

---

# **ASGARD Management Center v3 Manual**

**Nextron Systems**

**Apr 10, 2024**



# CONTENTS

<b>1</b>	<b>Requirements</b>	<b>3</b>
1.1	Introduction . . . . .	3
1.2	Before You Begin . . . . .	3
1.3	Hardware Requirements . . . . .	4
1.4	Agent Requirements . . . . .	4
1.5	Network Requirements . . . . .	5
1.6	Antivirus and EDR Exclusions . . . . .	9
1.7	Verify the Downloaded ISO (Optional) . . . . .	11
<b>2</b>	<b>Setup Guide</b>	<b>15</b>
2.1	Create a new ESX VM and Mount the ISO . . . . .	15
2.2	Navigate through the installer . . . . .	15
2.3	Network Configuration . . . . .	20
2.4	Choosing a password . . . . .	22
2.5	Partitioning the Hard Disk . . . . .	22
2.6	Proxy Configuration . . . . .	24
2.7	Changing the IP-Address . . . . .	24
2.8	Install the ASGARD Management Center Service . . . . .	25
<b>3</b>	<b>Administration</b>	<b>31</b>
3.1	System Status . . . . .	31
3.2	ASGARD Agent Deployment . . . . .	34
3.3	Uninstall ASGARD Agents . . . . .	40
3.4	Asset Management . . . . .	41
3.5	Scan Control . . . . .	48
3.6	Scan a Single System . . . . .	53
3.7	Scan a Group of Systems . . . . .	54
3.8	Scheduled Group Scan . . . . .	59
3.9	Syslog Forwarding . . . . .	59
3.10	Response Control . . . . .	61
3.11	Service Control . . . . .	69
3.12	Aurora . . . . .	70
3.13	Sigma . . . . .	76
3.14	IOC Management . . . . .	85
3.15	Evidence Collection . . . . .	94
3.16	Download Links . . . . .	95
3.17	Licensing . . . . .	97
3.18	Updates . . . . .	99
3.19	User Management . . . . .	102
3.20	Additional Settings . . . . .	106

3.21	Advanced Settings . . . . .	117
3.22	User Settings . . . . .	119
<b>4</b>	<b>Master ASGARD</b>	<b>123</b>
4.1	Installation . . . . .	123
4.2	Hardware Requirements for Master ASGARD . . . . .	123
4.3	License Management . . . . .	124
4.4	Setting up Master ASGARD . . . . .	124
4.5	Link ASGARD Systems with Master ASGARD . . . . .	124
4.6	Scan Control . . . . .	125
4.7	Asset Management . . . . .	125
4.8	IOC Management . . . . .	127
4.9	Service Control . . . . .	127
4.10	Evidence Collection . . . . .	127
4.11	Download Section . . . . .	127
4.12	Updates . . . . .	127
4.13	User Management . . . . .	128
4.14	Master ASGARD and Analysis Cockpit . . . . .	128
4.15	Master ASGARD API . . . . .	128
<b>5</b>	<b>Maintenance</b>	<b>131</b>
5.1	Log Rotation and Retention . . . . .	131
5.2	Regain Disk Space . . . . .	132
<b>6</b>	<b>Advanced Configuration</b>	<b>133</b>
6.1	Performance Tuning . . . . .	133
6.2	Managing Logs . . . . .	134
6.3	Agent and Agent Installer Update . . . . .	136
6.4	Creating Custom Agent Installer . . . . .	138
6.5	Backup and Restore . . . . .	138
6.6	Disable Remote Console Globally . . . . .	142
<b>7</b>	<b>Troubleshooting</b>	<b>143</b>
7.1	Diagnostic Pack . . . . .	143
7.2	Agent Debugging . . . . .	144
7.3	SSL Interception . . . . .	146
7.4	Using Hostname instead of FQDN . . . . .	146
7.5	ASGARD Errors . . . . .	149
7.6	Resetting TLS/SSL Certificates . . . . .	149
7.7	Admin User Password Reset . . . . .	150
7.8	Resetting Two Factor Authentication . . . . .	150
7.9	Scheduled Scans have incorrect time . . . . .	151
7.10	Aurora has too many False Positives . . . . .	152
<b>8</b>	<b>Known Issues</b>	<b>153</b>
8.1	Known Issues . . . . .	153
<b>9</b>	<b>Appendix</b>	<b>161</b>
9.1	Installing ASGARD Agent via Powershell Script . . . . .	161
9.2	Deploy ASGARD Agents via SCCM . . . . .	162
9.3	Broken file and folder permissions . . . . .	163
9.4	Installing ASGARD Agent on a Golden Image . . . . .	164
9.5	Install TLS certificates on ASGARD and MASTER ASGARD . . . . .	165
<b>10</b>	<b>Upgrade from Management Center v2 to v3</b>	<b>185</b>



10.1 Upgrade . . . . .	185
<b>11 Changelog</b>	<b>189</b>
11.1 Management Center v3 . . . . .	189
<b>12 Indices and tables</b>	<b>191</b>
<b>Index</b>	<b>193</b>



Welcome to Nextron System's Manual for the ASGARD Management Center v3.

---

**Note:** If you are still using an older version of the Management Center, please click [here](#) to see the older version of the documentation.

---

ASGARD Management Center is the central management platform for THOR scans. It manages distributed THOR scans on thousands of systems, collects and forwards scan results.

Furthermore, ASGARD can control and execute complex response tasks, if needed. It features built-in response playbooks for quarantining endpoints, creating and collecting triage packs, opening a remote command line and other actions incident response specialists will find useful.



## **REQUIREMENTS**

In this chapter we will go over the requirements needed to get your Management Center up and running. Please follow the following steps carefully and don't skip anything, as you might encounter problems during or after the installation.

### **1.1 Introduction**

ASGARD Management Center is the central management platform for THOR scans. It manages distributed THOR scans on thousands of systems, collects and forwards scan results.

The ASGARD Management Center can control and execute complex response tasks if needed. It features built-in response playbooks for quarantining endpoints creating and collecting triage packs, opening live remote command prompts and other actions incident response specialists will find useful.

ASGARD additionally provides an easy to use interface for creating custom multi-step response playbooks, which can execute any command on your endpoints and collect the respective outputs.

ASGARD Management Center is available as a virtual appliance and also as a hardware appliance. Both are based on Debian Bullseye and require a setup procedure in order to generate customized agent installers and cryptographic keys.

This document describes all functions and steps for the setup and operation of the ASGARD Management Center. It will describe how to add systems for scanning and performing individual or group scanning with separate parameters.

### **1.2 Before You Begin**

This chapter contains high level information which will help you plan and implement the ASGARD Management Center within your existing environment.

---

**Hint:** Within this manual we might call the ASGARD Management Center just ASGARD or Management Center for the sake of simplicity.

---

## 1.2.1 Agent to ASGARD Communication

There are a few things to consider before you start with the installation. The communication between ASGARD and the ASGARD agent is unidirectional. The ASGARD agent polls the in a given time frame and ask for tasks to execute. There is no active triggering from ASGARD to the ASGARD agent – we have designed it that way, because we believe that opening a port on all connected endpoints should and can be avoided.

## 1.2.2 Performance Considerations

In environments with up to 500 endpoints, the default polling interval is around 20 seconds. In larger environments the polling interval increases automatically up to one minute for 2.000 endpoints and 10 minutes for configurations with 25.000 endpoints connected to a single ASGARD.

For this reason larger environments are not as responsive as small environments when it comes to opening remote shells or executing urgent response tasks. It may take up to 10 minutes for the shell to open or results of a THOR scan to show up. Once a task is running, like the remote console for example, the connection becomes almost instant.

Most environments contain endpoints which need faster polling between the agent and your ASGARD Management Center. For this reason we implemented a **Fast Poll** mode which can be set individually on a per host basis. For more information, please see [Asset Overview](#).

## 1.2.3 Using a Proxy between ASGARD Agent and ASGARD

ASGARD supports using a standard http proxy for the entire Agent to ASGARD communication. In order to use a proxy, the ASGARD agent must be repacked after installation. For details, see [Creating Custom Agent Installer](#).

## 1.3 Hardware Requirements

ASGARDs hardware requirements depend on the number of connected endpoints and also on the intended use. For example, you should consider using more disk space if you are planning to use Bifrost or ASGARD's evidence collection feature extensively.

Connected Endpoints	Minimum Hardware Requirements
up to 500 <sup>1</sup>	System memory: 4 GB, Hard disk: 500 GB, CPU Cores: 2
up to 10,000 <sup>1</sup>	System memory: 8 GB, Hard disk: 1TB, CPU Cores: 4
up to 25,000 <sup>1</sup>	System memory: 16 GB, Hard disk: 1TB SSD (min 100 MB/s), CPU Cores: 4

## 1.4 Agent Requirements

The ASGARD Agent, which needs to be installed on endpoints, is a lightweight service which is used to establish as secure connection with your Management Center. Memory usage of the agent is around 50 MB, which makes it very unobtrusive. THOR uses up to 1 GB of RAM additionally when scanning is in progress. This value will vary depending on the operating system THOR is running on. We observed lower RAM usage on unix systems all together, whereas Windows endpoints generally use more RAM.

<sup>1</sup> THOR and AURORA count as individual endpoints in this calculation. AURORA is more demanding than THOR. This results in a maximum of 200/4000/10000 endpoints if THOR **and** AURORA are installed on each endpoint.

The agent will use up to 50 MB of hard disk. Together with THOR and its temporary files it uses a maximum of 200 MB in total.

Please note that some response actions, such as collecting triage packs or collecting the system's RAM, require additional disk space.

There are no requirements pertaining to the CPU as scans can be scheduled in a way that THOR reduces its own process priority. This limits the CPU usage to a configurable percentage, with the tradeoff being prolonged scan times. There are multiple ways to facilitate THOR scans to your environment, which you can find in our separate [THOR Manual](#).

Supported operating systems are the ones [supported by THOR](#). Not supported are the operating systems with limited or special THOR support.

## 1.5 Network Requirements

ASGARD and other systems which will have to communicate with each other, need the following ports opened within the network. For a detailed and up to date list of our update and licensing servers, please visit <https://www.nextron-systems.com/hosts/>.

### 1.5.1 From ASGARD Agent to ASGARD Server

Description	Ports
Agent / Server communication	443/tcp
Syslog Forwarder (optional)	514/udp <sup>1</sup>
ASGARD online check (optional)	ICMP

The syslog port is optional, since your agents will work fine without it. Please see [Syslog Forwarding](#) for more information.

---

**Hint:** Your ASGARD Agents will check if they can reach your ASGARD via HTTPs. ICMP is not necessary, but helps during troubleshooting.

---

### 1.5.2 From Management Workstation to ASGARD Server

Description	Ports
Administrative web interface	8443/tcp
Command line administration	22/tcp

---

<sup>1</sup> You can configure any port and protocol combination for this, e.g. 6514/tcp

### 1.5.3 From ASGARD to SIEM

Description	Ports
Syslog forwarder	514/udp <small>Page 5, 1</small>

### 1.5.4 From ASGARD to Analysis Cockpit

Ports	Description
Asset Synchronization, Log- and Sample forwarding	7443/tcp
Syslog forwarder (optional)	514/udp <small>Page 5, 1</small>

### 1.5.5 From ASGARD and Master ASGARD to the Internet

The ASGARD systems are configured to retrieve updates from the following remote systems via HTTPS on port 443/tcp:

Product	Remote Systems
ASGARD packages	update-301.nexttron-systems.com
THOR updates	update1.nexttron-systems.com
THOR updates	update2.nexttron-systems.com

All proxy systems should be configured to allow access to these URLs without TLS/SSL interception. (ASGARD uses client-side SSL certificates for authentication). It is possible to configure a proxy server, username and password during the setup process of the ASGARD platform. Only BASIC authentication is supported (no NTLM authentication support).

### 1.5.6 From Master ASGARD to ASGARD

Direction	Port
From Master ASGARD to ASGARD Management Center	5443/tcp

You cannot manage ASGARD v3 systems from a Master ASGARD v2.

### 1.5.7 From Management Workstation to Master ASGARD

Description	Port
Administrative web interface	8443/tcp
Command line administration	22/tcp



### 1.5.8 Time Synchronization

ASGARD tries to reach the public Debian time servers by default.

Server	Port
0.debian.pool.ntp.org	123/udp
1.debian.pool.ntp.org	123/udp
2.debian.pool.ntp.org	123/udp

The NTP server configuration can be changed.

### 1.5.9 DNS

ASGARD needs to be able to resolve internal and external IP addresses.

**Warning:** Please make sure that you install your ASGARD with a domain name (see *Network Configuration*). If you do not set the Domain Name and install the ASGARD package, your clients won't be able to connect to your ASGARD.

All components you install should have a proper domain name configured to avoid issues further during the configuration.

### 1.5.10 Internet Access during Installation

The Nextron Universal Installer requires Internet access during the setup. The installation process will fail if required packages cannot be loaded from <https://update-301.nextron-systems.com>

### SSL/TLS Interception

The installation and update processes do not accept an unknown but valid SSL/TLS certificate presented by an intercepting entity and therefore don't support SSL/TLS interception.

Since our products are usually used in possibly compromised environments, the integrity of our software and update packages has highest priority.

### 1.5.11 Architecture Overview

The following image shows an architecture overview with all products and their communication relationships.

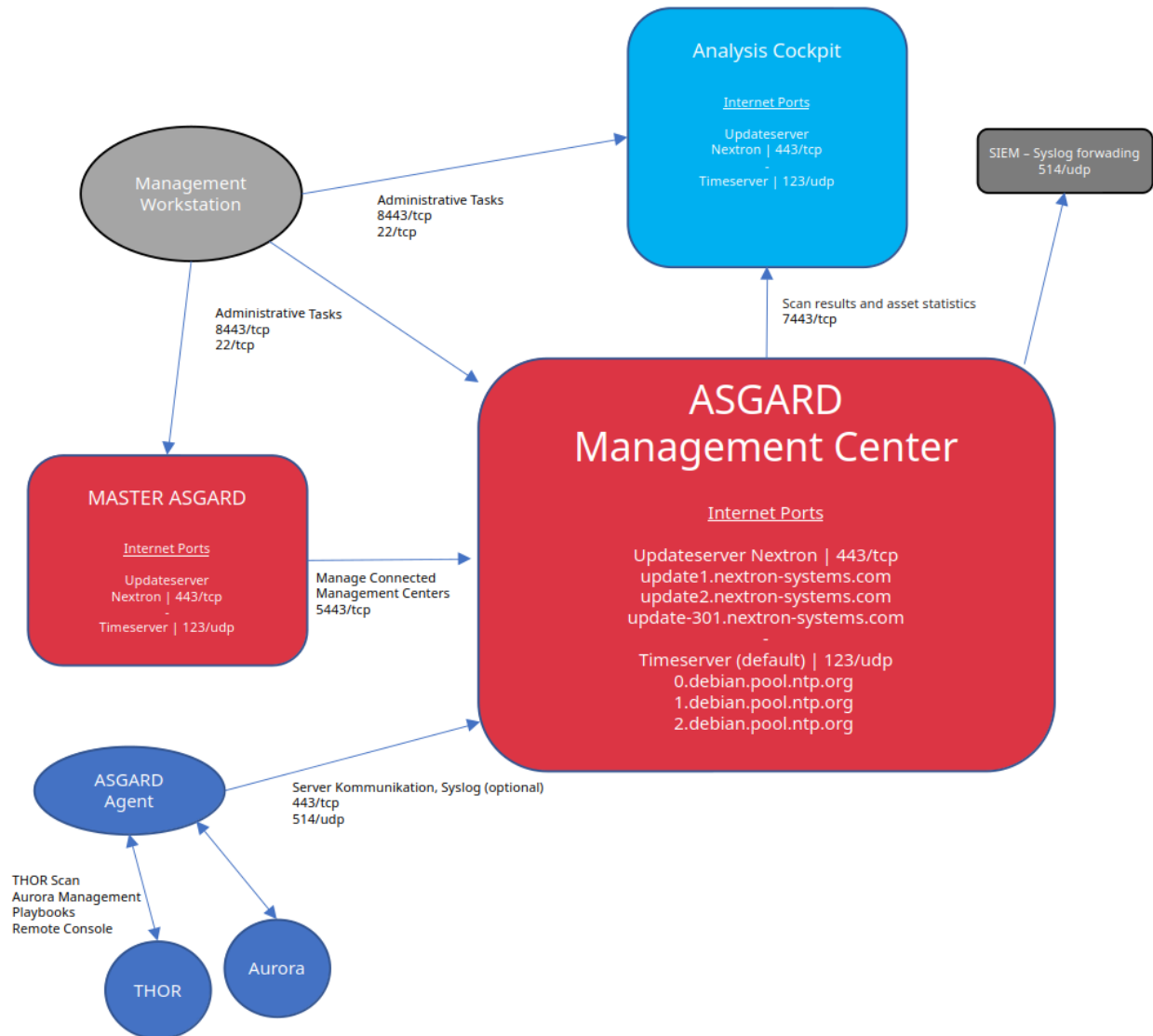


Fig. 1: Full Architecture

## 1.6 Antivirus and EDR Exclusions

We recommend excluding certain folders and binaries from Antivirus scanning.

The exclusions will not only prevent Antivirus engines from removing the agents and scanner executables but also increase scan speed, since their real-time engines won't check every file that the scanner has opened for analysis. This can improve the scan speed by up to 30% and also reduces the system's CPU load.

### 1.6.1 General Recommendation

We recommend using this list - include all sub folders:

Folder Exclusions including Subfolders	
<b>Windows</b>	%SYSTEMROOT%\System32\asgard2-agent\ %SYSTEMROOT%\Temp\asgard2-agent\
<b>Linux</b>	/usr/sbin/asgard2-agent-service /var/lib/asgard2-agent/ /var/tmp/asgard2-agent/
<b>macOS</b>	/var/lib/asgard2-agent/ /var/tmp/asgard2-agent/

**Note:** If you have obfuscated the agent name, replace *asgard2-agent* with your custom agent name.

If you have to create a more specific list that can use wildcards, use the following list (and replace [random] with the wildcard). If you have the choice, the broader approach above should be preferred.

Specific File/Process Exclusions	
<b>Windows</b>	%SYSTEMROOT%\System32\asgard2-agent\asgard2-agent.exe %SYSTEMROOT%\System32\asgard2-agent\asgard2-agent-service.exe %SYSTEMROOT%\System32\asgard2-agent\bin\thor.exe %SYSTEMROOT%\System32\asgard2-agent\bin\interrogate.exe %SYSTEMROOT%\System32\asgard2-agent\bin\console.exe %SYSTEMROOT%\System32\asgard2-agent\asgard2-agent_sc.exe %SYSTEMROOT%\System32\asgard2-agent\asgard2-agent_sc-service.exe %SYSTEMROOT%\Temp\asgard2-agent\ (and all sub folders)
<b>Especially And/Or</b>	%SYSTEMROOT%\Temp\asgard2-agent\[random]\thor\thor.exe %SYSTEMROOT%\Temp\asgard2-agent\[random]\thor\thor64.exe %SYSTEMROOT%\Temp\asgard2-agent-sc\ (and all sub folders)
<b>Especially And/Or</b>	%SYSTEMROOT%\Temp\asgard2-agent-sc\aurora\[random]\aurora\aurora-agent.exe %SYSTEMROOT%\Temp\asgard2-agent-sc\aurora\[random]\aurora\aurora-agent-64.exe
<b>Linux</b>	/usr/sbin/asgard2-agent-service /var/lib/asgard2-agent/asgard2-agent /var/lib/asgard2-agent/bin/console /var/lib/asgard2-agent/bin/interrogate /var/lib/asgard2-agent/bin/thor

continues on next page

Table 1 – continued from previous page

Specific File/Process Exclusions	
	/var/lib/asgard2-agent/bin/update
	/var/tmp/asgard2-agent/[random]/thor/thor-linux
	/var/tmp/asgard2-agent/[random]/thor/thor-linux-64
<b>macOS</b>	/var/lib/asgard2-agent/asgard2-agent-service
	/var/lib/asgard2-agent/asgard2-agent
	/var/lib/asgard2-agent/asgard2-agent/bin/console
	/var/lib/asgard2-agent/asgard2-agent/bin/interrogate
	/var/lib/asgard2-agent/asgard2-agent/bin/thor
	/var/lib/asgard2-agent/asgard2-agent/bin/update
	/var/tmp/asgard2-agent/[random]/thor/thor-macosx

Using the more specific list, we've experienced problems with some AV solutions that even trigger on certain keywords in filenames. They don't kill the excluded executable but block write access to disk if certain keywords like **bloodhound** or **mimikatz** appear in filenames. In these cases, the executable exclusions are not enough and you should use the recommended list of two folders and all sub folders (see above).

## 1.6.2 McAfee EDR Exclusions

McAfee needs Exclusions set in multiple locations. In addition to the general recommendation, customers with McAfee EDR need to set the following exclusions.

### McAfee On-Access Scan

McAfee On-Access Scan Exclusions	
<b>Low Risk</b>	thor.exe
	thor64.exe
	interrogate.exe
	generic.exe
	asgard2-agent.exe
	asgard2-agent-service.exe
	aurora-agent-64.exe
	aurora-agent.exe
<b>Exclusions</b> (include sub folders)	%SYSTEMROOT%\System32\asgard2-agent\
	%SYSTEMROOT%\Temp\asgard2-agent\
	%SYSTEMROOT%\Temp\asgard2-agent-sc\
<b>Access Protection</b>	thor.exe
	thor64.exe
	interrogate.exe
	generic.exe
	aurora-agent.exe
	aurora-agent-64.exe
	asgard2-agent.exe
	asgard2-agent-service.exe

continues on next page

Table 2 – continued from previous page

McAfee On-Access Scan Exclusions	
	asgard2-agent-windows-amd64.exe
	asgard2-agent-windows-386.exe
	C:\Windows\Temp\asgard2-agent\*\thor\*
	C:\Windows\Temp\asgard2-agent\*\thor\*\*
	C:\Windows\Temp\asgard2-agent\*
	C:\Windows\Temp\asgard2-agent-sc\aurora\*\aurora\*
	C:\Windows\Temp\asgard2-agent-sc\aurora\*\aurora\*\*
	C:\Windows\Temp\asgard2-agent-sc\aurora\*
	%SYSTEMROOT%\System32\asgard2-agent\bin\*
	%SYSTEMROOT%\System32\asgard2-agent\*

## McAfee EDR

McAfee EDR Exclusions	
<b>Network Flow</b>	C:\Windows\System32\asgard2-agent\asgard2-agent.exe
	C:\Windows\System32\asgard2-agent\bin\generic.exe
	C:\Windows\System32\asgard2-agent\bin\interrogate.exe
	C:\Windows\System32\asgard2-agent\bin\thor.exe
<b>Trace</b>	C:\Windows\System32\asgard2-agent\asgard2-agent.exe
	C:\Windows\System32\asgard2-agent\bin\generic.exe
	C:\Windows\System32\asgard2-agent\bin\interrogate.exe
	C:\Windows\System32\asgard2-agent\bin\thor.exe
<b>File Hashing</b>	C:\Windows\System32\asgard2-agent\
	C:\Windows\System32\asgard2-agent\*\
	C:\Windows\Temp\asgard2-agent\
	C:\Windows\Temp\asgard2-agent\*\
	C:\Windows\Temp\asgard2-agent-sc\
	C:\Windows\Temp\asgard2-agent-sc\*\

## 1.7 Verify the Downloaded ISO (Optional)

You can do a quick hash check to verify that the download was not corrupted. We recommend to verify the downloaded ISO's signature as this is the cryptographically sound method.

The hash and signature file are both part of the ZIP archive you download from our [portal server](#).

## 1.7.1 Via Hash

Extract the ZIP and check the sha256 hash:

On Linux

```
user@unix:~/nextron-universal-installer$ sha256sum -c nextron-universal-installer.iso.
↳sha256
nextron-universal-installer.iso: OK
```

or in Windows command prompt

```
C:\temp\nextron-universal-installer>type nextron-universal-installer.iso.sha256
efccb4df0a95aa8e562d42707cb5409b866bd5ae8071c4f05eec6a10778f354b nextron-universal-
↳installer.iso
C:\temp\nextron-universal-installer>certutil -hashfile nextron-universal-installer.iso.
↳SHA256
SHA256 hash of nextron-universal-installer.iso:
efccb4df0a95aa8e562d42707cb5409b866bd5ae8071c4f05eec6a10778f354b
CertUtil: -hashfile command completed successfully.
```

or in Powershell

```
PS C:\temp\nextron-universal-installer>type .\nextron-universal-installer.iso.sha256
efccb4df0a95aa8e562d42707cb5409b866bd5ae8071c4f05eec6a10778f354b nextron-universal-
↳installer.iso
PS C:\temp\nextron-universal-installer>Get-FileHash .\nextron-universal-installer.iso

Algorithm      Hash
↳Path
-----
--
SHA256         EFCCB4DF0A95AA8E562D42707CB5409B866BD5AE8071C4F05EEC6A10778F354B
↳C:\Users\user\Desktop\asgard2-installer\nextron-universal-installer.iso
```

## 1.7.2 Via Signature (Recommended)

Extract the ZIP, download the public signature and verify the signed ISO:

On Linux

```
use@unix:~/temp$ wget https://www.nextron-systems.com/certs/codesign.pem
use@unix:~/temp$ openssl dgst -sha256 -verify codesign.pem -signature nextron-universal-
↳installer.iso.sig nextron-universal-installer.iso
Verified OK
```

or in Powershell

```
PS C:\temp\nextron-universal-installer>Invoke-WebRequest -Uri https://www.nextron-
↳systems.com/certs/codesign.pem -OutFile codesign.pem
PS C:\temp\nextron-universal-installer>"C:\Program Files\OpenSSL-Win64\bin\openssl.exe"
↳dgst -sha256 -verify codesign.pem -signature nextron-universal-installer.iso.sig
↳nextron-universal-installer.iso
Verified OK
```

---

**Note:** If openssl is not present on your system you can easily install it using winget: `winget install openssl`.

---





## SETUP GUIDE

In this chapter we will show an example installation with VMware ESXi and the provided ISO image to install the Management Center. Please pay good attention to the setup during the Debian Installer, since this contains important steps which might break your installation!

