

Installation Guide

TUXGUARD
PRO ENDPOINT

TUXGUARD
ECM SERVER



Table of Contents

Home

●	TUXGUARD ICM Defense DEVICE SECURITY	9
---	--------------------------------------	---

Installation

	Device Security & DCM	10
--	-----------------------	----

●	TUXGUARD IDCM DEFENSE DEVICE SECURITY and DEVICE SECURITY CENTRAL MANAGER	10
●	TUXGUARD DEVICE SECURITY	10
●	DEVICE SECURITY Central Manager (DCM)	10

	Quickguide - DCM Installation	10
--	-------------------------------	----

●	Quick Installation Guide	10
●	Ports	10
●	Download and boot the DCM ISO image	11
●	Boot the DCM system	13
●	Use DCM configurator	13
●	Connect to GUI	14

	First Steps - DCM Configuration	14
--	---------------------------------	----

●	First Steps	14
●	Import a license	15
●	Download the default bundle	15
●	Installation	15

Deployment Hints	15
● TUXGUARD DEVICE Deployment	15
● Deployment using Windows Management Instrumentation (WMI)	16
● Deployment using PSEXec	16
● Deployment using startup script via GPO	16
Hosting Hints	17
● Hosting Comparison	17
TLS Certificates	19
● Managing certificates via GUI	19
● Replacing the certificate via CLI	20
Migration from CentOS	21
● OS Migration	21
● Why AlmaLinux?	21
● The Migration Script	21
● Performing the migration	21
<hr/>	
GUI	
Dashboard	23
● Device Health	23
● Quarantine	23
● Licenses	24
● Endpoint Version	25
● Running Scans	25
● Commands	26
● Virus Definition Files	26

Devices	26
● Device Status	26
● OK (green)	27
● Warning (yellow)	27
● Critical (red)	27
● Unknown (purple)	27
● Actions	27
License	28
Commands	28
● Error Codes	28
Bundling	29
Users	29
● Hierarchy Example	30
● Users	30
● Groups	31
● Example: Create a user for managing Customer X's PRIO ENDPOINT instances	31
Quarantine	33
Alerts	34
Profile	35
● General	35
● Profile name	35
● Description	35
● TUXGUARD PRO ENDPOINT	35
● Enable TUXGUARD PRO ENDPOINT	35

● ACTION OD Scan	35
● Action OA Scan	35
● Updates	36
● Telemetry	36
● Loglevel	36
● Show notifications	36
● DCM License URL	36
● Heartbeatstatus URL	37
● Heartbeatcommand URL	37
● Update server URL	37
● Disable certificate validation	37
● Archive Scan OD	37
● Archive Scan OA	37
● Maximum directory recursion	38
● Maximum archive size	38
● On Access Scan	38
● On Access Scan	38
● OA Scan of remote files	38
● OA Scan Timeout	38
● Scheduled Scan	38
● Scheduled scan interval	38
● Scan Type	38
● Day	38
● Time	38
● Proxy Settings	39
● Proxy Server	39
● User	39
● Password	39

●	Scan Settings	39
●	Heuristic	39
●	Scan Mailbox	39
●	Scan MIME	39
●	False Positive Control	39
●	Detect local phishing	39
●	SPR	40
●	PUA	40
●	PFS	40
●	Cloud Scan	40
●	Mode	40
●	Cloud Scan connection timeout	40
●	Cloud Scan timeout	40
●	Cloud Scan process in detail	41
Exceptions		41
●	File Exceptions	41
OA Extensions		42
●	OAExtensionList	42
Reporting		42
●	Live Views	43
●	CPU	43
●	CPU Frequency	43
●	Temperature	44
●	Load	44
●	System Status	45
●	Service Status	45
●	CPU	47

● CPU Statistics	47
● Disk Space	48
● Memory Usage	49
Logs	49

Device Security

Scans	50
● AV Scans	50
● On Access vs. On Demand Scans	50

System

Operating System	51
● DCM System	51
● Partitioning	51
● Data Partition	52
Settings	52
● Settings View	52
● Host	52
● Hostname (FQDN)	52
● Host IP Address	52
● Gateway IP Address	52
● Netmask	52
● GUI Port	53
● Additional IPs	53

● TUXGUARD Hosts	53
● Certificates	53
● DCM Settings	53
● DCM Management	53
● Command Storage Duration	53
● Heartbeat Exchange	53
● Number of Command Workers	53
● Number of Heartbeat Workers	54
● License Proxy	54
● Number of Proxy Workers	54
● Enable TLS	54
● SMTP Settings	54
● Alert Settings	54
Configurator	54
DCM Update	55
Modules	56
● TUXGUARD DCM Modules	56
● Manager	56
● Config	56
● Heartbeat API	58
● Config	58
● Heartbeat Exchange	58
● Config	58
● Alert Manager	59
● Config	59
● License Proxy	59
● Config	60

● License API	60
● Config	60
● Extern	61
● Redis	61
● RabbitMQ	61
● Postgres	61
● NginX	61
Useful commands	61
● Collection of useful terminal commands	61
● Change root password	61
● Restart DCM	61
● Restart DCM configuration tool	61
● Show unit status	61
● Restart a unit	62
● Live log view	62
● DCM Update	62
● Trigger DCM VDF Update	62
Ports/Firewall	62
● Firewall	62

FAQ

Frequently Asked Questions	64
● Difference between PC and Server Package	64
● DEVICE SECURITY version is out of date	64

Changelog

Changelog	65
-----------	----

● DCM 1.2.0	65
-------------	----

**TUXGUARD ICM Defense DEVICE
SECURITY**

Installation

TUXGUARD IDCM DEFENSE DEVICE SECURITY and DEVICE SECURITY CENTRAL MANAGER

Welcome to the manual of TUXGUARD DEVICE SECURITY and DEVICE SECURITY Central Manager.

TUXGUARD DEVICE SECURITY

TUXGUARD DEVICE SECURITY is a lightweight & fast realtime anti-virus scanner for Windows PC and Windows Server. Currently two versions are available:

- Basic: anti-virus scanner
- Advanced: anti-virus scanner and webfilter module

DEVICE SECURITY Central Manager (DCM)

The DCM is a free Alma Linux based system for managing TUXGUARD DEVICE SECURITY instances. You are free to install it inside the infrastructure of you customer or host it on your own as a service for your customers.

Quick Installation Guide

In order to make the DCM installation as easy as possible we rely on a predefined ISO image (<https://repo.tgfw.de/ECM/iso/stable/ecm-1.1.iso>), which contains an operating system and all necessary packages. You do not have to download Setups. This will do the DCM for you. In order to install the DCM the following steps need to be done:

1. Download and boot the ISO image
2. Boot the DCM system
3. Use DCM configurator
4. Connect to GUI

Ports

The following ports will need to be open for the host system:

- 443
- 8443

- 22 (optional for ssh connection)
- 873 (rsync, only outgoing) for DEVICE SECURITY updates

More information is available [here](#)

Download and boot the DCM ISO image

First of all the `ecm.iso` (<https://repo.tgfw.de/ECM/iso/stable/ecm-1.1.iso>) needs to be downloaded. The ISO file can then be either booted inside a virtual environment or on a bare metal server. In either of those settings several requirements need to be set. The minimal requirements are as following:

- 50 GB Hard Disk Space
- 2 Core (1.4GHz, 64 Bit, x86 Processor)
- 8 GB RAM
- 1 Gigabit Network Interface
- SecureBoot disabled

Note

In order to boot on a bare metal server the image needs to be burnt to a CD or be flashed to a USB drive.

Note

The DCM will install on hard drives with more storage, but will not utilize the available space right away. At the end of the configuration step a prompt will ask whether the partition should be resized to use the whole partition. For more information on the partition, see [System/Partitions](#)

The system supports Legacy BIOS and UEFI.

1. After a successful boot the TUXGUARD bootloader menu will show up, which can be confirmed with enter:



2. Following some security checks, the user will be prompted by a disclaimer which needs to be accepted twice:

```

Getting /dev/sda3 info...
Getting /dev/sda4 info...
*****
The following step is to restore an image to the hard disk/partition(s) on this machine: "/home/part
imag/ecm-img" -> "sda sda1 sda2 sda3 sda4"
The image was created at: 2021-0527-1240
WARNING!!! WARNING!!! WARNING!!!
WARNING. THE EXISTING DATA IN THIS HARDDISK/PARTITION(S) WILL BE OVERWRITTEN! ALL EXISTING DATA WILL
BE LOST:
*****
Machine: VirtualBox
sda (64.4GB_VBOX_HARDDISK__VBOX_HARDDISK_VB799d83de-ebdd3c4a)
sda1 (1.2G_ext4(In_VBOX_HARDDISK_)_VBOX_HARDDISK_VB799d83de-ebdd3c4a)
sda2 (43G_LVM2_member(In_VBOX_HARDDISK_)_VBOX_HARDDISK_VB799d83de-ebdd3c4a)
sda3 (1007K_BIOS(In_VBOX_HARDDISK_)_VBOX_HARDDISK_VB799d83de-ebdd3c4a)
sda4 (828.3M_vfat_0x41:_Dirty_(In_VBOX_HARDDISK_)_VBOX_HARDDISK_VB799d83de-ebdd3c4a)
*****
Are you sure you want to continue? (y/n) y
OK, let's do it!!
This program is not started by clonezilla server.
*****
Let me ask you again.
The following step is to restore an image to the hard disk/partition(s) on this machine: "/home/part
imag/ecm-img" -> "sda sda1 sda2 sda3 sda4"
The image was created at: 2021-0527-1240
WARNING!!! WARNING!!! WARNING!!!
WARNING. THE EXISTING DATA IN THIS HARDDISK/PARTITION(S) WILL BE OVERWRITTEN! ALL EXISTING DATA WILL
BE LOST:
*****
Machine: VirtualBox
sda (64.4GB_VBOX_HARDDISK__VBOX_HARDDISK_VB799d83de-ebdd3c4a)
sda1 (1.2G_ext4(In_VBOX_HARDDISK_)_VBOX_HARDDISK_VB799d83de-ebdd3c4a)
sda2 (43G_LVM2_member(In_VBOX_HARDDISK_)_VBOX_HARDDISK_VB799d83de-ebdd3c4a)
sda3 (1007K_BIOS(In_VBOX_HARDDISK_)_VBOX_HARDDISK_VB799d83de-ebdd3c4a)
sda4 (828.3M_vfat_0x41:_Dirty_(In_VBOX_HARDDISK_)_VBOX_HARDDISK_VB799d83de-ebdd3c4a)
*****
Are you sure you want to continue? (y/n)

```

Boot the DCM system

The system will reboot automatically and prompt the user with a login screen, for which the credentials are as following:

- Username: root
- Password: tuxguard

Note

After the first boot the user will be prompted to change the default password.

Use DCM configurator

After logging in, the user will be welcomed by the DCM configurator. Here we are able to set our network configuration and some general first configurations.

```
CentOS Linux 8
Kernel 4.18.0-240.el8.x86_64 on an x86_64

Activate the web console with: systemctl enable --now cockpit.socket

localhost login: root
Password:
Last login: Thu May 20 20:09:10 on tty1
TUXGUARD Endpoint Central Management
? Welcome to TUXGUARD ECM!
  ■ Initial Configuration
    Quit
```

See the configurator section for more information.

Connect to GUI

The last step is simply using the DCM. At the end of the configurator we will see the URL under which the GUI can be accessed. Following this URL we are greeted by the DCM Login Screen. Here we use the default super user:

- Username: sysadm
- Password: sysadm



Info

On first login the user will be prompted for a new password of the sysadm user.

