Click an entry to access its details page.

The **Most Recent Logs** table displays the most recently created entries in the [Incident Logs](#) (page 179). Click  in the last table column of an entry to go its details page.

The **External Analysis** table displays any further external information on the event, such as external links, comments on the event and so on.

The **Attributes** table displays all attributes assigned to the event.

The table contains the following information:


Field	Description
Updated At	The date and time when the attribute was last updated in the database.
Category	The category of the attribute.
Type	The type of the attribute.
Value	The value of the attribute. By mouseover you can see the full value in a tooltip.
Tags	The number of tags assigned to the attribute. By mouseover you can see the tags in a tooltip.
Indicator	The icon in this column indicates whether the attribute is an indicator of compromise or attack (☑) or not (☹).

### 6.4.3.3 Attributes

The **Attributes** submenu shows all event attributes contained in the intelligence database of Threat Defender.



The table provides the following information:

Field	Description
Updated At	The date and time when the attribute was last updated in the database.
Category	The category of the attribute.
Type	The type of the attribute.
Value	The value of the attribute. By mouseover you can see the full value in a tooltip.
Tags	The number of tags assigned to the attribute. By mouseover you can see the tags in a tooltip.
Indicator	The icon in this column indicates whether the attribute is an indicator of compromise or attack (☑) or not (☹).

Click the  icon in the last table column of an attribute to access the details page of the event this attribute is assigned to.

#### 6.4.3.4 IPS Rules



The **IPS Rules** table shows the IPS rules contained in the intelligence database of Threat Defender.

With the toggle in the first column you can enable () or disable () the IPS rule.

**Tip:** Hover the mouse on the number in the **Tags** column to display the tags in a tooltip.

To see further details on an IPS rule, click  in the last table column or double-click its row.


#### IPS Rule Details

The details page displays the name of the IPS rule. With the toggle you can enable () or disable () the IPS rule. The table shows the following details:

Field	Description
<b>Sid</b>	The signature ID of the IPS rule. It is unique for each rule in the database.
<b>Rev</b>	The revision number of the IPS rule.
<b>Created</b>	The date and time the IPS rule was created. Per <a href="#">ET<sup>23</sup></a> convention dates must not be empty, therefore 1970-01-01 is used as default if no date is specified.
<b>Updated</b>	The date and time when the IPS rule was last updated in the database. Per <a href="#">ET<sup>24</sup></a> convention dates must not be empty, therefore 1970-01-01 is used as default if no date is specified.
<b>Needed</b>	Indicates whether the IPS rule is required by a policy rule (☑) or not (☹).
<b>Loaded</b>	Indicates whether a needed IPS rule was loaded successfully (☑) or not (☹).
<b>Raw rule</b>	The raw rule content before it is parsed.

Under **Tags**, you see the tags assigned to the IPS rule in the database.



Under **References**, you see a list of references that document the IPS rule, if available.

The **Most Recent Logs** table displays the most recently created **Incident Logs** (page 179) for the IPS rule. Click  in the last table column of an entry to go its details page.

### 6.4.3.5 IPS Settings


Navigate to **Threats > Intelligence Database > IPS Settings** to upload and manage IPS rule sets.

All rules from all enabled IPS rule sets are loaded and evaluated. If two rule sets contain rules with an identical ID (**sid** (page 246) keyword), the rule with the higher revision number (**rev** (page 246) keyword) takes precedence.

The table displays the default rule set and the custom rule sets with their names, optional notes, and statistics. With the toggle in the first column you can enable () or disable () an IPS rule set. All rules in all enabled rule sets are loaded consecutively in the order displayed in the unsorted table.

**Note:** If you want to turn the IPS off, disable all IPS rule sets in this table.

The table shows the following details. Statistical information is only available for activated rule files.

Field	Description
	The toggle indicates whether the IPS rule set is enabled or not.
<b>Name</b>	The name of the IPS rule set.
<b>Note</b>	Optional: A short description of the IPS rule set.
<b>Number of Rules</b>	The number of rules that were identified and tried to be parsed.
<b>Usable Rules</b>	The number of rules that were successfully parsed.
<b>Newer Rules</b>	The number of rules from older rule files that were overwritten by this rule file.
<b>Outdated Rules</b>	The number of rules in this rule file that were not loaded because previously loaded rules took precedence.

<sup>23</sup> <https://doc.emergingthreats.net/>

<sup>24</sup> <https://doc.emergingthreats.net/>



The total number of active IPS rules amounts to the number of **Usable Rules** minus the sum of **Newer Rules** and **Outdated Rules**.

The icons in the last table column allow you to download or delete an IPS rule set.

**Note:** The default rule set `System IPS Rules.csv` cannot be deleted.


### IPS Rule Set Upload

genua regularly provides updated IDS rule sets that you can download at <https://files.cognitix.de/pattern/ids-rules.pfw>.

You can also write custom IPS rule set files. IPS rule set files can be `.rules`, `.csv` or `.txt` files.

To upload a new IPS/IDS rule set, click **Upload** above the overview table.

When you upload an IPS rule set file, the upload screen is displayed with the following elements:


Field	Description
	The toggle indicates whether the IPS rule set is enabled or not.
<b>SELECT</b>	Access the file system where you can select the IPS rule set file ( <code>.rules</code> , <code>.csv</code> or <code>.txt</code> format).
<b>Note</b>	Optional: Add a short description of the IPS rule set.

To use the IPS rule set file, click the **UPLOAD** button at the bottom of the screen. If you do not want to upload the file, click **CANCEL**.

### Additional References:

For information on the keywords used in IPS signatures, refer to [IPS Rule Definitions](#) (page 243).

## 6.5 Network

In the  Network menu, you can view the available processing interfaces of Threat Defender and organize them in bridges.

### 6.5.1 Overview



Navigate to **Network > Overview** to see the configured bridges and available processing interfaces.

The **Interfaces Analytics** link at the top of the screen takes you directly to the relevant charts under [Analytics](#) (page 142) and the **MAC Table Reporting** link takes you to the MAC table live view under [Diagnostics](#) (page 211).

The **Bridges** table shows the configured bridges with the following information:



Field	Description
Name	The name of the bridge.
Links Up / Links Down	The number of interfaces in the bridge that are up and/or down to indicate the status of the bridge.
Active MAC Addresses	The number of MAC addresses that communicate via the bridge.
Description	A short description of the bridge configuration.

The **Interfaces** table displays the interfaces available in the system:

Field	Description
Name	The name of the interface.
Link Detected	The connection status of the interface, i.e.  (up) or  (down).
Current Link Speed	The link speed of the interface.
Received Bytes / Sent Bytes	The number of bytes that were received and sent via the interface.
Received Packets / Sent Packets	The number of packets that were received and sent via the interface.
Errors	The number of errors generated. Hover the mouse over the number in the <b>Errors</b> column to display the error distribution in a tooltip.

## 6.5.2 Manage Processing Interfaces

Navigate to **Network > Manage Processing Interfaces** to see the current processing interfaces configuration.

With the toggle at the top of the screen you can enable () or disable () the default configuration. In the default configuration, all processing interfaces belong to a single bridge providing a working fallback setup.

**Note:** While the default configuration is active, changes of the processing interface groups have no effect. They will only be activated after you disable the default configuration and click **APPLY CHANGES**.

The table displays the available groups with port ID and VLAN range. The icons in the last table column allow you to edit or delete processing interface/bridge allocations.

**Tip:** Processing interfaces belonging to the same bridge have the same name in the **Bridge** column. To see which bridge contains what interfaces, click the **Bridge** header to organize the table by bridges.

To add a bridge, click the **Add** button above the overview table.

### 6.5.2.1 Processing Interface Group Settings

When you add or edit a bridge, the settings screen is displayed with the following elements:

Field	Description
Bridge	Enter the name of the bridge.
Port	Select the processing interface you want to assign to this bridge.
VLAN Range	Optional: Enter the VLAN ranges applicable to the bridge.

The buttons at the bottom of the screen allow you to store your changes (**SAVE**) or to discard them (**CANCEL**).

**Note:** Only interfaces that belong to the same bridge can communicate with each other.


To activate your customized processing interfaces configuration, you need to disable the default configuration.

---

**Additional References:**

For examples of useful interface configurations, see [Manage the Processing Interfaces](#) (page 46).




## 6.6 Logging

In the  **Logging** menu, you can access the audit logs and local logs on Threat Defender. You can also set up notification channels for the audit logs and configure the logging system to export logging messages to your own **IPFIX** and/or **syslog** server or via JSONL.


### 6.6.1 Audit Logs

Navigate to **Logging > Audit Logs** to view the audit logs created by Threat Defender. Audit logs aggregate reported events from the user and asset logs, system logs, as well as incident logs.

The chart displays the events logged in the previous 24 hours over time and by category.

You can filter the audit log entries using the  filter field above the table. Alternatively, you can filter the log table by hovering the mouse over one of the cells and clicking  to include or  to exclude matching elements in the filtered results.

#### 6.6.1.1 Event Details

Click  in the last table column or double-click its row to display the entry in a separate audit log page.

The table displays the following information:

Field	Description
<b>Created At</b>	The date when the audit log event was created in Threat Defender.
<b>State</b>	The state of the logged event, i.e. whether it was successful or failed.
<b>Action</b>	The action logged by the event.
<b>Tag</b>	The tag assigns the event to a certain log.
<b>Message</b>	A message describing the event. If applicable, this entry provides a link to the relevant screens.
<b>Username</b>	The login name of the user involved in the event.
<b>User IP Address</b>	The IP address of the user involved in the event.

## 6.6.2 Audit Log Channels

Threat Defender can send notifications of audit log events via email, webhook and desktop notification. The notifications contain reported events from the user and asset logs, system logs, as well as incident logs. Navigate to **Logging > Audit Log Channels** to set up notification channels.

To set up a new audit log channel, click the **Add** button above the overview table (see [Audit Log Channel Settings](#) (page 192)).


Threat Defender provides three audit log channels:

- **Email** – Threat Defender sends audit log information to a specified email address. For this purpose, Threat Defender needs to be able to contact a mail server.
- **Webhook** – Threat Defender sends audit log notifications via webhook to Slack-compatible applications.
- **Desktop** – Threat Defender pushes notifications as pop-ups to the desktop. To see the desktop notifications, you need to be logged in to the GUI of Threat Defender.

You can select various event categories to be included in the notifications, such as events concerning system actions (e.g. boot up, shutdown), license and update events, events concerning assets and users, TI incidents, etc.

The table displays the audit log channels configured in the system with an auto-generated, descriptive name, and the date and number of successfully transmitted messages as well as failures. The toggle in the first column allows you to enable () or disable () the audit log channel. The icons in the last column allow you to view the details on the respective audit log channel as well as to edit or delete the channel.

### 6.6.2.1 Audit Log Channel Details

To see the details of an audit log channel, click  in the overview table or double-click its row. The details page displays the available information on the channel in several tabs.

The buttons at the top of the page allow you to edit or delete the audit log channel.

#### Audit Log Channel

The **Audit Log Channel** tab displays general information on the audit log channel. Depending on the selected type of audit log channel, the **Configured** table shows its configuration details:

Field	Description
Enabled	The icon in this column indicates whether the audit log channel is enabled (☑) or disabled (☒).
Name	The auto-generated name of the channel.
Note	An optional description of the channel.
Type	The selected type of audit log channel.
From Address	Only for <b>Email</b> reports: The email address of the sender.
To Address	Only for <b>Email</b> reports: The email address of the recipient.
Hostname	Only for <b>Email</b> reports: The mail server used.
Port	Only for <b>Email</b> reports: The port that Threat Defender sends the messages to.
SMTPS	Only for <b>Email</b> reports: The icon in this column indicates whether the email is sent via SMTPS (☑) or not (☒).
Username	Only for <b>Email</b> reports: The username used for authentication at the mail server.
Password	Only for <b>Email</b> reports: The password used for authentication at the mail server.
Uri	Only for <b>Webhook</b> reports: The URI Threat Defender sends the notifications to.
Channel	Only for <b>Webhook</b> reports: The channel Threat Defender sends notifications to.
Username	Only for <b>Webhook</b> reports: The username of the sender of the notifications, e.g. td.
Icon URL	Only for <b>Webhook</b> reports: An optional URL if an icon is used in the notification.
Created At	The date when the channel was created in Threat Defender.
Updated At	The date when the channel was last updated in Threat Defender.

The **Statistics** table shows statistical information on the messages sent via the channel:

Field	Description
Sent At	The date when the most recent audit log notification was sent via the audit log channel.
Sent	The total number of notifications sent via this channel.


continues on next page

Table 43 – continued from previous page

Field	Description
Failed At	The date when sending an audit log notification most recently failed via the channel.
Failed	The total number of failed notifications via this channel.
Fail Message	An error message that indicates why the failure occurred.

Click **TEST CHANNEL** at the bottom of this page to test the audit log channel by immediately sending a notification.

### Matched Events and Unsent Events

The **Matched Events** tab displays the audit log events that were sent via this audit log channel. The **Unsent Events** tab displays the audit log events that were not yet sent via this audit log channel, but will be sent when the next notification is scheduled. Click  to access the respective event in the [Audit Logs](#) (page 189).





The tables on the two tabs show the following information:

Field	Description
Created At	The date and time the event was created in Threat Defender.
State	The state of the logged event, i.e. whether it was successful or failed.
Tag	The tag assigns the event to a certain log.
Action	The action logged by the event.
Message	A message describing the event.
Username	The login name of the user involved in the event.
User IP Address	The IP address of the user involved in the event.

### 6.6.2.2 Audit Log Channel Settings

If you add or edit an audit log channel, the settings screen is displayed with the following elements:



Field	Description
	The toggle indicates whether the audit log channel is enabled or not.
Note	Optional: Add a short description of the channel.
Report Type	Select the type of report you want to send by clicking the respective button.
Hostname	Only for <b>Email</b> reports: Specify the mail server you want to use.
Port	Only for <b>Email</b> reports: Specify the port that Threat Defender sends the messages to.
	Only for <b>Email</b> reports: Set the toggle to  to connect via TLS, or to  to connect via plain text.
Username	Only for <b>Email</b> reports: Enter the username for authentication at the mail server.
Password	Only for <b>Email</b> reports: Enter the password for authentication at the mail server. Optional: Click <b>Show Password</b> if you want to display the password in plaintext.
From Address	Only for <b>Email</b> reports: Enter the email address of the sender, e.g. td@company.com.
To Address	Only for <b>Email</b> reports: Enter the email address of the recipient.
Webhook URL	Only for <b>Webhook</b> reports: Enter the URL you want to send the notifications to.
Username	Only for <b>Webhook</b> reports: Enter the username of the sender of the notifications, e.g. td.
Channel	Only for <b>Webhook</b> reports: Enter the channel you want to send notifications to.
Icon URL	Only for <b>Webhook</b> reports: Optional. Enter a URL if you want to use an icon in the notification.
Filter by These Categories	Select the event categories you want to include in the report. You can type in the input field to narrow down the list to the categories that contain the characters you are typing. Click <b>X</b> next to an element to remove individual categories from the selection.

continues on next page

Table 45 – continued from previous page



Field	Description
Interval	Select the frequency in which notifications will be generated by clicking the respective button. If you select Immediate, you will be immediately notified of every new event.

The buttons at the bottom of the screen allow you to store your changes (**SAVE**) or to discard them (**CANCEL**).

### 6.6.3 Report Channels

cognitix Threat Defender can forward logging data to external recipients. Navigate to **Logging > Report Channels** to set up reporting channels for the log messages.


You can send log messages using **syslog**, **JSONL**, or **IPFIX**. See the appendix for further information on the **syslog Specification** (page 233), **JSON Lines Formatted Output** (page 223), and **IPFIX Specification** (page 226). When you use IPFIX to transmit traffic flow information, note that cognitix Threat Defender uses standard reporting events as well as custom events.

The table displays the reporting channels configured in the system with an auto-generated, descriptive name, connection state, and the number of transmitted and dropped messages. The toggle in the first column allows you to enable () or disable () the reporting channel. The icons in the last column allow you to edit or delete the respective reporting channel.

To set up a new reporting channel, click the **Add** button above the overview table.

#### 6.6.3.1 Report Channel Settings

If you add or edit a reporting channel, the settings screen is displayed with the following elements:

Field	Description
	The toggle indicates whether the reporting channel is enabled or not.
Note	Optional: Add a short description of the channel.
Report Type	Select the export standard by clicking the respective button.

continues on next page

Table 46 – continued from previous page

Field	Description
Message Type	Select what information you want to include in the messages.
Observation Domain Id	Only for IPFIX: Specify the observation domain ID used in the messages. It should be 0 when no specific observation domain ID is relevant for the entire IPFIX message.
Update Interval	Only for IPFIX: Set the IPFIX update interval.
Endpoint	Select the transport protocol you want to use by clicking the respective button, i.e. UDP, TCP, or TLS encryption.
IP Address	For UDP and TCP: Specify the IP address you want to send the reports to.
Hostname	Only for TLS encryption: Enter the hostname of the remote end you want to send the reports to.
Port	Specify the port that Threat Defender sends the messages to.
Reconnection Delay	Specify the intervals at which Threat Defender tries to re-establish the connection to the host.
Remote certificate authority	Only for TLS encryption: If you selected TLS encryption under <b>Endpoint</b> , select the remote CA (.pem format) created by the remote end.
Threat Defender certificate authority	Only for TLS encryption: You can download the CA created by cognitix Threat Defender in .pem format.