---

**Important:** ASGARD products require a FQDN, which needs to be resolvable from all onboarded assets. If assets cannot resolve the FQDN specified during installation, a connection will not be possible.

---

### 2.1 Create a new ESX VM and Mount the ISO

Create a new VM with your virtualization software. In this case, we will use VMWare ESX managed through a VMWare VCenter.

The new VM must be configured with a Linux base system and Debian GNU/Linux 12 (64 bits) as target version. It is recommended to upload the ASGARD or Master ASGARD ISO to an accessible data store and mount the same to your newly created VM.

Please make sure to select a suitable v-switch or physical interface that reflects the IP address scheme you are planning to use for the new ASGARD. Only use one Hard Disk for the installation.

### 2.2 Navigate through the installer

The installation Process is started by clicking on ASGARD Graphical install. The installer then loads the additional components from the ISO and lets you select location and language.

**Warning:** Please make sure to select the correct Country, as this will also set your local timezone!

If DHCP is available, network parameters will be configured automatically. Without DHCP, ASGARD drops into the manual network configuration dialogue.

Without DHCP, ASGARD proceeds with the manual network configuration dialogue.

## New Virtual Machine

### 1 Select a creation type

- 2 Select a name and folder
- 3 Select a compute resource
- 4 Select storage
- 5 Select compatibility
- 6 Select a guest OS
- 7 Customize hardware
- 8 Ready to complete

### Select a creation type

How would you like to create a virtual machine?

- Create a new virtual machine
- Deploy from template
- Clone an existing virtual machine
- Clone virtual machine to template
- Clone template to template
- Convert template to virtual machine

This option guides you through creating a new virtual machine. You will be able to customize processors, memory, network connections, and storage. You will need to install a guest operating system after creation.

CANCEL

BACK

NEXT

## New Virtual Machine

### ✓ 1 Select a creation type

### 2 Select a name and folder

- 3 Select a compute resource
- 4 Select storage
- 5 Select compatibility
- 6 Select a guest OS
- 7 Customize hardware
- 8 Ready to complete

### Select a name and folder

Specify a unique name and target location

Virtual machine name: asgard.nextron

Select a location for the virtual machine.

▼  vcenter

CANCEL

BACK

NEXT

## New Virtual Machine

✓ 1 Select a creation type

✓ 2 Select a name and folder

✓ 3 Select a compute resource

✓ 4 Select storage

✓ 5 Select compatibility

**6 Select a guest OS**

7 Customize hardware

8 Ready to complete

**Select a guest OS**

Choose the guest OS that will be installed on the virtual machine

Identifying the guest operating system here allows the wizard to provide the appropriate defaults for the operating system installation.

Guest OS Family: 

Linux

Guest OS Version: 

Debian GNU/Linux 10 (64-bit)

Compatibility: ESXi 6.7 and later (VM version 14)

CANCEL

BACK

NEXT

New Virtual Machine

- ✓ 1 Select a creation type
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Select storage
- ✓ 5 Select compatibility
- ✓ 6 Select a guest OS
- 7 Customize hardware**
- 8 Ready to complete

Customize hardware  
Configure the virtual machine hardware

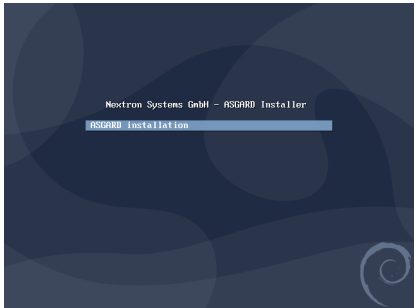
Virtual Hardware    VM Options

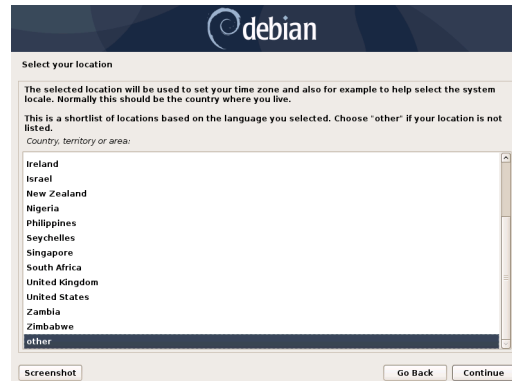
ADD NEW DEVICE

> CPU *	1		
> Memory *	16	GB	
> New Hard disk *	100	GB	
> New SCSI controller *	VMware Paravirtual		
> New Network *	VM Network		<input checked="" type="checkbox"/> Connect...
> New CD/DVD Drive *	Datastore ISO File		<input checked="" type="checkbox"/> Connect...
> Video card *	Specify custom settings		
VMCI device		Device on the virtual machine PCI bus that provides support for the virtual machine communication interface	
> Other	Additional Hardware		

Compatibility: ESXi 6.5 and later (VM version 13)

CANCEL    BACK    NEXT





debian

Select your location

The selected location will be used to set your time zone and also for example to help select the system locale. Normally this should be the country where you live.

This is a shortlist of locations based on the language you selected. Choose "other" if your location is not listed.

Country, territory or area:

- Ireland
- Israel
- New Zealand
- Nigeria
- Philippines
- Seychelles
- Singapore
- South Africa
- United Kingdom
- United States
- Zambia
- Zimbabwe
- other

Screenshot Go Back Continue



debian

Select your location


The selected location will be used to set your time zone and also for example to help select the system locale. Normally this should be the country where you live.

Listed are locations for: Europe. Use the «Go Back» option to select a different continent or region if your location is not listed.

Country, territory or area:

- Denmark
- Estonia
- Faroe Islands
- Finland
- France
- Georgia
- Germany
- Gibraltar
- Greece
- Greenland
- Guernsey
- Holy See (Vatican City State)
- Hungary

Screenshot Go Back Continue



debian

Configure locales

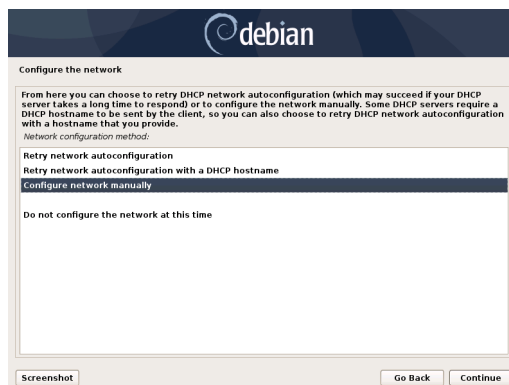
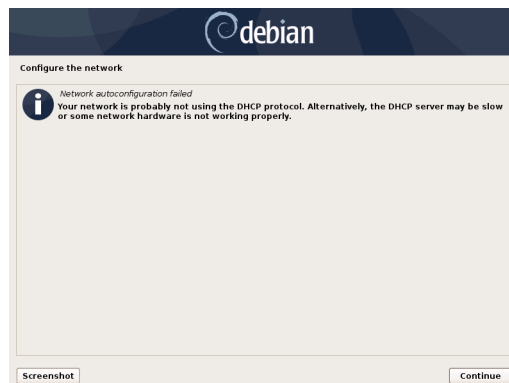
There is no locale defined for the combination of language and country you have selected. You can now select your preference from the locales available for the selected language. The locale that will be used is listed in the second column.

Country to base default locale settings on:

Canada	- en_CA.UTF-8
Hong Kong	- en_HK.UTF-8
India	- en_IN
Ireland	- en_IE.UTF-8
Israel	- en_IL
New Zealand	- en_NZ.UTF-8
Nigeria	- en_NG
Philippines	- en_PH.UTF-8
Seychelles	- en_SC.UTF-8
Singapore	- en_SG.UTF-8
South Africa	- en_ZA.UTF-8
United Kingdom	- en_GB.UTF-8
United States	- en_US.UTF-8
Zambia	- en_ZM
Zimbabwe	- en_ZW.UTF-8

Screenshot Help Go Back Continue

## 2.3 Network Configuration



**Warning:** ASGARD needs to be able to resolve internal and external IP addresses.

**Important: Important:** Make sure that the combination of hostname and domain creates an FQDN that can be resolved from the endpoints on which you intend to install the ASGARD agents. If you've configured a FQDN (hostname + domain) that cannot be resolved on the clients, no agent will be able to find and reconnect to the ASGARD server.

This is especially important since your Management Center will create some certificates during the installation, which will not contain an IP Address as its Subject Alternative Name (SAN), but only the FQDN! You will not be able to



Configure the network

The name servers are used to look up host names on the network. Please enter the IP addresses (not host names) of up to 3 name servers, separated by spaces. Do not use commas. The first name server in the list will be the first to be queried. If you don't want to use any name server, just leave this field blank.

Name server addresses:

Screenshot

Go Back

Continue



Configure the network

The gateway is an IP address (four numbers separated by periods) that indicates the gateway router, also known as the default router. All traffic that goes outside your LAN (for instance, to the Internet) is sent through this router. In rare circumstances, you may have no router; in that case, you can leave this blank. If you don't know the proper answer to this question, consult your network administrator.

Gateway:

Screenshot

Go Back

Continue



Configure the network

Please enter the hostname for this system.

The hostname is a single word that identifies your system to the network. If you don't know what your hostname should be, consult your network administrator. If you are setting up your own home network, you can make something up here.

Hostname:

Screenshot

Go Back

Continue

connect your ASGARD Management Center with your Analysis Cockpit via IP Address.

---

A screenshot of the Debian installer's network configuration window. The window has a dark blue header with the Debian logo and the word "debian" in white. Below the header, the title "Configure the network" is displayed. The main content area contains a text box with instructions: "The domain name is the part of your Internet address to the right of your host name. It is often something that ends in .com, .net, .edu, or .org. If you are setting up a home network, you can make something up, but make sure you use the same domain name on all your computers." Below this text is a label "Domain name:" followed by a text input field containing "intranet.example.org". At the bottom of the window, there are three buttons: "Screenshot" on the left, and "Go Back" and "Continue" on the right.

Configure the network

The domain name is the part of your Internet address to the right of your host name. It is often something that ends in .com, .net, .edu, or .org. If you are setting up a home network, you can make something up, but make sure you use the same domain name on all your computers.

Domain name:

intranet.example.org

Screenshot Go Back Continue

## 2.4 Choosing a password

## 2.5 Partitioning the Hard Disk

**Warning:** ASGARD is intended to be installed with only one disk. Do not configure your server with multiple disks. The system won't configure additional disks. Make sure that your disk has the recommended size. See [Hardware Requirements](#) for more information.

Finally, write your configuration to the disk by selecting "Yes" and clicking "Continue".





**Set up users and passwords**

A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.  
 Choose a password for the new user:


☐ Show Password in Clear

Please enter the same user password again to verify you have typed it correctly.  
 Re-enter password to verify:

☐ Show Password in Clear

Screenshot Go Back Continue

Fig. 1: Choosing a password for the nexttron user

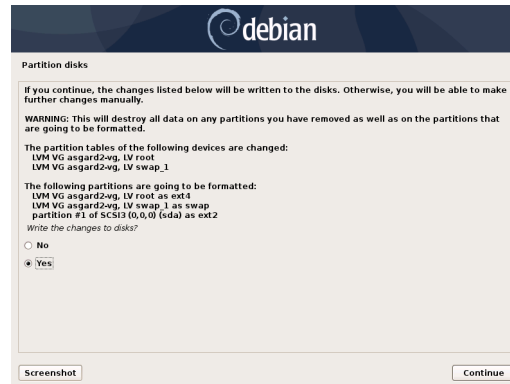


**Partition disks**

Note that all data on the disk you select will be erased, but not before you have confirmed that you really want to make the changes.  
 Select disk to partition:

SCSI3 (0,0,0) (sda) - 16.1 GB VMware, VMware Virtual S
--

Screenshot Go Back Continue



## 2.6 Proxy Configuration

If you are using a proxy to access the internet, enter the proxy details in the next step. Please note, Internet connectivity is required for the next step – the installation of the ASGARD service.



The base installation is now complete. In the next step we will install the ASGARD service. For this step Internet connectivity is required.

## 2.7 Changing the IP-Address

ASGARD's IP-Address can be changed in `/etc/network/interfaces`. The IP is configured with the address variable.

```
nexttron@asgard:~$ sudoedit /etc/network/interfaces
```

```
auto ens32
iface ens32 inet static
address 192.0.2.7
netmask 255.255.255.0
gateway 192.0.2.254
```

Important: There might be a case where the name of the network adaptor (in this example: `ens32`) can vary.

The new IP can be applied with the command **`sudo systemctl restart networking`**

## 2.7.1 Verifying DNS Settings

To verify if ASGARD is using the correct DNS Server, you can inspect the file `/etc/resolv.conf`:

```
nexttron@asgard:~$ cat /etc/resolv.conf
search example.org
nameserver 172.16.200.2
```

If you see errors in this configuration, you can change it with the following command:

```
nexttron@asgard:~$ sudoedit /etc/resolv.conf
```

## 2.8 Install the ASGARD Management Center Service

The Nextron Universal Installer is a web based installer which will guide you through the installation of our ASGARD products. The Nextron Universal Installer will install **one** of the following products on your server (this manual focuses on the ASGARD Management Center):

---

**Hint:** if you want to install the Master ASGARD, please use the correct license and product (Master ASGARD) in the Nextron Universal Installer.

---

- ASGARD Management Center; alternatively if your license permits:
  - ASGARD Broker
  - ASGARD Gatekeeper
  - ASGARD Lobby
- Master ASGARD
- ASGARD Analysis Cockpit; alternatively:
  - Elasticsearch Cluster Node for ASGARD Analysis Cockpit
- ASGARD Security Center, in the following variants:
  - ASGARD Security Center (Backend Only)
  - ASGARD Security Center (Frontend Only)
  - ASGARD Security Center (All-in-one, unrecommended)

---

**Note:** You can only install one product on one server, since the products are not designed to coexist on the same server. The exception being the ASGARD Security Center (All-in-one).

---

The installation takes roughly between 5-15 minutes, depending on your internet connection and the server you are installing the product on.

If you encounter problems during your installation, please see [Diagnostic Pack](#) for further instructions.

### 2.8.1 Requirements

The installation of the ASGARD Management Center requires the following:

- A valid license file for the ASGARD Management Center
- A configured FQDN (with some exceptions, see *Valid FQDN*)
- Internet access during installation (see *Connectivity Check*)

### 2.8.2 Installation

After the ISO installer is finished with the setup, you will be greeted at the console login prompt with the following message:

```
Nextron Universal Installer
Ready to complete your setup? Get started by visiting https://asgard.local.
To proceed, you'll need to enter the installation code Z9CU-6Q3H-VK24-X7YS in the Web UI.
asgard login: _
```

Follow the instructions and navigate to the webpage displayed on your console. You will most likely get a browser warning when you connect the first time to the page. This is due to the page using a self signed certificate, since it will only be used to install the ASGARD Management Center. You can safely ignore this warning and proceed to the page.

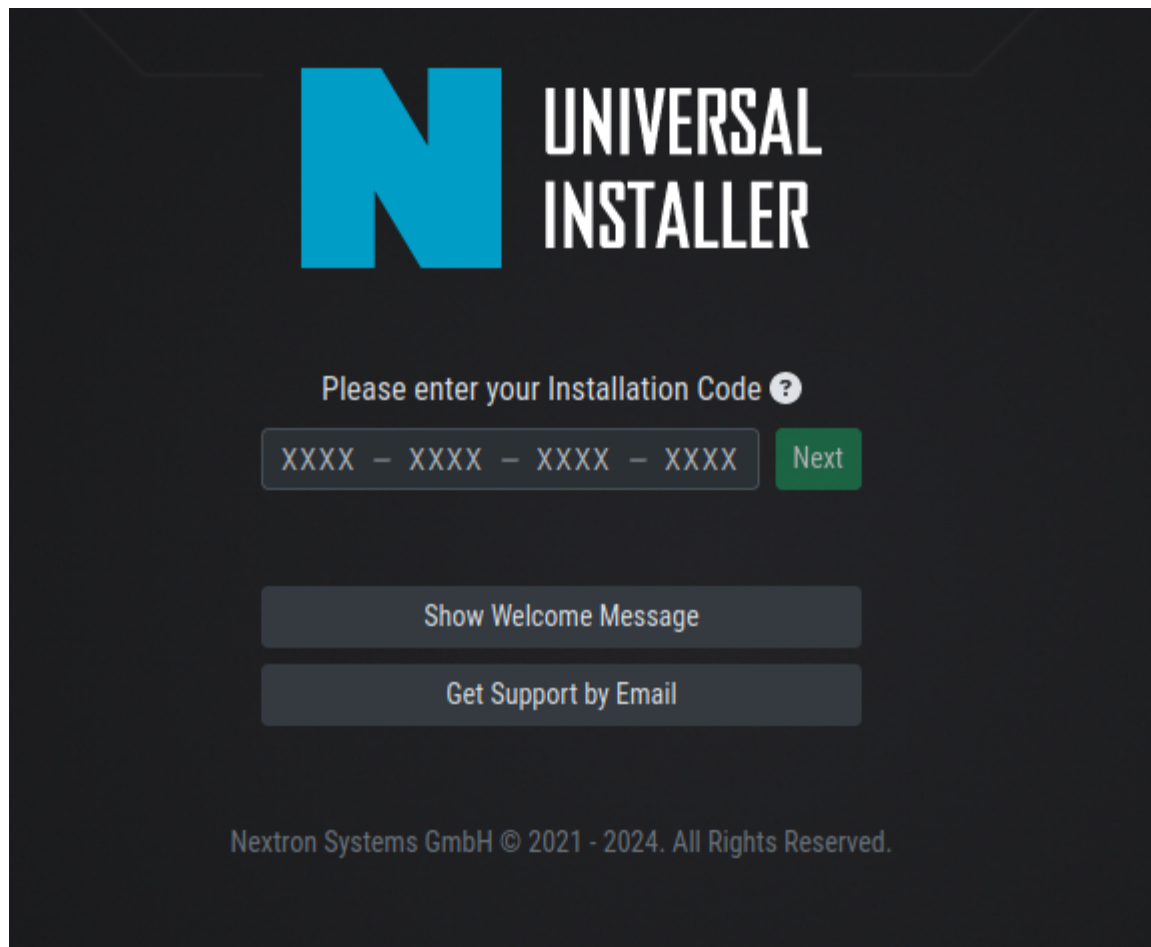
You will be greeted with a small introduction as to what the Nextron Universal Installer is and what it does. After you click **Next**, you will be presented with the landing page of the Nextron Universal Installer.

Enter the Installation Code from the terminal and click **Next**. The Installer will now guide you through the installation.

### 2.8.3 Connectivity Check

The Nextron Universal Installer will try to connect to our update server in order to download all the necessary packages once the installation starts. Make sure you can reach the update servers (see *Internet Access during Installation*).

Please configure your proxy settings if you are behind a proxy (see *Proxy and NTP Settings*).



## 2.8.4 Valid FQDN

The Nextron Universal Installer will prompt you to verify the FQDN which you configured during the installation of the base system (see [Network Configuration](#)). This is needed in order for your ASGARD Agents to communicate via a HTTPs connection with the ASGARD Management Center. The Agents will use the FQDN to connect to the ASGARD Management Center and also verify the Common Name of the certificate to verify its authenticity. If there is a mismatch the Agents will not be able to connect to the ASGARD Management Center.

If the displayed FQDN is not correct, you can change it by clicking on the [View FQDN Change Instructions](#) button. This will open a dialog with instructions on how to change the FQDN of your server. Once you have changed the FQDN, you can continue with the installation.

Progress bar: 1 Upload License, 2 Test Connectivity, 3 FQDN Acknowledgment, 4 Select Product, 5 Configuration, 6 Installation, 7 Restart System.

**Important Note:** The server's current FQDN is `asgard.local`.

Please be aware that once an Nextron Systems product has been installed, it is not possible to modify the FQDN. In order to proceed with the installation, please write your current FQDN below:

✓

Please enter your current FQDN

[View FQDN Change Instructions](#)

[Back](#) [Next](#)

If you are in a time critical engagement and need to proceed with the installation, you can just confirm the displayed (and technically invalid) FQDN and change it later (before you deploy your Agents). To do this, see [Regenerate ASGARD Server Certificate Agent Communication](#)

## 2.8.5 Proxy and NTP Settings

If you need to configure a proxy or change the NTP settings of your system, you can do so by clicking on the [Settings](#) button in the left menu of the Nextron Universal Installer.

UNIVERSAL INSTALLER

Settings > Proxy

Installation

Settings

Proxy

NTP

Diagnostics

**Proxy**

Scheme: http

Host:

Port:

Proxy User:

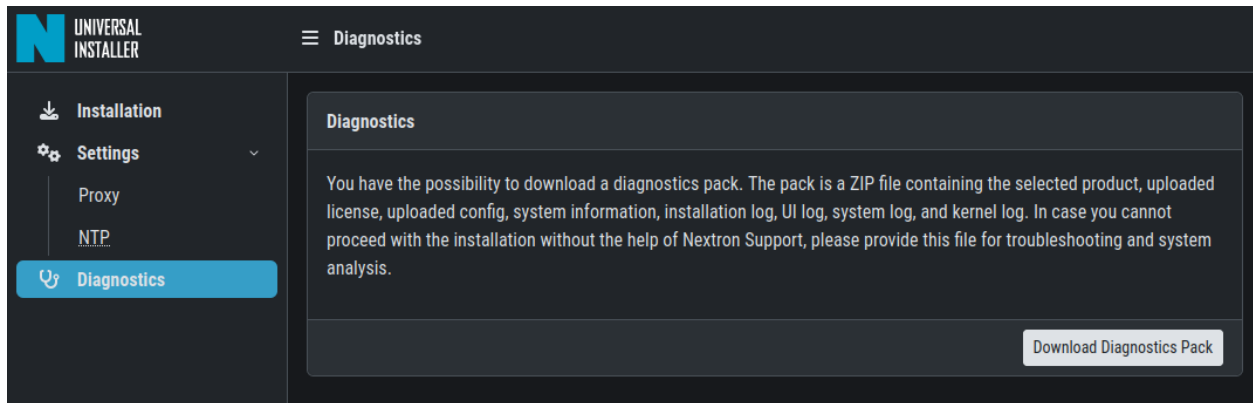
Proxy Password:

[Unset Proxy](#) [Set Proxy](#)

If you configured a proxy during the ISO installation, those settings will be carried over into the Universal Installer. The settings will also be carried over into your ASGARD Management Center. The same goes for NTP.

## 2.8.6 Diagnostic Pack

In case of errors or problems during the installation, you can download a diagnostic pack by navigating to the **Diagnostics** tab in the left menu of the Nextron Universal Installer. Click on the **Download Diagnostic Pack** button to download the diagnostic pack. You can then send the diagnostic pack to our support team for further analysis.







## ADMINISTRATION

This chapter focuses on the initial setup of your Management Center, installing agents and performing routine tasks in the Web UI.

### 3.1 System Status

#### 3.1.1 Status Overview

The initial system status page provides a summary of the most important system components.

It also includes the current resource consumption (disk, CPU and memory) and lists the currently installed Management Center software version, along with available versions of THOR. The connection status to the update servers, Master ASGARD and Cockpit are shown as well as multiple graphs which show asset connections and asset streams.

---

**Note:** The THOR version numbers may be missing in a new installation. THOR is **not** included in the installed packages and has to be downloaded first. The download is starting automatically after the installation, not later than one hour after installation.

---

#### 3.1.2 Diagnostics

The diagnostics sub menu shows the periodically performed checks and their status. Clicking the magnifying glass icon shows details of the performed check. If a check failed it gives a detailed error message and hints on which steps typically help in resolving the issue.

The indicator on the top right always shows if any of those checks failed by showing a warning or error (i.e. yellow or red icon). You can click the icon to view the diagnostics page as a pop-up.

#### 3.1.3 Logs

The logs section shows the latest and most relevant logs. Complete logs can be found at `/var/lib/asgard-management-center/log`. You can also download the selected log type directly.