First Steps

In order to deploy TUXGUARD DEVICE SECURITY following steps are need to be done:

1. Import a license
2. Download installation bundle

3. Install installation bundle on the local client

Import a license

1. On the *Administration - Licenses* Page click the Add License Button.
2. Fill in name, description and serial of the license you had purchased.
3. Your new license will be added to the License table. You can see the number of seats you've purchased, licensee name and the expiration date of the license.

Download the default bundle

1. In *Administration - Bundling* a new bundle will be created for your first license
2. Use the download icon to download the `default_bundle.zip`, which contains the TUXGUARD DEVICE SECURITY installer, the default profile and your first license.

Note

For any successive license you have to create the bundle manually, see [Bundle](#).

Installation

1. Unzip the bundle from the previous step.
2. Run `setup.exe` on the machine you would like to protect.
3. After several minutes, the TUXGUARD DEVICE SECURITY will register itself to the DCM.

Note

The parameters `/SILENT` and `/VERYSILENT` instruct the setup to be silent or very silent. When Setup is silent the wizard and the background window are not displayed but the installation progress window is. When a setup is very silent this installation progress window is not displayed. Everything else is normal so for example error messages during installation are displayed and the startup prompt is.

TUXGUARD DEVICE Deployment

There are multiple ways to deploy a previously created bundle. On this page you will find some useful hints.

In order to avoid the install wizard, use the parameters `/SILENT` or `/VERYSILENT`.

Deployment using Windows Management Instrumentation (WMI)

1. Create the Bundle you want to deploy
2. Extract the Bundle to a share, e.g. \\sharename\somename
\\TUXGUARD_PRO_ENDPOINT\ It will contain all installation files you need.
3. Ensure yourself that Windows Firewall does not block WMI traffic
4. Use following command to deploy the TUXGUARD_PRO_ENDPOINT

```
WMIC /node:[ip or name] /user:[username with admin privileges] /password:[user pw] process call create
"C:\[path to setup]\TUXGUARD-EPP-Setup.exe /VERYSILENT"
```

Deployment using PSEXec

PSEXec is a light-weight telnet-replacement that lets you execute processes on other systems, complete with full interactivity for console applications, without having to manually install client Software
see (<https://docs.microsoft.com/en-us/sysinternals/downloads/psexec>)

1. Create the Bundle you want to deploy
2. Extract the Bundle to a share, e.g. \\sharename\somename
\\TUXGUARD_PRO_ENDPOINT\ It will contain all installation files you need.
3. Download PSEXec (<https://download.sysinternals.com/files/PSTools.zip>)
4. Way A: Use following command to deploy the TUXGUARD_PRO_ENDPOINT

```
psexec \\[PCNAME],[PCNAME2] -u [domain\adminuser] -p [adminpassword] \\sharename\somename
\TUXGUARD_PRO_ENDPOINT\bundlename\TUXGUARD-EPP-Setup.exe /VERYSILENT
```

1. Way B: Create a txt file containing all computers you want to deploy e.g C:\computers.txt and use @ parameter to refer to the txt files

```
psexec -u [domain\adminuser] -p [adminpassword] @C:\computers.txt \\sharename\somename
\TUXGUARD_DEVICE_SECURITY\bundlename\TUXGUARD-EPP-Setup.exe /VERYSILENT
```

Deployment using startup script via GPO

The setup file is currently a setup.exe (not MSI), therefore you cannot distribute it via "Computer Configuration\Policies\Software Settings\Software Installation" policy.

Hence, using a startup script under "Computer Configuration\Policies\Windows Settings\Scripts\Startup" is another choice to deploy your software. However, the software should only install once and not each startup. The popular way to do it is

to check whether a specific installation file is available, which is then read on startup and if the file exists, then don't install. We are checking for AVRealtime.exe in the example script.

1. Create the Bundle you want to deploy
2. Extract the Bundle to a share, e.g. \sharename\somecoolname
 \tuxguard_device_security\ It will contain all installation files you need.
3. Edit following startup script and add it to the startup properties using the group policy management console.
4. TUXGUARD DEVICE SECURITY will be installed at the next startup phase
5. About 10 minutes after the installation the TUXGUARD DEVICE SECURITY instance will be registered with DCM

Your batch script should look like this, please edit the location of the share and insert the correct executable name:

```
@echo off
REM TUXGUARD DEPLOY SCRIPT
REM check software existance advanced
IF EXIST "%PROGRAMFILES(X86)%\TUXGUARD\TUXGUARD_DEVICE_SECURITY\AVRealtime.exe" GOTO end

REM check software existance basic
IF EXIST "%PROGRAMFILES(X86)%\TUXGUARD\TUXGUARD_DEVICE_SECURITY\AVRealtime.exe" GOTO end

REM run installer in VESYSILENT Mode, make sure all file are readable.
REM if you want to show installation progress, you can use /SILENT instead of /VERYSILENT

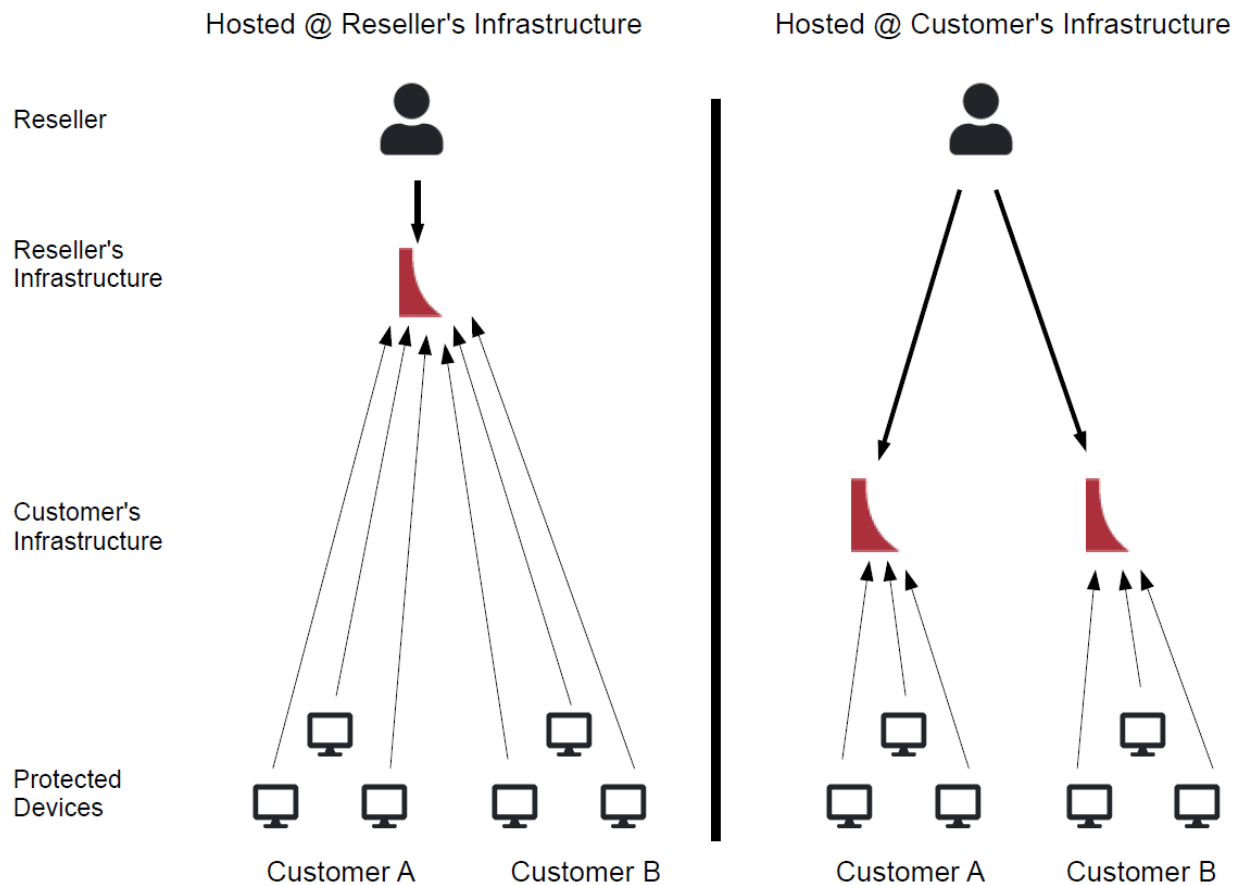
REM EDIT THIS LINE!
\\sharename\somecoolname\tuxguard_device_security\bundlename\tuxguard-epp-setup.exe /VERYSILENT

:end
```

Hosting Comparison

The DCM, as an on-premise solution for TUXGUARD DEVICE SECURITY management, allows you as a reseller to host it wherever you like. There are two main scenarios for hosting:

- DCM hosted inside the infrastructure of your customer (customer in-house)
- DCM hosted inside your infrastructure (outside of the customer's infrastructure)



Both scenarios have advantages and disadvantages, outlined in the following table.

Issue	Hosted inside Reseller's infrastructure	Hosted inside Customer's infrastructure
Device management of the customer	If the resellers allows, the customer is able to manage his own instances. This can be done via user & group settings. A full control over the DCM is not possible for the customer.	If the resellers allows, the customer is able to manage his own instances. This can be done via user & group settings. A full control over the DCM is possible for the customer if the admin account is handed over.
Device management of the reseller	Reseller can manage all instances via his own DCM.	Reseller can manage instances via accessing customer's DCM.
Location of usage data	Usage data is stored at Reseller's DCM.	Usage data is stored at Customer's DCM.

Issue	Hosted inside Reseller's infrastructure	Hosted inside Customer's infrastructure
DEVICE SECURITY Updates	Instances will update themselves from Reseller's DCM. This will not save external network traffic.	Instances can update themselves from Customer's DCM. This will can save external network traffic.
Management of multiple customers	The reseller can manage multiple customers with only one hosted DCM	The reseller cannot manage multiple customers with only one DCM. He has to access each DCM one by one.

TLS Certificates

During the installation process, a self-signed TLS certificate is being generated by DCM Server and placed in the following directory:

/home/ecm/tls

The relevant files are:

- DCM_certificate.pem (full certificate chain file)
- ecm_key.key (keyfile)

Managing certificates via GUI

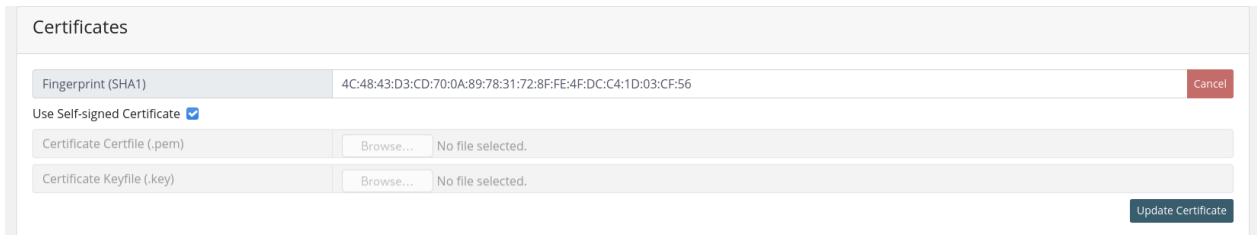
The certificate settings can be changed under 'System settings' --> 'Core' and by default are displaying the SHA1 fingerprint of the current certificate. The label on the left also indicates whether the autogenerated default self-signed certificate is currently used.