The buttons at the bottom of the screen allow you to store your changes (**SAVE**) or to discard them (**CANCEL**).

#### Additional References:


- See the [syslog Specification](#) (page 233).
- See [JSON Lines Formatted Output](#) (page 223).
- See the [IPFIX Specification](#) (page 226).

### 6.6.4 Local Logs

Navigate to **Logging > Local Logs** to see the local logs of system events, errors, etc.

By default, the logs are automatically updated to display the latest messages. If you want to disable automatic updating, set the **Auto Update** toggle to . The logs are then no longer updated until you turn the automatic update back on.


## | 6.7 Settings

In the  **Settings** menu, you can configure the general system settings of Threat Defender, such as the hostname and time settings. Furthermore, you can set up proxy access, configure the management interface, set up monitoring connections, manage the system users and updates, install a license as well as create and restore system backups. In addition, you can manage a connection to a genucenter system. You can also reboot Threat Defender and clear the reporting, assets and users databases.

### 6.7.1 General

Navigate to **Settings > General** to configure the general system settings of Threat Defender, [proxy server](#) access, the management interface, and time settings.

#### 6.7.1.1 General Settings

The table in this section displays the currently active system settings of Threat Defender. To change these settings, click the  icon in the last column of the table.

The settings screen contains the following elements:

Field	Description
Hostname	Enter the hostname of Threat Defender.
System Uri	Enter the URI you want to use in emails and PDF reports to identify Threat Defender.
Analytics Mode	Select a privacy mode for Threat Defender: <ul style="list-style-type: none"> <li>• <b>On</b> – Threat Defender collects all available information, including all user-related data.</li> <li>• <b>Realtime</b> – Threat Defender stores data related to individual users for only one minute.</li> <li>• <b>Off</b> – Threat Defender does not collect any data that can be allocated to individual users.</li> </ul>

continues on next page


Table 47 – continued from previous page

Field	Description
<b>Password Strength</b>	<p>Set the global requirements for system user passwords:</p> <ul style="list-style-type: none"> <li>• <b>Minimum Length</b> - the minimum permissible password length is 6 characters.</li> <li>• Use the toggles to enable or disable complexity requirements and password expiration.</li> <li>• If password expiration is enabled, specify the expiration period in months.</li> </ul>

The buttons at the bottom of the screen allow you to store your changes (**SAVE**) or to discard them (**CANCEL**).

Click the **APPLY CHANGES** button at the top of the main navigation to activate your configuration changes.

### 6.7.1.2 Management Interface

The table in this section displays the management interface and its configuration. The  icon in the last column allows you to change the settings of the management interface.

The settings screen contains the following elements:

Field	Description
<b>DHCP Client</b>	Select this checkbox if you want to enable DHCP and automatically assign an IP address to the management interface.
<b>Address</b>	Only available if DHCP is disabled: Enter the static IP address of the management interface in <b>CIDR</b> notation.
<b>Gateway</b>	Only available if DHCP is disabled: Enter the gateway of the management interface.
<b>DNS Addresses</b>	Only available if DHCP is disabled: Enter the IP addresses of the domain name servers that resolve host and domain name requests. The IP addresses have to be separated by commas.






**Warning:** If you change the IP address of the management interface, the web interface will no longer respond at the previous address. To access the web interface after changing the IP address of the management interface, open a new browser tab and enter the new IP address in the address bar.


The buttons at the bottom of the screen allow you to store your changes (**SAVE**) or to discard them (**CANCEL**).

Click the **APPLY CHANGES** button at the top of the main navigation to activate your configuration changes.

### 6.7.1.3 Proxy

The table in this section displays the proxy configuration. The toggle in the first column allows you to enable () or disable () the proxy. Click the  icon in the last column to edit the proxy settings.

The proxy settings screen contains the following elements:


Field	Description
	The toggle indicates whether proxy access is enabled or disabled.
Proxy	Enter the URI of the proxy server, e.g. <code>http://proxy.example.com:8080</code> . If you also want to specify a username and password for the proxy, use the following format: <code>http://username:password@proxy.example.com:8080</code>
Note	Optional: Add a short description of the proxy.

**Tip:** When using domains in the username, avoid the backslash by using `|5C` instead.

The buttons at the bottom of the screen allow you to store your changes (**SAVE**) or to discard them (**CANCEL**).

Click the **APPLY CHANGES** button at the top of the main navigation to activate your configuration changes.

### 6.7.1.4 Time

The table in this section displays the current time settings of Threat Defender. To change these settings, click the  icon in the last column of the table.

The settings screen contains the following elements:

Field	Description
Time Zone	Select the correct time zone from the drop-down list.
NTP	Set the toggle to <input type="checkbox"/> if you want to use an NTP server.
NTP Servers	If you enable NTP, enter the desired NTP servers. You can enter multiple servers separated by commas.
MANUALLY SET CURRENT TIME	Click this button to manually set the date and time of Threat Defender using a date picker.

The buttons at the bottom of the screen allow you to store your changes (**SAVE**) or to discard them (**CANCEL**).

If NTP is activated, this section also shows NTP server information:

- Click **Force Time Synchronization** to manually synchronize the system time to the time server.

**Note:** When you force time synchronization, there is a brief cleanup period during which the system displays error messages. Wait a few moments until the synchronization is complete.

- Under **System Time** you can see what time is currently set on the system.
- The list under **NTP Servers Status** displays the connection statuses of the selected time servers.

Click the **APPLY CHANGES** button at the top of the main navigation to activate your configuration changes.




## 6.7.2 Monitoring





cognitix Threat Defender provides monitoring information about its system components. Under **Settings > Monitoring**, you can set up SNMP to connect cognitix Threat Defender to a central monitoring system. You can also set up monitoring via [checkmk](https://checkmk.com/)<sup>25</sup>.

<sup>25</sup> <https://checkmk.com/>






### 6.7.2.1 SNMP






The **SNMP** table displays the current SNMP connection settings. With the toggle in the first column you can enable () or disable () SNMP. Click  in the table to edit the settings.

Field	Description
 / 	The toggle indicates whether SNMP is enabled or disabled.
<b>System Contact</b>	Optional: Specify a contact person and contact information for the managed node, i.e. your cognitix Threat Defender.
<b>System Location</b>	Optional: Specify the physical location of this node.
<b>V2 Communities</b>	If you use SNMPv2c, click <b>ADD COMMUNITY</b> to add SNMP connection information. Enter the <b>IP Address</b> of the target monitoring system. Click  to delete the SNMP connection information.
<b>V3 Users</b>	If you use SNMPv3, click <b>ADD USER</b> to add SNMP connection information. Enter the <b>Username</b> . Specify the authentication and encryption methods used in the connection. Click  to delete the SNMP connection information.

The buttons at the bottom of the screen allow you to store your changes (**SAVE**) or to discard them (**CANCEL**).

### 6.7.2.2 Checkmk

The **Checkmk** table displays the current checkmk settings. With the toggle in the first column you can enable () or disable () checkmk. Click  in the table to edit the settings.

Field	Description
 / 	The toggle indicates whether checkmk is enabled or disabled.
<b>IP Addresses</b>	Enter the IP addresses that are allowed to query Threat Defender into the input field and click <b>ADD</b> . The IP addresses are listed under <b>Value</b> . Click  to remove an address.
 /  <b>Encryption</b>	Click the toggle to enable or disable encryption for the checkmk connection.

continues on next page

Table 52 – continued from previous page

Field	Description
Encryption Password	Set the password to be used if encryption is enabled. Passwords must consist of 8 to 255 alphanumeric and special characters excluding ", # and \.

The buttons at the bottom of the screen allow you to store your changes (**SAVE**) or to discard them (**CANCEL**).

Click the **APPLY CHANGES** button at the top of the main navigation to activate your configuration changes.

### 6.7.3 System Users

Navigate to **Settings > System Users** to edit existing users and to set up new users for Threat Defender.

**Tip:** Do not confuse system users with users of the network assets (see [Users](#) (page 169)).

The table displays the existing system users with their username, role, password validity information, and a note. The icons in the last column allow you to edit or delete the respective user.

**Note:** You cannot delete the user you used to sign in, as at least one user has to be configured in the system.

To set up a new user, click the **Add** button above the overview table.

#### 6.7.3.1 User Settings

If you add or edit a system user, the settings screen is displayed with the following elements:

Field	Description
<b>Username</b>	Enter a unique username for the user that also serves as login name (case-sensitive). The username may consist of alphanumeric characters and special characters. It may not contain blank spaces.
<b>Note</b>	Optional: Add a short description of the user.
<b>E-mail</b>	Optional: Enter an email address for the user.
<b>Password</b>	Enter a password for the user to log in to Threat Defender. Passwords may consist of up to 72 alpha-numeric and special characters. Click <b>Show Password</b> if you want to display the password in plaintext.
<b>Idle timeout</b>	Specify a timeout in minutes after which an idle user is automatically logged out. Enter 0 to disable the idle timeout. Any changes to this settings are applied at the next user login.
<b>Role</b>	Assign a role to the user (see <a href="#">Access Rights by User Roles</a> (page 216) in the appendix for information on the individual roles and rights).

The buttons at the bottom of the screen allow you to store your changes (**SAVE**) or to discard them (**CANCEL**).

#### 6.7.4 Updates

Navigate to **Settings > Updates** to install system and module updates.

If it is connected to the Internet, Threat Defender automatically checks for available updates once per hour. Otherwise, you need to manually check for new updates.

The **Add** button allows you to manually upload a firmware file (see [Manual Firmware Upload](#) (page 204)). This is useful if your Threat Defender is not connected to the Internet, for example.

The **Installed Software** table displays the software modules currently installed on Threat Defender.

The **CHECK FOR UPDATES** button allows you to manually check for available updates. This is useful if Threat Defender has only a temporary Internet connection. Next to this button, you can see when the last check for updates was performed and the status of the update check.

The update table displays any available updates with their type and product description. It also displays the currently installed software version and the update version, an update description, the size of the update and when it was downloaded.

**Tip:** Hover the mouse over the entries in the **Current Version** and **Update Version** columns to display release and build information in a tooltip.

The following update types are provided:

- cognitix Threat Defender firmware
- cognitix IOC feeds
- cognitix IPS signatures

Click the **INSTALL NOW** button in the last column to install the respective update immediately. Firmware updates require a reboot of the system to complete the installation. This is indicated by the **INSTALL AND REBOOT NOW** button in the last column of the table.

**Note:** You need to apply all pending changes before you can install an update.

**Tip:** Before installing a system update, you may want to create a new backup of your configuration and download it so that you can restore this configuration later if necessary. For further information, see [Configurations](#) (page 206).

Failed updates are also displayed in the table. Under **Description**, you see the reason why the update could not be downloaded or installed.

#### 6.7.4.1 Manual Firmware Upload

After clicking **Add**, the upload screen is displayed. Click **SELECT** to access the file system and select the file you want to upload.

**Note:** Update files always have the `.pfw` format.

To install the update file, click the **UPLOAD FIRMWARE FILE** button at the bottom of the screen. Click **CANCEL** if you do not want to upload the file.

#### 6.7.5 Update Schedules

Navigate to **Settings > Update Schedules** to set up time schedules for update installation.



If update schedules are configured, Threat Defender automatically installs available updates at the specified time. This allows you to schedule the update installation at a time when it does not disrupt network operation.

**Note:** When firmware updates are installed, Threat Defender is automatically re-booted.

Automatic daily installation of updates makes sure that your system remains up-to-date. You can set up individual schedules for individual types of updates.


**Note:** Updates can only be installed if there are no pending configuration changes. Otherwise, Threat Defender aborts the installation and tries to install the update again at the next scheduled time. Threat Defender also creates a [syslog](#) message on the failed installation attempt.

To set up a new update schedule, click the **Add** button above the overview table.

The table displays all update schedules configured in the system. The toggle in the first column allows you to enable () or disable () the update schedule. The icons in the last column allow you to edit or delete the respective update schedule.

### 6.7.5.1 Update Schedule Settings

If you add or edit an update schedule, the settings screen is displayed with the following elements:

Field	Description
	The toggle indicates whether the update schedule is enabled or disabled.
<b>Time</b>	Enter the time when the update is to be installed in HH:MM format.
<b>Note</b>	Optional: Add a short description of the update schedule.
<b>Type</b>	From the drop-down list, select the update type you want to install at the specified time. You can only select one update type per schedule.

The buttons at the bottom of the screen allow you to store your changes (**SAVE**) or to discard them (**CANCEL**).

## 6.7.6 License

Navigate to **Settings > License** to display the licenses available in the system and to add a new license file (see also [Add a License](#) (page 39)).

**Note:** Only one license may be enabled at a time. When you add a new license, it is enabled by default and any previously active license is automatically disabled.

The table displays the available licenses with their name, contract ID, version, validity period, and the maximum number of tracked assets included in the license. The toggle in the first column allows you to enable () or disable () the respective license. The button in the last column allows you to delete the license.



**Warning:** If no license is active, the throughput of Threat Defender is limited to 1 Mbit/s (transmitted and received traffic in total) and no assets are tracked. Also, the system is not able to connect to the license and update server.

### Additional References:

For information on how to install a license, refer to [Add a License](#) (page 39).

## 6.7.7 Configurations

Navigate to **Settings > Configurations** to manage backup files of your system configuration. The buttons at the top of the screen allow you to create and upload configuration files.

**Note:** Configuration files only contain the activated configuration. Pending changes are not backed up.

For each available configuration file, the table displays the date and time it was created, its automatically generated file name, the user who generated the file, and a note. The icons in last column of the table allow you to view details of the file and install it, edit its note, download, or delete the respective configuration file.

**Note:** Whenever a new configuration is applied, Threat Defender automatically generates a new configuration file called `most-recent-apply`. Note that Threat Defender stores only one automatically generated configuration file. This means older files are overwritten when a new file is auto-generated.

### 6.7.7.1 Configuration Details

To see the details of a configuration file, click  in the overview table or double-click its row.

The buttons at the top of the page allow you to edit the descriptive note of the file, and to delete or download the file.

The table shows general information about the configuration file:

Field	Description
Name	The automatically generated file name.
Note	A short description, if available.
Username	The user who created the backup.
Created At	The date the configuration file was created.
Updated At	The date the configuration file was last updated.

The buttons below the table allow you to select which part of the configuration you want to restore:

Field	Description
All Configuration	Restores the entire configuration.
Network	Restores only the network configuration.
Policy	Restores only the policy configuration.
Asset	Restores only the asset database.
Monitoring	Restores only the monitoring configuration.
genucenter	Restores only the genucenter configuration.
License	Restores only the license.

Click **INSTALL** to restore the selected configuration. Do not shut down Threat Defender during the installation of the configuration.

### 6.7.8 genucenter



Under **Settings > genucenter**, you can connect cognitix Threat Defender to a genucenter central management system.

cognitix Threat Defender transmits the following information to genucenter:

- General information (name, appliance type, software version, etc.)
- Extended information (description, tags, location)

- Tracked assets (created, updated, and seen assets in the previous 24 hours as well as currently active assets)
- Incidents reported in the previous 24 hours by severity (high, medium, low, notice)
- License details
- Hardware details
- Latest incident logs (the ten most recent entries)
- Latest audit logs (the ten most recent entries)
- Latest failed audit logs (the ten most recent entries)
- Network statistics (currently open flows, new flows, and throughput)
- System health information



This information is transmitted automatically at specified intervals. Click **Send Now** at the top of the screen if you want to immediately send information to the connected genucenter systems.

The table displays the current genucenter connections and their settings. With the toggle in the first column you can enable () or disable () a connection. The icons in the last column allow you to edit or delete the respective connection.

Click the **Add** above the overview table to access the configuration assistant where you can set up a new genucenter connection.

The connection has to be set up on both systems, cognitix Threat Defender and genucenter. This chapter describes the process from the point of view of Threat Defender. For detailed instructions on the connection setup on genucenter, refer to the respective genucenter documentation.

### 6.7.8.1 Setup

When you add or edit a connection to a genucenter system, the toggle allows you to enable () or disable () the connection.

Three tabs guide you through the connection setup.

#### Introduction

On the **Introduction** tab, click **INITIALIZE** to generate an SSH key pair that will be used to authenticate cognitix Threat Defender at the genucenter system.



## genucenter Steps

The **genucenter Steps** tab explains the setup steps you need to perform on the genucenter system that will receive status information from cognitix Threat Defender. For more detailed information, refer to your genucenter documentation.

The **SSH public key** field contains the public SSH key that you need to provide to genucenter (see step 3).

When you have completed the genucenter setup as detailed on this tab, click **NEXT STEP** to proceed.

## Configuration Upload

On the **Configuration Upload** tab, import the configuration file provided by genucenter.