Available logs and their content:

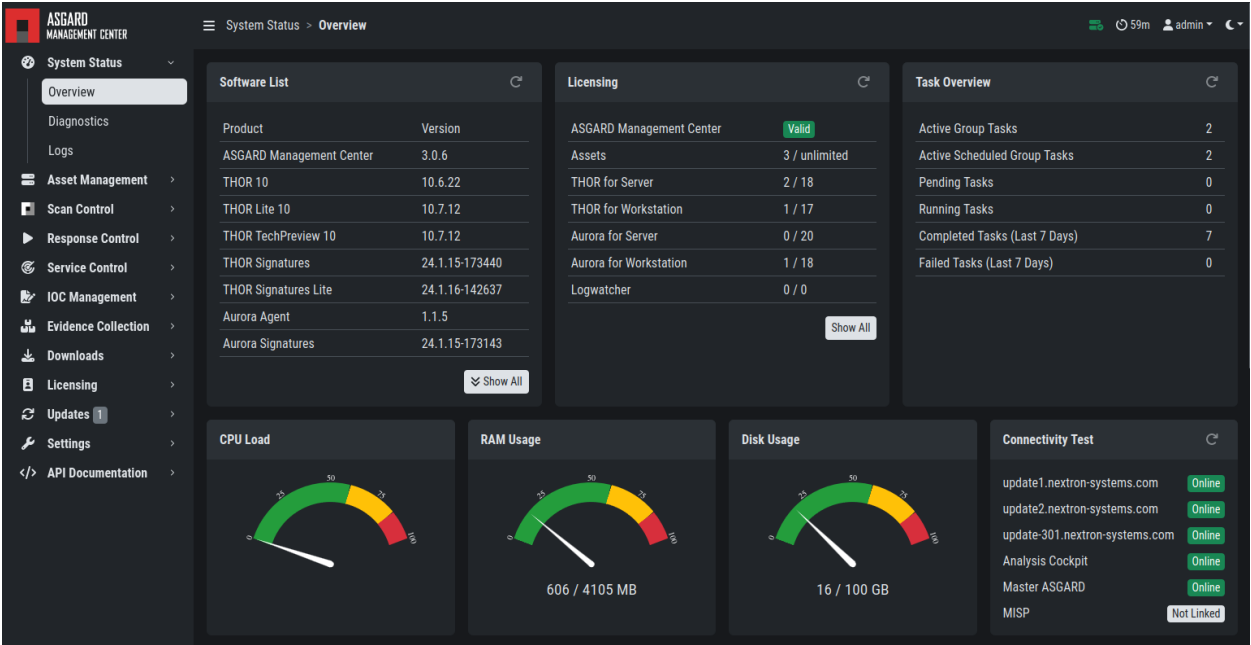


Fig. 1: Overview Top Half

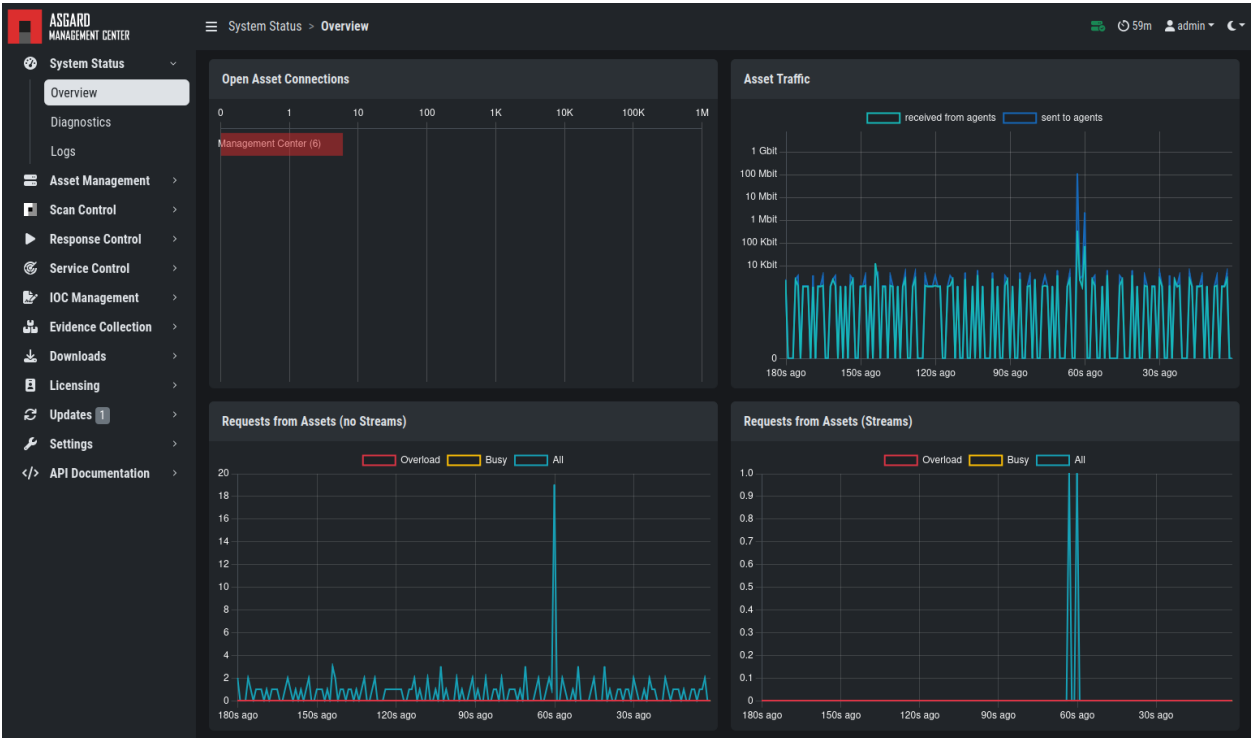
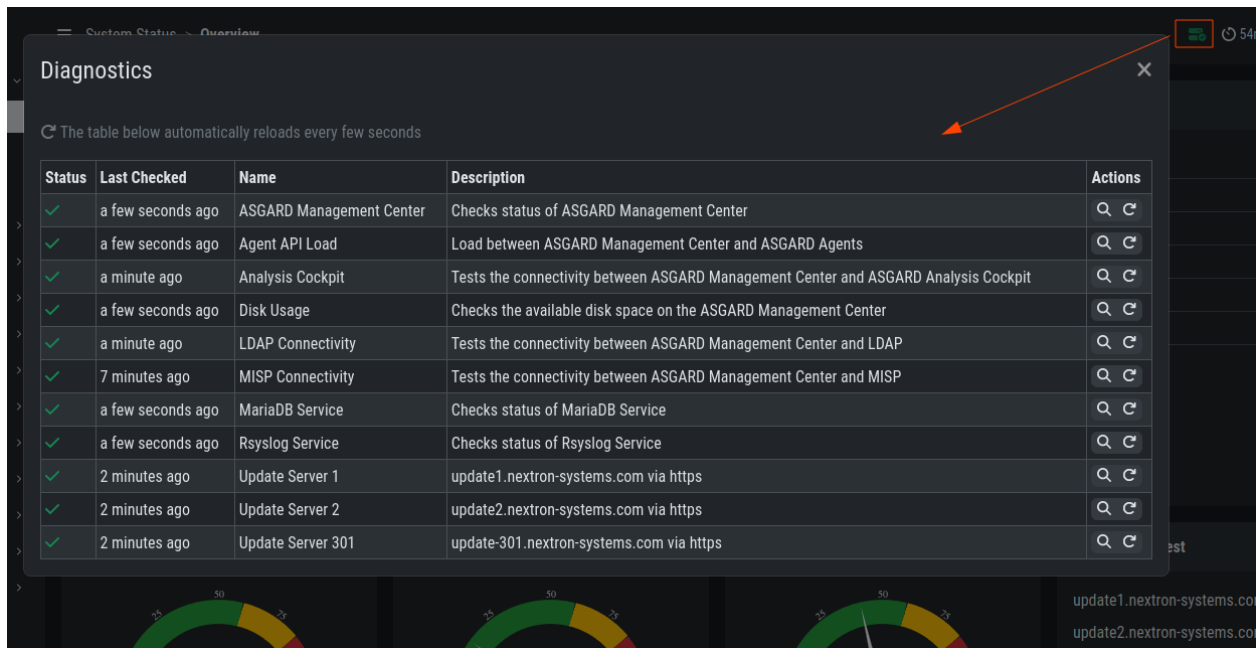


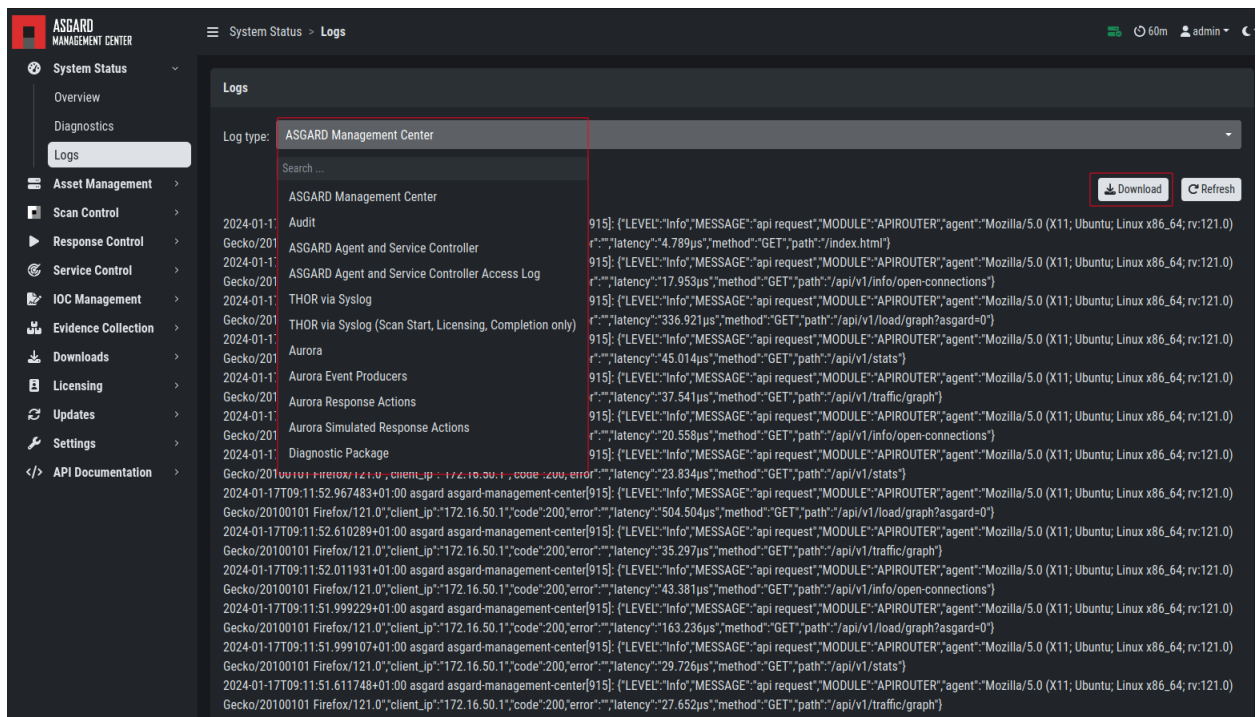
Fig. 2: Overview Bottom Half



The table below automatically reloads every few seconds

Status	Last Checked	Name	Description	Actions
✓	a few seconds ago	ASGARD Management Center	Checks status of ASGARD Management Center	Q ↻
✓	a few seconds ago	Agent API Load	Load between ASGARD Management Center and ASGARD Agents	Q ↻
✓	a minute ago	Analysis Cockpit	Tests the connectivity between ASGARD Management Center and ASGARD Analysis Cockpit	Q ↻
✓	a few seconds ago	Disk Usage	Checks the available disk space on the ASGARD Management Center	Q ↻
✓	a minute ago	LDAP Connectivity	Tests the connectivity between ASGARD Management Center and LDAP	Q ↻
✓	7 minutes ago	MISP Connectivity	Tests the connectivity between ASGARD Management Center and MISP	Q ↻
✓	a few seconds ago	MariaDB Service	Checks status of MariaDB Service	Q ↻
✓	a few seconds ago	Rsyslog Service	Checks status of Rsyslog Service	Q ↻
✓	2 minutes ago	Update Server 1	update1.nextron-systems.com via https	Q ↻
✓	2 minutes ago	Update Server 2	update2.nextron-systems.com via https	Q ↻
✓	2 minutes ago	Update Server 301	update-301.nextron-systems.com via https	Q ↻

Fig. 3: Overview Over Periodic Diagnostic Checks



Log type: ASGARD Management Center

Search ...

Download Refresh

Log type	Log	Log details
ASGARD Management Center	Audit	915]: {"LEVEL":"Info","MESSAGE":"api request","MODULE":"APIROUTER","agent":"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:121.0) r...","latency":"4.789µs","method":"GET","path":"/index.html"}
ASGARD Agent and Service Controller	Gecko/201	915]: {"LEVEL":"Info","MESSAGE":"api request","MODULE":"APIROUTER","agent":"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:121.0) r...","latency":"17.953µs","method":"GET","path":"/api/v1/info/open-connections"}
ASGARD Agent and Service Controller Access Log	Gecko/201	915]: {"LEVEL":"Info","MESSAGE":"api request","MODULE":"APIROUTER","agent":"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:121.0) r...","latency":"336.921µs","method":"GET","path":"/api/v1/load/graph?asgard=0"}
THOR via Syslog	Gecko/201	915]: {"LEVEL":"Info","MESSAGE":"api request","MODULE":"APIROUTER","agent":"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:121.0) r...","latency":"45.014µs","method":"GET","path":"/api/v1/stats"}
THOR via Syslog (Scan Start, Licensing, Completion only)	Gecko/201	915]: {"LEVEL":"Info","MESSAGE":"api request","MODULE":"APIROUTER","agent":"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:121.0) r...","latency":"37.541µs","method":"GET","path":"/api/v1/traffic/graph"}
Aurora	Gecko/201	915]: {"LEVEL":"Info","MESSAGE":"api request","MODULE":"APIROUTER","agent":"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:121.0) r...","latency":"20.558µs","method":"GET","path":"/api/v1/info/open-connections"}
Aurora Event Producers	Gecko/201	915]: {"LEVEL":"Info","MESSAGE":"api request","MODULE":"APIROUTER","agent":"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:121.0) r...","latency":"23.834µs","method":"GET","path":"/api/v1/stats"}
Aurora Response Actions	Gecko/201	2024-01-17T09:11:52.967483+01:00 asgard asgard-management-center[915]: {"LEVEL":"Info","MESSAGE":"api request","MODULE":"APIROUTER","agent":"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:121.0) r...","latency":"504.504µs","method":"GET","path":"/api/v1/load/graph?asgard=0"}
Aurora Simulated Response Actions	Gecko/201	2024-01-17T09:11:52.610289+01:00 asgard asgard-management-center[915]: {"LEVEL":"Info","MESSAGE":"api request","MODULE":"APIROUTER","agent":"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:121.0) r...","latency":"43.381µs","method":"GET","path":"/api/v1/info/open-connections"}
Diagnostic Package	Gecko/201	2024-01-17T09:11:52.011931+01:00 asgard asgard-management-center[915]: {"LEVEL":"Info","MESSAGE":"api request","MODULE":"APIROUTER","agent":"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:121.0) r...","latency":"163.236µs","method":"GET","path":"/api/v1/load/graph?asgard=0"}
	Gecko/201	2024-01-17T09:11:51.999107+01:00 asgard asgard-management-center[915]: {"LEVEL":"Info","MESSAGE":"api request","MODULE":"APIROUTER","agent":"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:121.0) r...","latency":"29.726µs","method":"GET","path":"/api/v1/stats"}
	Gecko/201	2024-01-17T09:11:51.611748+01:00 asgard asgard-management-center[915]: {"LEVEL":"Info","MESSAGE":"api request","MODULE":"APIROUTER","agent":"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:121.0) r...","latency":"27.652µs","method":"GET","path":"/api/v1/traffic/graph"}

Fig. 4: Logs Section

Log Type	Explanation
ASGARD Management Center	Overall status of the Management Center, general errors and warnings
Audit	Containing user login/logout and changes done over the UI
ASGARD Agent and Service Controller	Status of the agents deployed on assets
ASGARD Agent and Service Controller Access Log	Logs of agents and service controllers communicating with the Management Center
THOR via Syslog	Received syslog events of THOR scans. Partial results if a scan did not complete
THOR via Syslog (Scan Start, Licensing, Completion only)	As the name suggest, only those three event types
Aurora	All Aurora events
Aurora Event Producers	The top 10 event producing processes per endpoint
Aurora Response Actions	Only response action events of Aurora
Aurora Simulated Response Actions	Only simulated response action events of Aurora
Diagnostic Pack	Button for generating and downloading a diagnostic pack that may be asked for by support

## 3.2 ASGARD Agent Deployment

In order to register a new endpoint to the ASGARD Management Center, download and install the ASGARD Agent on the system you want to register.

The ASGARD Agent can be directly downloaded from the Management Center login screen through the button **Download Agent Installers**. A list of available agents for various operating systems appears.

---

**Hint:** You can disable the downloading of agents on the login screen. Please see [Advanced Settings](#).

---

After the installation, the endpoints will connect to your Management Center, register automatically and appear in the Asset Management Section in the tab **Asset Requests**. Please allow two or three minutes for systems to show up. The agents use the FQDN to connect to your Management Center, so ensure that your endpoints can resolve and reach the Management Center via FQDN.

---

**Note:** Full administrative privileges are required for the ASGARD agent and THOR to operate properly.

---

In the requests tab, select the agents you want to allow on your Management Center to manage and click **Accept Asset Requests**. After that, the endpoint shows up in the assets overview and is now ready to be managed and scanned.

A registered agent will poll the Management Center at a given interval between 10 seconds and 10 Minutes – depending on the number of connected endpoints (see [Performance Tuning](#) for details). If your Management Center has scheduled a task for the endpoint (for example: run THOR scan) it will be executed directly after the poll.

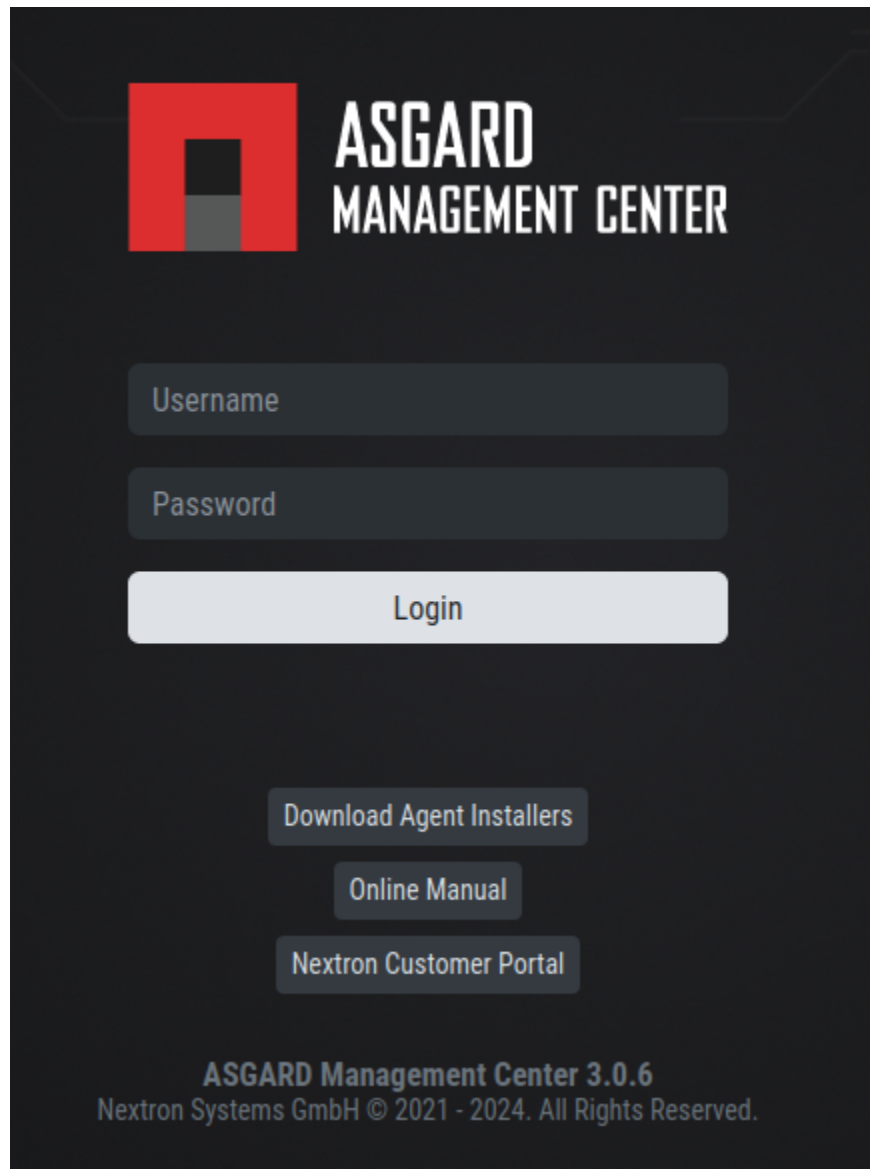


Fig. 5: Download Agent Installers from Login Screen

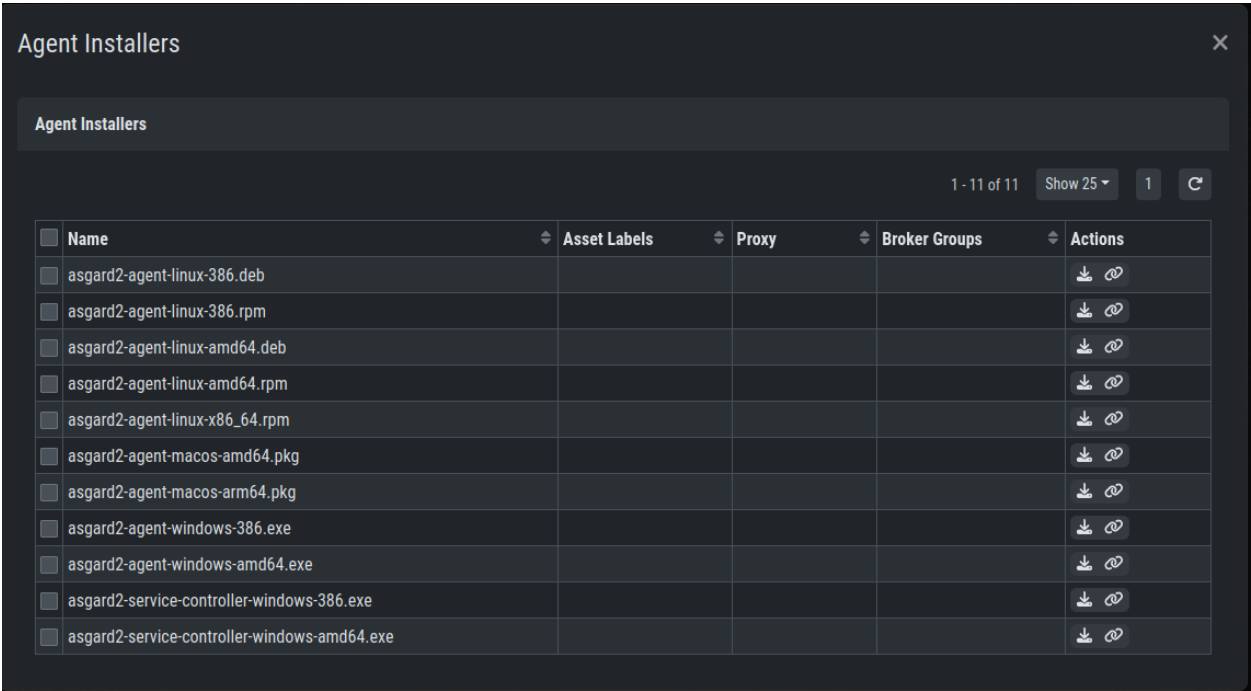


Fig. 6: Agents Overview

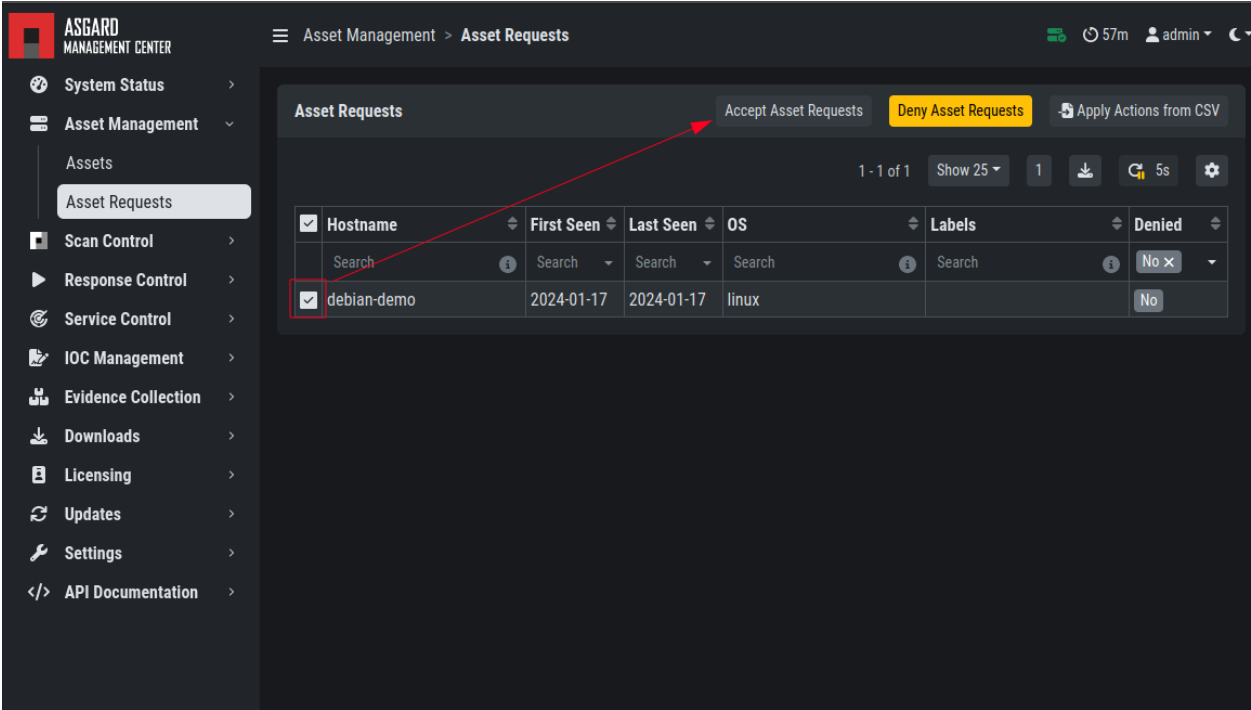


Fig. 7: Accepting ASGARD Agent Requests

### 3.2.1 Windows Agent Deployment

Since the Agent Installer for Windows is a normal .exe file and not a .msi file, you need to write your own scripts to deploy the agent via your management system of choice. We have written an example script in PowerShell, which should work for most of the tools. Please see the section [Installing ASGARD Agent via Powershell Script](#) and [Deploy ASGARD Agents via SCCM](#).

Alternatively, if you want to deploy the ASGARD Agent manually, you can just execute the installer by hand.

### 3.2.2 Linux Agent Deployment

To deploy the ASGARD Agent on a linux system, you can use the following commands:

Listing 1: Debian based systems

```
user@unix:~/Downloads$ sudo dpkg -i asgard2-agent-linux-amd64.deb
```

Listing 2: RHEL, CentOS and Fedora

```
user@unix:~/Downloads$ sudo rpm -i asgard2-agent-linux-amd64.rpm
```

You will be able to deploy your agents via most of the common linux tools, just make sure that the installer is being installed with administrative privileges.

### 3.2.3 macOS Agent Deployment

Starting with macOS Big Sur (v11.0), Apple requires software developers to notarize applications.

Due to the nature of the asgard2-agent installer, which is generated during installation time on your Management Center, and making it unique for each Management Center installation, it is currently not possible to notarize the installer.

This document aims to describe possible workarounds, intended to be a reference for IT administrators or IT packaging teams to bypass Apple verifications and install the personalized asgard2-agents on macOS Big Sur (or newer) workstations.

**Warning:** Executing any of the workarounds described in this document puts your system at risk for a short period of time. This document will deactivate global security mechanisms of the operating system, which are intended to protect the integrity of the system. Please make sure to follow the below steps carefully and enable those security mechanisms after you are done.