The screenshot shows a 'Certificates' section with a 'Fingerprint (SHA1)' field containing the value '4C:48:43:D3:CD:70:0A:89:78:31:72:8F:FE:4F:DC:C4:1D:03:CF:56'. To the right of the field is a 'Change Certificate' button.

An edit menu can be accessed by clicking on the 'Change certificate' button on the right where one can upload a certificate file and the matching key file.

The screenshot shows the 'Certificates' section with the 'Fingerprint (SHA1)' field and a 'Cancel' button. Below this is a 'Use Self-signed Certificate' checkbox. There are two rows for file selection: 'Certificate Certificate (.pem)' and 'Certificate Keyfile (.key)', each with a 'Browse...' button and the text 'No file selected.' At the bottom right is an 'Update Certificate' button.

The autogenerated certificate can be activated using the 'Use self-signed Certificate' checkbox.



After making the desired changes, click on the 'Update Certificate' button on the bottom right to start the certificate replacement process. In case both uploaded files have been successfully verified, a message will appear and the page will be reloaded after 10 seconds.

Replacing the certificate via CLI

Currently this is only possible by connecting to your DCM Server host via SSH i.e. uploading a certificate and the matching keyfile via SCP:

```
scp <path_to_your_certfile.pem> root@<your_ecm_server_host_ip>:/home/ecm/ecm_certificate.pem
scp <path_to_your_keyfile.pem> root@<your_ecm_server_host_ip>:/home/ecm/ecm_key.key
```

Note

Your certificate file must be in .pem format and contain the following in the specified order:

- end-user certificate
- ca certificate
- intermediate certificates

After replacing the certificates it is necessary to restart the ecm-manager and 'nginx' service on your ECM Server host:

```
systemctl restart ecm-manager
systemctl restart nginx
```

Note

If you are using a self-signed certificate, please make your sure you've disabled certificate validation in the profiles you are using. Otherwise the devices are not able to retrieve updates from your DCM.

OS Migration

Why AlmaLinux?

Since CentOS 8 is no longer supported since 01.01.2022, you will no longer be able to perform system updates on your DCM host.

The new base OS used by the DCM server is AlmaLinux 8 (<https://almalinux.org> (<https://almalinux.org>)) which is 100% binary compatible with CentOS 8 and will be supported until at least 2029.

The Migration Script

We provide a migration script (https://repo.tgfw.de/ECM/scripts/migrate_centos.sh) that automates the process of converting your host from CentOS 8 to AlmaLinux 8. The script performs the following steps:

1. Verify OS name and version
2. Delete CentOS related GPG keys and repositories
3. Delete CentOS specific packages
4. Download compatible AlmaLinux release package
5. Adjust Redis 6 package source
6. Perform a distro-sync (this can take a while, since old packages are being removed, upgraded and installed)
7. Cleanup operations (remove old boot-entries, fix Redis config file location)

Performing the migration

Important

We highly recommend that you backup or snapshot your host before running the migration to avoid any unforeseen loss of data!

1. Login to your ecm host via ssh
2. The configurator will appear, navigate to the Quit menuitem and press Enter
3. Run the migration script using

```
bash <(curl https://repo.tgfw.de/ECM/scripts/migrate_centos.sh)
```

4. A confirmation prompt should appear:

```
This script will migrate your CentOS Installation to AlmaLinux and reboot your system after completion.
=====
!!! Important !!!
By running this script you acknowledge that you have read and accepted the instructions and disclaimers
as stated in the manual (https://pro-ep-manual.tuxguard.com/installation/centos\_migration.html)
=====
Proceed with migration? [y/N]
```

Press y to confirm

5. Wait until the migration script terminates and a prompt appears asking your for a reboot

```
Migration successful.
Reboot now? [y/N]
```

6. Press y to confirm and wait for the system to reboot

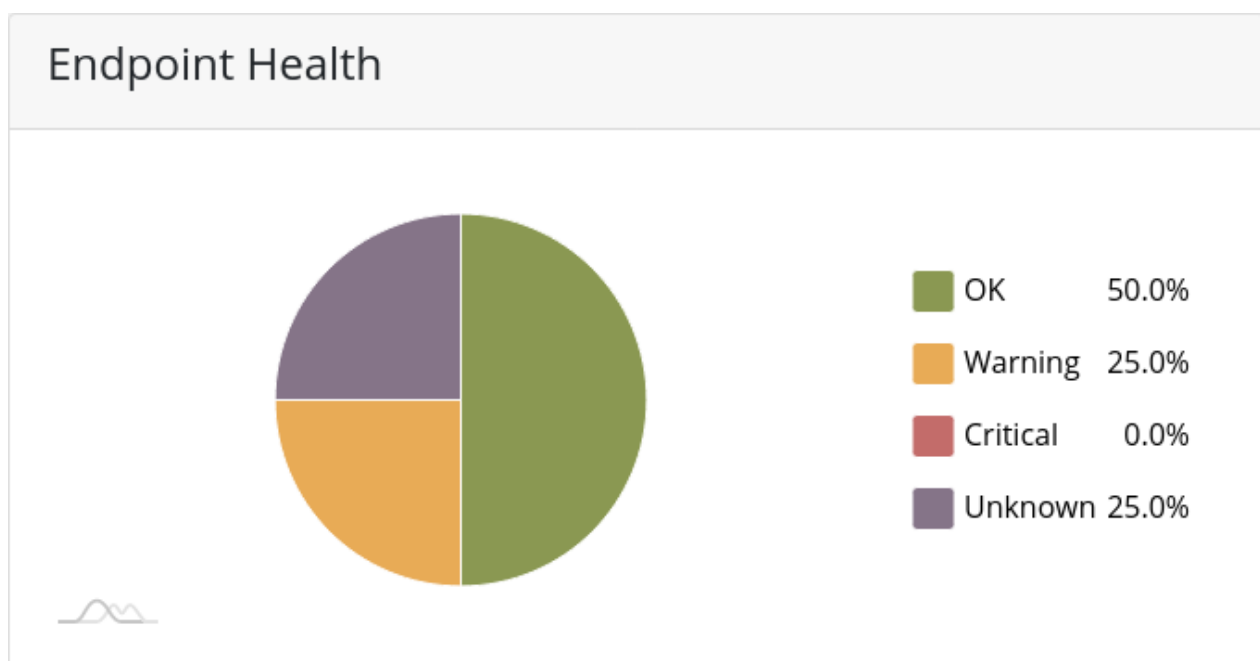
GUI

Dashboard

The dashboard is the landing page of the DCM user interface. It provides the user with all the necessary information about the server and its registered endpoints. It is conveniently structured in multiple tiles which convey the most useful information in one spot.

Device Health

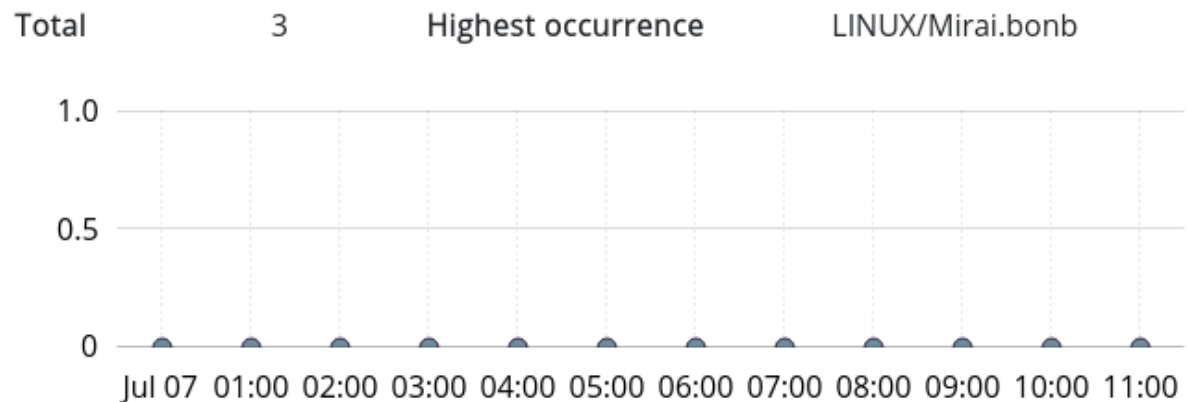
The Endpoint Health tile utilizes a pie chart in order to quickly present the user with the health status of all endpoints under his licenses. The pie chart is interactable, which means it will respond to mouse hover and click events.



Quarantine

The Quarantine tile presents the current status of all quarantine findings of the last 12 hours. It also shows the total number of files in quarantine and the highest occurring finding.

Quarantine



Licenses

The License tile provides quick information about the current status of all installed licenses. The most important information, the expiration date and the number of free seats are displayed in a table, with licenses about to expire highlighted in orange and licenses that have already expired highlighted in red.

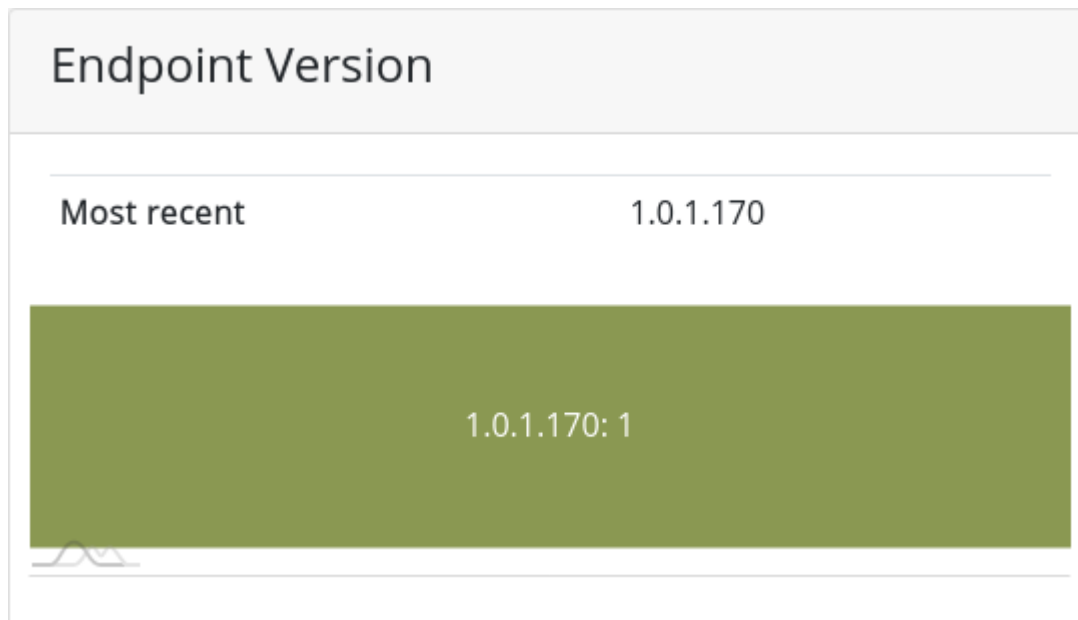
Licenses

Installed 4
Last added 16:08 - 29.04.2021

Licensee	Seats	Enddate
DONT_DELETE_ME	1/78	12.06.2021
DONT_DELETE_ME	0/123	16.02.2024
Jan_neue_lizenz	1/25	01.07.2021
DONT_DELETE_ME	2/150	22.04.2024

Endpoint Version

The Endpoint Version tile provides a quick overview over deployed PRO ENDPOINT versions.