Click **SELECT** to access the file system. Select the config file exported from genucenter (.json format). The input fields will be filled automatically with the exported settings. You can adjust them, if required.

Field	Description
Host	The IP address of the genucenter appliance that receives information from Threat Defender.
Port	The port that Threat Defender sends the information to.
Appliance ID	The ID used to identify Threat Defender.
Host SSH Key	The SSH key used by genucenter to establish the connection.
Time Interval	The time interval at which Threat Defender automatically transmits information to genucenter.

The buttons at the bottom of the screen allow you to store your changes (**SAVE**) or to discard them (**CANCEL**).

**Note:** When you restore the genucenter configuration on a fresh Threat Defender installation via a backup file, make sure that the SSH keys and the known server configuration file exist on the system. If any one of those three files is missing, the genucenter configuration is disabled. In this case you will have to set it up again as described above.

### 6.7.9 System Actions


Navigate to **Settings > System Actions** to reboot or turn off the system or to reset the databases and logs.

**Note:** Deleting databases and logs may temporarily cause error messages to be displayed until the system reaches a consistent state. In this case, wait a few minutes until the deletion process is fully completed.

Click the respective button to carry out the desired action. The system prompts you to confirm the action. The following buttons are available:

Field	Description
REBOOT	Restarts Threat Defender using the currently installed firmware version and reloading the currently applied configuration.
SHUTDOWN	Powers Threat Defender off completely. It can only be turned back on at the hardware.
RESET REPORTING DATA	Deletes all data in the reporting database. After clearing the reporting data, all reports and charts in the <b>Analytics</b> menu will be empty.
PURGE OLD LOGS	Deletes all incident log entries that are older than 32 days.
KEEP LAST 1K LOGS	Deletes all incident log entries except the most recent 1,000 entries.
RESET ASSETS	Deletes all tracked assets and their metadata from the database. The asset logs will be retained.
RESET AUDIT LOG	Deletes all audit logs. The databases of tracked assets and users will be retained.
RESET USERS	Deletes all tracked users and their metadata from the database. The user API logs will be retained.

## | 6.8 Diagnostics

In the  **Diagnostics** menu, you can see status information on the system hardware, generate and download troubleshooting and flow table reports, and access the MAC table reporting.

### 6.8.1 Overview

Navigate to **Diagnostics > Overview** to display hardware information.

With the buttons at the top of the content area, you can select the reporting period. The information fields and the charts contain the following information:

- CPU usage
- Memory usage
- Number of flow table entries
- Core temperatures
- Disk usage
- Disk input/output

**Note:** This data can only be displayed if the operating system is able to analyze it on your appliance.

### 6.8.2 System Health

Navigate to **Diagnostics > System Health** to view information on the status of the system.

The table shows the current status of the individual system components as well as any warnings reported by the system.


### 6.8.3 Troubleshooting

Navigate to **Diagnostics > Troubleshooting** to create a troubleshooting report in a compressed folder.

Click the **Generate Core Troubleshoot Report** button to create a new troubleshooting report. These reports contain various log files that help you locate and analyze any issues in the system.

The table displays the latest troubleshooting report with its creation date, an automatically generated filename, and the file size.

**Note:** Older troubleshooting reports are overwritten when a new report is created.

With the  icon in the last column, you can download the troubleshooting report to your file system.

## 6.8.4 Flow Table Reporting

Navigate to **Diagnostics > Flow Table Reporting** to create a **flow** table report. These reports contain information on the traffic flows that pass through Threat Defender.

cognitix Threat Defender tracks flows to enforce rules and to monitor network traffic.

The size of the flow table depends on the memory available in your system. For example, on small systems with 8GB RAM it can hold around 80,000 entries. As each entry represents a flow, 80,000 concurrent flows are possible.

Entries in the table may timeout and are removed after a certain period of time. Currently, the following timeouts exist:

- **1 hour (3600 s) for:**
  - established TCP flows
  - NETFLOW/IPFIX flows
- **2 minutes (120 s) for:**
  - TCP flows closed by one party
  - bidirectional UDP flows as well as QUIC flows
  - flows being intercepted by Threat Defender (having triggered a policy with a drop or reject action)
- **5 seconds for:**
  - TCP flows closed by both parties
  - connectionless flows, such as unidirectional UDP

When a timeout expires, the corresponding flow is removed from the table. Therefore, any new data on this flow is considered a new flow.




**Warning:** When the flow table is full, Threat Defender does no longer accept any new flows.

Click the **Generate Anonymized Core Flow Table Report** button to create an anonymized flow table report that contains no IP addresses.

Click the **Generate Plain Core Flow Table Report** button to create a plain flow table report that includes IP addresses.

The table displays the latest flow table report with its creation date, an automatically generated filename, and the file size.

With the  icon in the last table column, you can download the flow table report to your file system.

**Note:** Older flow table reports are overwritten when a new report is created.

#### Additional References:

For further information on the content of flow table reports, see [Flow Table Reports](#) (page 241) in the appendix.

### 6.8.5 MAC Table Reporting

Navigate to **Diagnostics > MAC Table Reporting** to see a live report on the MAC table that shows you what devices communicate via which bridge. You can use this information to troubleshoot issues with your bridge configuration.

The **Network Overview** link takes you to the network configuration under **Network > Overview**.

The table shows the configured bridges with the following information:

Field	Description
MAC	The MAC address of the device.
Bridge	The name of the bridge over that the device communicates.
Port Name	The ID of the network interface that receives/sends the traffic of the device.
VLAN Range	The VLAN range used in the bridge, if any.
RX Broadcast	The broadcast traffic received by the device.
RX Unicast	The unicast traffic received by the device.
TX Unicast	The unicast traffic transmitted by the device.



| Chapter 7

# Appendix

## 7.1 Access Rights by User Roles

Under **Settings > System Users**, you can assign roles to system users with the following access rights:

Access Rights	Reporting Viewer	Auditor	Net- work Admin	Se- curity Admin	Full Admin	Read- only Admin
<b>Analytics: Network</b>						
View 1st level (overview)	✓	✓	✓	✓	✓	✓
View 2nd level	✓		✓	✓	✓	✓
View 3rd level (details)	✓		✓	✓	✓	✓
<b>Analytics: Assets</b>						
View 1st level (overview)	✓	✓	✓	✓	✓	✓
View 2nd level	✓		✓	✓	✓	✓
View 3rd level (details)				✓	✓	✓
<b>Analytics: Policy</b>						
View 1st level (overview)	✓	✓	✓	✓	✓	✓
View 2nd level	✓		✓	✓	✓	✓
View 3rd level (details)	✓			✓	✓	✓
<b>Policy: Rules</b>						
View all rules		✓	✓	✓	✓	✓
Reorder rules				✓	✓	
Add, edit, delete global rules				✓	✓	
<b>Policy: Advanced Correlation</b>						
View scenarios		✓	✓	✓	✓	✓
View scenario de- tails		✓	✓	✓	✓	✓
Reorder scenarios				✓	✓	

continues on next page



Table 1 – continued from previous page

Access Rights	Reporting Viewer	Auditor	Net- work Admin	Se- curity Admin	Full Admin	Read- only Admin
Add, edit, delete scenarios				✓	✓	
<b>Policy: Network Objects - Static Network Objects</b>						
View SNOs		✓	✓	✓	✓	✓
Add, edit, delete SNOs			✓		✓	
<b>Policy: Network Objects - Dynamic Network Objects</b>						
View DNOs		✓	✓	✓	✓	✓
Add, edit, delete DNOs				✓	✓	
<b>Policy: Network Objects - VLANs</b>						
View VLANs		✓	✓	✓	✓	✓
Add, edit, delete VLANs			✓		✓	
<b>Policy: Schedules</b>						
View schedules		✓	✓	✓	✓	✓
Add, edit, delete schedules				✓	✓	
<b>Policy: Event Tracking Tables</b>						
View ETTs		✓	✓	✓	✓	✓
<b>Inventory: Assets</b>						
View assets	✓	✓	✓	✓	✓	✓
View asset details	✓	✓	✓	✓	✓	✓
Add, edit, delete assets			✓		✓	
<b>Inventory: Asset Logs</b>						
View asset logs		✓	✓	✓	✓	✓
<b>Inventory: Asset Setting</b>						
Edit asset setting			✓		✓	
<b>Inventory: Users</b>						
View users	✓	✓	✓	✓	✓	✓

continues on next page

Table 1 – continued from previous page

Access Rights	Reporting Viewer	Auditor	Net-work Admin	Se-curity Admin	Full Admin	Read-only Admin
View user details		✓	✓	✓	✓	✓
Add, edit, delete users				✓	✓	
<b>Inventory: User API Logs</b>						
View user API logs		✓		✓	✓	✓
<b>Inventory: User API Settings</b>						
Edit user API settings			✓		✓	
<b>Inventory: Backup/Restore - Assets/Users</b>						
View backups		✓	✓		✓	✓
Generate backups			✓		✓	
Restore backups		✓	✓		✓	✓
<b>Inventory: Data Exports</b>						
View data exports		✓		✓	✓	
Create, download, delete data exports		✓		✓	✓	
<b>Threats: Overview</b>						
View 1st level (overview)	✓	✓	✓	✓	✓	✓
<b>Threats: Incident Logs</b>						
View incident logs	✓	✓	✓	✓	✓	✓
Create/download reports	✓	✓	✓	✓	✓	✓
View incident details		✓	✓	✓	✓	✓
Create/download incident details reports		✓	✓	✓	✓	✓
<b>Threats: Intelligence Database - Summary</b>						

continues on next page

Table 1 – continued from previous page

Access Rights	Reporting Viewer	Auditor	Net-work Admin	Se-curity Admin	Full Admin	Read-only Admin
View database summary	✓	✓	✓	✓	✓	✓
<b>Threats: Intelligence Database - Events</b>						
View events	✓	✓	✓	✓	✓	✓
View events de-tails	✓	✓	✓	✓	✓	✓
<b>Threats: Intelligence Database - Attributes</b>						
View attributes	✓	✓	✓	✓	✓	✓
<b>Threats: Intelligence Database - IPS Rules</b>						
View IPS rules	✓	✓	✓	✓	✓	✓
View IPS rules de-tails	✓	✓	✓	✓	✓	✓
Enable/disable IPS rules					✓	
Upload custom IPS rules					✓	
<b>Network: Overview</b>						
View interfaces overview		✓	✓		✓	✓
<b>Network: Manage Processing Interfaces</b>						
View interface groups		✓	✓		✓	✓
Add, edit, delete groups			✓		✓	
Enable/Disable default config			✓		✓	
<b>Logging: Audit Logs</b>						
View audit logs		✓		✓	✓	✓
View audit logs details		✓		✓	✓	✓
<b>Logging: Audit Log Channels</b>						

continues on next page

Table 1 – continued from previous page

Access Rights	Reporting Viewer	Auditor	Net- work Admin	Se- curity Admin	Full Admin	Read- only Admin
View audit log channels		✓		✓	✓	✓
Add, edit, delete audit log channels					✓	
<b>Logging: Reporting Channels</b>						
View reporting channels		✓		✓	✓	✓
Add, edit, delete reporting channels					✓	
<b>Logging: Local Logs</b>						
View local logs		✓		✓	✓	✓
<b>Settings: General</b>						
View general settings		✓			✓	✓
Edit general settings					✓	
<b>Settings: Monitoring</b>						
View monitoring settings			✓		✓	✓
Edit monitoring settings			✓		✓	
<b>Settings: System Users</b>						
View system users		✓			✓	✓
Add, edit, delete system users					✓	
<b>Settings: Updates</b>						
View updates		✓			✓	✓
Install updates					✓	
<b>Settings: Update Schedules</b>						

continues on next page

Table 1 – continued from previous page

Access Rights	Reporting Viewer	Auditor	Net-work Admin	Se-curity Admin	Full Admin	Read-only Admin
View update schedules		✓			✓	✓
Add, edit, delete update schedules					✓	
<b>Settings: License</b>						
View license		✓			✓	✓
Add, enable, disable licenses					✓	
<b>Settings: Configurations</b>						
View configurations		✓			✓	✓
View configuration details		✓			✓	✓
Add, edit, delete, upload, download					✓	
<b>Settings: genucenter</b>						
Edit genucenter setup		✓			✓	✓
<b>Settings: System Actions</b>						
Execute system actions					✓	
<b>Diagnostics: Overview</b>						
View diagnostics			✓	✓	✓	✓
<b>Diagnostics: System Health</b>						
View system health stats					✓	✓
<b>Diagnostics: Troubleshooting</b>						
Generate, download troubleshooting report			✓	✓	✓	

continues on next page

Table 1 – continued from previous page

Access Rights	Reporting Viewer	Auditor	Net- work Admin	Se- curity Admin	Full Admin	Read- only Admin
<b>Diagnostics: Flow Table Reporting</b>						
Generate, down- load flow table reports			✓	✓	✓	
<b>Diagnostics: MAC Table Reporting</b>						
View MAC table reporting			✓		✓	✓

## 7.2 JSON Lines Formatted Output

The reporting channels under **Logging > Report Channels** support **JSON Lines**<sup>26</sup> formatted output.

**Note:** JSON Lines is a collection of newline-separated JSON objects. The internal format follows the **Elastic Common Schema 1.4**.<sup>27</sup>

<sup>27</sup> <https://www.elastic.co/guide/en/ecs/1.4/index.html>

The following events are generated. The name of an event is also the value of the `event.action` field.

The **flow** tracking generates:

- `flow-update` at regular intervals with updated information about a flow.
- `flow-deleted` when a flow is destroyed.

Threats are reported by:

- `ips-hit` when an IPS rule matches.
- `ioc-hit` when an IOC match is found.
- `policy-hit` when a rule with the policy hit flag in the logging action is triggered.

The policy engine also emits events of the type:

- `policy-log` for matched policy rules with enabled logging.

The asset database emits:

- `asset-created` - a single asset was created
- `asset-modified` - an asset was updated
- `asset-deleted` - an asset was removed
- `asset-auto-created` - a new asset was created by auto-tracking
- `assetdb-loaded` - the whole asset database was loaded and replaced with a new one

The following fields are present in all messages:

- `@timestamp`
- `ecs.version="1.4"`
- `observer.hostname`
- `observer.vendor="Genua"`
- `observer.product="TD"`

---

<sup>26</sup> <https://jsonlines.org/>

- `observer.type="ips"`
- `event.action`
- `event.category`
- `event.kind`
- `event.type`

Messages of the types `flow-update`, `flow-deleted`, `ips-hit`, `ioc-hit`, `policy-hit`, and `policy-log` additionally contain the following fields:

- `network.transport`
- `network.type`
- `network.protocol`
- `network.app`
- `network.flow_id` - custom field
- `network.vlan_tag` - custom field
- `network.bridge_id` - custom field
- `{client, server}.packets`
- `{client, server}.bytes`
- `{client, server}.port`
- `{client, server}.ip`
- `{client, server}.mac`
- `{client, server}.geo.country_iso_code`
- `{client, server}.asset.id` - custom field, optional
- `{client, server}.asset.name` - custom field, optional

Messages of the types `policy-hit` and `policy-log` additionally contain the following fields:

- `rule.id`
- `rule.name`
- `rule.rulesetid` - ID of the scenario
- `rule.ruleset` - name of the scenario
- `rule.action` - this field can be `continue`, `allowed`, `blocked`, or `teardown`

Messages of the type `ips-hit` additionally contain the following fields:

- `ips.id` - integer, identifier of the matched IPS rule
- `ips.rev` - integer, revision number of the IPS rule signature



- `ips.description` - string, description of the IPS rule signature
- `ips.plain` - string, the IPS rule signature itself
- `ips.updated_at` - string, timestamp signaling when the IPS rule signature was updated
- `ips.references` - array of objects, the object key indicates the reference type and the object value contains the actual reference string
- `ips.tags` - array of strings, information about the classification of IPS rules

Messages of the type `ioc-hit` additionally contain the following fields:

- `ioc.kind` - the type of detected **IoC**, either `ipv4`, `domain`, or `uri`
- `ioc.value` - the actual IoC found

Messages of the types `ips-hit`, `policy-hit`, and `policy-log` additionally contain:

- `event.severity`, where
  - 1 = info,
  - 2 = notice,
  - 3 = warning,
  - 4 = critical

Messages where `event.action="asset-*` contain the fields:

- `asset.id`
- `asset.name`

## 7.3 IPFIX Specification

This specification defines all generic and cognitix-specific events.

### 7.3.1 IPFIX Setup

The IPFIX interface is based on IETF RFC 7011<sup>28</sup>. It also uses bidirectional reporting as described in RFC 5103<sup>29</sup> (esp. sections 5 and 6.3).

Additionally, cognitix defines and uses own elements for specific fields.

The implementation is based on TCP for safe transmission. UDP is also supported for IPFIX channels.

The data source sends all IPFIX templates on demand just before a message using the template is sent. The templates are resent if a certain time has passed after sending the last template.