Please always keep in mind to check your system after performing any of the described actions, to ensure that all security mechanisms are in place and are re-activated after performing the described actions.

Please follow the below steps to install the ASGARD Agent on macOS.

1. Open a new terminal session
2. Deactivate macOS Gatekeeper
  - `sudo spctl --master-disable`
3. Close the terminal and open a new terminal session
4. Install the asgard2-agent

- `sudo installer -pkg /path/to/asgard2-agent-macos-amd64.pkg -target /`
5. Close the terminal and open a new terminal session
  6. Reactivate macOS Gatekeeper
    - `sudo spctl --master-enable`

**Warning:** Make sure to activate the macOS Gatekeeper once you are done:

```
sudo spctl --master-enable
```

You can verify the state of the macOS Gatekeeper with:

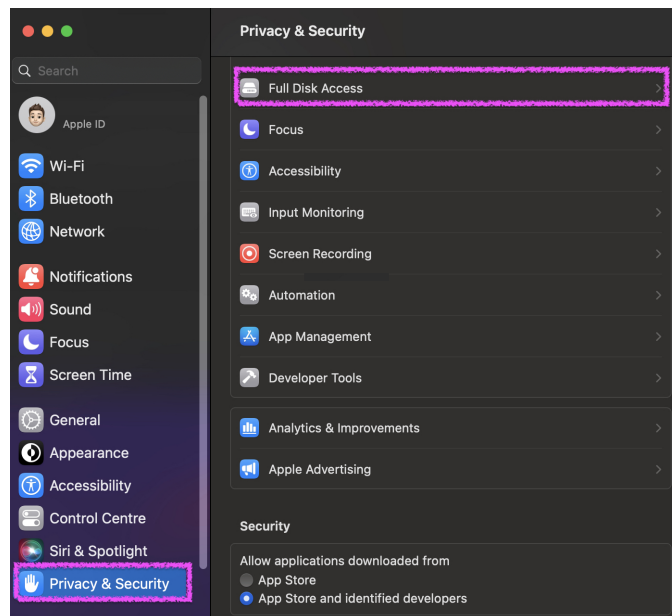
```
MacBook-Pro:~ nexttron$ spctl --status
assessments enabled
```

On a system with activated Gatekeeper, the output has to be `assessments enabled`.

### macOS Full Disk Access

Since macOS Ventura (v13.0) the ASGARD Agent needs full disk access to function properly. After you have deployed the ASGARD Agent, you need to grant the service the required access permissions. Please keep in mind that administrative privileges on the machine are needed to perform this change.

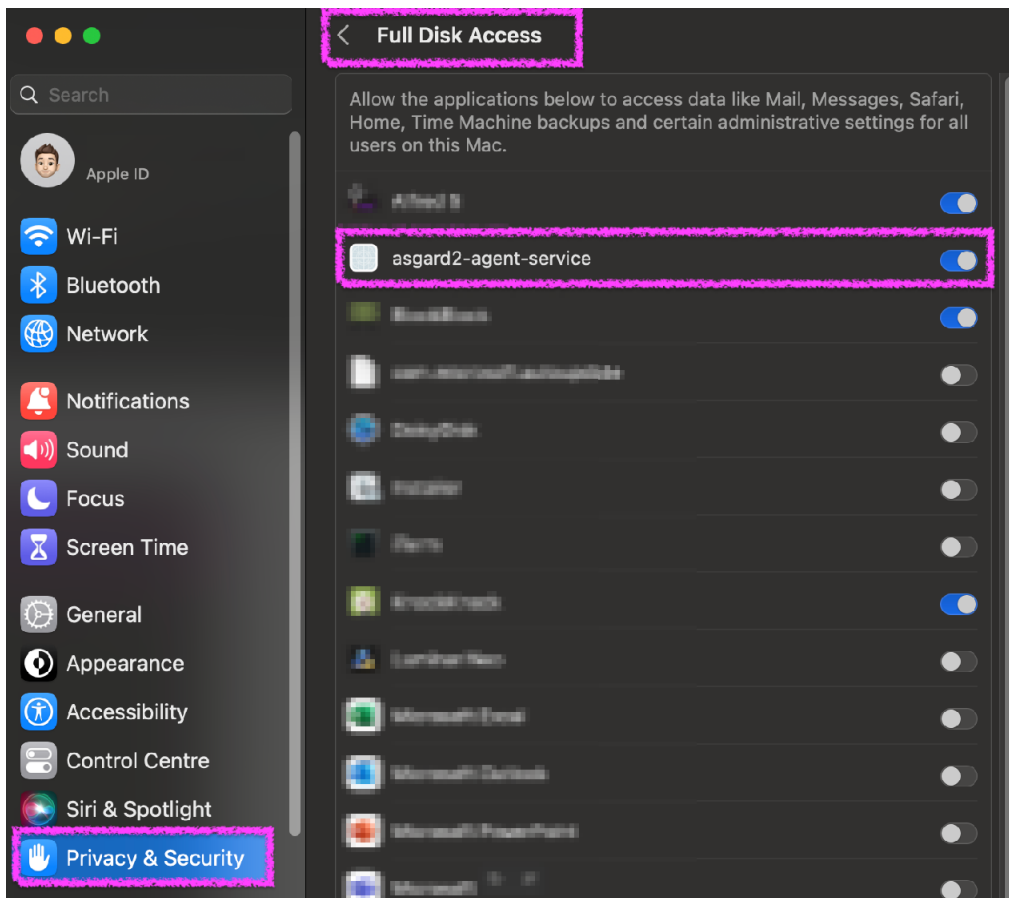
To do this, navigate on your Mac to **System Settings > Privacy & Security > Full Disk Access**:



You need to enable the `asgard2-agent-service` slider:

**Note:** There is no workaround to this step, since it is an integral part of the security design of Apple devices. If you are having trouble with THOR scans via ASGARD on macOS, please check if the Full Disk Access permission for the ASGARD agent was granted. Since macOS Mojave (v10.14), you need to grant the same permissions to removable volumes, if you plan on scanning those.





## 3.3 Uninstall ASGARD Agents

The following listings contain commands to uninstall ASGARD Agents on endpoints.

---

**Note:** The commands contain names used by the default installer packages. If you have generated custom installer packages with a custom service and binary name, you have to adjust the commands accordingly.

---

### 3.3.1 Uninstall ASGARD Agents on Windows

You need administrative privileges to remove the ASGARD Agent from Windows. Open a command prompt with administrative privileges and run the following commands:

```

1 C:\Windows\system32>sc stop asgard2-agent
2 C:\Windows\system32>sc delete asgard2-agent
3 C:\Windows\system32>sc stop asgard2-agent_sc
4 C:\Windows\system32>sc delete asgard2-agent_sc
5 C:\Windows\system32>rmdir /S /Q C:\Windows\System32\asgard2-agent
6 C:\Windows\system32>rmdir /S /Q C:\ProgramData\thor

```

---

**Note:** Line 3 and 4 are only necessary if the new service controller (on ASGARD 2.11+) has been installed.

---

The commands above will:

- Disable the ASGARD agent's service
- Delete the ASGARD agent's service
- Remove all files associated with the ASGARD agent

### 3.3.2 Uninstall ASGARD Agents on Linux

RPMs via yum

```

user@host:~$ sudo yum remove asgard2-agent
user@host:~$ sudo rm -r /var/lib/thor

```

DEBs via dpkg

```

user@host:~$ sudo dpkg -P asgard2-agent
user@host:~$ sudo rm -r /var/lib/thor

```

Manual uninstall

```

root@host:~# /usr/sbin/asgard2-agent-amd64 stop
root@host:~# /usr/sbin/asgard2-agent-amd64 uninstall
root@host:~# rm -r /usr/sbin/asgard2-agent-amd64
root@host:~# rm -r /var/tmp/nextron/asgard2-agent
root@host:~# rm -r /var/lib/nextron/asgard2-agent
root@host:~# rm -r /var/lib/thor

```

### 3.3.3 Uninstall ASGARD Agents on macOS

```
user@mac:~$ sudo /var/lib/asgard2-agent/asgard2-agent --uninstall
user@mac:~$ sudo rm -r /var/lib/asgard2-agent/asgard2-agent
user@mac:~$ sudo rm -r /var/lib/thor
```

#### Uninstall ASGARD Service Controller

If you only want to uninstall the ASGARD Service Controller (Aurora), but leave the normal ASGARD Agent as it is, execute the following command:

```
C:\Windows\system32>C:\Windows\System32\asgard2-agent\asgard2-agent_sc.exe -uninstall
```

## 3.4 Asset Management

In the **Assets** view you can see all the connected ASGARD agents. New assets will be placed under **Asset Requests** and need a manual approval before being able to connect to your ASGARD (for auto accept see [Advanced Settings](#)).

If the **Duplicate Assets** view is visible, you should try to remediate the issues in a timely manner, since this might cause unwanted side effects on the duplicate hosts.

**Warning:** Assets in the **Duplicate Assets** view indicate that one or more agents are running on multiple endpoints. This might be caused by cloning a system with an already installed ASGARD Agent. Undesirable side effects of duplicate assets are alternating hostnames and tasks that fail immediately.

For remediation please see [Duplicate Assets Remediation](#)

### 3.4.1 Asset Overview

Management of all endpoints registered with ASGARD can be performed in Asset Management. The assets will be presented as a table with an individual ASGARD ID, their IP addresses and host names.

By clicking the control buttons in the **Actions** column, you can start a new scan, run a response playbook, open a command line or switch the endpoints ping rate to a few seconds instead of a maximum of 10 minutes.

#### Note:

- The internal ping between the ASGARD agent and ASGARD is based on HTTPS not ICMP
- Depending on the user's role some of the control buttons may be disabled
- The **Run Scan** button might be greyed out in new installations - this is because ASGARD did not download the THOR packages yet. You can either wait for a few minutes, or see the chapter [Updates of THOR and THOR Signatures](#), to trigger a download manually.

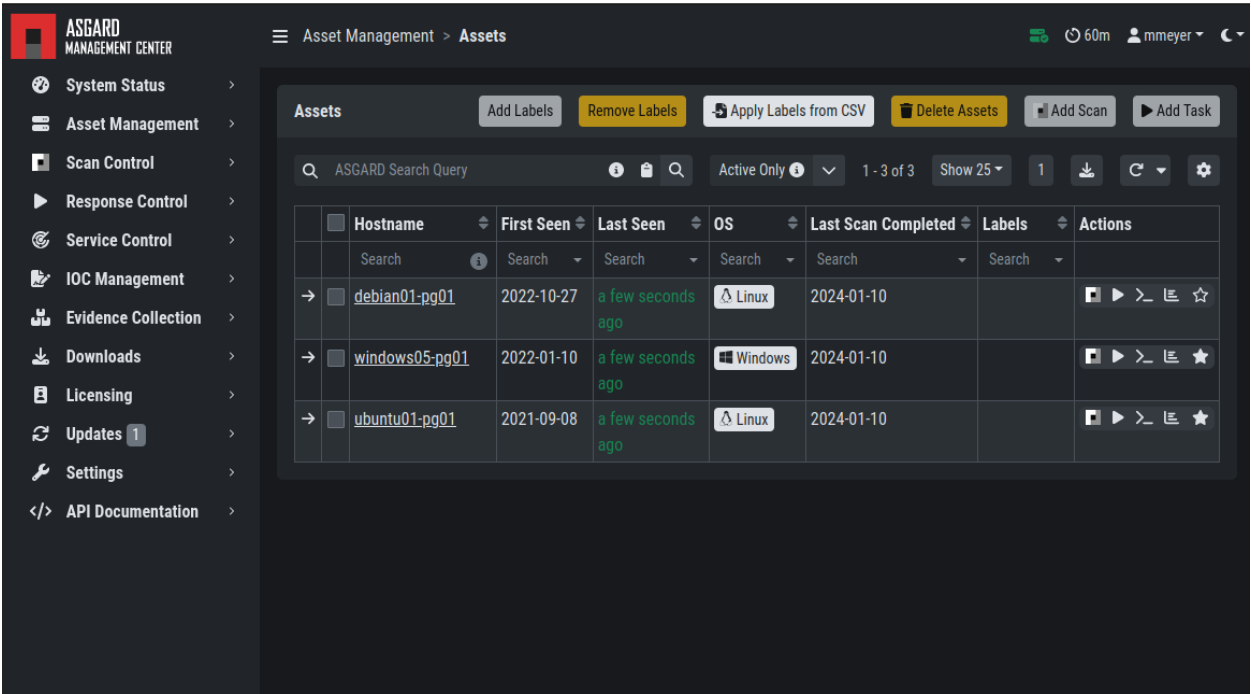


Fig. 8: Asset View

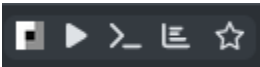


Fig. 9: Available Actions (left to right): Run Scan, Run Task, Connect To Remote Console, Show Timeline, Enable/Disable Fast Poll Mode

### 3.4.2 Column Visibility

Users can select various columns and adjust their view according to their needs by clicking the gear wheel in the top right corner of any table. You can toggle visibility of columns by clicking the icon next to the name. You can also drag and drop the columns to change the order in the table view.

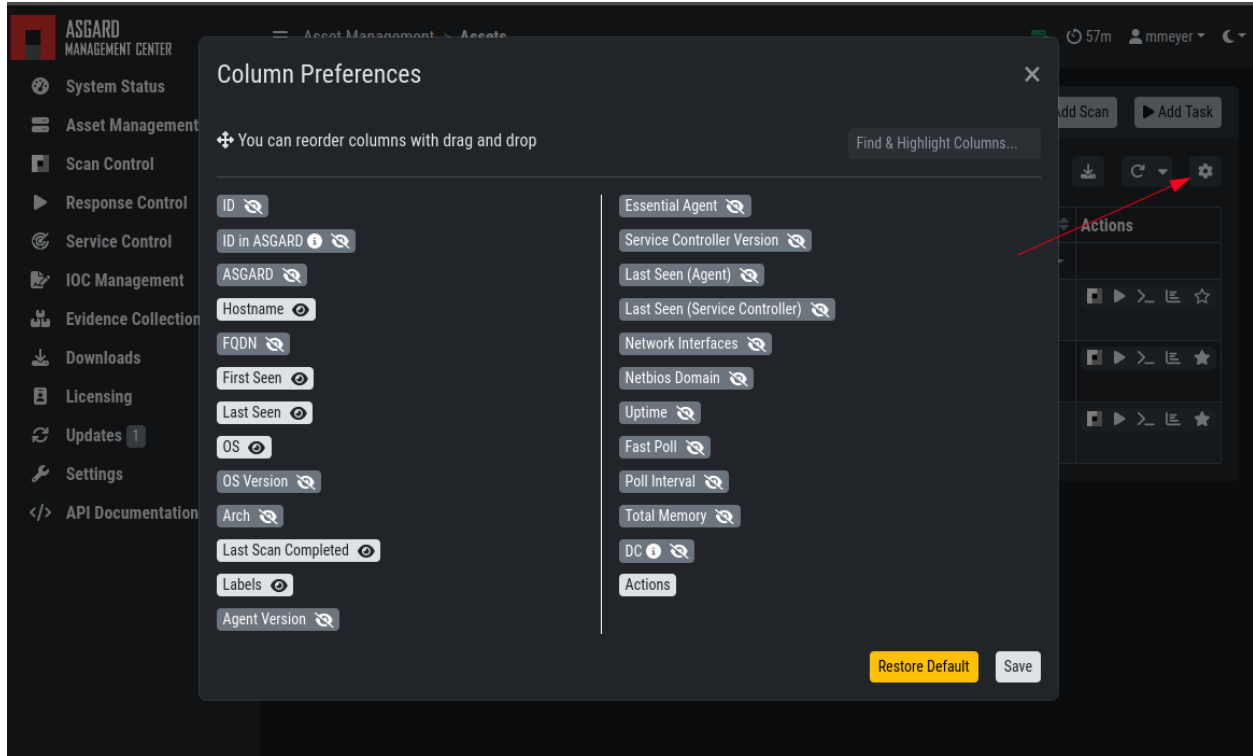


Fig. 10: Available columns in Asset Management

### 3.4.3 Asset Labels

Labels are used to group assets. These groups can then be used in scans or tasks.

You can add multiple labels to an asset or a group of assets. This is done by selecting the particular assets in the left column, typing the label name (e.g. New\_Label) and clicking the blue Add Labels button.

**Note:** Don't use labels with white space characters as it could cause issues in syncs with your Analysis Cockpit, exports/imports or other underlying legacy functions.

In order to remove labels, select your assets, click the yellow Remove Labels button and type the name of the label you want to remove for these assets.

The asset management section has extensive filtering capabilities, e.g. it is easy to select only Linux endpoints that have been online today and have a particular label assigned.

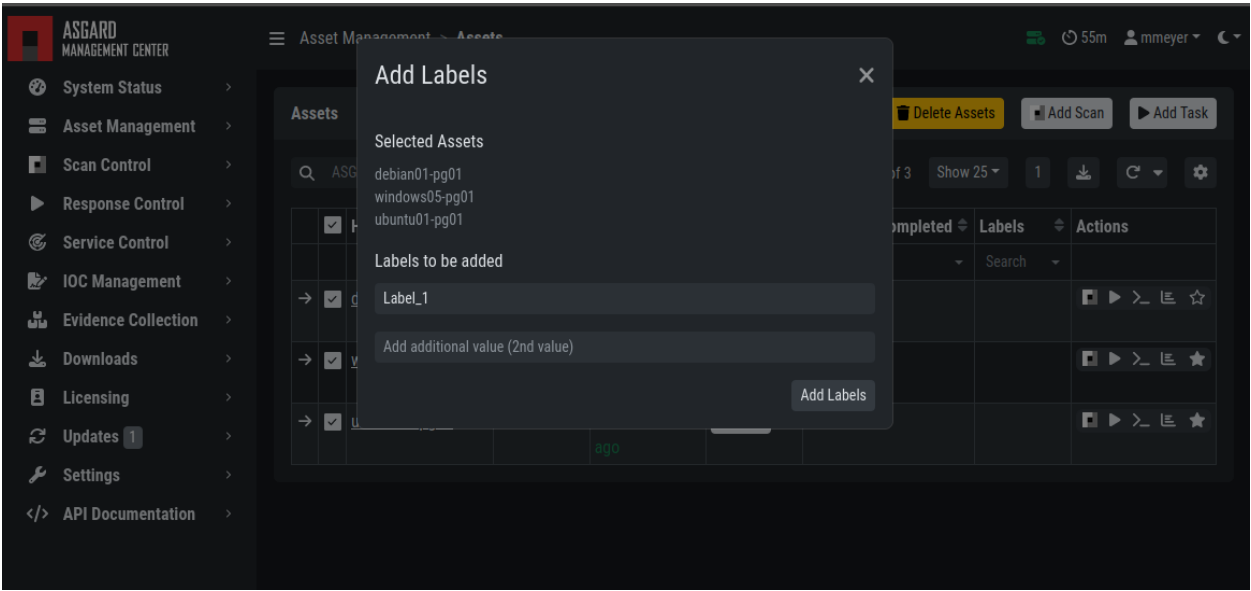


Fig. 11: Add labels

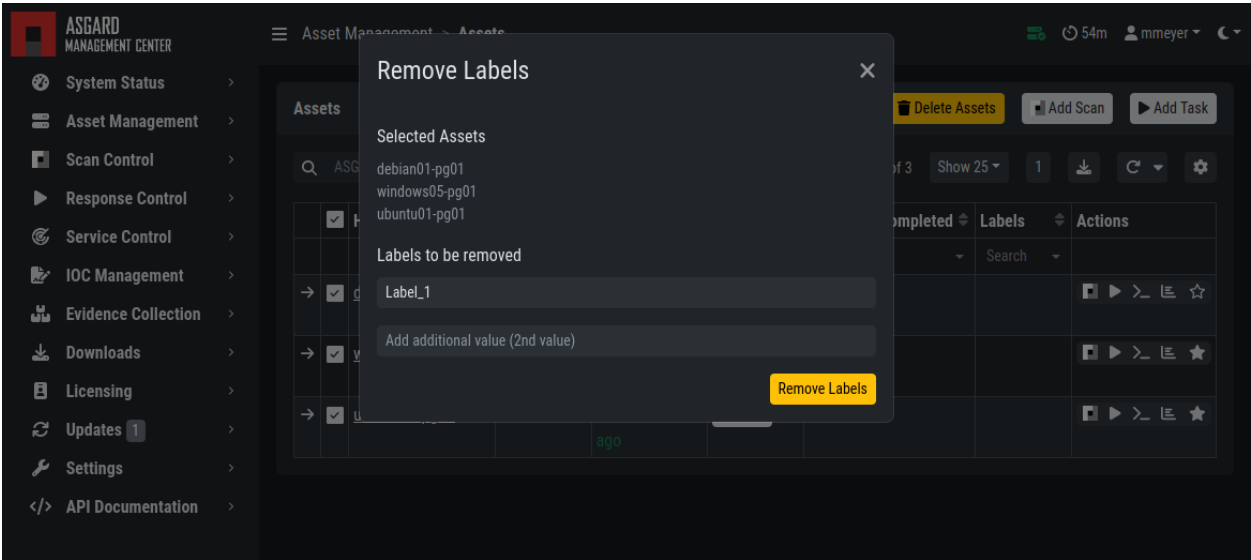


Fig. 12: Remove labels

## Export Asset List

The Import/Export Section allows you to export your assets to a CSV formatted file.

## Import Labels

The import function allows you to add or remove labels on assets based on columns in the previously generated CSV formatted file.

The import function processes the values in the columns **Add Labels ...** and **Remove Labels ...** only. In order to change labels, use the already exported list, add values in these columns and re-import it by using the **Apply Labels from CSV** button. Separate multiple labels with comma. Leading or ending white space characters will be stripped from the labels.

	A	B	C	D	E	F	G	H	I	J
1	ID	Hostname	FQDN	System	Arch	Version	Interfaces	Labels	Add Labels ...	Remove Labels ...
2	7	asgard2-dev	asgard2-dev.	linux	amd64	Debian GNU	127.0.0.1,::1	deb,linux,x64	test, test2	
3	8	centos7-dev	centos7-dev.	linux	amd64	CentOS Linux	127.0.0.1,::1	linux,rpm,x,x64,y		
4	9	win7-1x64-d	win7-1x64-d	windows	amd64	Windows 7 F	fe80::949c:a1	windows,x,x64,y		
5										

Fig. 13: Asset Labeling via CSV

## 3.4.4 ASGARD Search Query

You can search for Assets in your Management Center with the **ASGARD Search Query**. This allows you to write more complex queries to search for assets. Additionally, this helps you to be more flexible with your scan/response tasks, since you can just specify a query and not set labels for all assets first. A good example of this might be if you want to scan a specific subnet every week, and a new agent is being deployed in this subnet. You don't have to think of all the labels or troubleshoot why scans are not being deployed. One example you could achieve this with is the following query:

```
system = "linux" and interfaces = "172.16.50.0/24"
```

This would run the task on all linux systems in the subnet 172.16.50.0/24.

The following operators are available:

Operator	Example
<b>Equals</b>	hostname = "win10-dev"
<b>Equals</b>	cpu_count = 1
<b>Contains</b>	hostname contains "win"
<b>Begins With</b>	hostname begins with "win"
<b>Ends With</b>	hostname ends with "dev"
<b>Numerical Comparison</b>	total_memory >= 4 GB
<b>Numerical Comparison</b>	last_seen < 3 days ago (assets that have not been seen since 3 days)
<b>Numerical Comparison</b>	last_seen > 1 hour ago (assets that have been seen in the last hour)
<b>Numerical Comparison</b>	last_scan_completed < 2022-08-17 (assets that have not been scanned since 2022-08-17)
<b>Numerical Comparison</b>	last_scan_completed < 2022-08-17 15:00:00 (assets that have not been scanned since 2022-08-17 15:00:00)
<b>Numerical Comparison</b>	last_scan_completed is never
<b>Boolean</b>	is_domain_controller is true
<b>Boolean</b>	nextping is true (shows all assets with Fast Poll enabled)
<b>Not</b>	not hostname contains "win"
<b>Not</b>	not hostname ends with "dev"
<b>And</b>	hostname contains "win" and not hostname ends with "dev"
<b>Or</b>	hostname begins with "dev" or hostname ends with "dev"
<b>Nested</b>	hostname ends with "dev" and (hostname contains "win" or hostname contains "lin")
<b>Set / Not Set</b>	labels is set (assets that have at least one label)
<b>Set / Not Set</b>	labels is not set (assets that have no labels)
<b>Regular Expression</b>	hostname matches "[a-z0-9]{(0,6)}\$"
<b>Pattern</b>	Use _ to match any single character and % to match an arbitrary number of characters, including zero characters.
<b>Pattern</b>	arch like "a__64" (matches amd64 and arm64, but not aarch64)
<b>Pattern</b>	arch like "%64" (all 64 bit systems, e.g. amd64, arm64, aarch64 or ppc64)
<b>IP Range</b>	interfaces = "172.28.30.0/24"

You can create simple or complex queries this way. You can group/separate queries with brackets:

```
(system = "linux" and interfaces = "172.28.30.0/24") or (system = "windows" and
interfaces = "172.28.50.0/24")
```

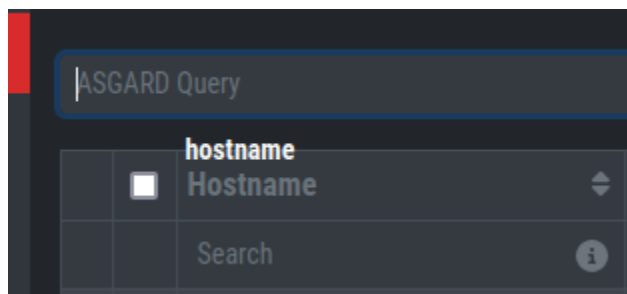
```
(system = "linux" and interfaces = "172.28.30.0/24" and labels = "my-label") or labels =
"robot-test"
```

The following keys for the asset query are available:



Key	Column Name
arch	Arch
client	Agent Version
client_sc	Service Controller Version
first_seen	First Seen
fqdn	FQDN
hostname	Hostname
id	ID
interfaces	Network Interfaces
is_domain_controller	DC
labels	Labels
last_scan_completed	Last Scan Completed
last_seen_agent	Last Seen Agent
last_seen	Last Seen
last_seen_sc	Last Seen Service Controller
nextping	Fast Poll
ping_interval	Poll Interval
system	OS
total_memory	Total Memory
uptime	Uptime
version	OS Version

**Hint:** You can see which query-name a field has by enabling the column in your asset view and clicking into the query text field:



The ASGARD Search Query is the preferred tool to manage scans and assets. If you are using the Analysis Cockpit and need to labels, you can still use them.