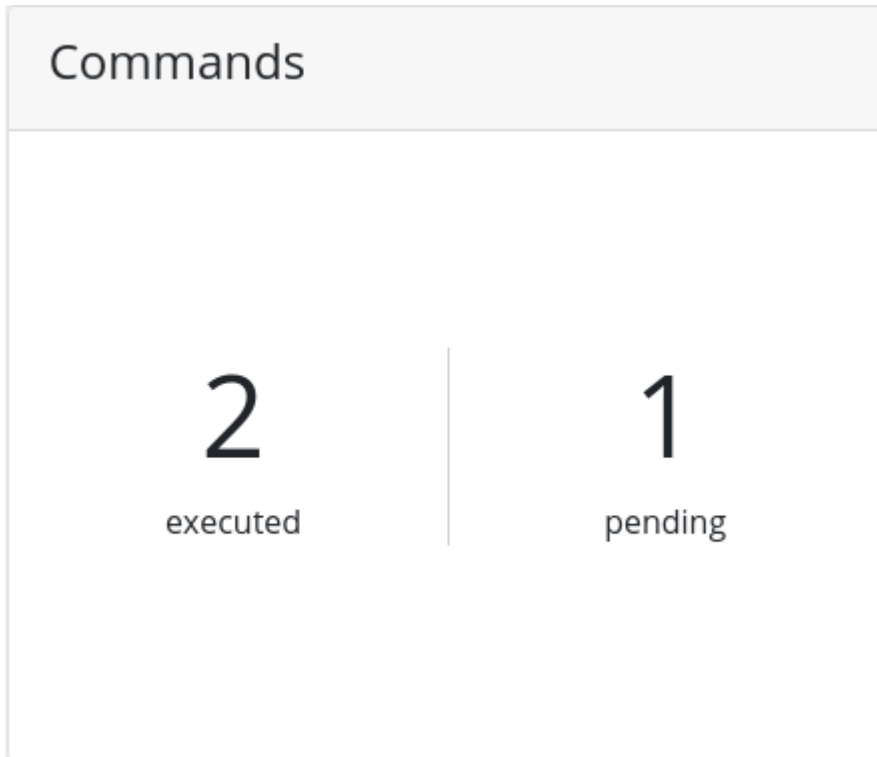
Running Scans

The Running Scans tile shows a accumulative view of all the running scans on all PRO ENDPOINT installations.

Running Scans	
Systemscan	0
Scan	0
Userscan	0
Customscan	0

Commands

The Commands tile represents the internal workflow between DCM and PRO ENDPOINT. Since the infrastructure works asynchronous it might be useful to know how much commands might be still in process by the PRO ENDPOINT instances.



Virus Definition Files

The tile represents the versions of the Virus Definition Files. Latest Remote version is the most recent version. Latest Local version shows the current version available on your DCM. the Deployed table shows the VDF versions of your devices.

Devices

The device table lists all endpoints which have established a successful connection to the DCM and their license has been added to the DCM.

Attention

Devices for which there is no license installed in the DCM will not be accepted and thus will not show up.

Device Status

A TUXGUARD DEVICE SECURITY instance has one of four possible states:

OK (green)

An instance is considered as OK, if:

- less than six file are quarantined
- less than three update attempts failed
- heartbeat information is newer than 4h

Warning (yellow)

An instance is in a warning state, if:

- more than five files are quarantined
- more than two updates attempts failed

Critical (red)

An instance is in a critical state, if:

- more than ten files are quarantined
- more than eight updates attempts failed
- antimalware or realtime (OA) scan is disabled

Unknown (purple)

An instance is considered as unknown if no heartbeat information was received by the DCM in the past 4 hours. Possible reasons are:

- instance is powered off
- instance is offline or cannot reach the DCM
- ConsoleAgent service is not running

Actions

Action	Description
Start Scan	Trigger a scan command on the selected instances
Stop Scan	Stop a scan
Replace Profile	Deploy a new profile to the selected instances
Update	Start a vdf and engine update on the selected instances
Replace License	Deploy a new license to the selected instances
Delete	Remove the selected instance from DCM

Attention

When triggering the Delete action:

Make sure you uninstall TUXGUARD DEVICE SECURITY properly or the instance will reconnect again!

License

All installed licenses are listed at this page. Licenses can be added via the Add License button. The table contains the following columns.

Column	Description
Name	Chosen by the user
Description	Chosen by the user
Serial	An individual serial specific to a single license
Licensee	The owner of the license
Seats	Shows the maximum allowed and currently used amount of installed endpoint instances using this license
Startdate	The expiration date of a license
Enddate	The starting date of a license

A click on a license reveals a detailed page.

Commands

The *Commands* view lists all triggered commands of the past 24h.

A successful command execution will return OK, an unsuccessful one will return an error code.

The execution of a command will happen asynchronous, i.e. a command will be answered as soon as an endpoint has fetched the command and send the corresponding answer.

Error Codes

Error	Description
ERR:PROTOCOL_MISMATCH	the command or parameter was invalid
ERR:SCAN_IN_PROGRESS	the command could not be executed because a scan is running.
ERR:NO_SCAN_RUNNING	the stop scan command failed because no scan was running

Error	Description
ERR:NOFILESFOUND	the command failed because the requested files did not exist anymore (e.g. restoring a quarantined file which was deleted manually)
ERR:CANT_SAVE_FILE	the profile deployment failed (e.g. invalid profile)

Bundling

The Bundling Page allows you to create installation bundles.

Please remember that a bundle always contains the latest version of the TUXGUARD DEVICE SECURITY setup at the time of bundle creation. If you want a newer setup version in your bundle, please create it again.

Click the *make bundle* button in order to create a zip archive containing:

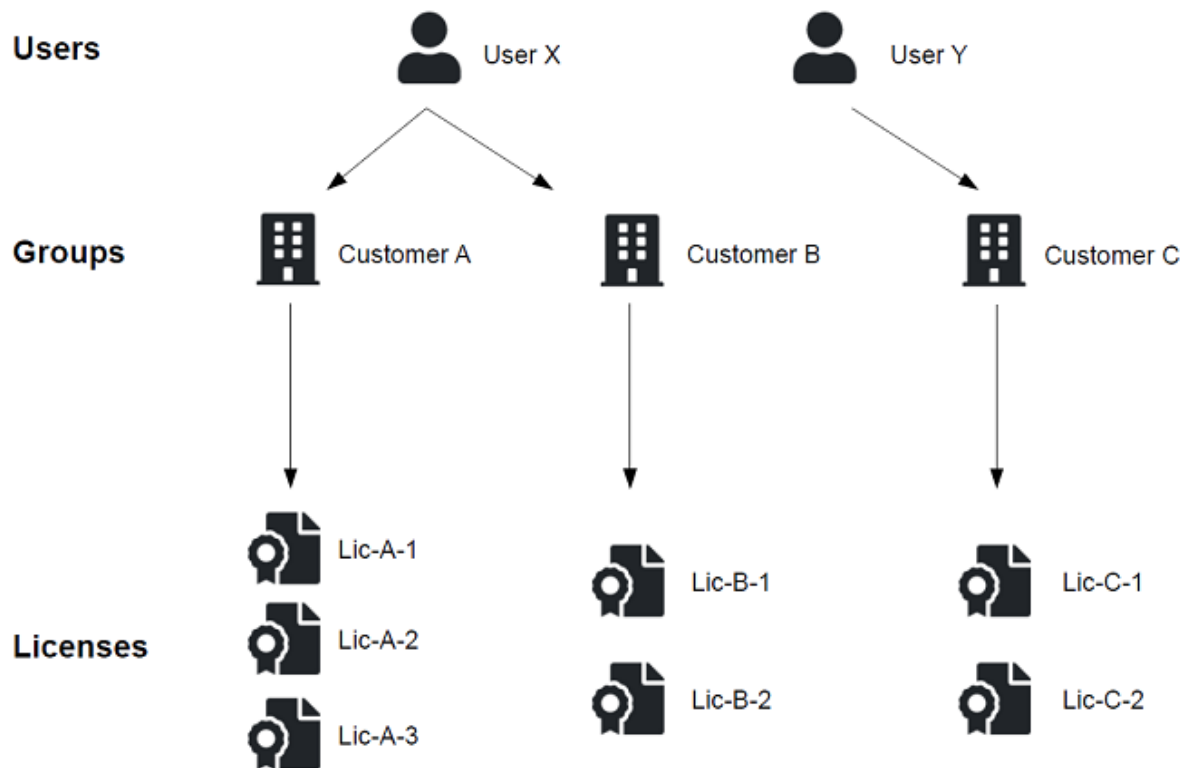
- the selected setup
- profile
- license

Users

This view allows the administrator to manage user accounts and groups in order to create a hierarchical administration structure.

Users can only manage DEVICE SECURITY instances based on their group membership.

Hierarchy Example



This image shows a hierarchical sample structure. This example contains:

- Two users (*User X* , *User Y*)
- Three Customer Groups (*Customer A*, *Customer B* and *Customer C*)
- Three Licenses of Customer A, two licenses of Customer B and C

In order to achieve this structure, the licenses of Customer A are allocated to the *Customer A* group, the licenses of Customer B to the *Customer B* group ...

User X is a member of the groups *Customer A* and *Customer B*. *User Y* is just a member of *Customer C*. As a result of these group memberships, *User X* is able to manage all DEVICE SECURITY instances which are using the licenses of *Customer A* and *Customer B*. *User Y* can manage all instances of *Customer C*.

Users

Comparison of user and admin

Feature	Admin	User
Dashboard	can see all stats	can see only stats of allocated EPs
Licenses	can manage all licenses	can manage only allocated licenses

Feature	Admin	User
Users	can manage users and groups	cannot manage this view
Profiles	can manage all profiles	can manage only own profiles
Quarantine	can manage all quarantined files	can manage only quarantined files of allocated EPs
Report	can access reporting view	cannot access the reporting view
System settings	can manage system settings	cannot manage system settings

Groups

The group features allows the creation of groups containing users and licenses (many-to-many relationship). A user can only manage TUXGUARD PRO ENDPOINT instances of the corresponding group.

In order to create a license group, please execute the following steps:

1. Navigate to Administration / users
2. Click the *Add Group* Button
3. Set name and group description
4. Add user to the license group
5. Add licenses to the group
6. Click the *Add Group* Button

Example: Create a user for managing Customer X's PRIO ENDPOINT instances

In order to create a user for specific customer please follow the steps.