### 7.3.2 IPFIX Records

The cognitix IPFIX templates use preassigned IANA elements, where possible. The data types follow RFC 7102<sup>30</sup>. For the definitions of the IPFIX information events used by cognitix, see the IANA<sup>31</sup> table.

**Note:** `sourceIPv4Address/sourceIPv6Address` and `destinationIPv4Address/destinationIPv6Address` describe the outermost IP addresses of an observed flow.

Fields not provided by IPFIX are described using custom fields with the cognitix IPFIX Private Enterprise Number (PEN 45480).

### 7.3.3 cognitix IPFIX Enterprise Elements

The cognitix IANA number (PEN 45480) defines the following new enterprise elements:

<sup>28</sup> <https://datatracker.ietf.org/doc/html/rfc7011>

<sup>29</sup> <https://datatracker.ietf.org/doc/html/rfc5103>

<sup>30</sup> <https://datatracker.ietf.org/doc/html/rfc7102>

<sup>31</sup> <http://www.iana.org/assignments/ipfix/ipfix.xhtml>

Property	Enterprise Field ID	Data type	Description
<code>cognitixDpiProtocol</code>	10	un-signed16	This field describes the protocol of the flow as detected by the DPI engine.
<code>cognitixDpiApplication</code>	11	un-signed16	This field describes the application of the flow as detected by the DPI engine.
<code>cognitixDpiClassification</code>	13	un-signed32	This field contains the combined values of the protocol and application of the flow as detected by the DPI engine. It represents the DPI classification of the cleartext message. The combined value is calculated using $\text{applicationID} * 10,000 + \text{protocolID}$ .
<code>cognitixCountrySource</code>	20	string	This field contains the 2-byte ISO 3166 country code of the flow source as detected by the GeoIP engine. If no country code could be detected, this field will contain ZZ, which is defined as private IP address range.
<code>cognitixCountryDestination</code>	21	string	This field contains the 2-byte ISO 3166 country code of the flow destination as detected by the GeoIP engine. If no country code could be detected, this field will contain ZZ, which is defined as private IP address range.

continues on next page

Table 2 – continued from previous page

Property	Enterprise Field ID	Data type	Description
cognitixPolicyRuleId	30	string	The policy rule ID string describes which policy rule matched for a given flow, stating its internal unique ID.
cognitixIPSRuleId	31	un-signed32	The IPS rule ID indicates which IPS rule matched for the given flow. If it is 0, no IPS rule was hit.
cognitixIPSRuleDescription	38	string	The IPS rule description matching the IPS rule ID.
cognitixPolicyRuleName	32	string	The policy rule name variable-length string indicates which policy rule matched for a flow, stating its user-defined name.
cognitixPolicyRuleAction	33	unsigned8	The type of policy rule action. It can be: <ul style="list-style-type: none"> <li>• 0 = no action</li> <li>• 1 = drop</li> <li>• 2 = allow</li> <li>• 3 = tear down (reject)</li> <li>• 4 = redirect</li> </ul>
cognitixPolicyId	34	string	The policy hit ID variable-length string.
cognitixPolicyName	35	string	The policy hit name variable-length string.

continues on next page

Table 2 – continued from previous page

Property	Enterprise Field ID	Data type	Description
cognitixLogSeverity	36	unsigned8	The log severity indicates which event will be reported regarding the defined severity level. It can be: <ul style="list-style-type: none"> <li>• 0 = notice</li> <li>• 1 = low</li> <li>• 2 = medium</li> <li>• 3 = high</li> </ul>
cognitixPolicyHit	37	unsigned8	The policy hit flag indicates that the policy was marked as an incident by the corresponding flag in the log action of a policy rule.
cognitixHostname	50	string	The hostname of the observed URL of a HTTP request as variable-length string that has been classified by the URL filter engine.
cognitixIocValueType	75	unsigned8	The match type that hit an IOC feed. It can be: <ul style="list-style-type: none"> <li>• 0 = none</li> <li>• 1 = source IP</li> <li>• 2 = destination IP</li> <li>• 3 = domain name</li> <li>• 4 = URL</li> </ul>
cognitixIocValue	76	string	The string representation of the IoC value being hit. Its type is given in the cognitixIocValueType field.

continues on next page

Table 2 – continued from previous page

Property	Enterprise Field ID	Data type	Description
cognitixSrcLocation	80	unsigned8	Location of the source host as determined by the NetworkObject matching. Values are: <ul style="list-style-type: none"> <li>• 0 = internal</li> <li>• 1 = external</li> </ul>
cognitixDstLocation	81	unsigned8	Location of the destination host as determined by the NetworkObject matching. Values are: <ul style="list-style-type: none"> <li>• 0 = internal</li> <li>• 1 = external</li> </ul>
cognitixSrcAssetId	90	string	The internal ID of the source asset.
cognitixDstAssetId	91	string	The internal ID of the destination asset.
cognitixUserId	92	string	The internal ID of the user associated with the source asset.
cognitixBridgeId	93	string	The name of the bridge on which the event was observed.

### 7.3.4 cognitix Threat Defender IPFIX Events

All events contain IANA-defined fields (see the [IANA<sup>32</sup>](http://www.iana.org/assignments/ipfix/ipfix.xhtml) definitions) and [cognitix IPFIX Enterprise Elements](#) (page 226). See the following sections for further information on the fields used.

### 7.3.5 Common Event Fields

The following fields are used in all cognitix IPFIX events:

<sup>32</sup> <http://www.iana.org/assignments/ipfix/ipfix.xhtml>

Property	Data Type
sourceTransportPort	unsigned16
sourceIPv4Address	ipv4Address
destinationTransportPort	unsigned16
destinationIPv4Address	ipv4Address
sourceIPv6Address	ipv6Address
destinationIPv6Address	ipv6Address
sourceMacAddress	macAddress
destinationMacAddress	macAddress
octetTotalCount	unsigned64
octetTotalCountReverse	unsigned64
packetTotalCount	unsigned64
packetTotalCountReverse	unsigned64
flowId	unsigned64
flowStartMilliseconds	dateTimeMilliseconds
flowEndMilliseconds	dateTimeMilliseconds
firewallEvent	unsigned8
ingressPhysicalInterface	unsigned32
egressPhysicalInterface	unsigned32
cognitixSrcLocation	unsigned8
cognitixDstLocation	unsigned8
cognitixSrcAssetId	string
cognitixDstAssetId	string
cognitixUserId	string
cognitixBridgeId	string

### 7.3.6 Message Types

Messages of the types flow-update and flow-end additionally contain the following elements:

- firewallEvent, with a value of either 2 (flow-end) or 5 (flow-update)
- octetDeltaCount, the number of transferred bytes from client to server
- octetDeltaCountReverse , the number of transferred bytes from server to client
- packetDeltaCount, the number of transferred packets from client to server
- packetDeltaCountReverse , the number of transferred packets from server to client

Messages of the type hostname additionally contain the following element:

- `cognitixHostname`, an observed domain name

Messages of the type `policy-rule-matched` additionally contain the following elements:

- `firewallEvent`, with a value of 4 (flow-alert)
- `cognitixPolicyId`
- `cognitixPolicyName`
- `cognitixPolicyRuleName`
- `cognitixPolicyRuleId`
- `cognitixPolicyRuleAction`
- `httpRequestHost`
- `httpRequestTarget`

Messages of the types `policy-hit` and `policy-log` additionally contain the following elements:

- `firewallEvent`, with a value of 4 (flow-alert)
- `cognitixPolicyId`
- `cognitixPolicyName`
- `cognitixPolicyRuleName`
- `cognitixPolicyRuleId`
- `cognitixPolicyRuleAction`
- `cognitixLogSeverity`

Messages of the type `ips-hit` additionally contain the following elements:

- `firewallEvent`, with a value of 4 (flow-alert)
- `cognitixLogSeverity`
- `cognitixIPSRuleId`
- `cognitixIPSRuleDescription`

Messages of the type `ioc-hit` additionally contain the following elements:

- `firewallEvent`, with a value of 4 (flow-alert)
- `cognitixLogSeverity`
- `cognitixIocValueType`
- `cognitixIocValue`



## 7.4 syslog Specification

**syslog** is a standard for message logging that separates the software that generates messages, the system that stores them, and the software that reports and analyzes them. cognitix Threat Defender supports syslog in the [Report Channels](#) (page 194).

This specification defines all syslog messages with their information elements used in cognitix-specific events.

### 7.4.1 syslog Setup

The *pw-core* application generates reporting messages in syslog format that are readable in the **Logging** section of the Threat Defender user interface. These messages can then be exported to external syslog receivers as desired.

### 7.4.2 syslog Messages in General

Every syslog message generated by the *pw-core* application displays the APP-NAME “*pw-core*” and can thereby be distinguished from any other syslog message generated by cognitix Threat Defender.

All syslog datasets are provided as key-value pairs separated by =, where never the `key` but always the `value` is quoted.

As far as possible, the syslog datasets of *pw-core* follow the **Splunk** CIM. But *pw-core* also introduces custom dataset definitions where none of the existing ones fit.

### 7.4.3 Message Types

The following events are generated. The name of an event is also the value of the `event_type` field.

The **flow** tracking generates:

- `flow-update` at regular intervals with updated information about a flow.
- `flow-deleted` when a flow is destroyed.

Threats are reported by:

- `ips-hit` when an IPS rule matches.
- `ioc-hit` when an IOC match is found.
- `policy-hit` when a rule with the `policy-hit` flag in the logging action is triggered.

The policy engine also emits events of the type:

- `policy-rule-log` for matched policy rules with enabled logging.

### 7.4.4 syslog Fields

The following fields are used by pw-core:

Field Name	Field Origin	Data Type	Description
action	Splunk CIM	string	The action taken by the network device that was triggered by a policy rule hit. Only the values “allowed”, “blocked” and “tear-down” are valid.
app	Splunk CIM	string	The application and protocol of the traffic, reporting the layer 7 application and protocol classification results as short names, e.g.: “reddit:ssl”
asset_id	cognitix	string	The ID of an asset, in the format asset-uuid.
asset_name	cognitix	string	The name of an asset.
bridge_id	cognitix	string	The name of the bridge on which the event was observed.
dest_asset_name	cognitix	string	The ID of the asset matching the destination host, in the format asset-uuid.
dest_bytes_tx	cognitix	number	Bytes transmitted from destination to source.
dest_country_code	cognitix	string	The destination country of a flow, encoded following ISO 3165-1 alpha-2, e.g. “FR”, “DE” or “ZZ” for unknown countries.
dest_host	Splunk CIM	string	The host name served by the webserver or proxy, in the format punycodeIDNA-encoded-domain.

continues on next page

Table 4 – continued from previous page

Field Name	Field Origin	Data Type	Description
dest_interface	Splunk CIM	string	The interface that is listening remotely or receiving packets locally; can also be referred to as the “egress interface”.
dest_interface_name	cognitix	string	The name of the egress interface.
dest_ip	Splunk CIM	string	The IP address of the destination, in the format ipv4-or-ipv6.
dest_location	cognitix	string	The location of the destination host as determined by network object matching, can only be “internal” or “external”.
dest_mac	Splunk CIM	string	The destination TCP/IP layer 1 <b>MAC address</b> of a packet’s destination, such as 06:10:9f:eb:8f:14. Has the format macAddress. <b>Note:</b> Always force lower case on this field. Always use colons instead of dashes, spaces, or no separator.
dest_packets_tx	cognitix	number	Packets transmitted from destination to source.
dest_port	Splunk CIM	number	The destination port of the network traffic.
dpi_classification	cognitix	number	The application and protocol of the traffic, reporting the layer 7 application and protocol classification results as a number.
event_type	Splunk CIM	string	The reporting event type.
flow_id	Splunk CIM	number	A unique numeric identifier for the flow (uint64).

continues on next page

Table 4 – continued from previous page

Field Name	Field Origin	Data Type	Description
ioc_tags	cognitix	string	A comma-separated list of IoC tags associated with an IoC value.
ioc_value	cognitix	string	The latest IoC matched for a flow, e.g. “9.20.11.3”, “www.example.com”, “www.badurl.nz/kiwi”.
ioc_value_type	cognitix	string	The IoC indicator type. Only the values “ipv3”, “domain”, “url” are valid.
ips_rule_id	cognitix	number	The ID of an IPS rule.
ips_rule_description	cognitix	string	The description string of an IPS rule.
policy_id	cognitix	string	The ID of a policy scenario, defined in the policy configuration.
policy_name	cognitix	string	The name of a policy scenario, defined in the policy configuration.
product	Splunk CIM	string	The product name, will always be set to “td”.
protocol	Splunk CIM	string	The OSI layer 2 (network) protocol of the traffic observed, in lower case. For example: ip, applealk, ipx.
protocol_version	Splunk CIM	string	Version of the OSI layer 3 protocol.
rule	cognitix	string	The name of a policy rule, defined in the policy configuration, that defines the action that was taken in the network event.

continues on next page

Table 4 – continued from previous page

Field Name	Field Origin	Data Type	Description
rule_id	cognitix	string	The ID of a policy rule, defined in the policy configuration, that defines the action that was taken in the network event.
severity	Splunk CIM	string	The log action severity according to the CIM naming scheme. Only the values “informational”, “low”, “medium”, “high” are valid.
src_asset_name	cognitix	string	The ID of the asset matching the source host, in the format asset-uuid.
src_bytes_tx	cognitix	number	Bytes transmitted from source to destination.
src_country_code	cognitix	string	The source country of a flow, encoded following ISO 3165-1 alpha-2, e.g. “FR”, “DE” or “ZZ” for unknown countries.
src_interface	Splunk CIM	string	The interface that is listening remotely or sending packets locally. Can also be referred to as the “ingress interface”.
src_interface_name	cognitix	string	The name of the “ingress” interface.
src_ip	Splunk CIM	string	The IP address of the source, in the format ipv4-or-ipv6.
src_location	cognitix	string	The location of the source host as determined by network object matching, can only be “internal” or “external”.

continues on next page

Table 4 – continued from previous page

Field Name	Field Origin	Data Type	Description
src_mac	Splunk CIM	string	The source TCP/IP layer 1 <b>MAC address</b> of a packet’s destination, such as 06:10:9f:eb:8f:14. Has the format <code>macAddress</code> . <b>Note:</b> Always force lower case on this field. Always use colons instead of dashes, spaces, or no separator.
src_packets_tx	cognitix	number	Packets transmitted from source to destination.
src_port	Splunk CIM	number	The source port of the network traffic.
timestamp	cognitix	number	The timestamp when the message was emitted in ISO 8601 format with a millisecond resolution.
host	Splunk CIM	string	The hostname of the cognitix Threat Defender instance reporting this event.
uri_path	Splunk CIM	string	The path of the resource served by the webserver or proxy.
user_id	cognitix	string	The ID of the user who is responsible for the existence of the flow.
vendor	Splunk CIM	string	The vendor name; will always be set to “cognitix”.
vendor_severity	Splunk CIM	string	The log action severity according to the cognitix naming scheme. Only the values “notice”, “low”, “medium”, “high” are valid.
vlan_id	cognitix	number	The outermost VLAN tag.

## 7.4.5 cognitix Threat Defender syslog Message Types

### 7.4.5.1 Fields

Every syslog message contains the following fields:

- vendor
- product
- host
- event\_type

Depending on the value of the event\_type dataset, the following datasets are appended to a syslog message.

Currently all event types contain flow information. It consists of:

- bridge\_id
- src\_interface
- src\_interface\_name
- dest\_interface (optional)
- dest\_interface\_name (optional)
- src\_mac
- dest\_mac
- protocol
- protocol\_version
- src\_ip
- dest\_ip
- transport
- src\_port
- dest\_port
- timestamp
- src\_location
- dest\_location
- src\_country\_code (optional)
- dest\_country\_code (optional)
- flow\_id

- app
- dpi\_classification
- src\_packets\_tx
- dest\_packets\_tx
- src\_bytes\_tx
- dest\_bytes\_tx
- vlan\_id (optional)
- src\_asset\_id (optional)
- src\_asset\_name (optional)
- dest\_asset\_id (optional)
- dest\_asset\_name (optional)
- user\_id (optional)
- user\_name (optional)

Events of the types `policy-hit` and `policy-rule-log` additionally contain:

- severity
- vendor\_severity
- policy\_id
- policy\_name
- rule\_id
- rule
- action (optional)

Events of the type `ips-hit` additionally contain:

- ips\_rule\_id
- ips\_rule\_description
- dest\_host (optional)
- uri\_path (optional)

Events of the type `ioc-hit` additionally contain:

- ioc\_tags
- ioc\_value
- ioc\_value\_type
- dest\_host (optional)
- uri\_path (optional)



## 7.5 Flow Table Reports

Flow table reports contain various information on the traffic flows passing Threat Defender. Using Threat Defender, you can generate plain flow table reports and anonymized flow table reports that do not contain IP addresses (see [Flow Table Reporting](#) (page 212)).

The following table contains the content of flow table reports in the order they are reported.