### 3.4.5 Asset Migration

You can move an asset from one Management Center to another via the Maintenance Module of the Response Control. To do this, navigate to **Assets** and select the assets you want to migrate. Alternatively you can navigate to **Response Control** and add a new task. You can now click the **Add Task** button to open the Task Menu. Choose the **Maintenance** module and then the **Move asset to another ASGARD Type**. You have to upload an agent installer from the ASGARD you want to migrate the asset to.

**Note:** The target OS or Arch of the installer doesn't matter, we will only use the installers configuration data for the migration.

The task will fail if the migrated asset is unable to communicate with the new Management Center. In this case, the asset will remain on the Management Center which issued the migration task. Only the asset will be migrated (it shows up as a brand new asset on your new Management Center), no scan or response tasks and also no logs will be migrated.

### 3.4.6 Delete Assets

Deleting assets will remove the assets from the **Active Only** asset view and will invalidate the authentication for those assets.

To delete an asset, go to the **Assets View** and mark the assets you want to delete. Click the **Delete Assets** Button on the top right corner. Confirm that you want to delete the assets.

To see all the deleted assets, change your view from **Active Only** to **Deleted Only**.

**Warning:** Deleted assets can no longer communicate with the ASGARD. Please use with caution. This cannot be undone, you have to manually fix the asset.

## 3.5 Scan Control

The Scan Control in your Management Center allows you to run different kind of scans on one or multiple assets. Additionally, you can create **Scan Templates** to use with new scans, so all your default options won't need to be configured for every new scan. You can also use **Scan Templates** to only allow certain users to execute new scans with them. **False-Positive Filters** can be set to exclude certain files from scan results, or even whole directories.

Your Management Center will also take care of THOR scans which stopped (e.g. the asset rebooted or lost connection to your Management Center during a scan), so that a scan will not fail if the asset is temporarily offline.

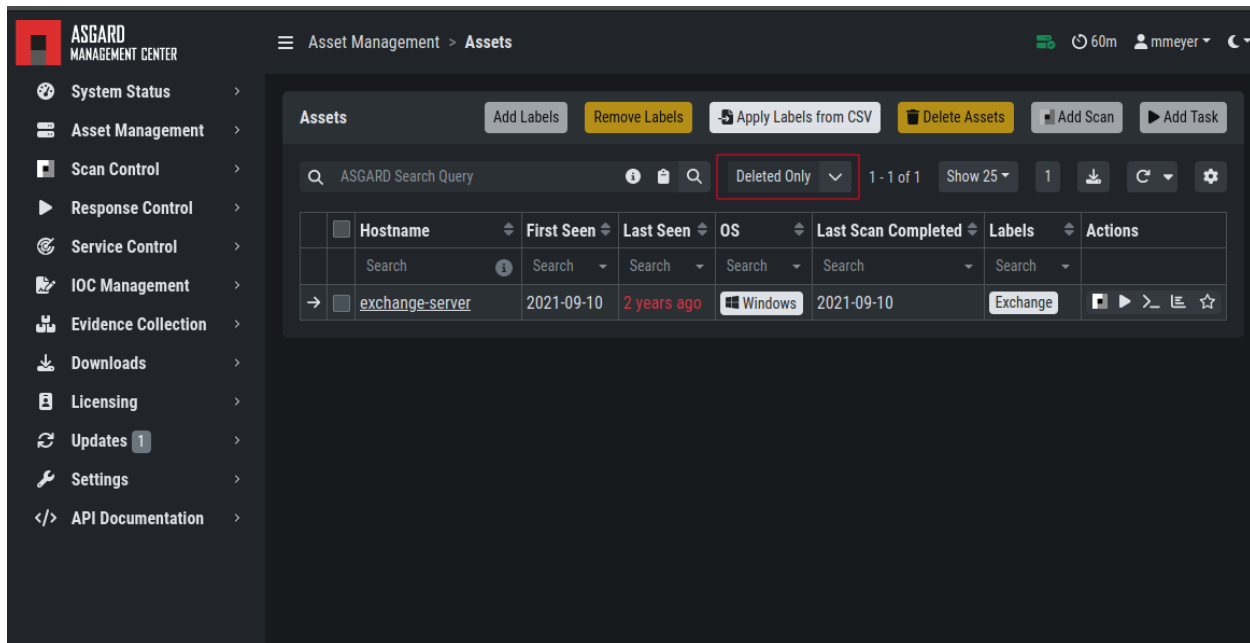


Fig. 14: Deleted Assets View

**Warning:** When creating a scan job, the Management Center offers almost all possible scan options that can be used with THOR. Please consider their use with care as there are options that may lead to incompatibilities, failing scans, or errors.

- Example 1: A combination of `--truncate 0` and `--allreasons` may lead to very long THOR event log lines (> 64 KB), which **cannot be processed by the Analysis Cockpit properly**.
- Example 2: The use of the `--processdump` flag will create files on endpoints that are **not** automatically cleaned up.

All options can be used in certain scenarios, but they have to be chosen with care.

### 3.5.1 Managing Scan Templates

Scan templates are the most convenient way to make use of THOR's rich set of scan options. It is possible to define scan parameters for THOR 10 and store them in different templates for later use in single scans and grouped scans. The scan templates are also very helpful if you want to automate scanning via the API, as you don't have to specify all the options, but rather only the template. This also means you don't have to change your API request, but only the template.

Imagine you want to use dedicated scan options for different system groups (e.g. Linux Servers, Domain Controllers, Workstations, etc.) and make sure to use exactly the same set of scan options every time you scan a particular group of systems. With your Management Center you can now add a scan template for every group.

A popular use case for scan templates is providing additional resource control – for example telling THOR to set the lowest process priority for itself and never use more than 50% of CPU.

Please keep in mind, that we have already optimized THOR to use the most relevant scan options for a particular system (based on type, numbers of CPUs, and system resources) and a comprehensive resource control is enabled by default.

For more details please refer to the [THOR manual](#). Only use the scan templates if you want to deviate from the default.

Scan templates are protected from being modified by users without the Manage Scan Templates-permission, and can also be restricted from being used by users in case the flag Force Scan Template is set for this user. (See section [Restrictions](#) for details).

By clicking the Import Scan Template button you can import a previously exported scan template.

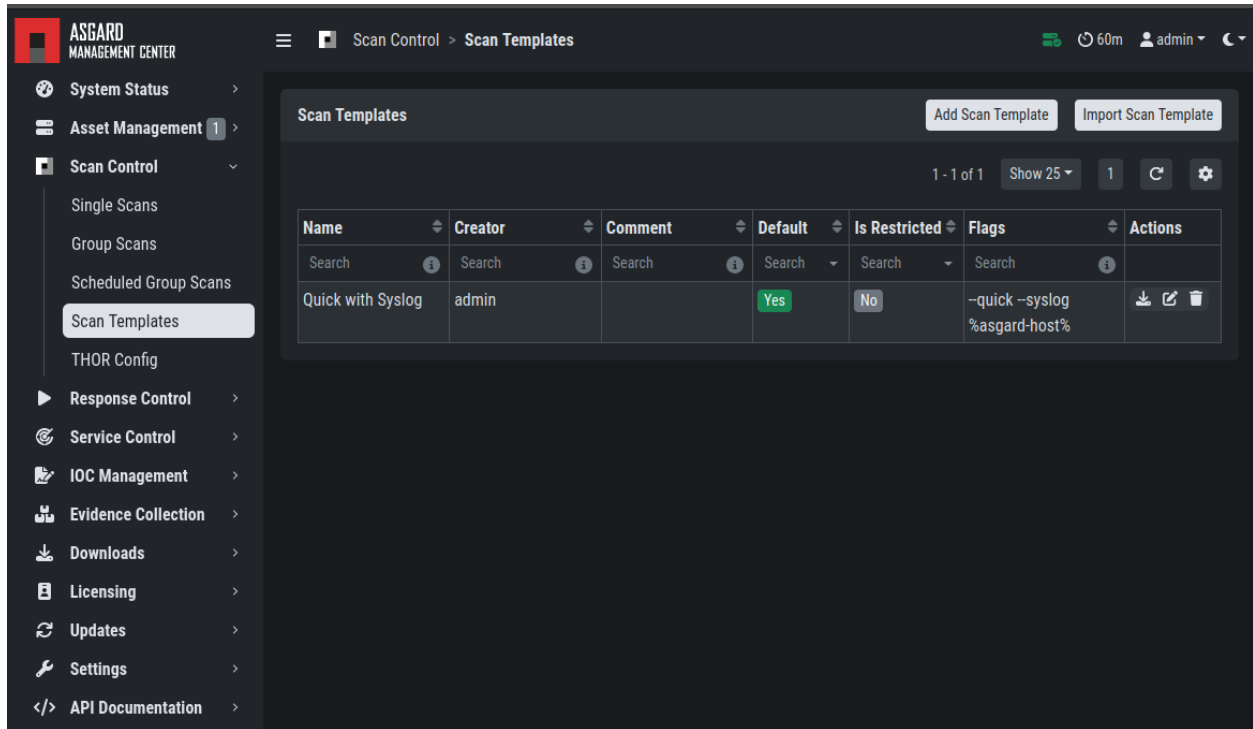


Fig. 15: Scan Templates Overview

In order to create a scan template, navigate to Scan Control > Scan Templates and click the Add Scan Template button. The Add Scan Template dialogue appears. The current THOR scanner version is chosen for you by default but can be changed if needed.

After choosing or changing a scanner you will find the most frequently used options on the top of this page in the "Favorite Flags" category. View all THOR options by clicking on the other categories or quickly search for known flags in the search bar. By clicking on the star symbols you can also edit your personal favorites.

By checking the "Default" box, you can make this scan template the default template for every new scan. There can only be one default template at a time and selecting the box will uncheck a previous default, if set. Checking the "Restricted" flag will make the template restricted, meaning only a restricted set of users can use the template for scans. The set of users consists of all users who do not have the "Force Scan Template" restriction set (by default those are all users who are not a member of the group "Operator Level 1").

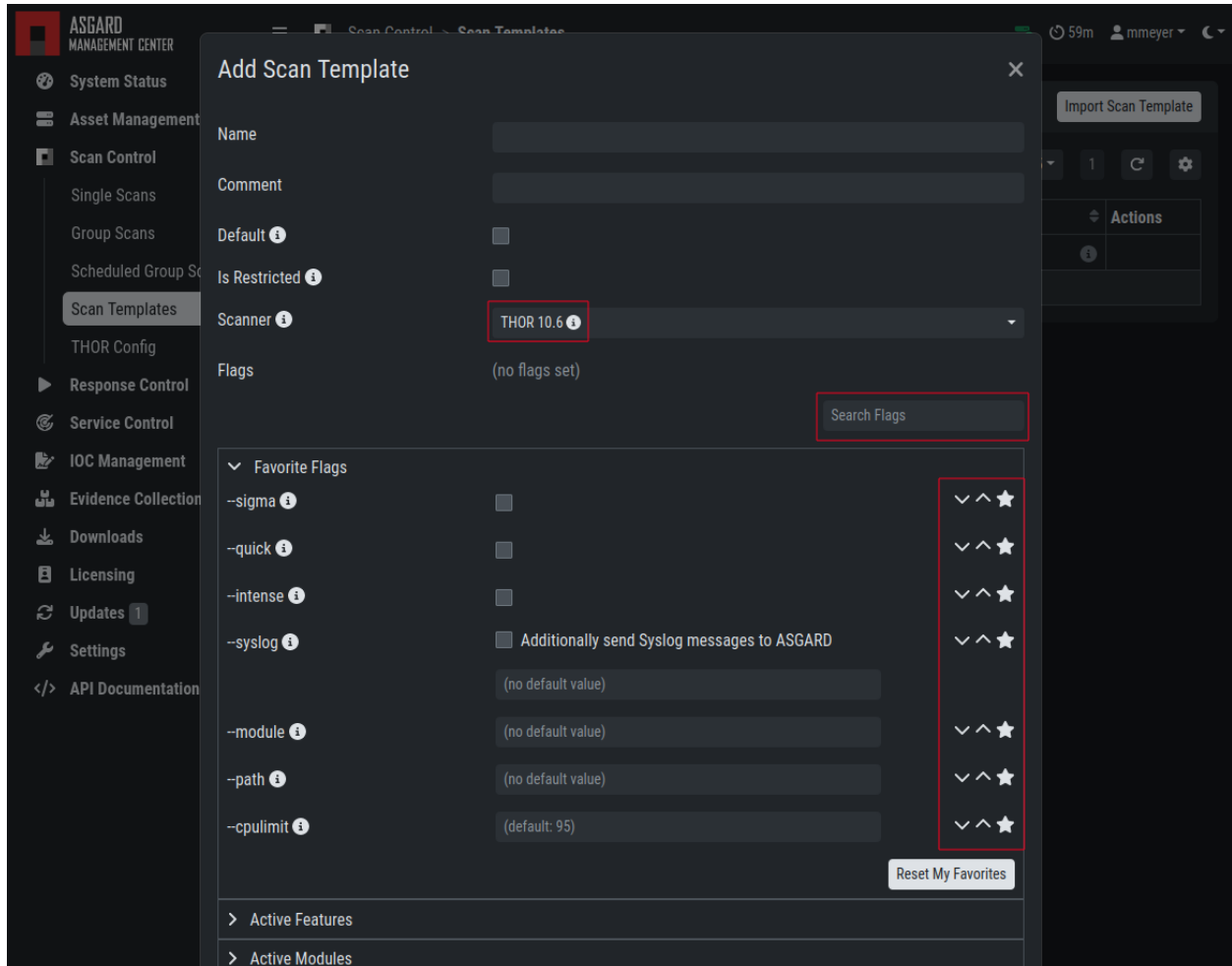


Fig. 16: Scan Flags

### 3.5.2 THOR Excludes and False-Positive Filters

In THOR you can define [directory](#) and [file excludes](#) and [false positive filters](#). With ASGARD 2.13+ these features can be globally defined in ASGARD at Scan Control > THOR Config.

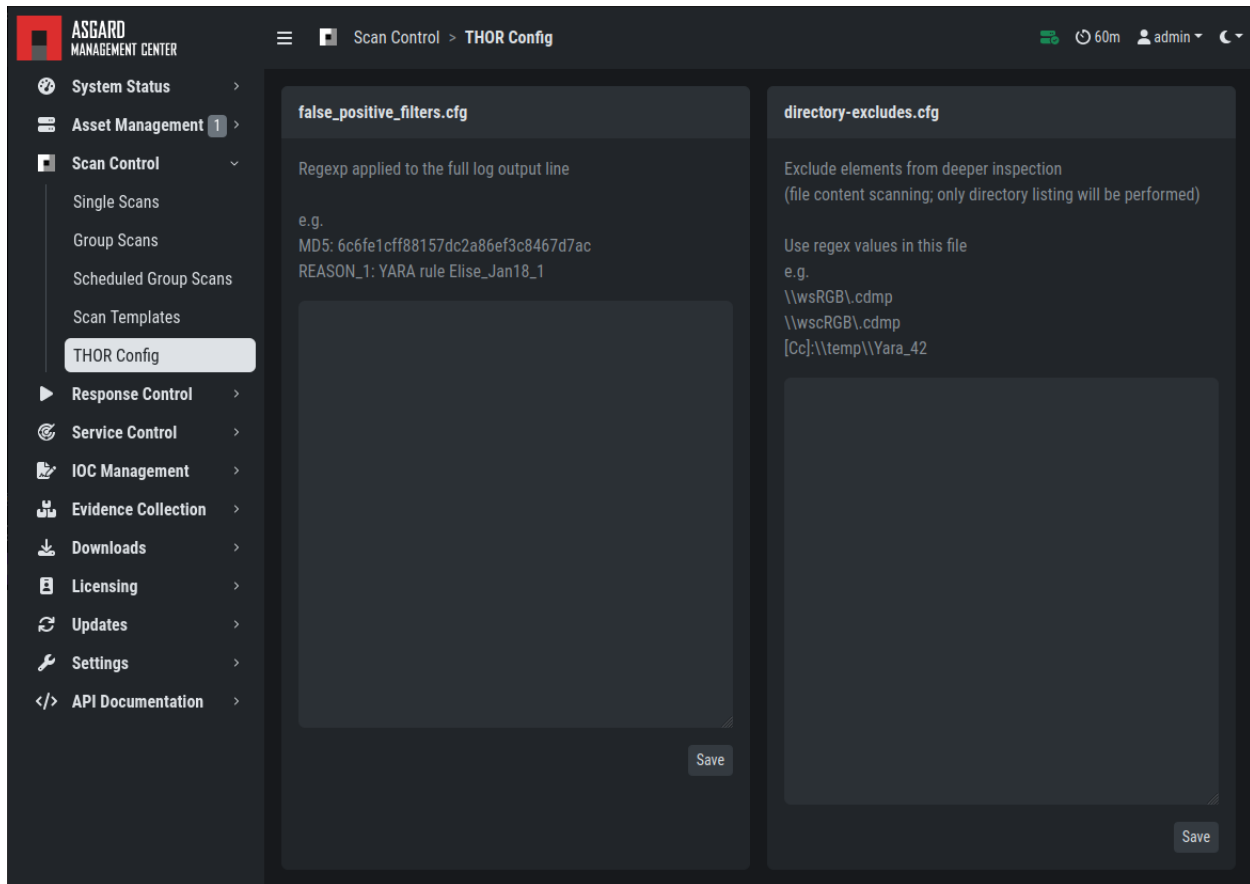


Fig. 17: Scan Control - Global Directory Exclude and FP Filtering

**Warning:** Be careful and do not use too broad filters or excludes, as this might cripple THOR's detection capabilities, if done incorrectly.

## 3.6 Scan a Single System

A single scan or standalone scan is a scan task which is assigned directly to one or more assets. This is meant to be used as a one time scan for a handful of assets.

### 3.6.1 Create a Single Scan

The creation of a scan is performed within the **Assets** view. There is a button for each asset to create a new scan and to show all past scans. You can also assign a single scan to multiple assets. To do this, select your assets and click the **Add Scan** button in the top right corner.

Click on the "THOR" button in the Action column in the Asset Management view.

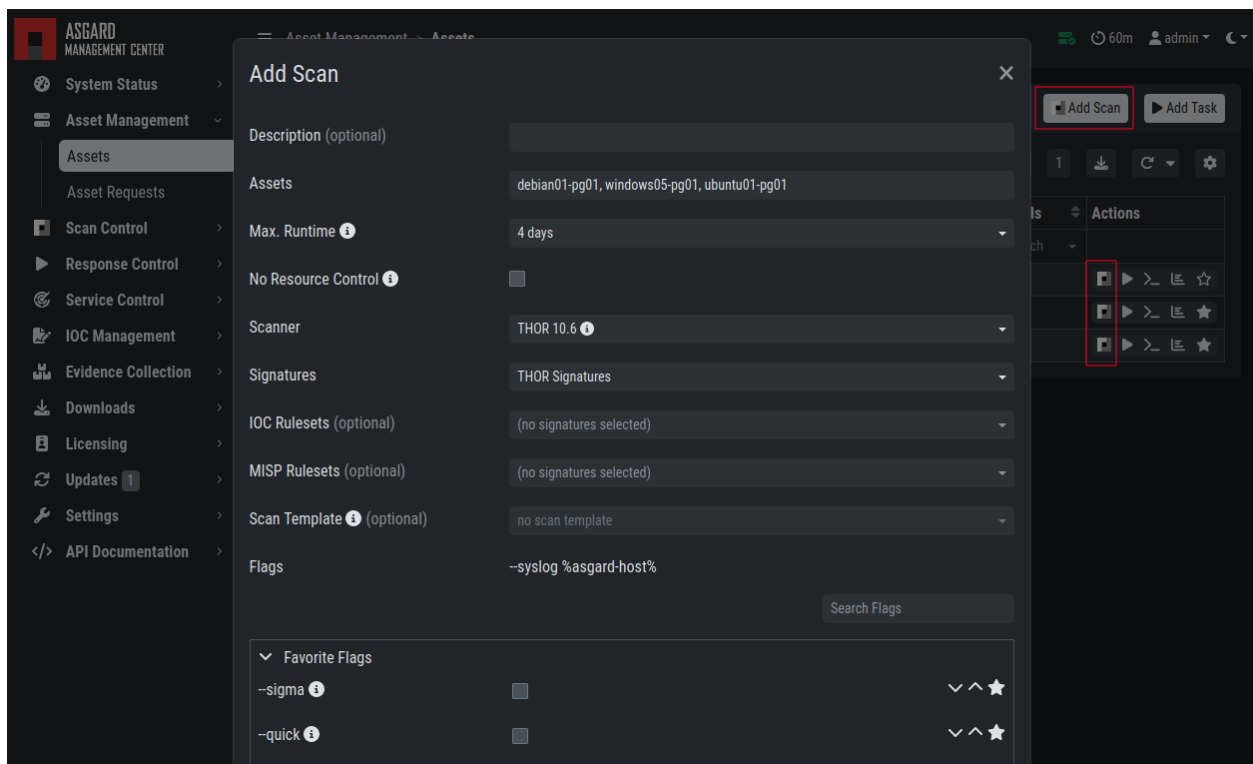


Fig. 18: Scan Control - Scan Creation

Within this form, you can choose the maximum runtime, module, scanner, scan flags, signatures or a template can also be selected.

After the desired parameters have been set, the scan can be started by clicking the **Add Scan** button.

### 3.6.2 Stopping a Single Scan

To stop a single scan, navigate to the "Single Scans" tab in Scan Control section and click the "stop" (square) button for the scan you want to stop.

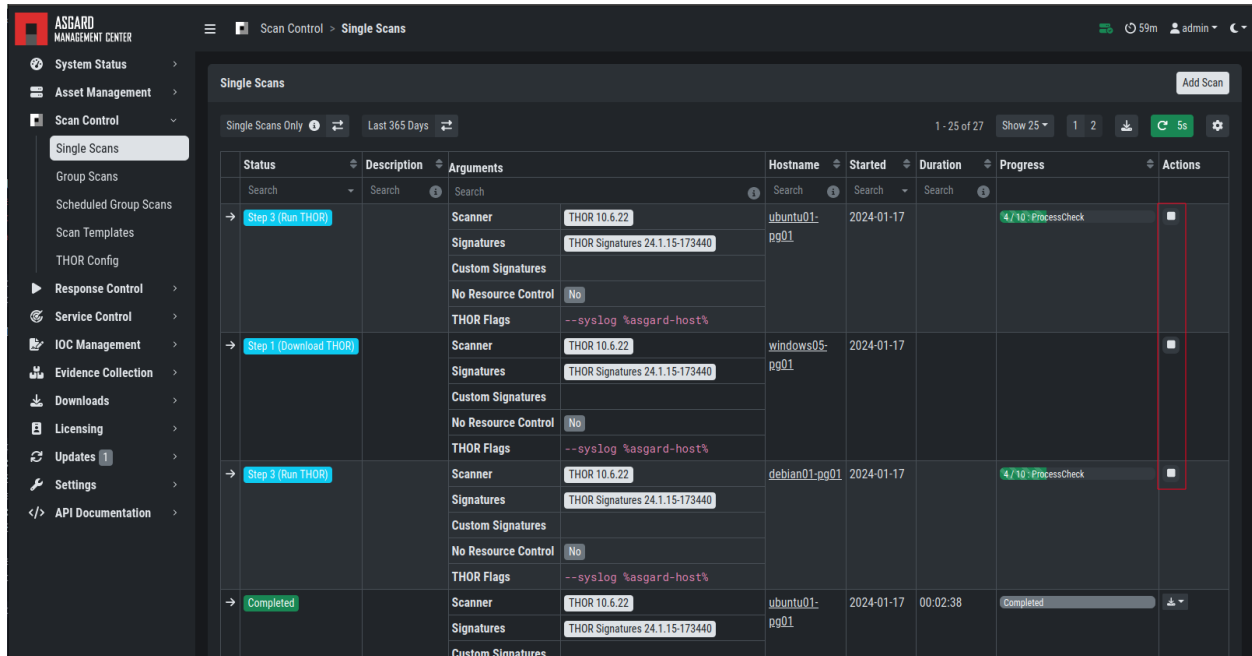


Fig. 19: Stopping a Single Scan

### 3.6.3 Download Scan Results

After the scan completion, you can download the scan results via the download button in the actions column.

The download button has the following options:

- Download Scan Result as TXT (the THOR text log file)
- Download Scan Result as JSON (only available if it was started with the `--json` flag)
- Download HTML Report (as \*.gz compressed file; available for successful scans only)
- Show HTML Report (opens another tab with the HTML report)

## 3.7 Scan a Group of Systems

A group scan is a scan task which is assigned to one or more asset **condition**. Those conditions can either be labels or the ASGARD Search Query. This is meant to be used if you want to scan a large group of assets with one scan configuration.



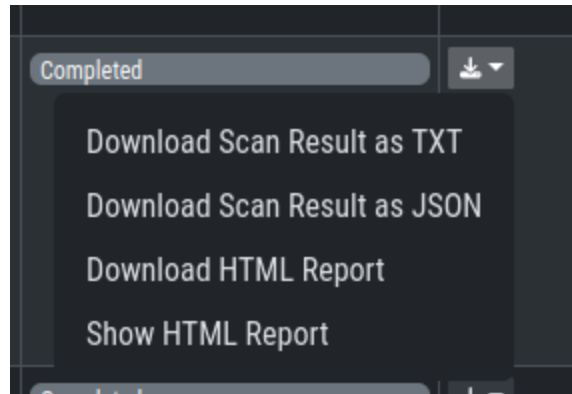


Fig. 20: Scan Control - Download Scan Results

### 3.7.1 Create Group Scans

A scan for a group of systems can be created in the Scan Control > Group Scans tab. Click the Add Group Scan button in the upper right corner.