1. Create a User e.g. named *admin_customer_x*

Add New User



Username

admin_customer_x



Password

12345678



E-Mail

mail@example.com



First Name

John



Last Name

Doe



Cancel

Add User

1. Create a Group e.g. named *customer_x*
2. Add a licenses of customer x to the group
3. Add user *customer_x* to the group

Add New Group

Groupname

Customer_X

Description

License Group for Customer X

Available Users

sysadm

Chosen Users

admin_customer_x

Available Licenses

Chosen Licenses

test

Cancel

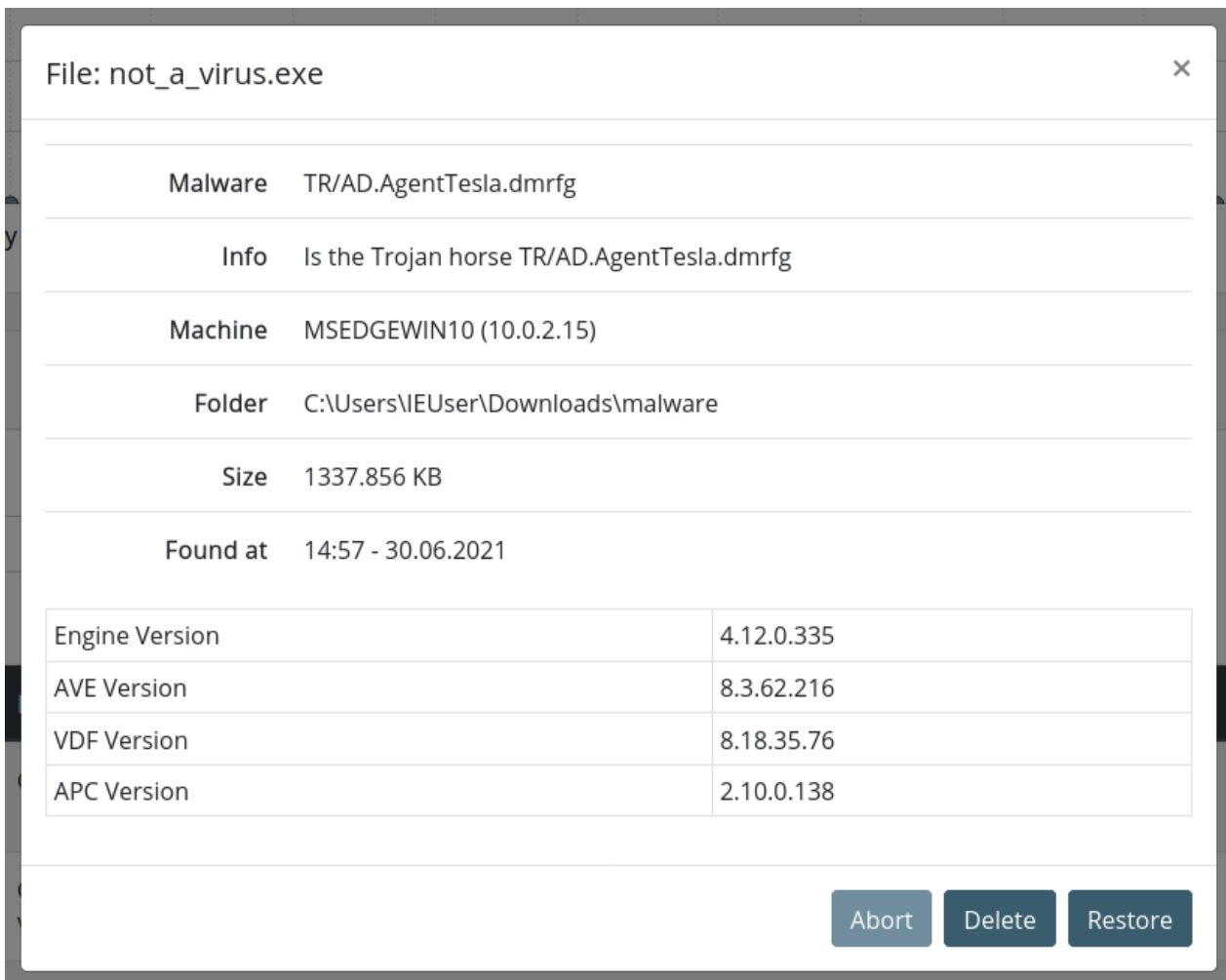
Add Group

1. Save the settings

Quarantine

The quarantine view shows all files currently in quarantine for all endpoints registered in the DCM and group settings. It also provides an overview of all findings in the last 2 months. These files can be filtered by the machines they were found in.

A click on a quarantine file provides some additional information and also the ability to delete or restore the quarantined file.



Alerts

The Alerts view shows active alerts for your DCM, licenses and devices. If you delete an alert but the issue is still active, the alert will be re-created.

Following alerts will be reported:

- critical device state
- warning device state
- expired licenses
- licenses which will expire soon
- outdated VDF version

Alerts

Delete

Search:

dw

q

Show

10

entries

<div><div></div><div>↓</div></div>	Detection Time	Type	Title	Serial	Message
<div><input type="checkbox"/></div>	12:08 - 13.06.2022	license	License Expired	2630348b-5bdd-4efe-a487-5a3df4797413	License testlic has expired
<div><input type="checkbox"/></div>	14:58 - 13.06.2022	system	VDF Version out of date		The VDF version is of your DCM is out of date: Latest8.19.100.196 ; Deployed: 8.19.17.196

Showing 1 to 2 of 2 entries

Previous

1

Next

Profile

General

Profile name

This is the name of the profile

Description

This is the description of the profile

TUXGUARD PRO ENDPOINT

Enable TUXGUARD PRO ENDPOINT

This option enables the Anti-Malware functionality

ACTION OD Scan

This option defines the automatic behavior when malware is detected via an On Demand Scan.

Action OA Scan

This option defines the automatic behavior when malware is detected via an On Access Scan (Real Time scan).

Updates

This option defines the update interval.

Telemetry

If turned on, TUXGUARD will receive several information of the client in order make the product more stable. Telemetry data will be send to MixPanel for further analytics.

Data will be send on specific events:

- update failed
- license expired
- engine crashed
- engine reload failures
- engine initialization

Data which will be send:

- event
- windows version
- product serial
- product version
- timestamp
- timezone
- random generated ID

Loglevel

This option defines which data will be logged. The last two option will generate a higher CPU usage of the product.

Show notifications

Notifies the user with a slideup on finished updates or scans, changed licenses etc.

DCM License URL

TUXGUARD PRO ENDPOINT will contact this url for licensing services. If the url is missing or incorrect, the DCM can not register the instance.

Heartbeatstatus URL

TUXGUARD PRO ENDPOINT will contact this url in order to deliver status information. If the url is missing or incorrect, no status information will be delivered to the DCM.

Heartbeatcommand URL

TUXGUARD PRO ENDPOINT will contact this url in order to receive commands. If the url is incorrect or missing, the client will not be able to execute commands.

Update server URL

URL of the update server for vdf and software updates. TUXGUARD's Download URL:

<https://update1.tuxguard.com>

Note

If updates should be downloaded from the DCM infrastructure, you must use signed certificates from a certificate authority. If you use a self-signed certificate please make sure you have disabled certificate validation.

Note

At the moment it's only possible to use one URL per setting (except update server url). If TUXGUARD PRO ENDPOINT instances should be able to reach the server whether they are in the internal network or not, you should create a domain pointing to the public IP. Additionally, you should create internal DNS entry pointing to the internal DCM IP.

Disable certificate validation

This option disables the certificate validation for update servers. Check this option if you use a self-signed certificate.

Archive Scan OD

This option defines whether archives should be scanned on an OD Scan

Archive Scan OA

This option defines whether archives should be scanned on an OA Scan

Maximum directory recursion

Defines the scanning depth of a directory

Maximum archive size

Defines the maximum allowed size in byte for any file within an archive, mailbox or mail.

On Access Scan

On Access Scan

Enables the OA Scan functionality. Information regarding the difference between ON Access Scanning and On Demand Scanning can be found in the Section PROENDPOINT / AV SCANS.

OA Scan of remote files

Enables OA Scanning on files accessed on a network location.

OA Scan Timeout

Sets the maximum number of seconds allowed to scan (OA) a file before aborting

Scheduled Scan

Scheduled scan interval

Sets the scheduled OD Scan interval

Scan Type

Sets the scan type of the scheduled scan

Day

day of the week when a scheduled scan should be performed

Time

time when the scan should be performed

Proxy Settings

Proxy Server

url of the proxy

User

user name of the connection

Password

Password of the proxy connection

Scan Settings

Heuristic

Defines the heuristic level of the engine.

- lazy heuristic: detection is the lowest possible mode. the detection is not very good but false positives will be low.
- normal heuristic: normal heuristic detection
- high heuristic: detection is the highest possible mode, but false positives will be higher.

Scan Mailbox

Activates detection and scanning of mailboxes.

Scan MIME

Activates detection and scanning of mails.

False Positive Control

Enables a new layer of security regarding false positive prevention.

Detect local phishing

Enables detection of local phishing pages.

SPR

Enables the detection of security and privacy risk programs as malware.

PUA

Enables the detection of potentially unwanted applications as malware.

PFS

Enables the detection of possible fraudulent software as malware.

Cloud Scan

Sends suspicious hashes and files to a cloud scanning services. internet connection is required. Only PE Files are uploaded to the service.

Mode

- off: disables cloud scan functionality
- only hash checks: only hashes are submitted to the service
- full: hash checks and some times PE Files are submitted to the service for further analysis.

Cloud Scan connection timeout

Defines the cloud scan connection timeout in seconds.

Must meet the condition:

```
apc connection timeout < apc scan time < scan timeout
```

Cloud Scan timeout

Defines the cloud scan timeout in seconds

Must meet the condition:

```
apc connection timeout < apc scan time < scan timeout
```

Cloud Scan process in detail

Process:

1. TUXGUARD PRO ENDPOINT scans a PE file, which is considered clean at the moment but has a high risk level.
2. The hash of the file is generated and sent to the cloud service
3. The hash is compared against known file hashes. There are two possible cases:
4. The hash belongs to a file that has been previously analyzed and was categorized as *"clean"* or *"malicious"*
5. The hash is unknown. The file will be uploaded and scanned
6. The result will be send to TUXGUARD PRO ENDPOINT. If it was classified as *malware*, the threat will be handled.

File Exceptions

Set files and directories to be excepted from scanning OnDemand and OnAccess. If set to empty string, then no objects will be excluded from scanning.

The list entries must be separated using a semicolon (;).

The maximum length of the string is 10.000 characters. It is recommended to keep this list short as it will be checked during each scan.

Note

Always use fully qualified file and directory names like in these examples:
c:\samples;c:\mydatabases\database.db;%USERPROFILE%\excludedfolder

Important

- wildcards like file*.db are not accepted, due to the high risk of misconfiguration and of high latency.
- single files like malware.exe will be ignored.
- it is acceptable to enter environment variables like %USERPROFILE%. The variables are expanded at startup.

- it is acceptable to enter shared folders \server\share

OAExtensionList

Set OnAccess scanner file extensions list. If set to empty string, all files are scanned.

Maximum extension length is 12 characters, the maximum number of extensions is 150 extensions.

The extensions specified here are only considered for files not being mapped for execution.

Any file mapped for execution, no matter its extension, will be scanned (PE files).

It is therefore possible that files having extensions others than those defined here will be scanned.

Wildcards are not accepted.

Use a semicolon as separator, present whitespaces are considered as being part of the extension.

Example

Example:.doc;.xls;.txt;.avi

Tuxguard_default

.exe;.com;.dll;.386;.htm;.html;.hta;.ani;.apk;.bas;.bat;.bin;.chm;.class;.cmd;.cpl;.cpx;.crt;.csh;.dll;.dlo;.
.job;.js;.lnk;.lsp;.mb;.mpp;.mpt;.ocx;.olb;.osd;.pcd;.pdf;.pif;.pkg;
.pl;.pot;.pps;.pptx;.ppt;.prg;.ps1;.psh;.pwz;.reg;.rpl;.rtf;.scr;
.script;.sys;.shtm;.shtml;.swf;.sys;.tsp;.ttf.vb;.vir;.vbs;.vxd;
.vxo;.xls;.xlsx;.xxx

Reporting

The reporting page provides useful information about the server status. It consists of multiple tiles which are explained more in following. All graphs respond to mouse over and/or click events.

Info

This view is only accessible to the DCM administrator.