Column Header	Description
thread_id	ID of the processing thread. It starts at 0 and is incremented for each new processing thread.
vlan_tag	VLAN tag assigned to the flow. If the flow has no VLAN tag, this entry is 0.
src_ip	Source IP address of the flow. In anonymized reports, these entries are hashed.
src_port	Source port of the flow.
dst_ip	Destination IP address of the flow. In anonymized reports, these entries are hashed.
dst_port	Destination port of the flow.
l4_protocol	Layer 4 protocol ID as stated in the IP header.
client_ttl	TTL values used by the client.
server_ttl	TTL values used by the server.
src_asset	Source asset of the flow.
dst_asset	Destination asset of the flow.
src_asset_tags	Tags assigned to the source asset of the flow.
dst_asset_tags	Tags assigned to the destination asset of the flow.
user_id	ID of the user who initiated the flow.
flow_id	Flow ID
dpi_protocol	DPI protocol used by the flow.
dpi_application	DPI application used by the flow.
packets_src_to_dst	Number of packets sent from the flow source to the flow destination.
packets_dst_to_src	Number of packets sent from the flow destination to the flow source.
bytes_src_to_dst	Number of bytes sent from the flow source to the flow destination.

continues on next page

Table 5 – continued from previous page

Column Header	Description
bytes_dst_to_src	Number of bytes sent from the flow destination to the flow source.
flow_start_ts	Timestamp of the start of the flow in microsecond resolution.
flow_last_packet_ts	Timestamp of the last packet belonging to the flow in microsecond resolution.
hash_element_last_lazy_ts	Timestamp when the flow was last checked for timeout eviction.
hash_table_last_update_ts	Timestamp of the last flow table update in microsecond resolution.
hash_element_lifetime	Amount of time left in microseconds before this entry is evicted.
hash_element_timeout	Total amount of time in microseconds that this entry is allowed to persist.
hash_element_timeout_queue	Queue number where this entry is stored. 0 indicates a short timeout (5s); 1 indicates a medium timeout (60s); 2 indicates a long timeout (1hr).

## | 7.6 IPS Rule Definitions

The following chapters document the keywords supported by the cognitix Threat Defender IPS. You can use these keywords to create custom IPS rule sets that you can upload under Threats > Intelligence Database > IPS Settings, see [IPS Settings](#) (page 184).

### 7.6.1 Rule Syntax

An IPS rule must be represented with the following structure:

- The **action** tells cognitix Threat Defender what operation to perform on a rule hit.
- The **header** defines which protocol, IP network range, port ranges and which direction the rule will match.
- The rule definition encodes all information specifying the rule.

Example:

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"Example rule"; pcre:"/Pattern to match/i"; reference:url,example.org/rule-example; classtype:misc-activity; sid:9000000; rev:1;)
```

#### 7.6.1.1 Action

Currently, only the `alert` action is supported. When a rule hit occurs with this action, a log message is emitted to the reporting channels which have IPS rule hit logging enabled.

To apply an action on flows matching a certain type of IPS rules, specify tags as an IPS condition in a rule.

#### 7.6.1.2 Protocol

This protocol string instructs the cognitix Threat Defender IPS engine to match only on flows using a specific protocol such as:

- tcp
- udp
- tls (ssl included)
- http
- smtp
- ssh
- dns
- ip (matches any protocol above)

### 7.6.1.3 Source and Destination Address

The source and destination definition specifies on which IP address or networks the rule must be matched.

Operator	Description
../..	IP ranges (CIDR notation)
!	Negation
[.., ..]	IP set

You can also use variables to reference internal or external IP networks via \$HOME\_NET and \$EXTERNAL\_NET. Internal IP addresses can be defined by including them in a network object marked as internal.

### 7.6.1.4 Source and Destination Ports

A port is a communication endpoint represented as a 16-bit unsigned integer which identifies a port number. Such port numbers are used on TCP and UDP based traffic. The Internet Assigned Number Authority (IANA) assigns and maintains port numbers to well-known services. The IANA Port Number Registry is available at <https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml>

Operator	Description
:	Port ranges
!	Negation
[.., ..]	Port set

### 7.6.1.5 Direction

The direction defines in which way the signature has to match. Currently, only signatures with right arrow -> can be used:

```
source -> destination
```

### 7.6.1.6 Rule Options

Once the rule header is parsed, the rest of the rule is considered as options. The rule options section is enclosed within parentheses and are separated by semicolons. Some options follow a keyword: value syntax (e.g sid: 12345) whereas some are flags (nocase):

```
<keyword>: <value>;
<keyword>;
```

**Note:** Some keywords accept multiple values. In this case, all values are comma-separated. For example:

```
byte_test: 1, -1, relative, big;
```

See the documentation of the respective keyword for more information.

**Note:** The characters ; and " are part of the rule options syntax. If you want to match patterns containing these characters, they must be escaped with a backslash \. For example:

```
content:"3rxtc\"";Date";
```

As a consequence, the backslash character must be escaped with another one, if you want to use it.:

```
content:"HKLM\\\\Software\\\\Microsoft\\\\Internet Explorer\\\\Main\\\\Start_
↵Page";
```

## Modifier Keywords

Some keywords operate as modifiers. There are two types of modifiers:

- **Content modifiers** look back in the rule, e.g.:

```
alert http any any -> any any (content:"index.html"; nocase; sid:1;)
```

In the above example, the pattern `index.html` will be case insensitive.

- **Sticky buffers** are placed before the keyword. This type of modifier is applied on all following keywords, for example:

```
alert http any any -> any any (http.uri; content:"index.html"; sid:1;)
```

In the above example, the pattern `index.html` is inspected against the HTTP URI because it follows the `http.uri` keyword.

- Where relevant, both types can be used simultaneously. For example:

```
alert http any any -> any any (http.uri; content:"index.html"; nocase; sid:1;)
```

## 7.6.2 Metadata Keywords

Metadata keywords have no immediate effect on rule matching. However, they affect reporting when a rule matches.

### 7.6.2.1 msg

The keyword `msg` contains textual information about the signature and the possible alert.

The format of `msg` is:

```
msg: "some description";
```

Examples:

```
msg:"ATTACK-RESPONSES 403 Forbidden";  
msg:"ET EXPLOIT SMB-DS DCERPC PnP bind attempt";
```

**Note:** The following characters must be escaped inside the `msg`: `;` `\` `"`

### 7.6.2.2 sid

The keyword `sid` (signature ID) assigns an ID to every signature. This ID is given with a number. The format of `sid` is:

```
sid:123;
```

### 7.6.2.3 rev

`rev` represents the version of the signature. Each time a signature is updated, `rev` ought to be incremented. Its format is:

```
rev:123;
```

#### 7.6.2.4 classtype

The `classtype` keyword provides information on the classification of rules and alerts. It consists of a short name which can be translated as a priority for reporting purposes.

This example reports a hit of class “trojan-activity”:

```
drop tcp any any -> any any (msg:"classtype example"; content:"placeholder"; \
classtype:trojan-activity; sid:1; rev:1;)
```

**Tip:** It is a convention that `classtype` comes before `sid` and `rev` and after the rest of the keywords.

#### 7.6.2.5 reference

The `reference` keyword provides additional information on the purpose of the rule and the attack it detects. `reference` can appear multiple times in a signature. This keyword is meant for signature writers and analysts who investigate why a signature has matched.

It has the following format:

```
reference: type, reference
```

For example, a typical reference to `www.genua.de` would be:

```
reference: url, www.genua.de
```

In addition, there are also several systems that can be used as a reference. A commonly known example is the CVE-database that assigns numbers to vulnerabilities. You can refer to it as follows, for example:

```
reference: cve, CVE-2014-1234
```

This creates a reference to <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1234>.

#### 7.6.2.6 priority

**Note:** cognitix Threat Defender does not support this keyword.

### 7.6.2.7 metadata

With the `metadata` keyword, additional, non-functional information can be added to the signature. The format is:

```
metadata: key value;  
metadata: key value, key value;
```

The `metadata` keyword is often used to code the signature creation `created_at` and last update timestamp `updated_at`.

Example:

```
metadata:created_at 2010_09_23, updated_at 2010_09_23;
```

### 7.6.2.8 target

cognitix Threat Defender does not evaluate the `target` keyword.

## 7.6.3 Payload Keywords

Payload keywords inspect the content of a packet or a specific buffer.

### 7.6.3.1 content

The `content` keyword is the basis for all signatures. Its value must be a string between double quotes:

```
content: "lorem ipsum";
```

It is possible to use several contents in a signature.

Contents are matched on bytes. You can match on all printable characters by writing them in the `content` keyword. For non-printable characters, use their hexadecimal notations between pipe characters.

For example:

```
content: "GET /|69 6E 64 65 78 2E 68 74 6D 6C| HTTP/1.0";
```

Note that there are reserved characters you cannot use in the `content` keyword because they are meaningful in the signature. To match on these characters, you have to use hexadecimal



notation. It is a convention to write the hexadecimal notation in upper case characters. Reserved characters are:

Character	Hexadecimal Notation
“	22
;	3B
:	3A
	7C

Refer to the ASCII table for a comprehensive list of characters and their hexadecimal values. Furthermore, it is possible to use ! for exceptions in contents.

For example:

```
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"Outdated Firefox on
Windows"; content:"User-Agent|3A| Mozilla/5.0 |28|Windows|3B| ";
content:"Firefox/3."; distance:0; content:! "Firefox/3.6.13";
distance:-10; sid:9000000; rev:1;)
```

Here, `content:! "Firefox/3.6.13";` means that an alert will be generated if the used version of Firefox is not 3.6.13.

By default, the pattern matching is case sensitive.

### 7.6.3.2 nocase

If you do not want to make a distinction between uppercase and lowercase characters, you can use the `nocase` content modifier.

Place it after the content you want to modify, for example:

```
content: "abc"; nocase;
```

### 7.6.3.3 depth

The `depth` content modifier comes with a mandatory numeric value, for example:

```
depth:12;
```

The number after `depth` designates how many bytes from the beginning of the payload will be checked.

#### 7.6.3.4 offset

The `offset` keyword designates from which byte on the payload will be checked for a match.

The keywords `offset` and `depth` can be combined and are often used together.

For example:

```
content:"def"; offset:3; depth:3;
```

In this example, the payload is checked from the third byte to the sixth byte.

#### 7.6.3.5 distance

The `distance` keyword is a relative content modifier. This means it indicates a relation between the current content keyword and the content preceding it. `distance` takes effect after the preceding match.

The `distance` keyword comes with a mandatory signed value. This value determines the byte from which the payload will be checked for a match relative to the previous match.

`distance` determines where cognitix Threat Defender will start looking for a pattern. For example, `distance:5;` means the pattern can be anywhere after the previous match plus 5 bytes. To limit how far after the last match cognitix Threat Defender needs to look, use `within`.

#### 7.6.3.6 within

The `within` keyword is relative to the preceding match. The keyword `within` comes with a mandatory positive value. Using `within` makes sure there will only be a match if the content matches the payload within the set number of bytes.

#### 7.6.3.7 startswith

The `startswith` keyword is similar to `depth:<length of pattern>;`. It takes no arguments and must follow a content keyword. It modifies the content to match exactly at the start of a buffer.

Example:

```
content:"GET|20|"; startswith;
```

`startswith` is a short hand notation for:

```
content:"GET|20|"; depth:4; offset:0;
```

startswith cannot be mixed with depth, offset, within or distance for the same pattern.

### 7.6.3.8 endswith

The endswith keyword is similar to `isdataat:!1,relative;`. It takes no arguments and must follow a `content` keyword. It modifies the `content` to match exactly at the end of a buffer.

Example:

```
content:".php"; endswith;
```

endswith is a short hand notation for:

```
content:".php"; isdataat:!1,relative;
```

**Note:** You can combine `startswith` and `endswith` to check whether a pattern fills the complete buffer. Example:

```
http.uri; content:"/index.html"; startswith; endswith;
```

### 7.6.3.9 isdataat

The purpose of `isdataat` is to look if there is still data at a specific part of the payload. The keyword starts with a positive number (the position) and optionally followed by `relative` separated by a comma. Use `relative` to know if there is still data at a specific part of the payload relative to the last match.

The following example illustrates a signature which searches for byte 512 of the payload:

```
isdataat:512;
```

The second example illustrates a signature searching for byte 50 after the last match:

```
isdataat:50, relative;
```

The option `rawbytes` is not supported.

### 7.6.3.10 bsize

With the `bsize` keyword, you can match on the length of the buffer to add precision to the content match. Previously this could be done with `isdataat`.

### 7.6.3.11 dsize

With the `dsize` keyword, you can match on the size of the packet payload. For example, you can use the keyword to look for abnormal sizes of payloads. This may be convenient in detecting buffer overflows.

### 7.6.3.12 byte\_test

The `byte_test` keyword extracts the number of bytes specified in `bytes_to_convert` and performs an operation selected with `operator` against `value` at `offset`.

Format:

```
byte_test:<bytes_to_convert>, [!]<operator>, <value>, <offset> \
    [, relative][, <endian>][, string, <num>][, dce] \
    [, bitmask <bitmask_value>];
```

#### bytes\_to\_convert

The number of bytes selected from the packet to be converted; between 1 - 8.

#### value

Value to test the converted value against; between 0 - 4294967295.

#### offset

Number of bytes into the payload.

#### operator

- ! negation, can prefix other operators
- < less than
- > greater than
- = equal to
- <= less than or equal to
- >= greater than or equal to
- & bitwise AND
- ^ bitwise OR

**relative**

Offset relative to last content match.

**endian**

- big (most significant byte at lowest address)
- little (most significant byte at the highest address)

**string <num>**

- dec (converts string to decimal)
- hex (converts string to hexadecimal)
- oct (converts string to octal)

**dce**

not supported

**bitmask**

not supported

Example:

```

alert tcp any any -> any any (msg:" Matches User-Agent 'genua'"; \
http.header; content:"User-Agent: "; \
byte_test:5, =, 113685342544138, 0, relative, big; sid:1; rev:1)

alert http any any -> any any (msg:" Matches Content-Length value"; \
http.header; content:"Content-Length: "; \
byte_test:0, >=, 1000, 0, string, dec; sid:1; rev:1)

```

Note that endian and string cannot be used in the same byte\_test operation.

**7.6.3.13 byte\_jump**

The byte\_jump keyword allows for the ability to select bytes\_to\_convert from an offset and moves the detection pointer to that position. Subsequent content matches will then be based off the new position.

Format:

```

byte_jump:<bytes_to_convert>, <offset> [, relative][, multiplier <mult_value>] \
[, <endian>][, string, <number_type>][, align][, from_beginning][, from_end] \
[, post_offset <adjustment value>][, dce][, bitmask <bitmask_value>];

```

### bytes\_to\_convert

The number of bytes selected from the packet to be converted, between 1 - 8.

### offset

Number of bytes into the payload.

### relative

Offset relative to last content match.

### multiplier

Multiplies the converted byte by the value.

### endian

- `big` (most significant byte at lowest address)
- `little` (most significant byte at the highest address)

### string <num>

- `dec` (converts string to decimal)
- `hex` (converts string to hexadecimal)
- `oct` (converts string to octal)

### align

Rounds the number up to the next 32-bit boundary.

### from\_beginning

Jumps forward from the beginning of the packet, instead of where the detection pointer is set.

### from\_end

not supported

### post\_offset

After the jump operation has been performed, the specified number of bytes be will jumped additionally.

### dce

not supported

### bitmask

not supported

Example:

```
alert tcp any any -> any any (msg:"Jump on binary newline 10 bytes forward"; \
content:"/index.html HTTP/1.0\"; byte_jump:1,1,relative,big; \
content:\"genua\"; distance:0; sid:1; rev:1;)
```

#### 7.6.3.14 byte\_extract

**Note:** cognitix Threat Defender does not support this keyword.

#### 7.6.3.15 pcre (Perl Compatible Regular Expressions)

The `pcre` keyword matches specifically on [regular expressions](#)<sup>33</sup>.

Matching regular expressions causes a lot of processing overhead and is often combined with the `content` keyword. This way, the regular expression is only run if the `content` matches first.

Format of `pcre`:

```
pcre:"/<regex>/<modifiers>";
```

In the following example, the signature will match if the payload contains six consecutive numbers:

```
pcre:"/[0-9]{6}/";
```

**Note:** The following characters must be escaped inside the content: `;` `\` `"`

#### Perl/PCRE-compatible Modifiers

The matching behavior and the syntax interpretation of PCREs can be altered by several flags. The ones supported are listed here, with a short description and their internal PCRE name in parentheses.

- `i` (PCRE\_CASELESS)

If this modifier is set, letters in the pattern match both upper- and lowercase letters.

- `m` (PCRE\_MULTILINE)

By default, PCRE treats the subject string as consisting of a single “line” of characters (even if it actually contains several newlines). The “start of line” metacharacter (`^`) matches only at the start of the string, while the “end of line” metacharacter (`$`) matches only at the end of the string, or before a terminating newline (unless `E` modifier is set). When this modifier is set:

- `^` additionally matches after every newline character (and the start of the string)
- `$` additionally matches before every newline character (and the end of the string)

<sup>33</sup> [http://en.wikipedia.org/wiki/Regular\\_expression](http://en.wikipedia.org/wiki/Regular_expression)

If there are no `\n` characters in a subject string, or no occurrences of `^` or `$` in a pattern, setting this modifier has no effect.

- **s (PCRE\_DOTALL)**

If this modifier is set, a dot metacharacter in the pattern matches all characters, including newlines. Without it, newlines are excluded. A negative class such as `[^a]` always matches a newline character, independent of the setting of this modifier.

- **x (PCRE\_EXTENDED)**

If this modifier is set, whitespace characters in the pattern are totally ignored except when escaped or inside a character class. In this mode, `#` also introduces a line comment (that extends to the next `\n` character (inclusive)). `#` characters that are escaped or inside a character class are treated as normal. Whitespace characters may never appear within special character sequences in a pattern, for example within the sequence `(?(` which introduces a conditional subpattern.

- **A (PCRE\_ANCHORED)**

If this modifier is set, the pattern is forced to be “anchored”, that is, it is constrained to match only at the start of the string which is being searched (the “subject string”). This effect can also be achieved by appropriate constructs (`^`) in the pattern itself.

- **E (PCRE\_DOLLAR\_ENDONLY)**

If this modifier is set, a dollar metacharacter in the pattern matches only at the end of the subject string. Without this modifier, a dollar also matches immediately before the final character if it is a newline (but not before any other newlines). This modifier is ignored if `m` modifier is set.

**Note:** This modifier is sometimes represented with the letter `D` (e.g. PHP).

- **G (PCRE\_UNGREEDY)**

This modifier inverts the “greediness” of the quantifiers so that they are not greedy by default, but become greedy if followed by `?`. It can also be set by a `(?U)` modifier setting within the pattern. This can also be achieved by inverting the greediness of every quantifier individually by appending a question mark (e.g. `.* -> .*?`, `.+ -> .+?`, `x? -> x??`).

**Note:** This modifier is usually represented with the letter `U`.

## Custom Modifiers

The following custom modifiers are available:



- R: Match relative to the last pattern match. It is similar to `distance:0;`.
- B: Compatibility `pcre` modifier. This modifier has no effect.
- 0: not supported

## Custom Target Modifiers

There are several custom modifiers available to specify the buffer the pattern should match on. These stem mostly from the time modifier keywords were used to specify the target buffer, instead of the now prevalent sticky buffer keywords. They should be considered deprecated and the use of sticky buffer keywords should be preferred.

- C: Matches on the same buffer as `http.cookie`.
- D: not supported
- H: Matches on the same buffer as `http.header`.
- I: Matches on the same buffer as `http.uri.raw`.
- M: Matches on the same buffer as `http.method`.
- P: Matches on the same buffer as `http.request_body`.
- Q: Matches on the same buffer as `http.response_body`.
- S: Matches on the same buffer as `http.stat_code`.
- U: Synonym of I.
- V: Matches on the same buffer as `http.user_agent`.
- W: Matches on the same buffer as `http.host`.
- Y: Matches on the same buffer as `http.stat_msg`.
- Z: Matches on the same buffer as `http.host.raw`.

## 7.6.4 Flow Keywords

### 7.6.4.1 flowbits

`flowbits` consists of an action and the flowbits name.

Flowbits can perform the following actions:

Action	Description
flowbits: set, name	Will set the condition 'name' in the flow, if present.
flowbits: isset, name	The rule generates an alert when it matches and the condition is set in the flow.
flowbits: toggle, name	not supported
flowbits: unset, name	Unsets the condition in the flow.
flowbits: isnotset, name	The rule generates an alert when it matches and the condition is not set in the flow.
flowbits: noalert	No alert will be generated by this rule.

#### 7.6.4.2 flow

The `flow` keyword can be used to match on characteristics of a flow, such as its direction and if its connection is established or stateless.

The `flow` keyword can have the following options:

Option	Description
<code>to_client</code>	Match on packets from server to client.
<code>to_server</code>	Match on packets from client to server.
<code>from_client</code>	Match on packets from client to server (same as <code>to_server</code> ).
<code>from_server</code>	Match on packets from server to client (same as <code>to_client</code> ).
<code>established</code>	Match on established connections.
<code>not_established</code>	not supported
<code>stateless</code>	Match on packets that are and are not part of an established connection.
<code>only_stream</code>	not supported
<code>no_stream</code>	not supported
<code>only_frag</code>	not supported
<code>no_frag</code>	not supported

Multiple flow options can be combined, for example:

```
flow:to_client, established
flow:stateless
```

## 7.6.5 DNS Keywords

DNS keywords are designed to match on various fields of a DNS request. The buffers are normalized to allow content matching by using the literal domain name.

### 7.6.5.1 dns.query

Sticky buffer to match on the content of a DNS request query.

Example:

```
alert tls any any -> any any (classtype:misc-attack; \  
msg:"content matching in dns query field"; \  
dns.query; content:"mail.example.com"; sid:1; rev:1;)
```

**Note:** The older `dns_query` keyword is deprecated and should no longer be used.

## 7.6.6 HTTP Keywords

These keywords are specialized in matching specific parts of an HTTP flow.

All keywords can be used in combination with all content modifiers, such as `depth`, `distance`, `offset`, `nocase` and `within`.

**Note:** All buffers are **normalized** but the **raw** keywords. Any trailing carriage return and new line characters are removed.

The following **request** keywords are available:

Keyword	Type	Direction
http.uri	Sticky Buffer	Request
http.uri.raw	Sticky Buffer	Request
http.method	Sticky Buffer	Request
http.request_line	Sticky Buffer	Request
http.request_body	Sticky Buffer	Request
http.header	Sticky Buffer	Both
http.host	Sticky Buffer	Request
http.host.raw	Sticky Buffer	Request
http.user_agent	Sticky Buffer	Request
http.accept	Sticky Buffer	Request
http.accept_enc	Sticky Buffer	Request
http.accept_lang	Sticky Buffer	Request
http.cookie	Sticky Buffer	Both
http.referer	Sticky Buffer	Request
http.connection	Sticky Buffer	Request
http.content_type	Sticky Buffer	Both
http.content_len	Sticky Buffer	Both
http.protocol	Sticky Buffer	Both
http.header_names	Sticky Buffer	Both

The following response keywords are available:

Keyword	Type	Direction
http.location	Sticky Buffer	Response
http.stat_code	Sticky Buffer	Response
http.stat_msg	Sticky Buffer	Response
http.response_line	Sticky Buffer	Response
http.response_body	Sticky Buffer	Response
http.header	Sticky Buffer	Both
http.cookie	Sticky Buffer	Both
http.content_type	Sticky Buffer	Both
http.content_len	Sticky Buffer	Both
http.protocol	Sticky Buffer	Both
http.header_names	Sticky Buffer	Both

### 7.6.6.1 http.host

Sticky buffer to match on the normalized HTTP host. Normalization consists of truncating port information and converting all characters to be lowercase. Patterns matching on this buffer should be all lowercase or have the `nocase` flag set, although it is not strictly required.

Example:

```
alert http any any -> any any (http.host; content:"abc.com"; sid:1;)
```

### 7.6.6.2 http.host.raw

Sticky buffer to match on the raw HTTP host. This buffer might include port information.

Example:

```
alert http any any -> any any (http.host.raw; content:"AbC.com:80"; sid:1;)
```

### 7.6.6.3 http.method

Sticky buffer to match on the HTTP method. This buffer can match a maximum of 16 bytes. Examples of methods are: `GET`, `POST`, `PUT`, `HEAD`, `DELETE`, `TRACE`, `OPTIONS`, `CONNECT` and `PATCH`.

### 7.6.6.4 http.uri and http.uri.raw

Sticky buffers to match on the raw HTTP request URI. Currently, `http.uri` and `http.uri.raw` are synonyms. No normalization is performed for `http.uri`.

### 7.6.6.5 urilen

The `urilen` keyword is used to match on the length of the request URI. The `<` (less than) and `>` (greater than) operators can be used.

Possible formats of `urilen` are:

```
urilen:1;
urilen:>1;
urilen:<10;
urilen:10<>20;      (greater than 10, less than 20)
```

Example of `urilen` in a signature:

```
alert tcp any any -> any any (classtype:misc-attack; \
http.uri; content:\"placeholder\"; urilen:11<>13, raw; sid:1;)
```

You can also append `norm` or `raw` to define if you want to use normalized or raw buffers.

**Note:** Inspection of the normalized buffer (via `norm`) is currently not supported.

#### 7.6.6.6 http.protocol

Sticky buffer to match on the HTTP protocol field from the HTTP request or response line. If the request line is 'GET / HTTP/1.0rn', then this buffer will contain 'HTTP/1.0'.

Example:

```
alert http any any -> any any (http.protocol; content:"HTTP/1.0"; sid:1;)
```

#### 7.6.6.7 http.request\_line

Sticky buffer to match on the whole HTTP request line. Assuming the request line is 'GET / HTTP/1.1rn', then this buffer will contain 'GET / HTTP/1.1'.

Example:

```
alert http any any -> any any (http.request_line; content:"GET / HTTP/1.1"; sid:1;)
```

#### 7.6.6.8 http.header

Sticky buffer to match on the whole HTTP header.

Example:

```
alert http any any -> any any (http.header; content:"Sun, 03 May 2015 23:02:37 GMT";
↳sid:1;)
```

**Note:** The `http.header.raw` keyword is not supported.

### 7.6.6.9 http.cookie

Sticky buffer to match on the cookie content.

Example:

```
alert http any any -> any any (http.cookie; content:"OAID="; sid:1;)
```

### 7.6.6.10 http.user\_agent

Sticky buffer to match on the HTTP user agent in a HTTP request.

Example:

```
alert http any any -> any any (http.user_agent; content:"Bittorrent"; sid:1;)
```

### 7.6.6.11 http.accept

Sticky buffer to match on the HTTP accept header.

Example:

```
alert http any any -> any any (http.accept; content:"image/gif"; sid:1;)
```

### 7.6.6.12 http.accept\_enc

Sticky buffer to match on the HTTP accept encoding header.

Example:

```
alert http any any -> any any (http.accept_enc; content:"gzip"; sid:1;)
```

### 7.6.6.13 http.accept\_lang

Sticky buffer to match on the HTTP accept language header.

Example:

```
alert http any any -> any any (http.accept_lang; content:"en-us"; sid:1;)
```

#### 7.6.6.14 http.connection

Sticky buffer to match on the HTTP connection header.

Example:

```
alert http any any -> any any (http.connection; content:"keep-alive"; sid:1;)
```

#### 7.6.6.15 http.content\_type

Sticky buffer to match on the HTTP content type header.

Example:

```
alert http any any -> any any (http.content_type; content:"x-www-form-urlencoded"; sid:1;)
```

#### 7.6.6.16 http.content\_len

Sticky buffer to match on the HTTP content length header.

Example:

```
alert http any any -> any any (http.content_len; content:"1500"; sid:1;)
```

#### 7.6.6.17 http.referer

Sticky buffer to match on the HTTP referer header.

Example:

```
alert http any any -> any any (http.referer; content:".php"; sid:1;)
```

#### 7.6.6.18 http.header\_names

Sticky buffer to match on an artificial buffer containing only the names of all seen HTTP headers.

Example buffer:



```
\\r\\nHost\\r\\n\\r\\n
```

Example rule:

```
alert http any any -> any any (http.header_names; content:"|0d 0a|Host|0d 0a|"; sid:1;
↔)
```

Example to make sure *only* Host is present:

```
alert http any any -> any any (http.header_names; \
    content:"|0d 0a|Host|0d 0a 0d 0a|"; sid:1;)
```

Example to make sure *User-Agent* is directly after *Host*:

```
alert http any any -> any any (http.header_names; \
    content:"|0d 0a|Host|0d 0a|User-Agent|0d 0a|"; sid:1;)
```

Example to make sure *User-Agent* is after *Host*, but not necessarily directly after:

```
alert http any any -> any any (http.header_names; \
    content:"|0d 0a|Host|0d 0a|"; content:"|0a 0d|User-Agent|0d 0a|"; \
    distance:-2; sid:1;)
```

#### 7.6.6.19 http.request\_body

Sticky buffer to match on the HTTP request body.

**Note:** The older `http_client_body` modifier keyword is deprecated and should no longer be used.

#### 7.6.6.20 http.stat\_msg

Sticky buffer to match on the HTTP status message.

#### 7.6.6.21 http.stat\_code

Sticky buffer to match on the HTTP status code. This buffer can match a maximum of 16 bytes.

Example:

```
alert http any any -> any any (http.stat_code; content:"200"; sid:1;)
```

#### 7.6.6.22 http.response\_line

Sticky buffer to match on the HTTP response line.

Example:

```
alert http any any -> any any (http.response_line; content:"HTTP/1.0 200 OK"; sid:1;)
```

#### 7.6.6.23 http.response\_body

Sticky buffer to match on the HTTP response body.

Example:

```
alert http any any -> any any (http.response_body; content:"|0A 0B|</span>"; sid:1;)
```

#### Note:

- `http.response_body` matches on deflated data just like `file_data` does.
- The older `http_server_body` modifier keyword is deprecated and should no longer be used.

#### 7.6.6.24 http.location

Sticky buffer to match on the HTTP location headers.

Example:

```
alert http any any -> any any (http.location; content:"http://www.genua.de"; sid:1;)
```

#### 7.6.6.25 file\_data

Synonym for [http.response\\_body](#) (page 266).

#### 7.6.6.26 file.data

Synonym for [file\\_data](#) (page 266).

## 7.6.7 SSL/TLS Keywords

Several rule keywords to match on various properties of the TLS/SSL handshake. All supported fields are sticky buffers and can be used with `fast_pattern`.

### 7.6.7.1 `tls.cert_subject`

Matches the TLS/SSL certificate subject field.

Example:

```
alert tls any any -> any any (classtype:misc-attack; \  
msg:"content matching in tls subject field"; \  
tls.cert_subject; content:"Test Certificate ECDSA"; sid:1; rev:1;)
```

cognitix Threat Defender also supports the deprecated `tls_cert_subject` keyword, but we do not recommend using it.

### 7.6.7.2 `tls.cert_issuer`

Matches the TLS/SSL certificate issuer field.

Example:

```
alert tls any any -> any any (classtype:misc-attack; \  
msg:"content matching in tls issuer field"; \  
tls.cert_issuer; content:"Let's Encrypt"; sid:2; rev:1;)
```

cognitix Threat Defender also supports the deprecated `tls_cert_issuer` keyword, but we do not recommend using it.

### 7.6.7.3 `tls.cert_fingerprint`

Matches the TLS/SSL certificate fingerprint. This fingerprint is a SHA-1 digest of the whole certificate.

Example:

```
alert tls any any -> any any (classtype:misc-attack; \  
msg:"content matching in tls fingerprint"; \  
tls.cert_fingerprint; \  

```

(continues on next page)

(continued from previous page)

```
content:"54:4c:7e:23:4d:df:84:5f:75:39:42:45:5e:5f:1a:42:75:80:b3:d3"; \
sid:2; rev:1;)
```

The `tls.cert_fingerprint` can only be used with a `content` field which can be negated. This `content` field must represent a digest which is composed of 20 two-digit groups separated by colons (:).

cognitix Threat Defender also supports the deprecated `tls_cert_fingerprint` keyword, but we do not recommend using it.

#### 7.6.7.4 `tls.fingerprint`

Matches the TLS/SSL certificate fingerprint. This fingerprint is a SHA-1 digest of the whole certificate.

Example:

```
alert tls any any -> any any (classtype:misc-attack; \
msg:"content matching in tls fingerprint"; \
tls.fingerprint:"54:4c:7e:23:4d:df:84:5f:75:39:42:45:5e:5f:1a:42:75:80:b3:d3"; \
sid:3; rev:1;)
```

This `tls.fingerprint` field must represent a digest which be composed of 20 two-digit groups separated by colons (:). This field can be negated.

#### 7.6.7.5 `tls.sni`

Matches the TLS/SSL server name indication field.

Example:

```
alert tls any any -> any any (classtype:misc-attack; \
msg:"content matching in tls sni field"; \
tls.sni; content:"example.org"; sid:3; rev:1;)
```

cognitix Threat Defender also supports the deprecated `tls_sni` keyword, but we do not recommend using it.

#### 7.6.7.6 `tls.certs`

Does a “raw” match on each of the certificates in the TLS certificate chain.

Example:

```
alert tls any any -> any any (classtype:misc-attack; \  
msg:"content matching Algorithm Id sha256WithRSAEncryption"; \  
tls.certs; content:"|2a 86 48 86 f7 0d 01 01 0b|"; sid:4; rev:1;)
```

### 7.6.7.7 tls.cert\_serial

Matches the TLS/SSL certificate serial number field.

Example:

```
alert tls any any -> any any (classtype:misc-attack; \  
msg:"content matching on certificate serial number"; \  
tls.cert_serial; content:"7A:8C:A6:5F:B1:AA:FC:8A:8F:96:D4:BA"; sid:5; rev:1;)
```

The field must represent a byte series which is composed of two-digit groups separated by colons (:).

cognitix Threat Defender also supports the deprecated `tls_cert_serial` keyword, but we do not recommend using it.

## 7.6.8 JA3 Keywords

JA3 is an algorithm developed by Salesforce to fingerprint TLS endpoints based on metadata in their handshake.

More information about it can be found in this [Salesforce Engineering blogpost](#)<sup>34</sup>

### 7.6.8.1 ja3.hash

Matches on the MD5 hash of the TLS client JA3 signature.

Example:

```
alert tls any any -> any any (classtype:misc-attack; \  
msg:"content matching in ja3 fingerprint of a client"; \  
ja3.hash; content:"68b329da9893e34099c7d8ad5cb9c940"; sid:1; rev:1;)
```

`ja3.string` is a sticky buffer which can only with be used with a `content` field containing exactly 32 characters which cannot be negated.

<sup>34</sup> <https://engineering.salesforce.com/tls-fingerprinting-with-ja3-and-ja3s-247362855967>

### 7.6.8.2 ja3s.hash

Matches on the MD5 hash of the TLS server JA3 signature.

Example:

```
alert tls any any -> any any (classtype:misc-attack; \  
msg:"content matching in ja3 fingerprint of a server"; \  
ja3s.hash; content:"68b329da9893e34099c7d8ad5cb9c940"; sid:1; rev:1;)
```

ja3s.string is a sticky buffer which can only with be used with a content field containing exactly 32 characters which cannot be negated.

cognitix Threat Defender also supports the deprecated ja3\_hash keyword, but we do not recommend using it.

## 7.6.9 SSH Keywords

### 7.6.9.1 ssh.proto

Matches the protocol version string present in the SSH protocol banner. This keyword is a sticky buffer.

The software version string is defined in [RFC4253<sup>35</sup>](#):

```
This identification string MUST be:  
SSH-protoversion-softwareversion SP comments CR LF
```

Example:

```
alert ssh any any -> any any (classtype:misc-attack; \  
msg:"content matching on SSH protocol version"; \  
ssh.proto; content:"2.0"; sid:1; rev:1;)
```

cognitix Threat Defender also supports the deprecated ssh\_proto keyword, but we do not recommend using it.

### 7.6.9.2 ssh.software

Matches the software version string present in the SSH protocol banner. This keyword is a sticky buffer.

The software version string is defined in [RFC4253<sup>36</sup>](#):

<sup>35</sup> <https://datatracker.ietf.org/doc/html/rfc4253#section-4.2>

<sup>36</sup> <https://datatracker.ietf.org/doc/html/rfc4253#section-4.2>

This identification string MUST be:

```
SSH-protoversion-softwareversion SP comments CR LF
```

Example:

```
alert ssh any any -> any any (classtype:misc-attack; \
msg:"content matching on OpenSSH software string"; \
ssh.software; content:"OpenSSH"; sid:1; rev:1;)
```

cognitix Threat Defender also supports the deprecated `ssh_software` and `ssh.softwareversion` keywords, but we do not recommend using it.

## 7.6.10 Thresholding Keywords

### 7.6.10.1 threshold

The `threshold` keyword can be used to control the alert frequency of a rule. It has three modes: `threshold`, `limit` and `both`.

Syntax:

```
threshold: type <threshold|limit|both>, track <by_src|by_dst>, count <N>, seconds <T>
```

#### threshold

This type can be used to set a minimum threshold for a rule before it generates alerts. A `threshold` setting of `N` means that an alert is generated when the rule matches for the `N`th time.

Example:

```
alert tcp any any -> any any (msg: "threshold example"; \
classtype:misc-attack; content: "placeholder"; \
threshold: type threshold, track by_src, count 5, seconds 1; sid:1; rev:1;)
```

This signature only generates an alert if 5 or more packets contain the `placeholder` string within a one-second interval.

If a signature sets a flowbit, those actions are still performed on each match.

## limit

This type can be used to make sure the system will not be flooded with alerts. If `limit` is set to `N`, a maximum of `N` alerts are generated.

Example:

```
alert http any any -> any any (msg:"thresholding limit example"; \
http.header; content:"Accept"; \
threshold: type limit, track by_src, count 15, seconds 1800; sid:2; rev:1;)
```

In a 30-minute period, this signature generates at most 15 alerts for HTTP responses containing the string `Accept` in their headers.

If a signature sets a flowbit, those actions are still performed on each match.

## both

Using `both`, `threshold` and `limit` can be combined to enforce both thresholding and limiting.

Example:

```
alert http any any -> any any (msg:"thresholding limit example"; \
http.header; content:"Accept"; \
threshold: type both, track by_src, count 15, seconds 1800; sid:2; rev:1;)
```

This rule only generates an alert if there are 15 or more `Accept` headers in HTTP responses within 30 minutes. In this 30-minute period, only one alert will be generated.

If a signature sets a flowbit, those actions are still performed on each match.

### 7.6.10.2 detection\_filter

The `detection_filter` keyword can be used to alert on every match after a threshold has been reached. It differs from the `threshold` type as it generates an alert for each rule match after the initial threshold has been reached.

Syntax:

```
detection_filter: track <by_src|by_dst>, count <N>, seconds <T>
```

Example:



```
alert tcp any any -> any any (msg: "detection filter example"; \  
classtype:misc-attack; content: \"placeholder\"; \  
threshold: type detection_filter, track by_src, count 100, seconds 10; sid:1; rev=1;)
```

This rule generates an alert every time 100 or more matches have occurred within 10 seconds.

If a signature sets a flowbit, those actions are still performed on each match.

## 7.7 FAQ

### 7.7.1 Can I enable multiple conditions in a rule and how are they handled?

You can enable any number of conditions in a rule.

Conditions are **AND**-connected. This means: If you activate multiple conditions in a rule, the rule only matches if the traffic meets all active conditions.

Within a condition, however, the selected elements are **OR**-connected. This means the condition is met if the traffic contains one of the selected elements.

#### Example:

A rule has the following conditions:

1. **GeoIP** has Guyana as destination
2. **Classification** has the protocols HTTP and SSL

This rule matches HTTP traffic flows to Guyana as well as SSL traffic flows to Guyana. However, it will not match traffic to Guyana via any other protocol.

See [Rules](#) (page 145) for further information on rule setup.

### 7.7.2 In what order does Threat Defender process rules?

To view the policy configured on cognitix Threat Defender, navigate to **Policy > Rules**.

Policy rules are processed from top to bottom. We therefore recommend placing more specific rules at the top of the table and rules that apply to a broader range of traffic at the bottom.

Global rules (i.e. rules that are applied to all traffic) are always processed before rules in correlation scenarios.

To reorder global rules, click the **ACTIVATE GLOBAL RULES REORDER** button above the table. Move the rules to the desired positions using drag and drop.

To reorder correlation scenarios, navigate to **Policy > Advanced Correlation**. Click the **ACTIVATE REORDER** button above the table and move the scenarios using drag and drop.

### 7.7.3 How does Threat Defender perform in active mode compared to passive mode?

When Threat Defender is used in port mirroring to monitor the network traffic the policy is continuously evaluated for analytics purposes. Therefore, there is no extra performance strain when Threat Defender actively enforces the policy.

### 7.7.4 What can I do if Threat Defender doesn't boot?

If cognitix Threat Defender does not boot up correctly, there are several actions you can take:

1. At the IP address of the management interface, you will see the troubleshooting screen.

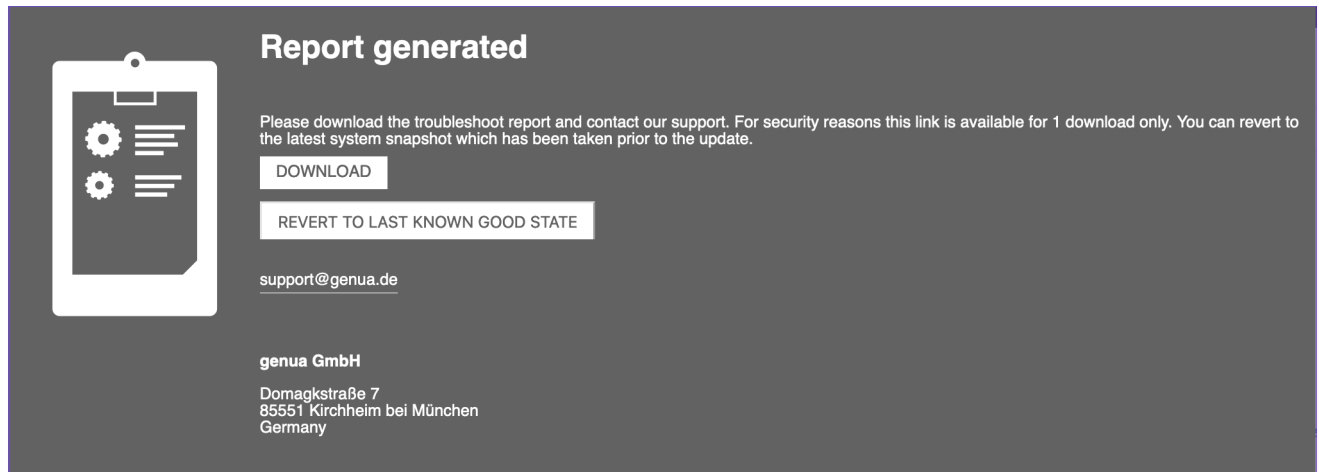


Fig. 1: Troubleshooting screen.

- Here, you can download a troubleshooting report and contact our support team at [support@genua.de](mailto:support@genua.de).
  - You can also revert the system to the last working state.
2. Alternatively, you can carry out a recovery installation by executing the installer. It checks the system for any existing backup files.

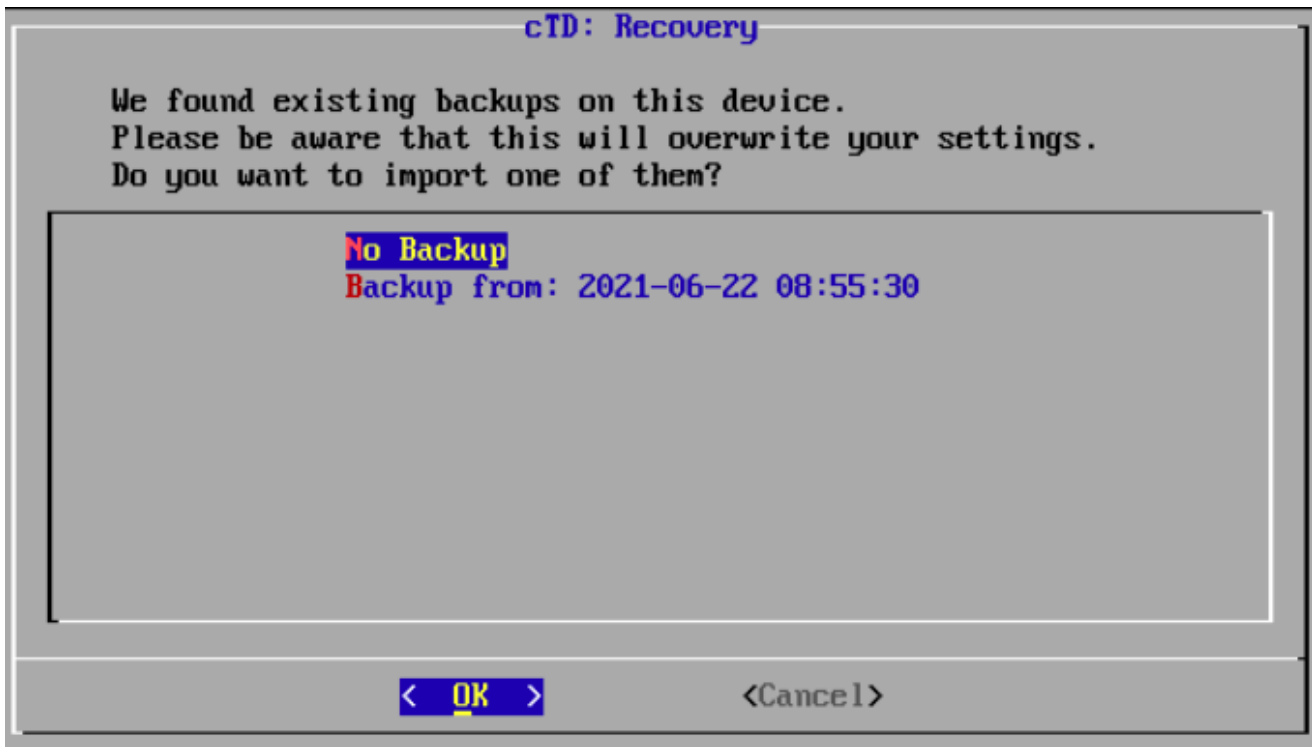


Fig. 2: Recovery screen.

Here, you can select a working backup to use in the recovery installation. Note that the backup may overwrite the other settings you configured in the installation wizard.

### 7.7.5 Why does the Threat Defender installer crash with minicom 2.8?

This is due to the incorrect transfer of UTF-8 characters with the minicom 2.8 package. To avoid this problem use the cu or screen packages.

| Chapter 8

# Glossary

## API

Application Programming Interface; provides a communication interface between multiple software applications or hardware appliances.

## ATT&CK

Adversarial Tactics, Techniques and Common Knowledge; a knowledge base for adversary techniques hosted by the MITRE corporation.

## Behavior-based correlation

If a device is infected with any kind of **malware**, the behavior in the network changes. For example, new connections are established to servers never talked to before, the malware tries to spread within the network, and to detect further systems and vulnerabilities. To distinguish this behavior from the normal actions of a device and to detect threats hidden in legitimate traffic, the behavior of the device has to be deducted from the entire network traffic of this device. By correlating the different flows of a device over time, its behavior can be determined. Then it is possible to detect deviations from the known legitimate behavior to indicate infections or malicious actors. See also the [detailed concept description](#) (page 74).

## BIOS

Basic Input/Output System; firmware used to initialize hardware during the booting process and to provide runtime services for operating systems and programs.

## BYOD

Bring Your Own Device (also called device management); the practice of allowing network users to access the (usually wireless) network of an organization with their own computers, smartphones, tablets and other devices. BYOD has a major impact on networks with large and diverse user bases, such as educational institutions or large and small business networks.

## C&C

Command and Control; a C&C server infrastructure usually controls a number of bots. Network traffic to known command and control servers is a certain sign of an infection.

## CIDR

Classless Inter-Domain Routing; a method for allocating IP addresses and IP routing. An IP address is stated with the number of leading 1 bits in the netmask, e.g. 192.0.2.0/24 for IPv4, 2001:db8::/32 for IPv6. For example, 10.10.10.100/24 is equivalent to IP 10.10.10.100 with netmask 255.255.255.0

## DMZ

Demilitarized Zone; a special network segment between two other larger segments

to provide secure services and special filtering to network traffic. Network access is allowed from each side to the application proxies and services within the DMZ but not from one side directly to the other. Only the services within the DMZ can initiate (controlled) network access to both sides.

## DNO

Dynamic Network Object; dynamic lists of addresses (MAC, IPv4 or IPv6) used in source/destination conditions of policies and rules. Device addresses are added by rule actions, for example when a specific behavior is detected for a device. The set of policies in effect for a certain device can change dynamically depending on whether the device is listed in a DNO or not. DNOs are one of the cornerstones of self-modifying policies and effects threat isolation and prevention.

## DNS

Domain Name System; a system that is used to translate structured, human-readable names like “www.genua.de” into machine readable data, such as IPv4 addresses, IPv6 addresses, responsible mail server, etc.

## DPDK

Data Plane Development Kit; an open source set of data plane libraries and NIC drivers for fast packet processing.

## ETT

Event Tracking Table; policy-specific tables that track and correlate pairs of enriched flow attributes over time. Rules can then check for the presence of certain attributes or count their number to influence how future flows are handled based on the attributes seen in earlier flows of communication. This is the cornerstone of behavior-based correlation to determine the behavior of users and devices and to monitor malicious behavior. See also the [concept description of ETTs](#) (page 78).

## External

In the setup of network objects, the **External** network is the part that is not monitored by Threat Defender.

## Flow

A logical connection of packets belonging to the same communication. For example, the request and response of an HTTP connection constitute one flow; the ICMP ping and its corresponding ICMP echo can also be seen as one flow.

## Gateway

The gateway in a **layer 3** network segment is the device where traffic is sent if the destination is not within the same network segment. The gateway is the default router to connect a specific network segment with the rest of the networks.

## Green

Green is the fourth color on the rainbow, between yellow and blue. It is often associated with nature, life, spring and wealth.

## HTTP

Hypertext Transfer Protocol; used for unencrypted communication over computer networks, including the Internet, to transfer text and similar documents from a server to the client. Most commonly used by web browsers but also by applications and malicious software.

## HTTPS

Encrypted version of HTTP; Transport Layer Security (TLS, formerly known as SSL) is used to encrypt the connection and to encapsulate the plain HTTP traffic. Authenticity of the server and optionally of the client is ensured using certificates and certificate authorities.

## Hyper-threading

Intel's proprietary simultaneous multithreading (SMT) implementation. For each physical processor core, the operating system addresses two virtual cores and shares the workload between them when possible. One physical core therefore appears as two processors to the operating system, allowing concurrent scheduling of two processes per core.

## IDS

Intrusion Detection System, see [IDS/IPS](#)

## IPS

Intrusion Prevention System, see [IDS/IPS](#)

## IDS/IPS

Intrusion Detection System/Intrusion Prevention System; a software or appliance that inspects and analyzes packets and data for numerous patterns of malicious behavior and different types of risks. When deployed as a detection system, it raises an alarm. When deployed as a prevention system, immediate action is taken to block the malicious traffic and alarm the network administrators.

## IETF

Internet Engineering Task Force; an open standards organization that develops and promotes voluntary Internet standards.

## Internal

In the setup of network objects, the **Internal** network refers to the part of the network that Threat Defender can see.



## IoA

Indicator of Attack; a marker to indicate an imminent or running attack. For example, IoA lists contain IP addresses of known botnets. Network traffic from these addresses can usually be blocked right away to prevent attacks and infections.

## IoC

Indicator of Compromise; a marker to indicate that the device might be infected with **malware**. IoC lists contain URLs, domains and IP addresses only seen in traffic between the malware and its C&C servers or when exfiltrating data. When devices access domains used for distributing malware, this may also be a sign for an imminent infection.

## IP address

An Internet Protocol address is a numerical label assigned to each device participating in a computer network that uses the Internet Protocol for communication. Human readable names are translated into IP addresses via **DNS**. There are **IPv4** and **IPv6** addresses.

## IPFIX

Internet Protocol Flow Information Export; provides a common, universal standard of export for Internet Protocol flow information from routers, probes and other devices. It defines how IP flow information is to be formatted and transferred from an exporter to a collector.

## IPv4

Internet Protocol version 4. IPv4 addresses are 32-bit addresses and are represented by 4 octets of decimal digits separated by a period, for example 172.16.254.1.

## IPv6

Internet Protocol version 6 was created in response to the depletion of available IPv4 addresses. IPv6 addresses are 128-bit addresses and are represented by 8 octets of hexadecimal digits, separated by a colon, for example 2001:db8:0000:0000:0000:0000:0000. IPv6 addresses can be abbreviated by replacing an occurrence of octets that are 0000 by a double colon; for example, the previous address can also be written as 2001:db8::.

## Layer 2

The data link layer in the **OSI** networking model. This layer provides the functional and procedural means required to transfer data between network entities.

## Layer 3

The network layer in the **OSI** networking model. This layer provides packet forwarding including routing through intermediate routers.

#### Layer 4

The transport layer in the [OSI](#) networking model. This layer provides the protocols for host-to-host communication services for applications.

#### Layer 7

The application layer in the [OSI](#) networking model. This layer is closest to the end user. This layer interacts with software applications that contain a communication component.

#### MAC address

Media Access Control address; a unique identifier assigned to a network interface used for network communication. A MAC address is assigned to a device by the manufacturer and so this address, unlike an IP address, does not normally change. MAC addresses are represented in notation by six groups of two hexadecimal digits, separated by hyphens or colons for example, 01:23:45:67:89:ab.

#### Malware

Malicious software that infects the system and performs unwanted and possibly harmful actions. Subtypes are trojans, worms, ransomware, and others.

#### Multihoming

Connecting a host or a computer network to more than one network to increase reliability and/or performance.

#### MISP

Malware Information Sharing Platform; an open source software for sharing of threat intelligence.

#### Network segmentation

A network can be divided into smaller segments for various reasons. Mostly it is used to protect the individual segments from each other. Each segment has its own layer 3 address range and routers are deployed to forward network traffic from one segment to another. If these routers are combined with a firewall, access from one segment to another can be controlled with firewall rules allowing or denying traffic. See also how Threat Defender implements [network segmentation](#) (page 122).

#### Network switch

A hardware device that connects network devices on [layer 2](#) (the Ethernet layer). Devices are identified by their MAC address and the switch forwards traffic as needed to a specific target device or broadcasts it to all devices.

#### NIC

Network Interface Controller; hardware component that connects a computer to a computer network.

**NUMA**

Non-Uniform Memory Access; a computer memory design used in multiprocessing, where the memory access time depends on the memory location relative to the processor. Under NUMA, a processor can access its own local memory faster than non-local memory.

**OSI**

Open Systems Interconnection model; a conceptual model that characterizes the communication functions of a communication system irrespective of its underlying internal structure and technology. It divides the system into abstraction layers.

**OUI**

Organizationally Unique Identifier; uniquely identifies the vendor or manufacturer of a piece of hardware. In combination with a 24-bit number the OUI forms the MAC address of a device.

**Packet**

A packet is a unit of data that is transmitted between communicating devices. A packet contains both the message being sent and control information, such as the source and destination address, source and destination port, transport protocol and sequence number.

**PEN**

Private enterprise number; public registration number that is created and maintained by the [IANA](https://www.iana.org/)<sup>37</sup>.

**Policy**

A set of rules, event tracking tables and dynamic network objects to describe legitimate and/or malicious behavior and to act on this behavior. While a single rule can only act on a specific **flow**, a policy acts on the behavior of a device and can affect the whole network traffic of a device for example by completely isolating an infected device.

**Port**

Port numbers are communication endpoints used to allow network communication. Different ports are used for different application-specific or process-specific purposes. For example, the HTTP protocol uses port 80.

**Proxy server**

A proxy server acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server and requests some service (e.g. a connection, web page, etc.) available from a different server. The proxy server then evaluates the request.

---

<sup>37</sup> <https://www.iana.org/>

## QUIC

Quick UDP Internet Connections; a transport layer protocol.

## Rule

A set of conditions of traffic parameters that trigger specified actions. When used in combination with cognitix event tracking tables (ETT) and dynamic network objects (DNO), more complex policies to describe the behavior of devices can be created.

## SCTP

Stream Control Transmission Protocol; a communications protocol that provides similar features as UDP and TCP, as well **multihoming** and redundant paths.

## Single-pass

The correlation and policy engine of Threat Defender classifies traffic and applies policies to it during a single pass through Threat Defender, minimizing delays and use of resources.

## SNMP

Simple Network Management Protocol, a protocol for monitoring network devices using a central monitoring system. cognitix Threat Defender supports SNMPv2 and SNMPv3.

## SPAN

Switched Port Analyzer; port mirroring

## Spoofing

By masquerading as something else, attackers try to get access to elevated permissions or just hide when entering and attacking networks. A local attacker might spoof their MAC address to disguise as a network printer to prevent detection. An attacker might spoof the IP address of another user to pretend to be that user and get past IP-based firewall rules to access more sensitive areas of the network.

## Subnet

A subnet is a segment of the network that is separated physically by routing network devices and/or logically by the different addressing of the nodes. Dividing the network into subnets increases performance by isolating traffic from network segments where it does not need to go, and it increases security by isolating access. The addressing scope of a subnet is defined by its IP address and subnet mask. Its connection to other networks is achieved using gateways and routers.

## syslog

A standard for message logging. It allows separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them. syslog is supported by a wide variety of platforms and devices.

## TCP

Transmission Control Protocol; a protocol that defines how communication is established and maintained via an IP network. It provides host-to-host connectivity at the transport layer of the OSI model.

## TCP reset

All packets of a TCP connection contain a TCP header with a bit known as the “reset” (RST) flag. If this bit is set to 1, it indicates that the receiving computer should immediately stop using this TCP connection and discard any further packets it receives with headers indicating they belong to that connection. A TCP reset instantly terminates a TCP connection.

## TLS / SSL

Transport Layer Security, formerly named Secure Sockets Layer (SSL) is a protocol for encrypting information that is transmitted over a network, including the Internet. SSL can be used for secure communications to a webserver (HTTPS) and for allowing remote users to access a network via a virtual private network.

## UDP

User Datagram Protocol; allows applications to send messages to other hosts in an IP network.

## UEFI

Unified Extensible Firmware Interface; defines a software interface between an operating system and platform firmware.

## URL

Uniform Resource Locator; a human readable text string that refers to a network resource. A URL mostly consists of a fully qualified domain name and the path in the server. For example, `https://www.genua.de/en/it-security-solutions` denotes the domain name `www.genua.de` and the path components `/en/it-security-solutions`. URLs are most commonly used on the Internet, where they are also known as web addresses. URLs can also be used in web filtering to block access to specific websites.

## UUID

Universally Unique Identifier; 128-bit number used to identify information in computer systems.

## VLAN

Virtual Local Area Network; used to logically divide a single local area network (LAN) into different parts that function independently. By adding the VLAN tag to the layer 2 encapsulation of network traffic, several layer 3 networks can share one physical connection without interfering with each other.

## VPN

Virtual Private Network; extends a private network across a public network. Applications running across a VPN benefit from the functionality, security and management of the private network. A VPN is created by establishing a virtual point-to-point connection using dedicated connections, virtual tunneling protocols and/or traffic encryption.

## Vulnerability

A weakness of a system or software that can be exploited. Vulnerabilities are usually caused by bugs in the implementation but some are also caused by problems in the design of a protocol or process. Known vulnerabilities are categorized by severity depending on the ramifications when exploited. Some vulnerabilities cause the target service to crash while others can be used to access data that is otherwise inaccessible. Other vulnerabilities can be exploited to execute arbitrary code and get elevated permissions for further exploits.

## Zero day

A **vulnerability** that is not widely known and for which no prevention or fix is available. Exploits for zero days are sold for higher prices as they promise certain access to the targeted system.

## Zero Trust

As networks grow more complex, applications become more distributed and interactions with foreign systems become more frequent. The classical notion of the trusted local network versus the untrusted outside world has to be forgotten. Instead, even the local networks cannot be trusted.

# Index

## A

Analytics, [54](#), [56](#), [142](#)

Assets, [144](#)

Network, [143](#)

Policy, [144](#)

API, [278](#)

Assets, [59](#), [60](#), [163](#)

Automatic discovery, [62](#), [169](#)

Network inventory, [61](#)

ATT&CK, see MITRE ATT&CK, [278](#)

Audit log channels, [189](#)

Audit logs, [189](#)

## B

Backup, [50](#), [175](#), [206](#)

Baselining, [113](#)

Behavior-based correlation, [278](#)

Behavior-based correlation, [73](#)

BIOS, [11](#), [278](#)

Bridges, [46](#), [186](#), [186](#)

BYOD, [278](#)

## C

C&C, [278](#)

checkmk, [200](#)

Checksum, [24](#)

CIDR, [278](#)

Correlation, [73](#)

Scenarios, [152](#)

Correlation examples, [85](#)

Access restriction, [86](#), [90](#)

ARP spoofing, [95](#)

Graylisting, [116](#)

Port scan, [102](#)

SSH brute forcing, [108](#)

Time-based baselining, [113](#)

## D

Data export, [177](#)

Default credentials, [33](#)

Diagnostics, [210](#)

Flow Table Reporting, [212](#)

MAC Table Reporting, [213](#)

Overview, [211](#)

System Health, [211](#)

Troubleshooting, [211](#)

DMZ, [72](#), [135](#), [278](#)

DNO, see Dynamic network objects, [279](#)

DNS, [279](#)

DPDK, [279](#)

Drill-down reporting, [54](#), [56](#), [142](#)

Dynamic network objects, [125](#), [128](#), [131](#), [156](#)

Examples, [86](#), [95](#)

## E

ELK, [63](#)

IPFIX via Filebeat, [64](#)

JSONL via Logstash, [68](#)

ETT, see Event tracking table, [279](#)

Event tracking table, [77](#), [84](#), [160](#)

Examples, [90](#), [95](#)

External, [279](#)

## F

Flow, [279](#)

Flow table reports, [212](#), [240](#)

## G

Gateway, [279](#)

genua hardware, [9](#)

genucenter, [207](#)

genugate, [94](#)

genuscreen, [94](#)

Global rules, [83](#)

Graylisting, [116](#)

Green, [280](#)

GUI, [36](#)

## H

Hardware

    genua hardware, [9](#)

    Requirements, [8](#)

    Troubleshooting, [10](#)

Hostname, [40](#), [197](#)

HTTP, [280](#)

HTTPS, [280](#)

Hyper-threading, [280](#)

## I

IDS, [94](#), [177](#), [280](#)

IDS/IPS, [280](#)

IETF, [280](#)

Incidents logs, [178](#)

Installation, [25](#)

    Image, [24](#), [25](#)

    Preparation, [24](#)

Interfaces, [186](#)

Internal, [280](#)

Inventory, [162](#)

    Asset Setting, [169](#)

    Assets, [163](#)

    Backup/Restore, [175](#)

    Data Export, [177](#)

    User API Setting, [174](#)

    Users, [169](#)

IoA, [281](#)

IoC, [281](#)

IP address, [281](#)

IPFIX, [64](#), [281](#)

    Specification, [225](#)

IPS, [177](#), [280](#)

IPS keywords, [242](#)

IPS rules, [183](#), [184](#), [242](#)

IPv4, [281](#)

IPv6, [281](#)

## J

JSONL, [68](#)

JSONL formatted output, [222](#)

## L

Layer 2, [281](#)

Layer 3, [281](#)

Layer 4, [282](#)

Layer 7, [282](#)

License, [39](#), [205](#)

Local logs, [195](#)

Logging, [188](#)

    Audit Logs, [189](#)

    Audit Logs Channels, [189](#)

    Local Logs, [195](#)

    Report Channels, [194](#)

## M

MAC address, [282](#)

MAC table, [213](#)

Malware, [282](#)

Management interface, [42](#), [198](#)

Mirror port, [54](#)

MISP, [282](#)

MITRE ATT&CK, [102](#)



T1001:003, [111](#)

T1046, [102](#)

T1110, [108](#)

T1200, [62](#)

Multihoming, [282](#)

## N

Network, [185](#)

Manage Processing Interfaces, [186](#)

Overview, [186](#)

Network objects, [122](#)

Network segmentation, [122](#), [282](#)

Examples, [130](#)

Network switch, [282](#)

NIC, [282](#)

drivers, [13](#)

firmware, [13](#)

NTP, [199](#)

NUMA, [283](#)

## O

OSI, [283](#)

OUI, [283](#)

## P

P-A-P, [94](#)

Packet, [283](#)

Password settings, [197](#)

PEN, [283](#)

Policy, [79](#), [83](#), [144](#), [283](#)

Advanced Correlation, [152](#)

Event Tracking Tables, [160](#)

Network Objects, [154](#)

Rules, [145](#)

Schedules, [159](#)

Port, [283](#)

Port monitoring, [56](#)

Processing interfaces, [46](#), [186](#)

Proxy, [42](#), [199](#)

Proxy server, [283](#)

## Q

QUIC, [284](#)

## R

Reboot, [209](#)

Release notes, [3](#)

Report channels, [63](#), [64](#), [194](#)

Encrypted, [68](#)

IPFIX, [225](#)

JSONL formatted output, [222](#)

syslog, [232](#)

Reset, [209](#)

Rule, [284](#)

Rule actions, [79](#)

Rule processing, [79](#)

Rules, [79](#), [145](#)

## S

Schedules, [159](#)

SCTP, [284](#)

Settings, [196](#)

Configurations, [206](#)

General, [197](#)

genucenter, [207](#)

License, [205](#)

Monitoring, [200](#)

System Actions, [209](#)

System Users, [202](#)

Update Schedules, [204](#)

Updates, [203](#)

Setup, [35](#)

Single-pass, [284](#)

SNMP, [200](#), [284](#)

SNO, see Static network objects

SPAN, [284](#)

Spoofing, [95](#), [284](#)  
Static network objects, [124](#), [126](#), [155](#)  
Subnet, [284](#)  
Switch monitoring, [54](#)  
syslog, [284](#)  
    Specification, [232](#)  
System requirements, [8](#)  
System settings, [196](#)  
System time, [40](#), [199](#)  
System users, [41](#), [202](#)  
    Roles, [216](#)

## T

TCP, [285](#)  
TCP reset, [285](#)  
Threats, [177](#)  
    Attributes, [182](#)  
    Events, [181](#)  
    Incidents Logs, [178](#)  
    Intelligence Database, [180](#)  
    IPS Rules, [183](#)  
    IPS Settings, [184](#)  
    Overview, [178](#)  
Time, [199](#)  
TLS / SSL, [285](#)  
Troubleshoot report, [211](#)

## U

UDP, [285](#)  
UEFI, [285](#)  
Update, [43](#), [203](#)  
    Schedule, [44](#), [204](#)  
URL, [285](#)  
USB installer drive, [24](#), [25](#)  
User API, [45](#), [174](#)  
User interface, [36](#)  
User mapping, [45](#)  
User roles, [216](#)

Users, [169](#)  
UUID, [285](#)

## V

Virtualization, [14](#)  
    QEMU/KVM, [17](#)  
    VirtualBox, [14](#)  
VLAN, [158](#), [285](#)  
    Breakout, [46](#), [72](#)  
    Port Extender, [46](#), [72](#)  
    Trunking, [49](#)  
VPN, [286](#)  
Vulnerability, [286](#)

## Z

Zero day, [286](#)  
Zero Trust, [286](#)