As with the single scans, various parameters can be set. Aside from the already mentioned parameters, the following parameters can be set:

Parameter	Value
<b>Description</b>	Freely selectable name for the group scan.
<b>Scan Target</b>	Here you can define which assets will be assigned the group scan. You can either use the Simple target option, which uses labels, or you can use the Advanced target options, which makes use of labels or the ASGARD Search Query. Leaving this option empty will scan all assets.
<b>Limit</b>	ASGARD will not send additional scans to the agents when the client limit is reached. Therefore you need to set a limit higher than the number of hosts you want to scan or enter 0 for no limit. If you are using MASTER ASGARD, this limit is applied on each single selected ASGARD.
<b>Rate</b>	The number of scans per minute that are issued by ASGARD. This is where the network load can be controlled. Additionally, it is recommended to use this parameter in virtualized and oversubscribed environments in order to limit the number of parallel scans on your endpoints.
<b>Expires</b>	After this time frame, no scan orders will be issued to the connected agents.
<b>Scheduled Start</b>	Select a date for a scheduled start of the scan.

After the group scan has been Saved or Saved and Started, you will automatically be forwarded to the list of grouped scans.

Add Group Scan

Description (optional)

Scan Target ⓘ (optional)

Germany (2 assets) ×

Advanced

Expires ⓘ

2024-01-24 11:00:00

Scheduled Start (optional)

Select a date for scheduled start (optionally)

Clear

Limit ⓘ

100

Rate

1 per minute

Max. Runtime ⓘ

4 days

No Resource Control ⓘ

☐

Scanner

THOR 10.6 ⓘ

Signatures

THOR Signatures

IOC Rulesets (optional)

(no signatures selected)

MISP Rulesets (optional)

(no signatures selected)

Scan Template ⓘ (optional)

no scan template

Flags

--syslog %asgard-host%

Search Flags

Fig. 21: Scan Control – Create Group Scan

### 3.7.2 List of all Group Scans

The list of all group scans contains, among other items, the unique Scan-ID and the name.

Status	Description	Arguments	Active Since	Issued	Completed	Actions
Active	Weekly-Scanner-Clients	Scanner: THOR 10.6 Signatures: THOR Signatures Custom Signatures: No Resource Control: No THOR Flags: --quick --sigma --syslog %asgard-host%	2024-01-10	3	3	[Icons]
Completed	Weekly-Scanner-Clients	Scanner: THOR 10.6 Signatures: THOR Signatures Custom Signatures: No Resource Control: No THOR Flags: --quick --sigma --syslog %asgard-host%	2024-01-03	3	3	[Icons]
Completed	Weekly-Scanner-Clients	Scanner: THOR 10.6 Signatures: THOR Signatures Custom Signatures: No Resource Control: No THOR Flags: --quick --sigma --syslog %asgard-host%	2023-12-27	3	3	[Icons]

Fig. 22: Scan Control – Group Scans – List

In addition, information can be found about the chosen scanner, the chosen parameters, the start and completion times and the affected assets (defined by labels). Additional columns can be added by clicking on "Column Visibility".

The Status field can have the following values:

Status	Value
<b>Paused</b>	The group scan has not yet started. Either click play or wait for the scheduled start date (the job will start in a 5 minute window around the scheduled time).
<b>Active</b>	Scan is started, ASGARD will issue scans with the given parameters.
<b>Inactive</b>	No additional scan jobs are being issued. All single scans that are currently running will continue to do so.
<b>Completed</b>	The group scan is completed. No further scan jobs will be issued.

### 3.7.3 Starting a Group Scan

A group scan can be started by clicking on the "play" button in the "Actions" column of a group scan. Subsequently, the scan will be listed as "Started".

### 3.7.4 Details of a Group Scan

Further information about a group scan can be observed from the detail side bar of the group scan. Click the arrow in the left column of the group scan you are interested in and the details section will appear on the right side of the window.

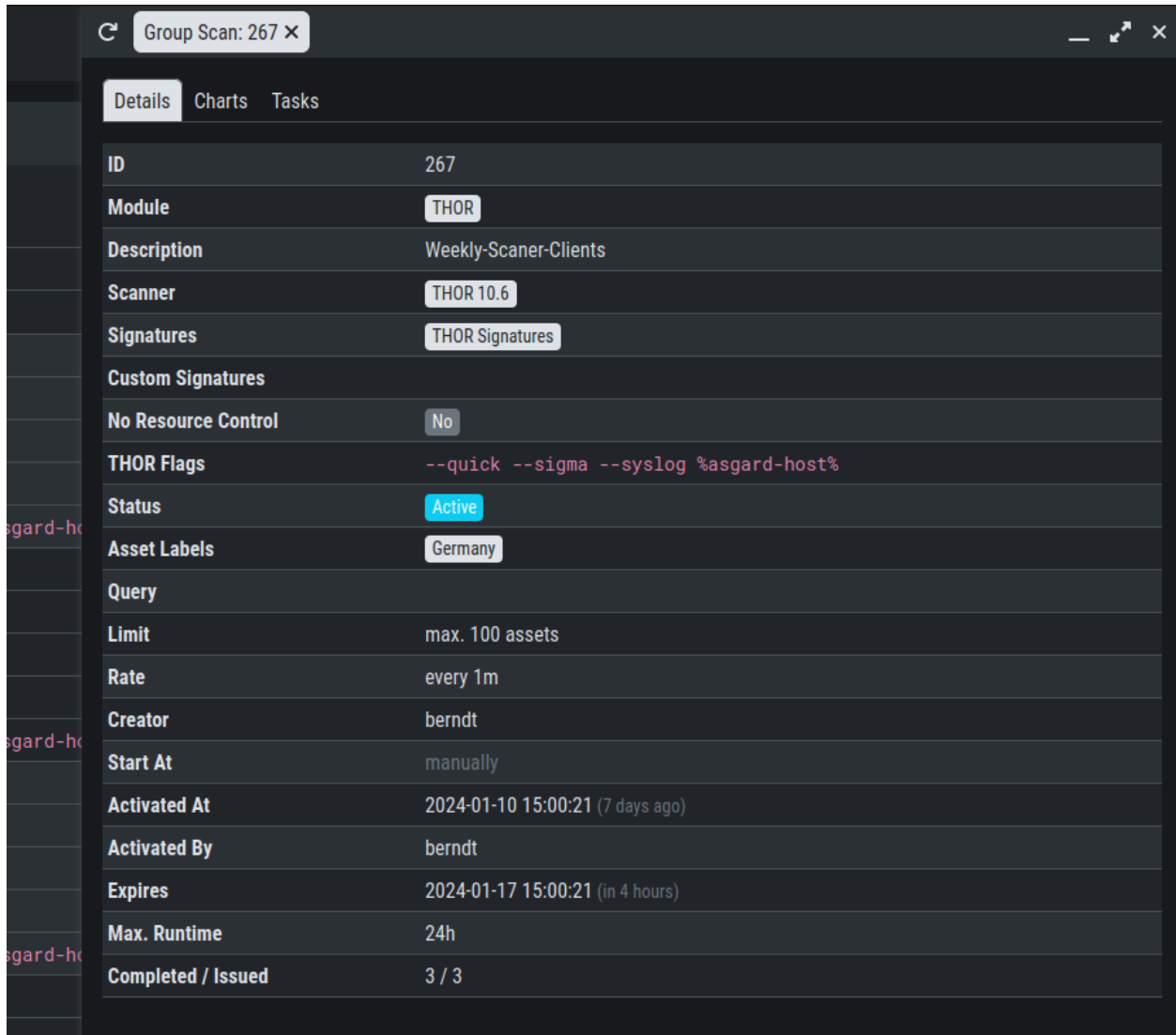
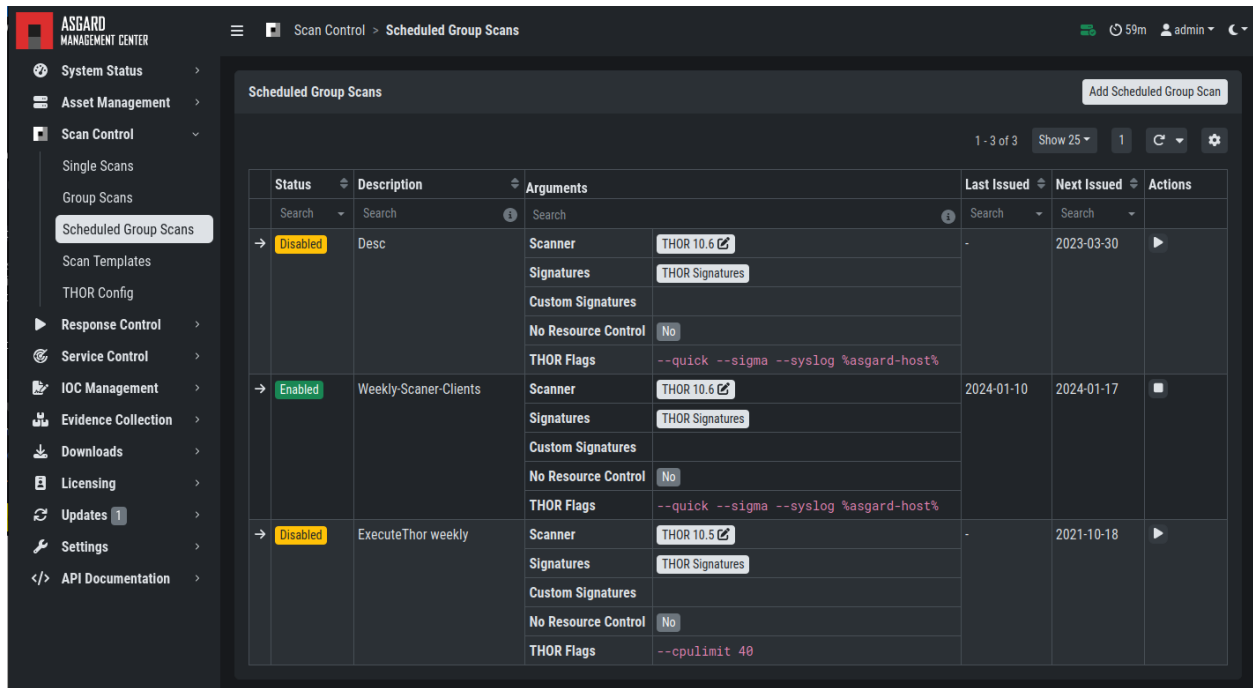


Fig. 23: Scan Control – Group Scans – Details

Aside from information about the group scan in the "Details" tab, there is a graph that shows the number of assets started and how many assets have already completed the scan in the "Charts" tab. In the "Tasks" tab you get information about the scanned assets.

## 3.8 Scheduled Group Scan

The Scheduled Group Scan section shows all scans that are to run on a frequent basis along with their periodicity. All group scans that have been started through the scheduler will show up on top of the Group Scan section the moment they are started. New scheduled tasks can be created by clicking the Add Scheduled Group Scan button.



Status	Description	Arguments	Last Issued	Next Issued	Actions
→ Disabled	Desc	Scanner: THOR 10.6 Signatures: THOR Signatures Custom Signatures: No Resource Control: No THOR Flags: --quick --sigma --syslog %asgard-host%	-	2023-03-30	▶
→ Enabled	Weekly-Scanner-Clients	Scanner: THOR 10.6 Signatures: THOR Signatures Custom Signatures: No Resource Control: No THOR Flags: --quick --sigma --syslog %asgard-host%	2024-01-10	2024-01-17	▶
→ Disabled	ExecuteThor weekly	Scanner: THOR 10.5 Signatures: THOR Signatures Custom Signatures: No Resource Control: No THOR Flags: --cpulimit 40	-	2021-10-18	▶

Fig. 24: Scan Control – Scheduled Group Scan

## 3.9 Syslog Forwarding

**Hint:** This chapter is optional

To configure Syslog Forwarding of logs, you can set the `--syslog` flag during scans. You have multiple options as to where you can send the logs.

The `--syslog` value is constructed of the following arguments. Please keep in mind that the fields need to be in the correct order. Values are separated with the colon sign :

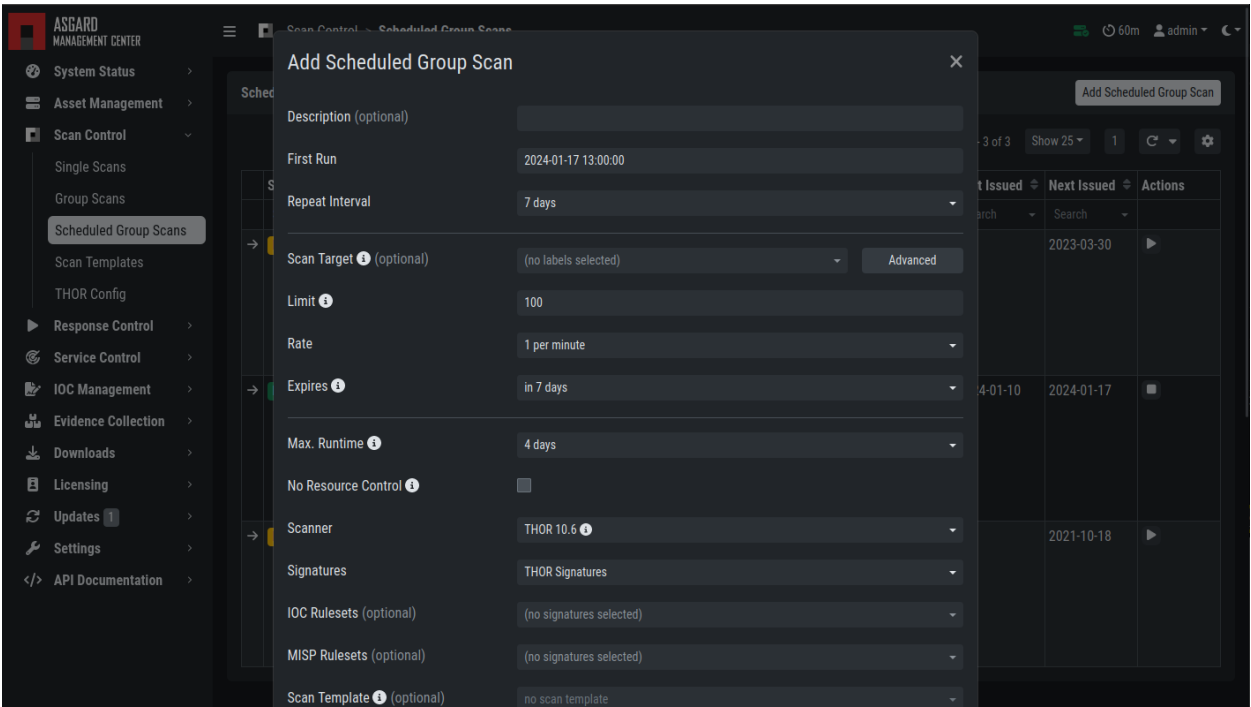
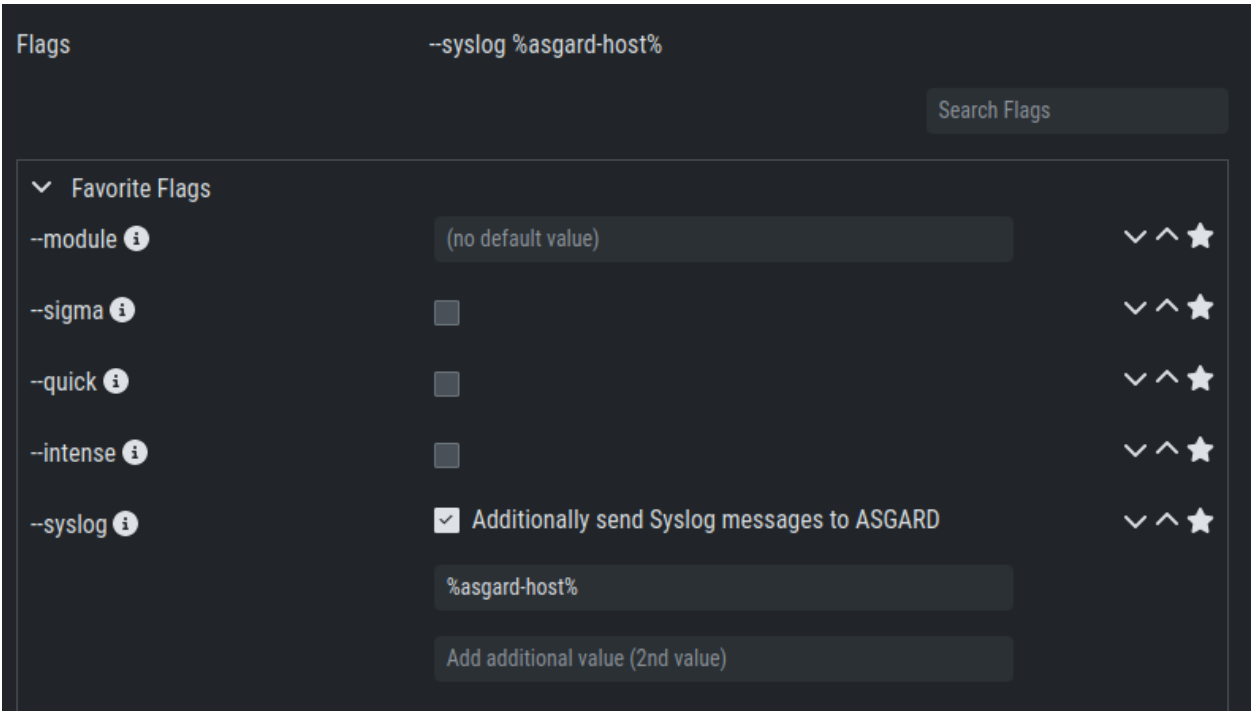


Fig. 25: Scan Control – New Scheduled Group Scan



Pos.	Field	Description	Possible Values
1	Server	The receiving server, %asgard-host% is the ASGARD which issued the Scan for the Agent	FQDN or IP of remote host
2	Port	<b>optional</b> - the listening port on the remote system, default is 514	1 - 65535
3	Format	<b>optional</b> - the log format, default is DEFAULT	- DEFAULT <sup>1</sup> - CEF - JSON - SYSLOGJSON - SYSLOGKV
4	Socket	<b>optional</b> - The socket type, default is UDP	- UDP - TCP - TCPTLS

**Hint:** The syslog listener on the Management Center is running on port UDP/514.

Examples:

- `cribl.local:6514`
- `172.16.20.10:514:SYSLOGKV:TCP`
- `rsyslog-forwarder.dom.int:514:JSON:TCP`
- `arcsight.dom.int:514:CEF:UDP`

If you choose to use the `--syslog` flag, please make sure that the necessary ports are allowed within your network/firewall. If you decide to forward your logs via ASGARD to a SIEM, please have a look at [Rsyslog Forwarding](#).

**Note:** If Syslog Forwarding is selected for a new THOR Scan, the default target will be set to %asgard-host%, which is your Management Center. Syslog Forwarding is optional and you do not lose any functionality if you are not using it (in most cases). If you want to forward logs in real-time from your Management Center to a SIEM (for example), you do however have to enable Syslog Forwarding.

Please see [Rsyslog Forwarding](#) for more information

## 3.10 Response Control

The Response Control is used to execute tasks on your agents. Those tasks can be:

- Run Playbook (pre-defined or custom)
- Run Interrogate (collect system information)
- Open Remote Console
- Maintenance
  - Upgrade Agent
  - Upgrade Service Controller

<sup>1</sup> This is the default log format of THOR.

- Configure the asset's proxy
- Move asset to another ASGARD

## 3.10.1 Opening a Remote Console on an endpoint

In order to open a remote console on an endpoint, open the Asset Management section and click the "command line" button in the Actions column.

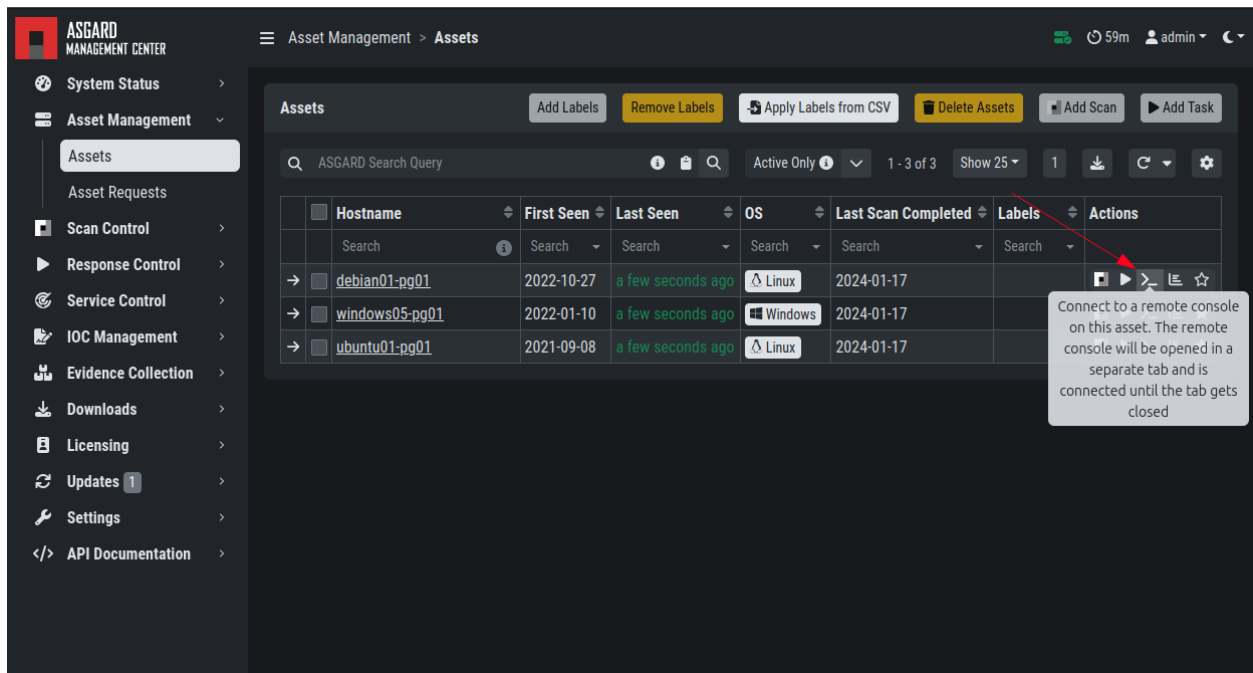


Fig. 26: Opening a Remote Console from the Asset View

Depending on your configuration it may take between 10 seconds and 10 minutes for the remote console to open. Please note that all actions within the remote console are recorded and can be audited. All consoles open with root or system privileges.

In order to replay a remote console session, navigate to Response Control, expand the task that represents your session by clicking the arrow to the left in the tasks row. Select the Console Log tab and click the play button in the bottom row.

ASGARD users can only see their own remote console session. Only users with the View Remote Console Log permission are able to replay all sessions from all users.

---

**Note:** The permission View Remote Console Log requires the Response Control permission.

---



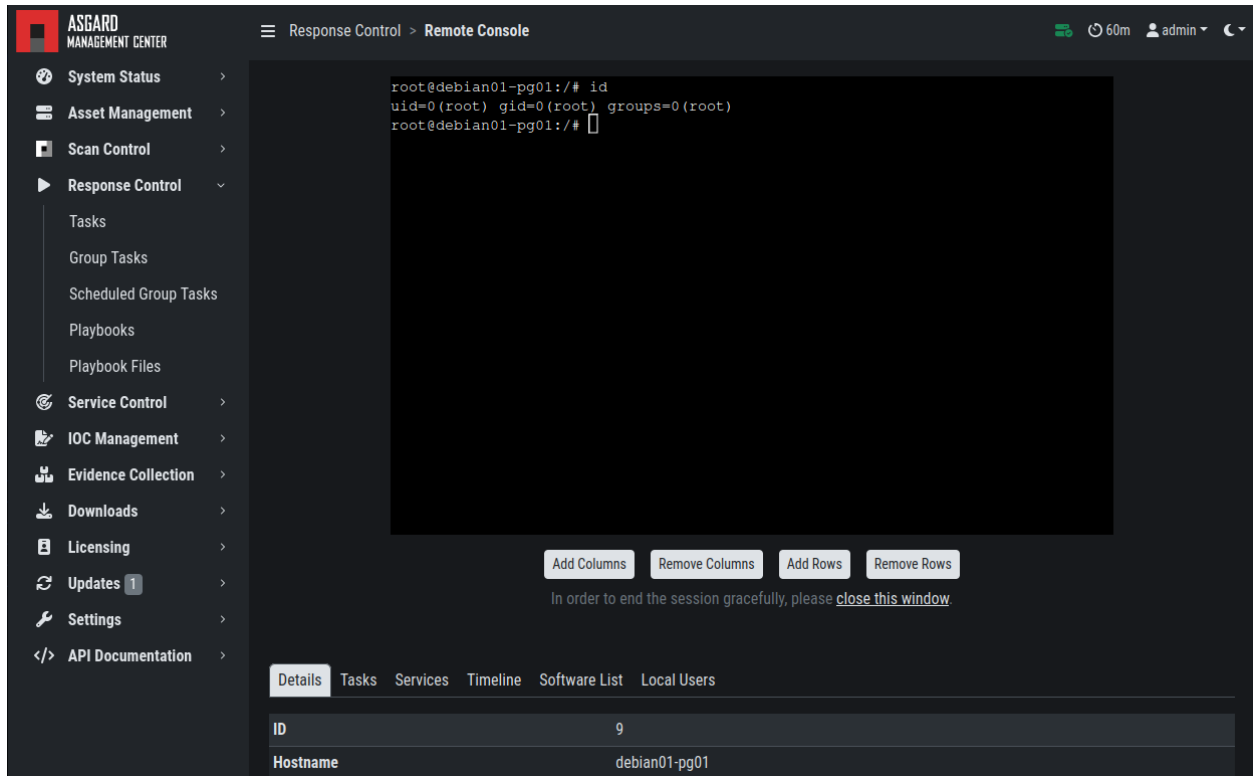


Fig. 27: Remote Shell

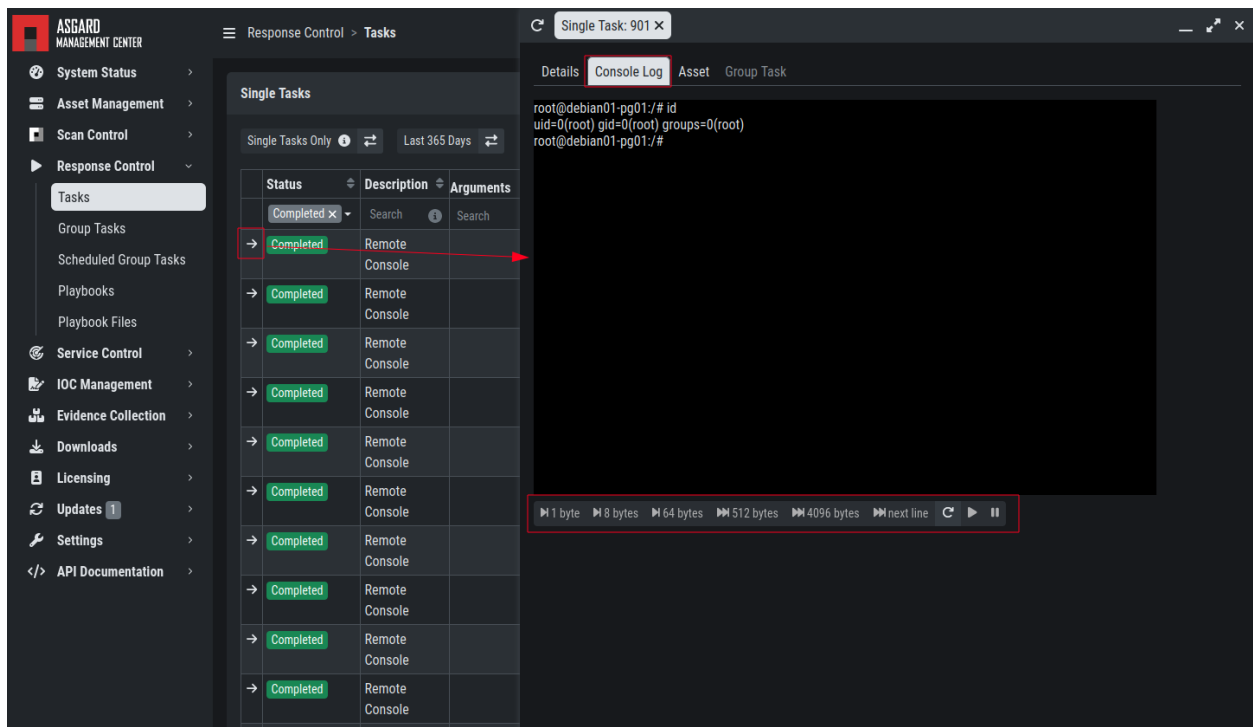


Fig. 28: Replay Remote Shell Session

### 3.10.2 Response Control with Pre-Defined Playbooks

In addition to controlling THOR scans, the Management Center contains extensive response functions. Through your Management Center, you can start or stop processes, modify and delete files or registry entries, quarantine endpoints, collect triage packages and execute literally any command on connected systems. All with one click and executed on one or multiple endpoints at once.