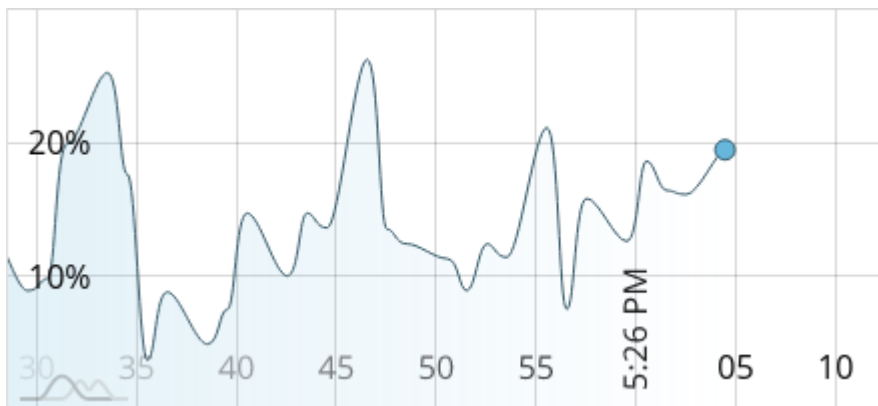
Note

The DCM server might not be able to reflect the true server status when running in a virtual environment.

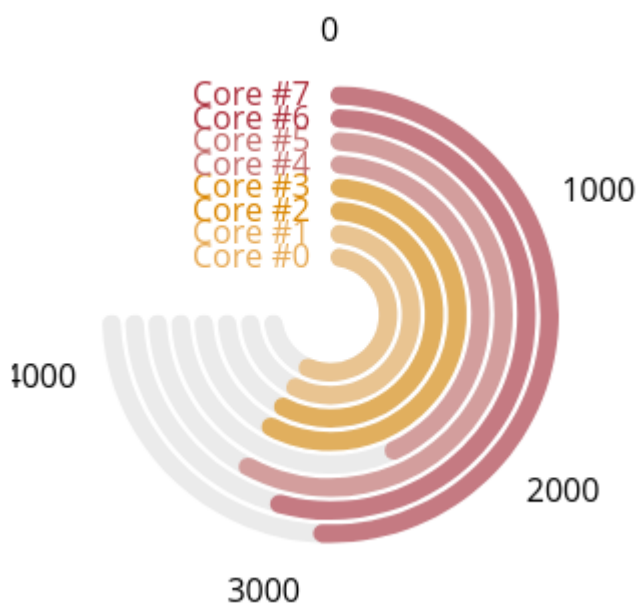
Live Views

The live views are useful to analyze the current behavior of the server.

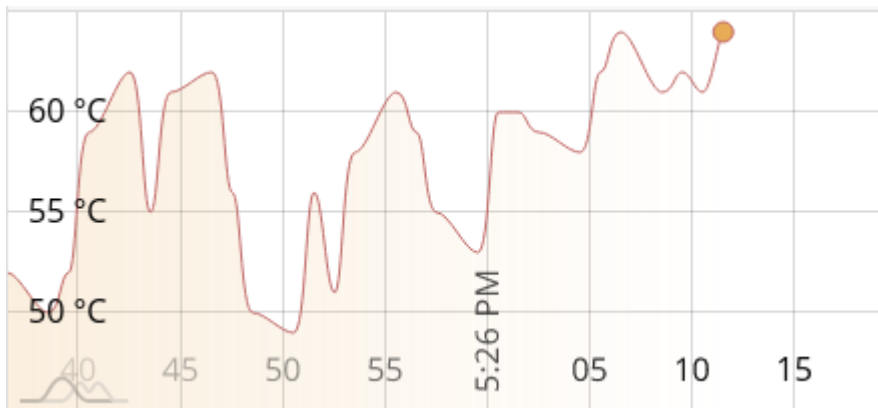
CPU



CPU Frequency



Temperature

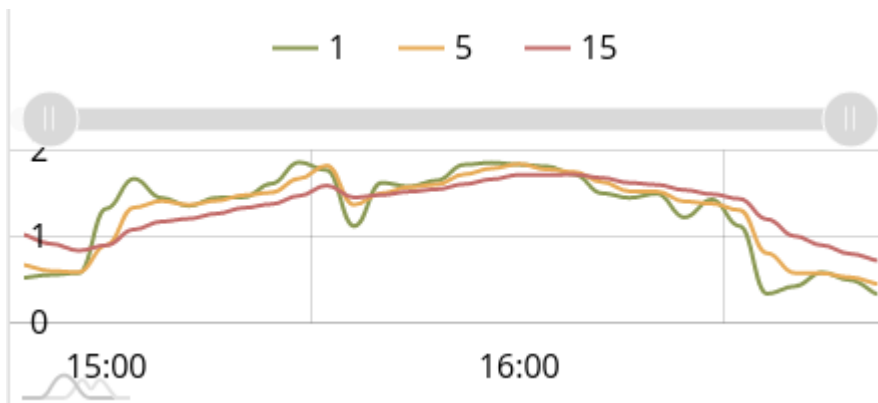


Note

The live graph for the temperature is only available for non-vm installations. This is due to the lack of sensor virtualization in virtual environments.

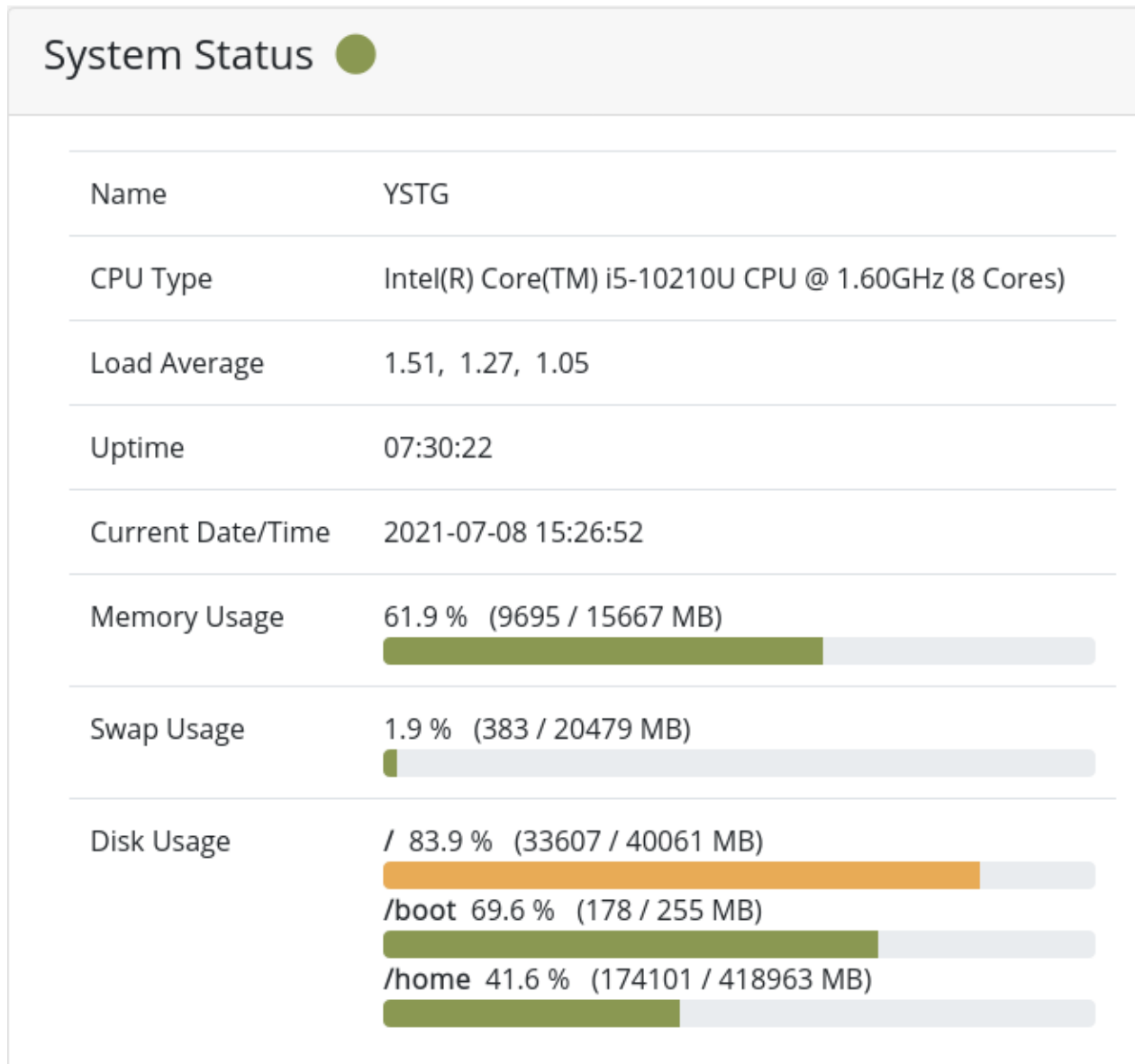
Load

The load tile gives a graphical representation for the different load averages over time, where as the numbers represent the average over this time in minutes, e.g. the orange line represents the load average over five minutes.



System Status

The system status tile aggregates some general information about the server. For an example see the figure below.



Service Status

The service status shows all the necessary services for the DCM. If something might not be working this should be the first stop for the administrator. The logs section gives more details on how to retrieve more informations about the services.

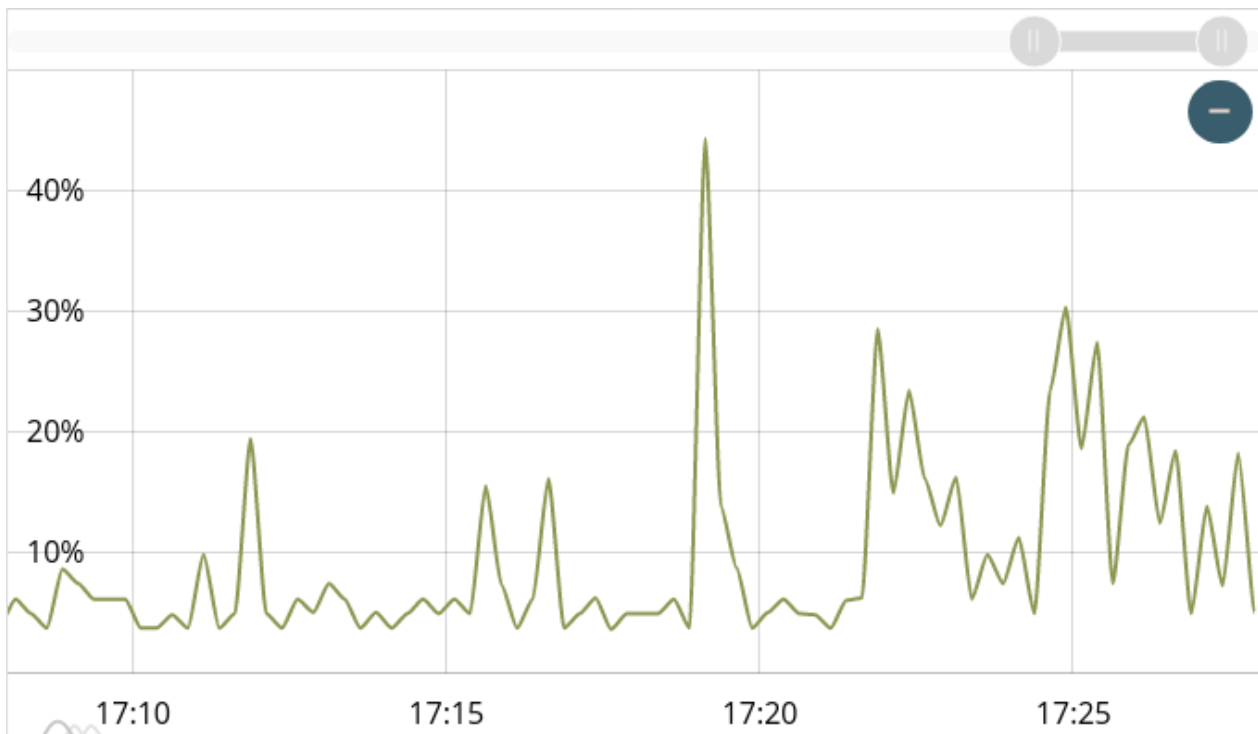
Services Status



chronyd	active/running
nginx	active/running
rabbitmq-server	active/running
postgresql	active/running
redis	active/running
firewalld	active/running
ecm-hb-api	active/running
ecm-hb-exchange	active/running
ecm-lic-api	active/running
ecm-lic-proxy	active/running
ecm-celery	active/running


CPU

The CPU graph provides a longer timeline for the CPU utilization. A scrollbar at the top can be used to extend the displayed history.



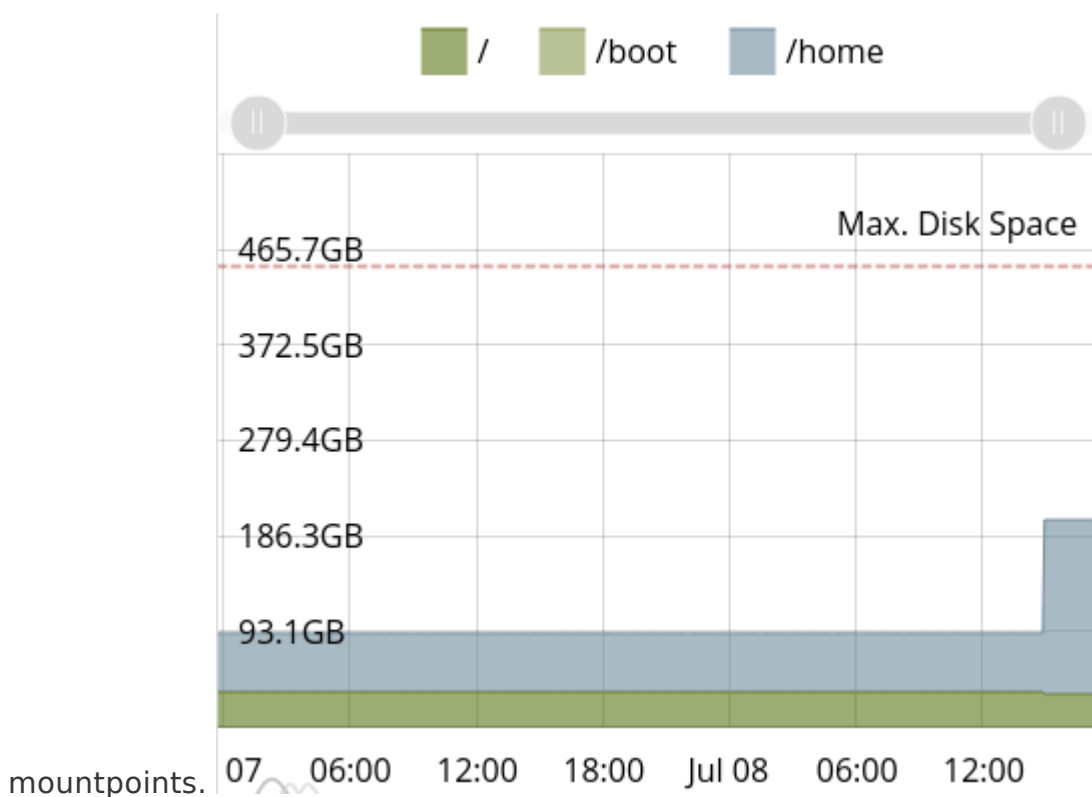
CPU Statistics

The CPU Statistics table collects various information about the runtime variables of the CPU.

CPU avg.	12.05%
Highest Measured Utilization	44.40%
Avg. temperature	55.28 °C
Up time	3, 7:31:31
Physical Cores	4
Capacity	4.20 GHz
Hyperthreading	

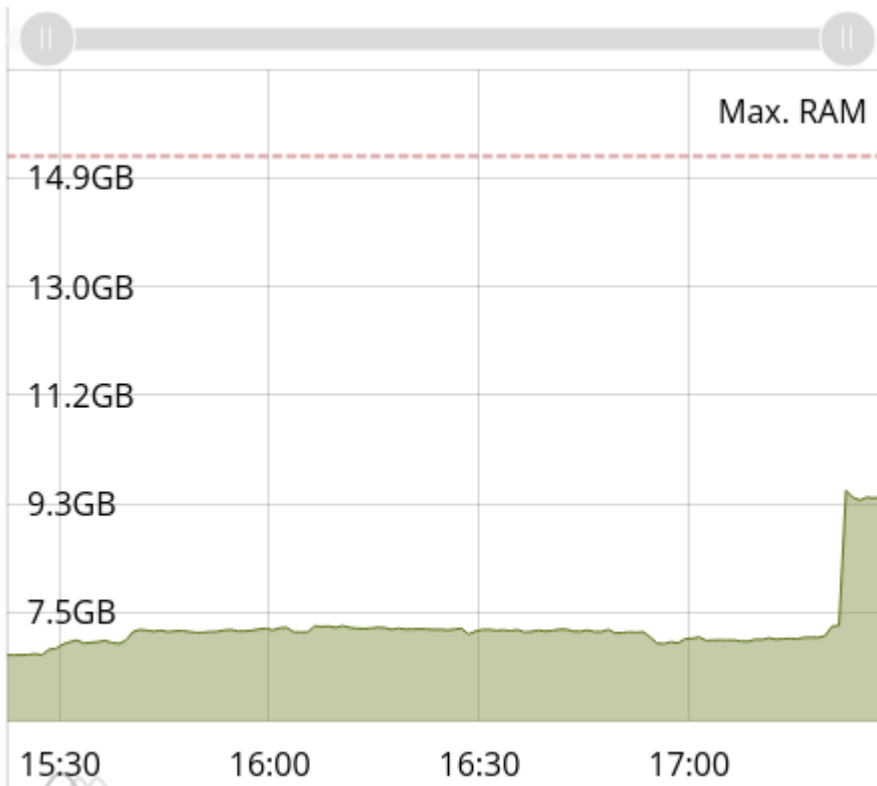
Disk Space

Here we see the disk space and the usage in the varying partitions and



Memory Usage

The Memory Usage tiles offers some insights into the temporal course of the RAM.



Logs

On this view you are able to generate an archive containing DCM logs. Click the *generate logs* button in order to collect and zip log data. If the collection of the logs was successful, a download link will appear.

If you want to collect them by yourself or get a live listing, you can find hints at the *useful commands* chapter. All log files can be found at:

/home/ecm/log

Info

This view is only accessible to the DCM administrator.

Device Security

AV Scans

On Access vs. On Demand Scans

On Demand scans are triggered by the DCM user, via tray menu or profile settings.

- Normal Scan: Scans the boot drive e.g. C:\
- Full Scan: Scans all drives
- User Scan: Scans the user folder of the currently logged in user.
- Quick Scan: Very fast scan which checks the origin of currently running processes.
- Custom Scan: scans a selected folder recursively. This scan can be triggered only on the local machine by tray menu.

On Access Scan is a functionality which will be triggered automatically if a file is accessed by the operating system or user processes (reading from, writing to, or execution). Files with defined extensions in *OA Scan Extensions* and PE files will be scanned.

System

DCM System

Since version 1.1 we migrated the base system from CentOS 8 to AlmaLinux 8. AlmaLinux builds upon CentOS and stays supported until at least 2029. All modules and their dependencies are currently installed on a AlmaLinux 8 minimal system, see <https://www.almalinux.org/> (<https://www.almalinux.org/>). Information on all our modules and their dependencies can be found in the modules section.

Important

CentOS 8 has been discontinued as of 01.01.2022!

For current installations that are still based on CentOS 8 we recommend performing a migration to ensure that system and security updates remain available.

Partitioning

During installation, the hard drive will be partitioned into a system partition and a data partition. The whole partition table looks as following, before running the configurator.

Name	Mountpoint	Size	Description
BIOS boot partition		1031kB	Used to boot on Legacy BIOS systems
EFI-system	/boot/efi	869MB	Used to boot on UEFI systems
Boot Partition	/boot/	1.2GB	Contains bootloader for BIOS systems
cl-root (LVM)	/	19GB	System partition, it contains all modules and their dependencies
cl-swap (LVM)	[SWAP]	4GB	Used by the operating system when the RAM might come to its limits
cl-home (LVM)	/home	20GB*	Data partition, contains all logs, configs, etc.

Note

* After running the initial configurator the setup asks whether the system should resize its partitions to use the whole disk space. In this case the free available space will be used to extend the data partition under /home.

Data Partition

Separating the data from the system files and modules has several advantages. It allows the user to create backups of their data themselves and enables Tuxguard to easily install any system critical updates without touching the user data. The data resides inside the /home/ecm folder:

Folder	Description
log	All DCM related log files
envs	All DCM related config files
config	All System related config files. (Redis, Postgres, RabbitMQ, nginx)

Settings View

This view allows changing various system settings and will update the related .env files upon saving by using the related "Apply Changes" button of a section.

Host

Host		Apply Changes
Hostname (FQDN)	ecm-dev.local	
Host IP Address	172.40.2.250	
Gateway IP Address	172.40.2.1	
Netmask	255.255.255.0	
GUI Port	8443	
Additional IPs		
TUXGUARD Hosts	https://tslv.tuxguard.com	

Hostname (FQDN)

Specifies the hostname of the DCM's host-machine, needs to be set to a valid FQDN.

Host IP Address

The IP address of the DCM's host-machine.

Gateway IP Address

The Gateway IP of the subnet of the DCM's host-machine.

Netmask

Netmask specifying the subnet of the DCM's host-machine

GUI Port

Port over which the DCM webinterface is reachable, default is 8443.

Additional IPs

Comma-separated list of additional IPs or DNS-names the DCM webinterface should be reachable from.

For example: if proxying from another IP to the Host IP Address, that IP needs to be added here.

TUXGUARD Hosts

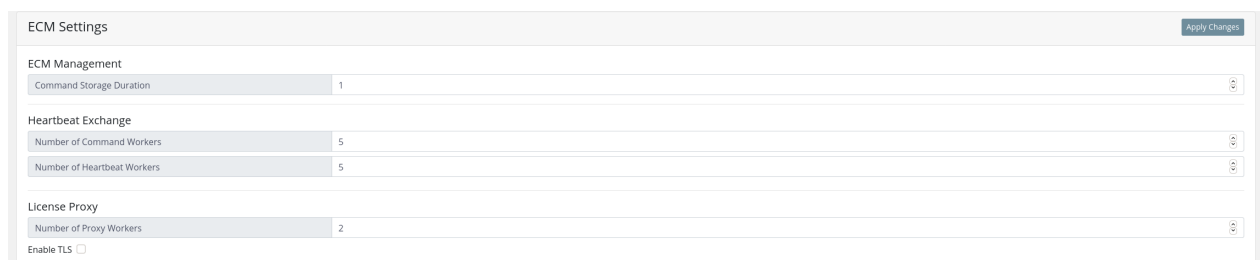
Comma-separated list of TUXGUARD License Worker hosts.

This should usually be set to its current default value (<https://tlsv.tuxguard.com>).

Certificates

see: TLS Certificates

DCM Settings



ECM Settings	
ECM Management	
Command Storage Duration	1
Heartbeat Exchange	
Number of Command Workers	5
Number of Heartbeat Workers	5
License Proxy	
Number of Proxy Workers	2
Enable TLS	<input type="checkbox"/>

This section handles various settings related to services running on the DCM host.