It is also possible to download specific suspicious files. You can transfer a suspicious file to the ASGARD Management Center and further analyze offline.

Name	Steps	Creator	Modified	Actions
Search		asgard	Search	
Collect ASGARD Agent Log	\$ASGARD_WORKING_DIR/log	ASGARD	2022-10-05	
Create and Collect Aurora Agent Diagnostics Pack (Windows)	aurora-agent-util.exe aurora-agent-util.exe diagnostics diagnostics.zip	ASGARD	2022-04-06	
Collect memory (Windows 64-bit)	winpmem_x64.exe winpmem_x64.exe mem.raw    VER>NUL mem.raw	ASGARD	2022-04-06	
Collect memory (Windows 32-bit)	winpmem_x86.exe winpmem_x86.exe mem.raw    VER>NUL mem.raw	ASGARD	2022-04-06	
Install ASGARD Service Controller (Windows 32-bit)	asgard2-service-controller-windows-386.exe asgard2-service-controller-windows-386.exe	ASGARD	2021-11-03	
Install ASGARD Service Controller (Windows 64-bit)	asgard2-service-controller-windows-amd64.exe asgard2-service-controller-windows-amd64.exe	ASGARD	2021-11-03	
Uninstall ASGARD 1 Agent on Linux (RPM)	rpm -e grr	ASGARD	2021-04-06	
Uninstall ASGARD 1 Agent on Linux (DEB)	dpkg --purge grr	ASGARD	2021-04-06	

Fig. 29: Built-in Playbooks

To execute a predefined response action one or more endpoints, navigate to the Assets view and either click the "play" button in the Actions Column, or selected multiple assets and press the "Add Task" button in the top right corner. This will lead you to a dialogue where you can select the desired action.

In this example, we collect the ASGARD Agent Logs.

ASGARD ships with pre-defined playbooks for the following tasks:

- Collect ASGARD Agent Log
- Create and Collect Aurora Agent Diagnostics Pack (Windows only)
- Collect full triage pack (Windows only)
- Isolate endpoint (Windows only)
- Collect system memory
- Collect file / directory
- Collect directory
- Collect Aurora diagnostics pack

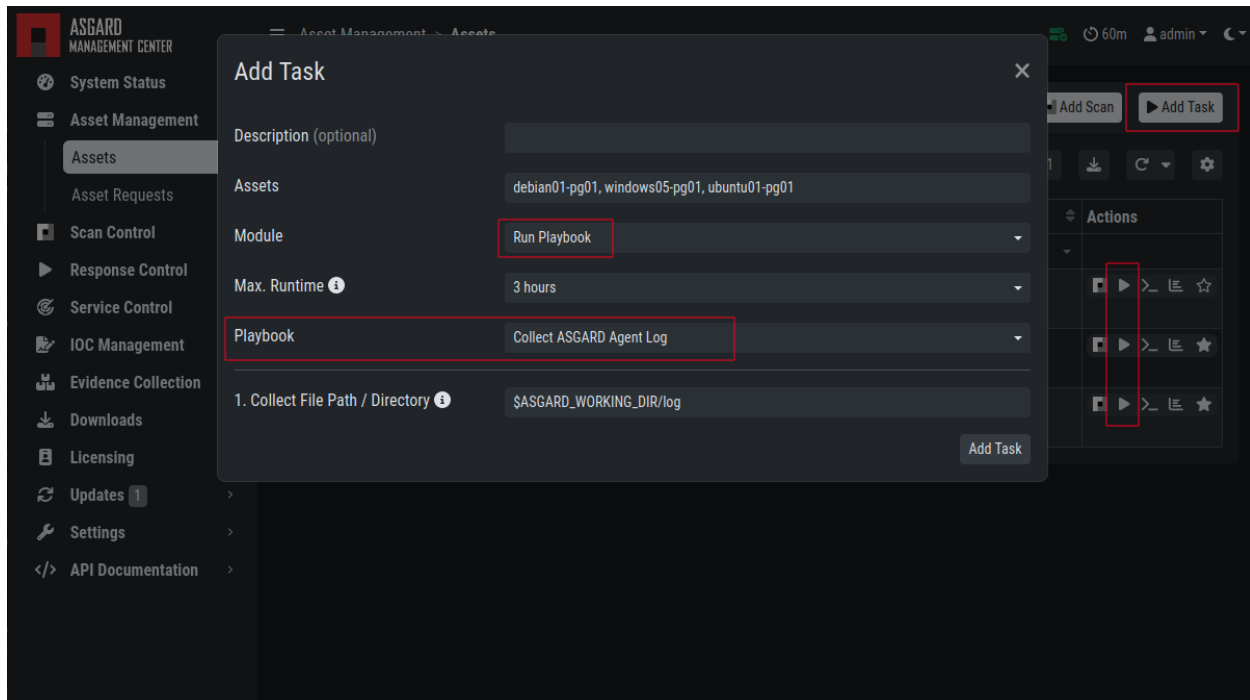


Fig. 30: Execute Playbook on Endpoints

- Execute command and collect stdout and stderr

**Warning:** The collection of memory can set the systems under high load and impacts the systems response times during the transmission of collected files. Consider all settings carefully! Also be aware that memory dumps may fail due to kernel incompatibilities or conflicting security mechanisms. Memory dumps have been successfully tested on all supported Windows operating systems with various patch levels. The memory collection on Linux systems depends on kernel settings and loaded modules, thus we cannot guarantee a successful collection. Additionally, memory dumps require temporary free disk space on the system drive and consume a significant amount of disk space on ASGARD as well. The ASGARD agent checks if there is enough memory on the system drive and adds a 50% safety buffer. If there is not enough free disk space, the memory dump will fail.

### 3.10.3 Response Control for Groups of Systems

Response functions for groups of systems can be defined in the Group Tasks tab or the New Scheduled Group Task tab.

This view should look already familiar, since it is similar to the Group Scan view. You can select the targets by either specifying one or more labels or by making use of the ASGARD Search Query.

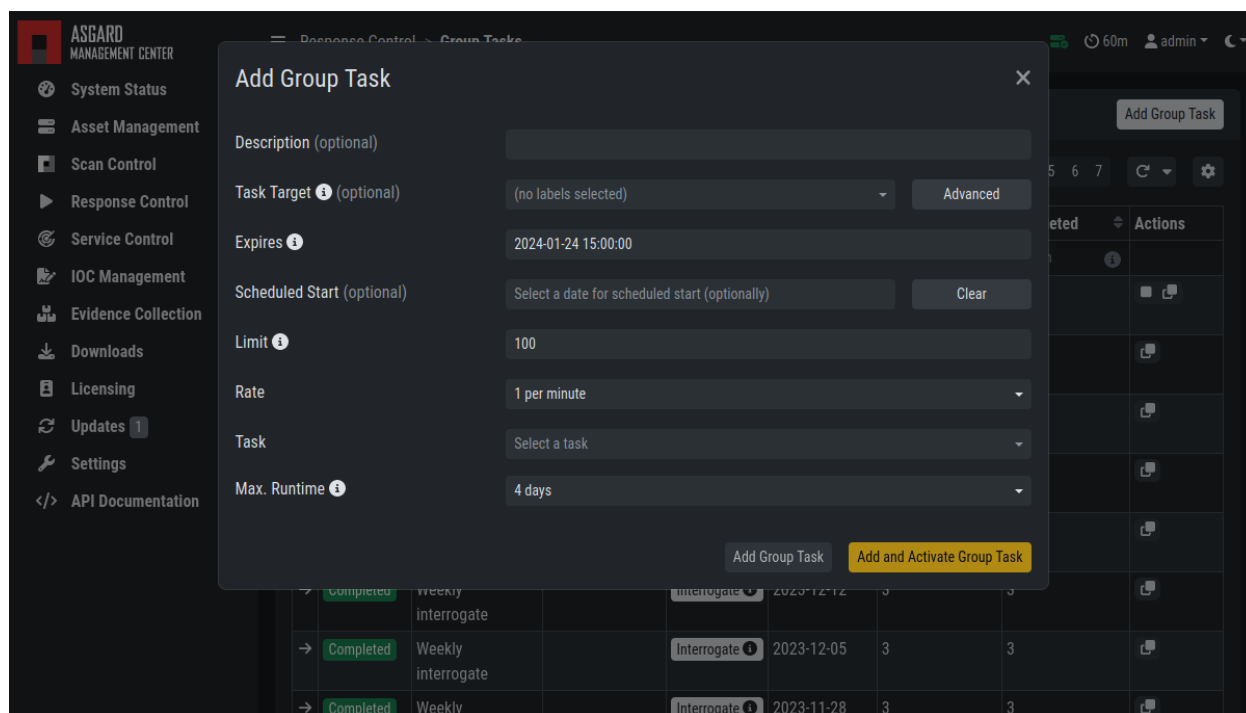


Fig. 31: Execute Playbook on Group of Endpoints

### 3.10.4 Response Control with Custom Playbooks

You can add your own custom playbook by clicking the Add Playbook button in the Response Control > Playbooks tab.

This lets you define a name and a description for your playbook. After clicking the Add Playbook button, click on the Edit steps of this playbook action.

This opens the side pane in which single playbook steps can be added using the Add Step button.

You can do create the following type of Playbook Steps:

- Run Command Line on Endsystem
- Upload File to ASGARD Management Center
- Download File from ASGARD Management Center

This allows you to download files from the Management Center to your endpoint and vice versa. This way you can directly collect evidence from your endpoints.

If you need custom files for your playbook (scripts, configurations, binaries, etc.) you can do so by selecting Upload New File when setting the type to Download File from ASGARD Management Center during the creation of the playbook step. Alternatively you upload (and manage) new files at Response Control > Playbook Files.

You can have up to 16 steps in each playbook, which are executed sequentially. If you execute a command the **stdout** and **stderr** can be reported back as well if you wish to do so.

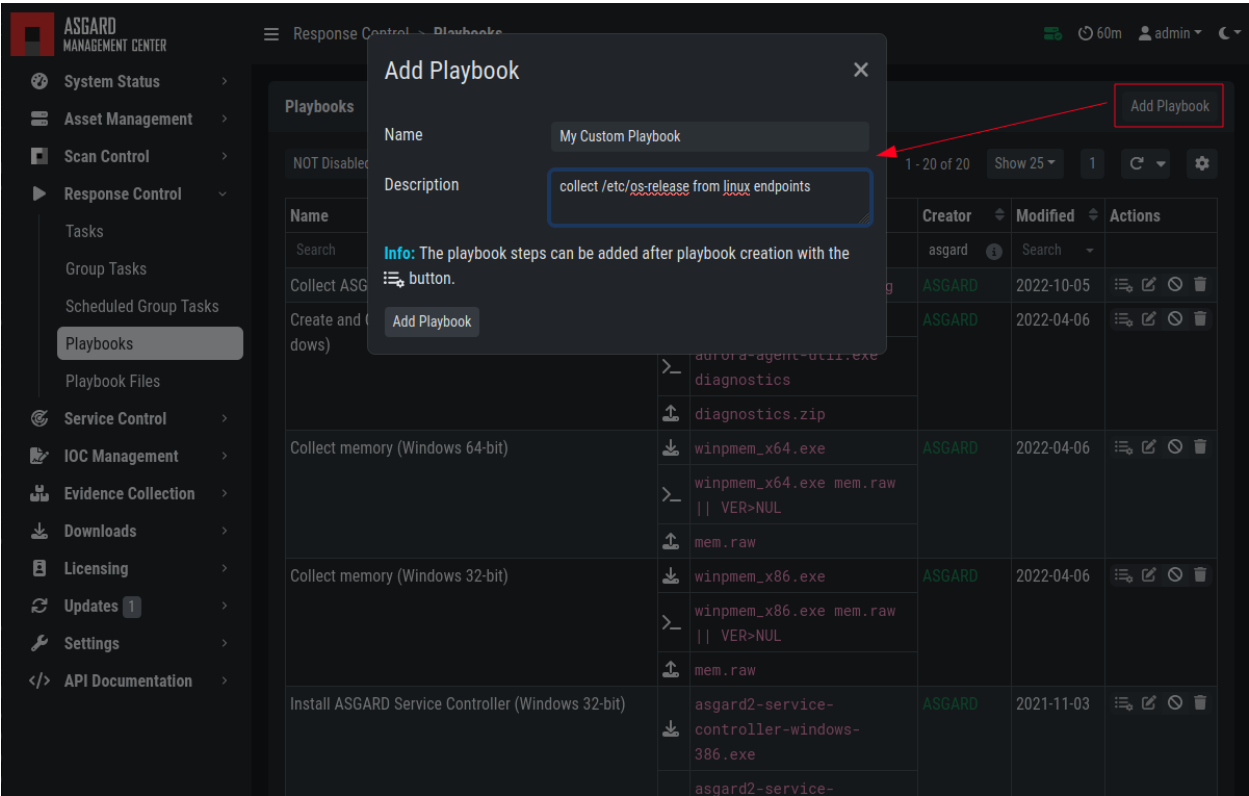


Fig. 32: Add Custom Playbook

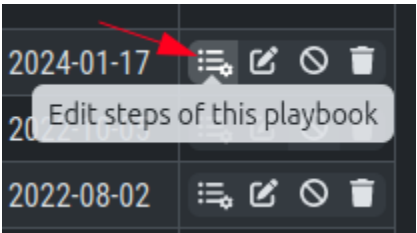


Fig. 33: Playbook Action Items

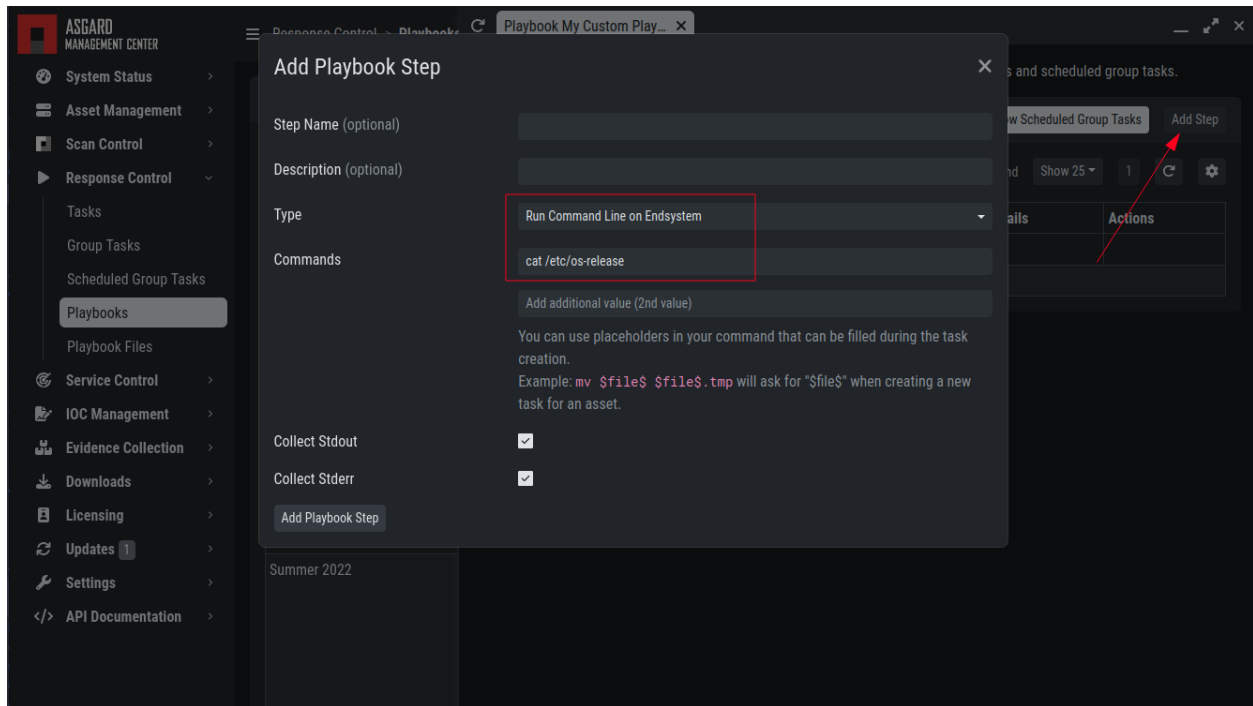


Fig. 34: Add Playbook Entry

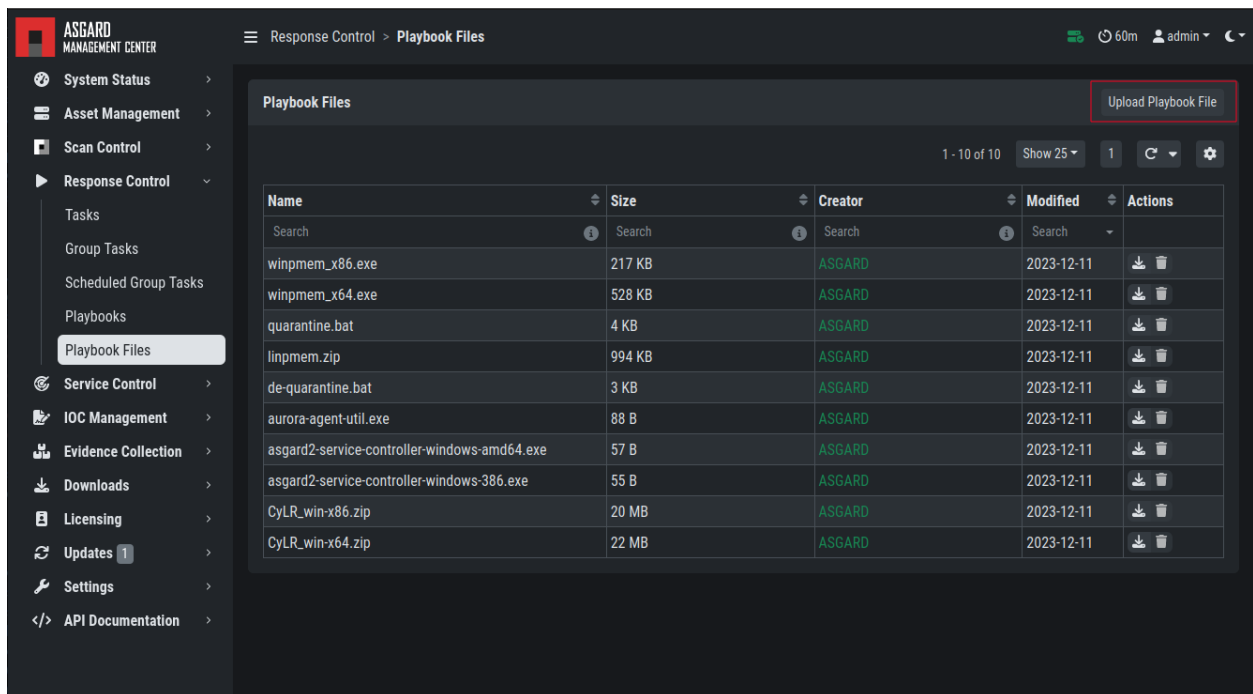


Fig. 35: Manage Playbook Files

### 3.10.5 Change the Asset(s) Proxy

You can change the Proxy Settings on your Assets via the Response Control. To do this, select the asset(s) and click Add Task in the top right corner. Next, set the Module to Maintenance and the Maintenance Type to Configure the asset's proxy. You can now set your proxy. Multiple proxies can be set, though only one FQDN/IP-Address per field can be set.

Fig. 36: Change/Set an assets Proxy

## 3.11 Service Control

Service Control is ASGARD's way of deploying real-time services on endpoints. Currently there only exist the Aurora service. To use Aurora, the service controller has to be installed on an asset.

### 3.11.1 Service Controller Installation

To install the ASGARD Service Controller on an asset, you need to install the ASGARD Agent first. If you already have installed the ASGARD Agent and accepted the asset in your Management Center, you can use the **"Install ASGARD Service Controller"** playbook to deploy the service controller on an asset. Optionally you can manually download and execute the `asgard2-service-controller` installer from the ASGARD downloads page.

Add Task

Description (optional)

Assets

windows05-pg01

Module

Run Playbook

Max. Runtime ⓘ

3 hours

Playbook

Install ASGARD Service Controller (Windows 64-bit)

1. Download File from ASGARD ⓘ

asgard2-service-controller-windows-amd64.exe

2. Execute Commands ⓘ

asgard2-service-controller-windows-amd64.exe

Add Task

Fig. 37: Install Service Controller

### 3.11.2 Service Controller Update

If an ASGARD update comes with a new service controller version, you need to update the service controller on the already rolled-out assets. You can do this using an "Update Agent" task. You can do that by either selecting one or multiple assets in the **Assets** view, or by creating a (scheduled) Group Task.

**Note:** If you don't see the **Update Agent** module, you need to enable **Show Advanced Tasks** in **Settings > Advanced**

## 3.12 Aurora

- Aurora is a lightweight endpoint agent that applies Sigma rules and IOCs on local event streams.
- It uses Event Tracing for Windows (ETW) to subscribe to certain event channels.
- It extends the Sigma standard with so-called "response actions" that can get executed after a rule match
- It supports multiple output channels: the Windows Eventlog, a log file and remote UDP targets

Its documentation can be found [here](#).



Fig. 38: Update Service Controller

### 3.12.1 Aurora Overview

Under **Service Control > Aurora > Asset View (Deployed)** the overview of all assets with installed Aurora is shown. Clicking on the entry opens a drop-down menu with details and additional information.

### 3.12.2 Deploy Aurora on Asset

You can also see an overview of all assets without Aurora installed under **Service Control > Aurora > Asset View (Not Deployed)** and install Aurora using the **Deploy Aurora** button. Those are all the assets which have the service controller installed, but the Aurora deployment was not done yet.

### 3.12.3 Change Service for an Asset

To change the Aurora configuration of an asset, navigate to **Service Control > Aurora > Asset View (Deployed)**, select the asset's checkbox and choose **> Change Aurora Configuration**. Then choose the desired service configuration > by clicking **Assign** and **Restart**.

If you want to enable or disable the Aurora service on an or more assets, select them with the checkbox and use the **Enable** or **Disable** button. Alternatively you can use the play or stop action icon on a single asset to achieve the same.

### 3.12.4 Create a Custom Aurora Configuration

Go to **Service Control > Aurora > Configurations > Add Configuration**, enter a name and add the rulesets that should apply for this service configuration. No rulesets is a viable option, if you only want to use the non-sigma matching modules. You don't need to edit any other option as sane defaults are given.