DCM Management

Command Storage Duration

Specifies number of days a EPP command should be queued.

Heartbeat Exchange

Number of Command Workers

Specifies the number of worker processes handling queued EPP Commands.

Number of Heartbeat Workers

Specifies the number of worker processes handling queued EPP Heartbeats.

License Proxy

Number of Proxy Workers

Specifies the number of worker processes for the License Proxy.

Recommended: 1 per core

Enable TLS

Allows toggling usage of TLS for the connection to a TUXGUARD License Worker host.

SMTP Settings

Specifies the SMTP settings for sending alerts via mail.

Alert Settings

Specifies the alert settings. Intervals are used to re-create an alert after the specified value. Multiple recipients are separated via comma. E.g. recipient1@mail.com,recipient2@mail.com

Configurator

The DCM configurator is a command line tool which helps in initializing the DCM. The configurator is controlled via the arrow keys. Currently it provides two submenus:

- Initial configuration

This menu provides an easy setup guide for the administrator to quickly get the DCM up and running. An example configuration can be seen in the following picture.


```

tuxguard-ecm-manager-1.0.0-1.el8.x86_64
Fertig.
[root@localhost yum.repos.d]# ecm-config
TUXGUARD Endpoint Central Management
? Welcome to TUXGUARD ECM!
? Select Network Device (default: enp0s3):  enp0s8
--- TUXGUARD ECM Initialization ---
Setup host settings
? FQDN:  localhost.localdomain
? Host IP Address:  192.168.56.10
? Gateway IP Address  192.168.56.1
? Use default Netmask: 255.255.255.0?  Yes
? Use default GUI Port (8443)?  Yes
? Use Gateway as DNS?  Yes
? TUXGUARD License Server URLs (comma-separated)  https://tslv.tuxguard.com
? Do you want to save this configuration?  Yes
Update .env files
Updating /opt/manager/.env.....
Updating /opt/lic-api/.env.....
Updating /opt/hb-api/.env.....
Updating /opt/hb-exchange/.env.....
Updating /opt/lic-proxy/.env.....
Updating /opt/alert-manager/.env.....
Update nginx config
Update /etc/nginx/conf.d/ecm-manager.default.conf...
Update /etc/nginx/conf.d/ecm-api.default.conf...
Applying IP Address and Gateway Changes
IP and Gateway set, restarting networking...
Syncing /etc/ecm/ecm.config to database...
Syncing host settings...
Syncing ecm-manager settings...
Syncing lic-proxy settings...
Syncing hb-exchange settings...
Restarting services
Checking internet connection...
? Check and apply updates now?  (Y/n)

```

After providing the network configuration, the configurator tries to update the server, pull the latest updates for PRO ENDPOINT and resize the partition to use the full partition size.

Important

Since the current ISO is still based on CentOS 8, updates will fail due to the distribution no longer being supported. Please perform a migration to AlmaLinux after running the configurator and update afterwards.

- Tools
 - *Change Password*
Use this to change the root password.
 - *Update System*
This menu entry updates the entire system.
 - *Shutdown*
Shutdown immediately.
 - *Restart*
Restart immediately.

DCM Update

Note

Before updating your DCM, please make a snapshot / backup at first!

Execute following command:

```
ecm-config
```

This will start the DCM configuration tool. Navigate to "Tools" and select "Update System".

Please restart your DCM after a successful update.

Modules

The DCM System consists of several subcomponents, which are explained in more detail further on. Every component runs as a separate systemd service with an own config file and a separate logging file. All of these modules are configured either via the webinterface or the configurator and usually do not need any inference. All TUXGUARD DCM configuration files are located under the `envs` folder. The remaining external configuration files are located under the `config` folder.

TUXGUARD DCM Modules

Manager

The Manager module is the core component of the DCM system and is responsible for building the bridge between database, Management API and GUI.

Config

`manager.env`

Option	Type	Description
DEBUG	Boolean	logs additional debug information when enabled
DATABASE_URL	String	contains all information about the database, is in the form: <code>postgres://ecm:tuxguard@localhost:5432/manager_db</code> .
SECRET_KEY	String	differs for all installations and provides an additional security layer

Option	Type	Description
ALLOWED_HOSTS	List [String]	a list of host URLs and/or IPs under which the Manager API and GUI will be accessible
LOGDIR	String	directory, in which logs will be saved
STATIC_ROOT	String	directory, in which static files will be stored
REDIS_HOST	String	Redis host
REDIS_PORT	String	Redis port
REDIS_USER	String	Redis username
REDIS_PASS	String	Redis password
RABBIT_VHOST	String	RabbitMQ virtual host
RABBIT_PORT	String	RabbitMQ port
RABBIT_USER	String	RabbitMQ username
RABBIT_PASS	String	RabbitMQ password
TG_LIC_WORKER	String	TUXGUARD WORKER which communicates with the DCM
SSL	Boolean	whether the connection to the TUXGUARD WORKER should use ssl or not
COMMAND_STORAGE_DURATION	Integer	how long commands should be stored inside the database, in days
COMMAND_CLEANUP_TRIGGER	String	in crontab notation, at which time the commands should be cleaned up
DOWNLOAD_FOLDER	String	folder serving the downloadable files
updatebasedir	String	under which folder endpoint update files will be served
bundlebasedir	String	under which folder endpoint bundles will be served
logsrclist	List [String]	additional log files which are considered for download

Heartbeat API

The Heartbeat API is the communication endpoint for all endpoints. Here commands, their responses and some general informations about an endpoint's health are exchanged.

Config

hb-api.env

Option	Type	Description
DEBUG	Boolean	logs additional debug information when enabled
LOGFILE	String	the logfile
SECRET_KEY	String	differs for all installations and provides an additional security layer
RABBIT_VHOST	String	RabbitMQ virtual host
RABBIT_PORT	String	RabbitMQ port
RABBIT_USER	String	RabbitMQ username
RABBIT_PASS	String	RabbitMQ password

Heartbeat Exchange

The Heartbeat Exchange is master-worker architecture which handles the messaging workload inside the DCM.

Config

hb-exchange.env

Option	Type	Description
DEBUG	Boolean	logs additional debug information when enabled
LOGFILE	String	the logfile
SECRET_KEY	String	differs for all DCM installation and provides an additional security layer
RABBIT_VHOST	String	RabbitMQ virtual host
RABBIT_PORT	String	RabbitMQ port
RABBIT_USER	String	RabbitMQ username
RABBIT_PASS	String	RabbitMQ password
POSTGRES_HOST	String	PostgreSQL host

Option	Type	Description
POSTGRES_PORT	String	PostgreSQL port
POSTGRES_USER	String	PostgreSQL username
POSTGRES_PASS	String	PostgreSQL password
COMMAND_WORKERS	Integer	amount of workers responsible for command messages
HEARTBEAT_WORKERS	Integer	amount of workers responsible for heartbeat messages

Alert Manager

The Alert Manager gathers information on the server status and might detect any faults for which then alerts might be created and be pushed to the manager.

Config

`alert-manager.env`

Option	Type	Description
DEBUG	Boolean	logs additional debug information when enabled
LOGFILE	String	the logfile
LOG_INTERVAL	String	the logfile
LOG_DIR	String	log directory containing all other logs
POSTGRES_HOST	String	PostgreSQL host
POSTGRES_PORT	String	PostgreSQL port
POSTGRES_USER	String	PostgreSQL username
POSTGRES_PASS	String	PostgreSQL password
REDIS_HOST	String	Redis host
REDIS_PORT	String	Redis port
REDIS_USER	String	Redis username
REDIS_PASS	String	Redis password

License Proxy

The License Proxy transfers any incoming license related request to the Tuxguard license server. The response is then pushed forward to the manager service, which will act accordingly.

Config`lic-proxy.env`

Option	Type	Description
DEBUG	Boolean	logs additional debug information when enabled
LOGFILE	String	the logfile
RABBIT_VHOST	String	RabbitMQ virtual host
RABBIT_PORT	String	RabbitMQ port
RABBIT_USER	String	RabbitMQ username
RABBIT_PASS	String	RabbitMQ password
NUM_WORKERS	Integer	amount of worker subprocesses
SSL	Boolean	whether the connection to the TUXGUARD WORKER should use ssl or not
TG_LIC_WORKER	String	TUXGUARD WORKER which communicates with the DCM

License API

The License API is the second entrypoint for all endpoints. This API deals with all license related requests.

Config`lic-api.env`

Option	Type	Description
DEBUG	Boolean	logs additional debug information when enabled
LOGFILE	String	the logfile
SECRET_KEY	String	differs for all installations and provides an additional security layer
RMQ_HOST	String	RabbitMQ host
RMQ_VHOST	String	RabbitMQ virtual host
RMQ_PORT	String	RabbitMQ port
RMQ_USER	String	RabbitMQ username
RMQ_PASS	String	RabbitMQ password

Extern

Redis

Redis is a cache based database, see <https://redis.io/> (*https://redis.io/*).

RabbitMQ

RabbitMQ is a queueing message broker, see <https://www.rabbitmq.com/> (*https://www.rabbitmq.com/*).

Postgres

Postgres is an open source, object-relational database, see <https://www.postgresql.org/> (*https://www.postgresql.org/*)

NginX

NginX is a web server, which can be utilized as load balancer, see <https://www.nginx.com/> (*https://www.nginx.com/*)

Collection of useful terminal commands

Change root password

```
passwd root
```

Restart DCM

```
shutdown -r now
```

Restart DCM configuration tool

```
ecm-config
```

Show unit status

```
systemctl status
```

Restart a unit

```
# Example: alert-manager-service
systemctl restart ecm-alert-manager.service
```

Live log view

```
# Example: Live view of ecm-manager.log
cd /home/ecm/log
tail -f ecm-manager.log
```

DCM Update

Note

Before you want to update your DCM, please make a snapshot / backup at first! *dnf --help* will list parameters.

```
# Really do a backup first!
dnf upgrade
```

Trigger DCM VDF Update

This will update your PRO ENDPOINT Setups and VDF files. If this update fails, please verify that an outgoing connection through port 873 is allowed.

```
cd /etc/ecm
su ecm
./datasync.sh
su
```

Firewall

Most of the communication with the DCM Server is handled via HTTPS using the following ports:

- 443 (used for communication between secured devices and DCM Server)
- 8443 (default port used to serve the GUI)
- 873 (outgoing) for updates

The GUI port can be configured using both the Configurator or the Settings page on the GUI itself.

Note

The port 443 is mandatory for communications with devices and cannot be changed. The same applies to port 873 (outgoing).

Optionally, port 22 should be opened for the host if ssh access to the host is desired.

FAQ

Frequently Asked Questions

Difference between PC and Server Package

PC	Server
6 scan threads	10 scan threads
AVSystray starts automatically	AVSystray does not start automatically
Webfilter module can be used	Webfilter module is not integrated
Windows Defender will be deactivated	Windows Defender will be set to passive mode

DEVICE SECURITY version is out of date

If the DEVICE SECURITY Setups or the VDFs files are out of date, please check whether an outgoing connection through port 873 (rsync) is allowed. You can verify this by triggering a DEVICE SECURITY and VDF files update .

Changelog

Changelog

DCM 1.2.0

- ECM was renamed to DCM
- Alert view added
- Added alert mail notification
- license name and description can be renamed now
- VDF Tile was added to the Dashboard
- multiple bug fixes
- multiple usability fixes