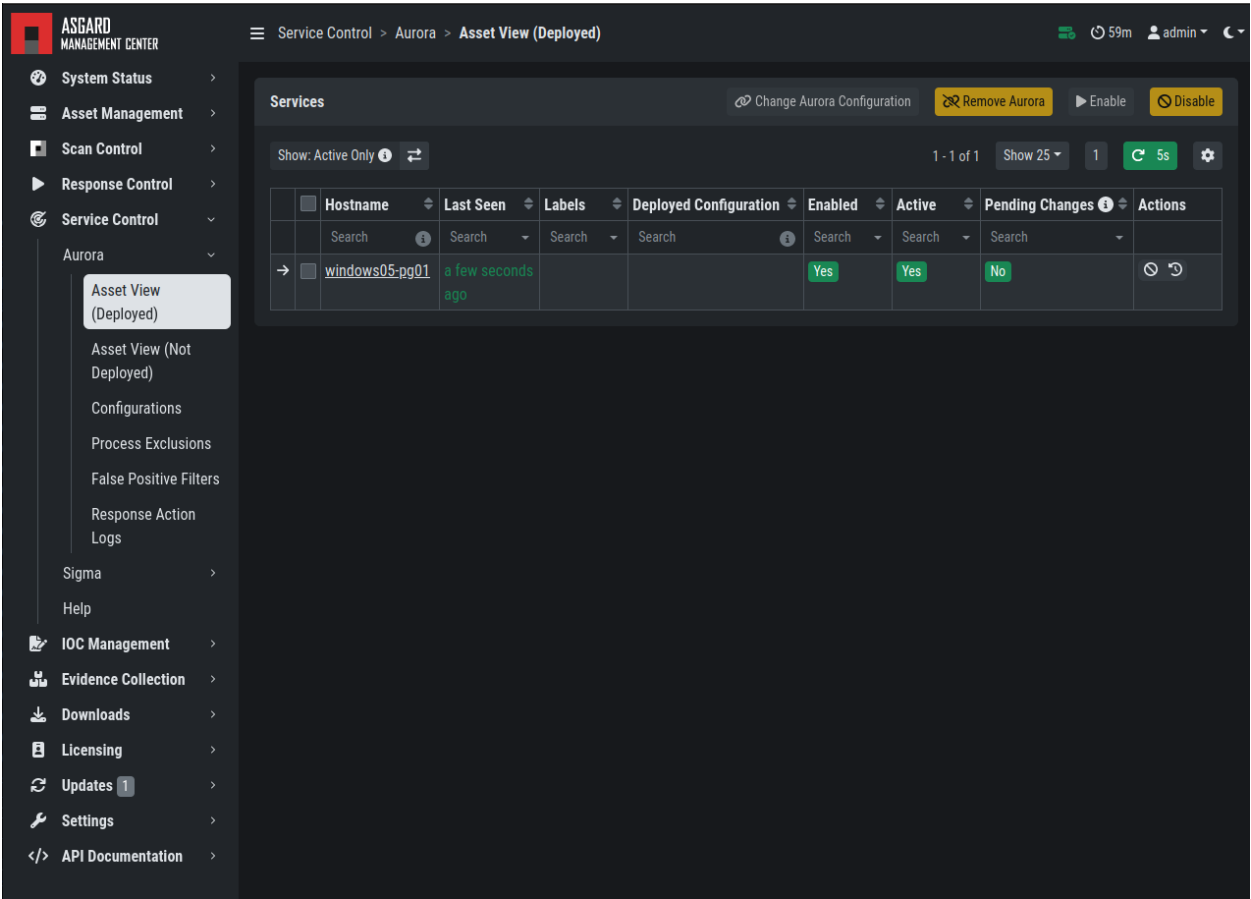


Fig. 39: Aurora Asset View

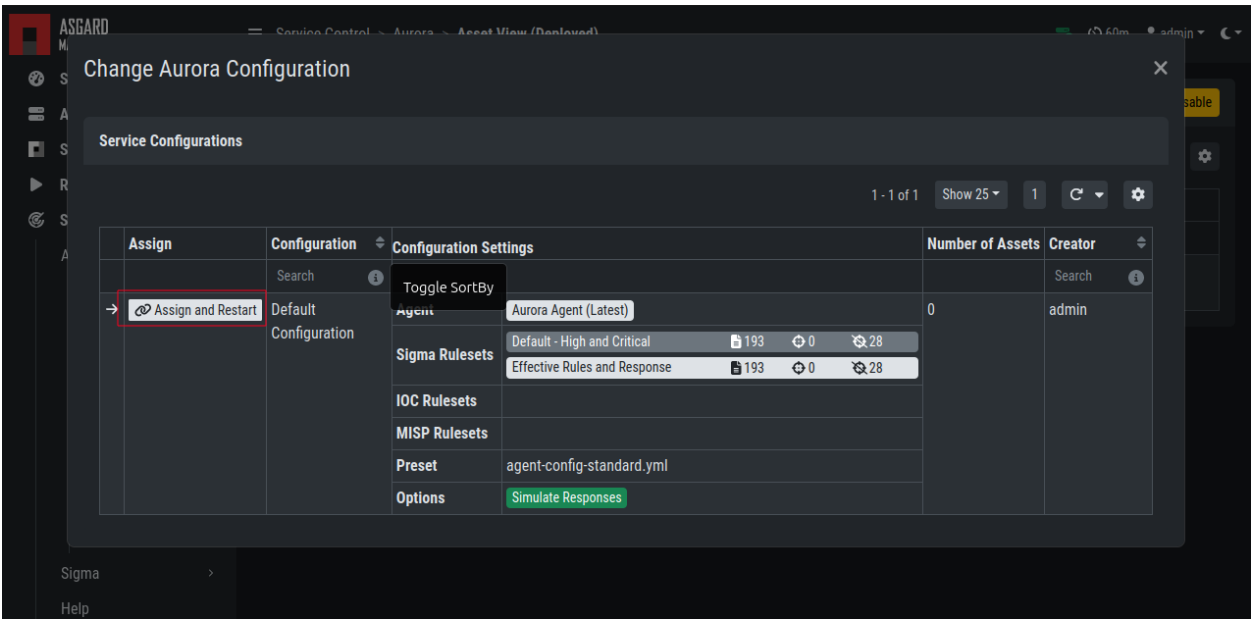


Fig. 40: Change Aurora Service Configuration

Fig. 41: Create a Custom Aurora Configuration

### 3.12.5 Process Excludes

If Aurora uses too much CPU cycles, the most common reason is a heavy event producer on the system (e.g. anti virus or communication software). In order to analyze the issue and define process exclusions, go to **Service Control > Aurora > Process Exclusions**

An overview over the top event producing processes is given on the bottom of the section. Another possibility is to download a [Aurora Diagnostics Pack](#) and look in the `status.txt` at the event statistics by process.

### 3.12.6 False Positive Filters

If needed, false positives can be globally defined on all Aurora agents at **Service Control > Aurora > False Positive Filters**. It is recommended to filter false positives at **Service Control > Sigma > Rules** and filter the false positives on a rule level using the "edit false positive" action (funnel icon). For more details see [False Positive Tuning of Sigma Rules](#). If this is not possible, because you need a quick fix and multiple rules are affected, the global false positive filter can help.

**Warning:** A too permissive filter will greatly reduce Aurora's detection and response capabilities.

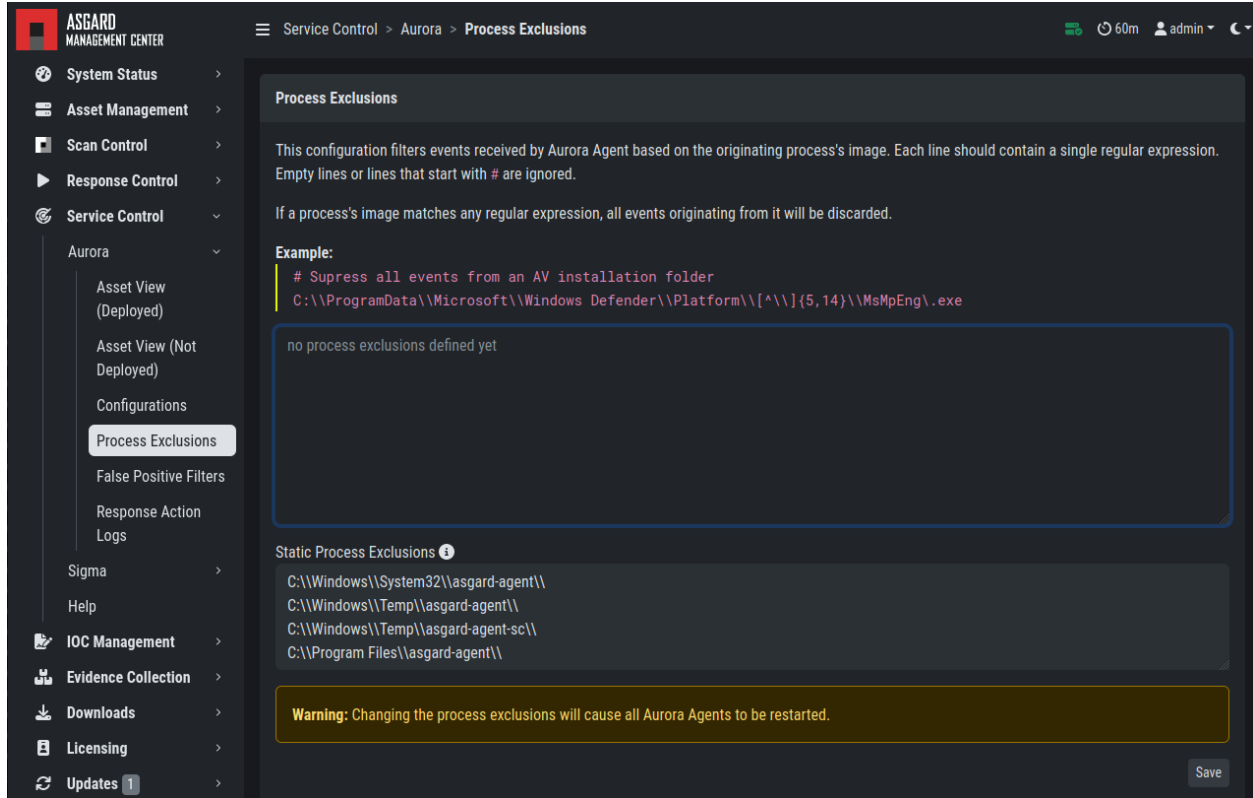


Fig. 42: Define Aurora Process Exclusion

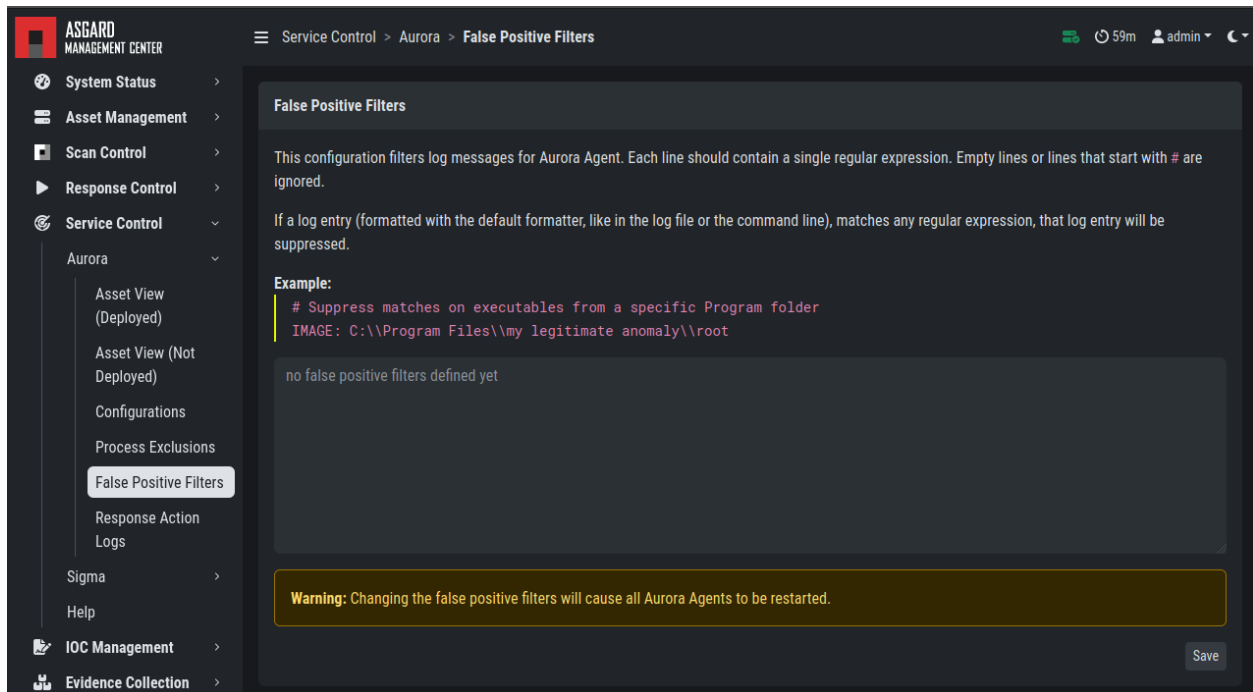


Fig. 43: Define Global Aurora False Positive Filters

### 3.12.7 Response Action Logs

You can view an overview and the logs of the Aurora response and simulated response actions under Service Control > Aurora > Response Action Logs.

The screenshot shows the ASGARD Management Center interface. The sidebar on the left contains navigation links: System Status, Asset Management, Scan Control, Response Control, Service Control (5), Sigma (5), and Help. The main content area is titled 'Service Control 5 > Aurora > Response Action Logs'. It features two statistics tables and two log entry sections.

Category	Count
Events Today	1
Events Yesterday	0
Events Last 3 Days	1
Events Last 7 Days	1
Events This Week	1
Events Last Week	0
Events Last 4 Weeks	1
Events on win10-at	1

Category	Count
Events Today	1
Events Yesterday	0
Events Last 3 Days	1
Events Last 7 Days	1
Events This Week	1
Events Last Week	0
Events Last 4 Weeks	1
Events on win10-at	1

**Response Action Log**

```
Feb 9 09:54:56 Win10-at AURORA: Warning MODULE: Sigma MESSAGE: Executed response action ACTION: kill
PROCESSES: 8396 / rundll32.exe, 10028 / cmd.exe, 10048 / conhost.exe RESPONSE_ORIGIN: inline RULE: CobaltStrike Load by Rundll32
RULE_ID: ae9c6a7c-9521-42a6-915e-5aaa8689d529 AURORA_EVENTID: 6000
```

**Simulated Response Action Log**

```
Feb 9 09:51:59 Win10-at AURORA: Info MODULE: Sigma MESSAGE: Simulated Response. This action was not executed because it is set to simulation mode. Activate it to change this behaviour. ACTION: kill
PROCESSES: 10028 / cmd.exe, 10048 / conhost.exe RESPONSE_ORIGIN: inline RULE: CobaltStrike Load by Rundll32
RULE_ID: ae9c6a7c-9521-42a6-915e-5aaa8689d529 AURORA_EVENTID: 6001
```

Fig. 44: Aurora Response Action Logs

### 3.12.8 Best Practices for Managing Aurora

1. Install the ASGARD agent on the asset (see [ASGARD Agent Deployment](#))
2. Install the ASGARD service controller on the asset (see [Service Controller Installation](#))
3. Deploy the Aurora Service on the asset using the [Default] Standard configuration with critical and high Sigma rules
4. configuration (see [Deploy Aurora on Asset](#))

If you want to enable the blocking capabilities of Aurora, we suggest to enable our included responses:

1. See the overview at Service Control > Aurora > Configurations. The Effective Rules and Response row shows how many responses are active. By default no responses are active. See [How to activate Responses](#).
2. Do not directly activate the responses in production environments. Monitor your environment for at least a month with simulated responses to verify that no false positive matches occur.

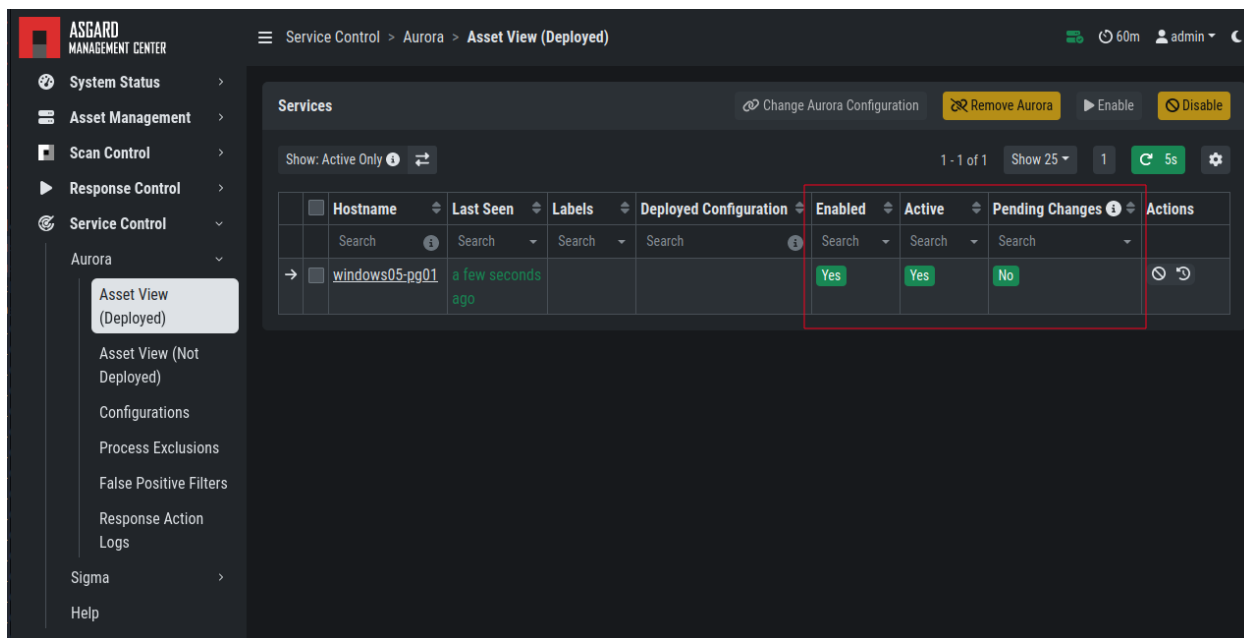


Fig. 45: Aurora Service Successfully Deployed

- In larger environments use different configurations and rulesets for different environments. As an example you can test changes to the configuration in a test environment, before adapting the changes for the production environment.

You can test the response functionality by entering the command

```
C:\Users\user>rundll32.exe AuroraFunctionTest.dll StartW
```

on the command line of an asset. As a result you should see following message in the Service Control > Aurora > Response Action Logs:

More tests are available from the [Function Tests section of the Aurora manual](#). Those tests only generate detection events but no responses. If your ASGARD Management Center is connected to an Analysis Cockpit, you can see the detection events at Events > Aurora Events or in the Windows EventLog of the asset.

## 3.13 Sigma

Aurora is using Sigma in order to define detections.

### 3.13.1 What is Sigma

From the [project website](#):

*Sigma is a generic and open signature format that allows you to describe relevant log events in a straightforward manner. The rule format is very flexible, easy to write and applicable to any type of log file. The main purpose of this project is to provide a structured form in which researchers or analysts can describe their once developed detection methods and make them shareable with others.*

*Sigma is for log files what Snort is for network traffic and YARA is for files.*

The screenshot shows the ASGARD Management Center v3 interface. The sidebar on the left contains navigation links: System Status, Asset Management, Scan Control, Response Control, Service Control (5), Aurora, Asset View (Deployed), Asset View (Not Deployed), Configurations, Process Exclusions, False Positive Filters, Response Action Logs, Sigma (5), Help, IOC Management (2), Evidence Collection, Downloads, Licensing, Updates (1), and Settings. The main content area is titled 'Service Control 5 > Aurora > Response Action Logs'. It features two statistics sections: 'Response Action Log Statistics' and 'Simulated Response Action Log Statistics', each with a 'Generate Statistics' button. Below these are two log sections: 'Response Action Log' and 'Simulated Response Action Log'. The 'Response Action Log' section shows three entries with details like timestamp, module, message, action, processes, response origin, rule, and event ID. The 'Simulated Response Action Log' section shows one entry indicating a simulated response that was not executed.

**Response Action Log Statistics**

**Simulated Response Action Log Statistics**

**Response Action Log**

Feb 9 10:00:18 Win10-at **AURORA:** Warning **MODULE:** Sigma **MESSAGE:** Executed response action **ACTION:** kill **PROCESSES:** 10180 / rundll32.exe, 10236 / cmd.exe, 5412 / conhost.exe **RESPONSE\_ORIGIN:** inline **RULE:** CobaltStrike Load by Rundll32 **RULE\_ID:** ae9c6a7c-9521-42a6-915e-5aaa8689d529 **AURORA\_EVENTID:** 6000

Feb 9 09:59:53 Win10-at **AURORA:** Warning **MODULE:** Sigma **MESSAGE:** Executed response action **ACTION:** kill **PROCESSES:** 3436 / rundll32.exe, 9440 / cmd.exe, 6836 / conhost.exe **RESPONSE\_ORIGIN:** inline **RULE:** CobaltStrike Load by Rundll32 **RULE\_ID:** ae9c6a7c-9521-42a6-915e-5aaa8689d529 **AURORA\_EVENTID:** 6000

Feb 9 09:54:56 Win10-at **AURORA:** Warning **MODULE:** Sigma **MESSAGE:** Executed response action **ACTION:** kill **PROCESSES:** 8396 / rundll32.exe, 10028 / cmd.exe, 10048 / conhost.exe **RESPONSE\_ORIGIN:** inline **RULE:** CobaltStrike Load by Rundll32 **RULE\_ID:** ae9c6a7c-9521-42a6-915e-5aaa8689d529 **AURORA\_EVENTID:** 6000

**Simulated Response Action Log**

Feb 9 09:51:59 Win10-at **AURORA:** Info **MODULE:** Sigma **MESSAGE:** Simulated Response. This action was not executed because it is set to simulation mode. Activate it to change this behaviour. **ACTION:** kill **PROCESSES:** 10028 / cmd.exe, 10048 / conhost.exe **RESPONSE\_ORIGIN:** inline **RULE:** CobaltStrike Load by Rundll32 **RULE\_ID:** ae9c6a7c-9521-42a6-915e-5aaa8689d529 **AURORA\_EVENTID:** 6001

Fig. 46: Aurora Simulated Response Action

### 3.13.2 Creating a Ruleset

Rulesets are used to group rules to manageable units. As an asset can only have one service configuration, rulesets are used to determine which rules are used in which service configuration. There exist default rulesets for high and critical Sigma rules. If you want to create a custom ruleset go to **Service Control > Sigma > Rulesets > Create Ruleset**.

Fig. 47: Create a Ruleset

If you have chosen that new Sigma rules should be added automatically to the new ruleset, they will be added now. If you didn't set any Sigma levels to automatically add to this rule, you now need to add the desired rules manually by going to **Service Control > Sigma > Rules**. Choose the rules that should be added to this ruleset by selecting the checkboxes and then **Add to Ruleset**. A rule can be assigned to multiple rulesets.

---

**Note:** You need to commit and push your changes after editing a ruleset. ASGARD has to restart the service controller to read new configurations. In order to prevent multiple restarts in the case of an admin performing several configuration changes in succession, the admin has to initiate the reloading of the new configuration by going to **Service Control > Sigma > Rulesets** and performing the **Compile ruleset** action (gear wheels). The need for compiling is indicated in the **Uncompiled Changes** column.





Fig. 48: Add a Rule to Rulesets

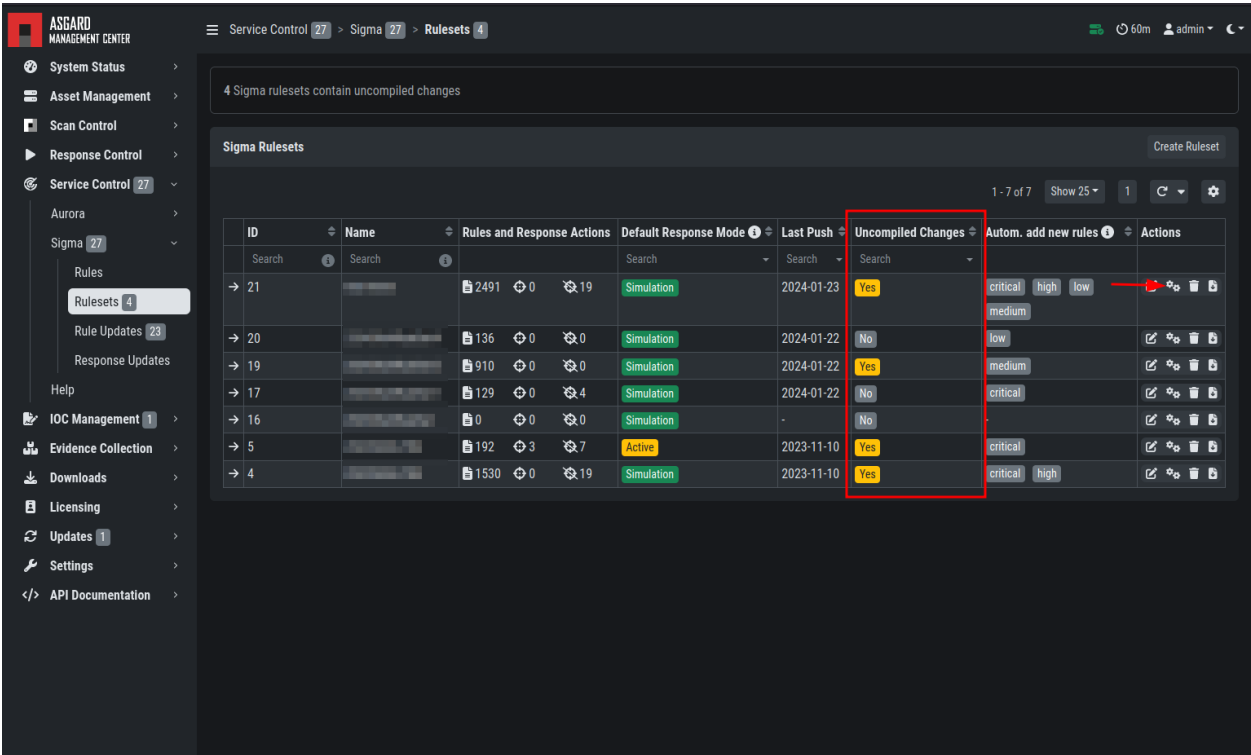


Fig. 49: Uncompiled Changes Indicator

### 3.13.3 Choosing which Rules to activate

It is not advised to enable all available rules on an asset. We suggest to start with all "critical" and then advance to all "high" rules. We already provide a default ruleset for those two levels for you to use. "Medium" rules should not be enabled in bulk, and "low"/"informational" at all. Single medium rules, which increase an organization's detection coverage and do not trigger a bigger number of false positives, can be added to the active configuration, but should be tested rule by rule.

In order to easily add rules to a ruleset you can use the column filters to select the desired rules and add the bulk to a ruleset. As an example you can add all rules of level "critical" to a ruleset:

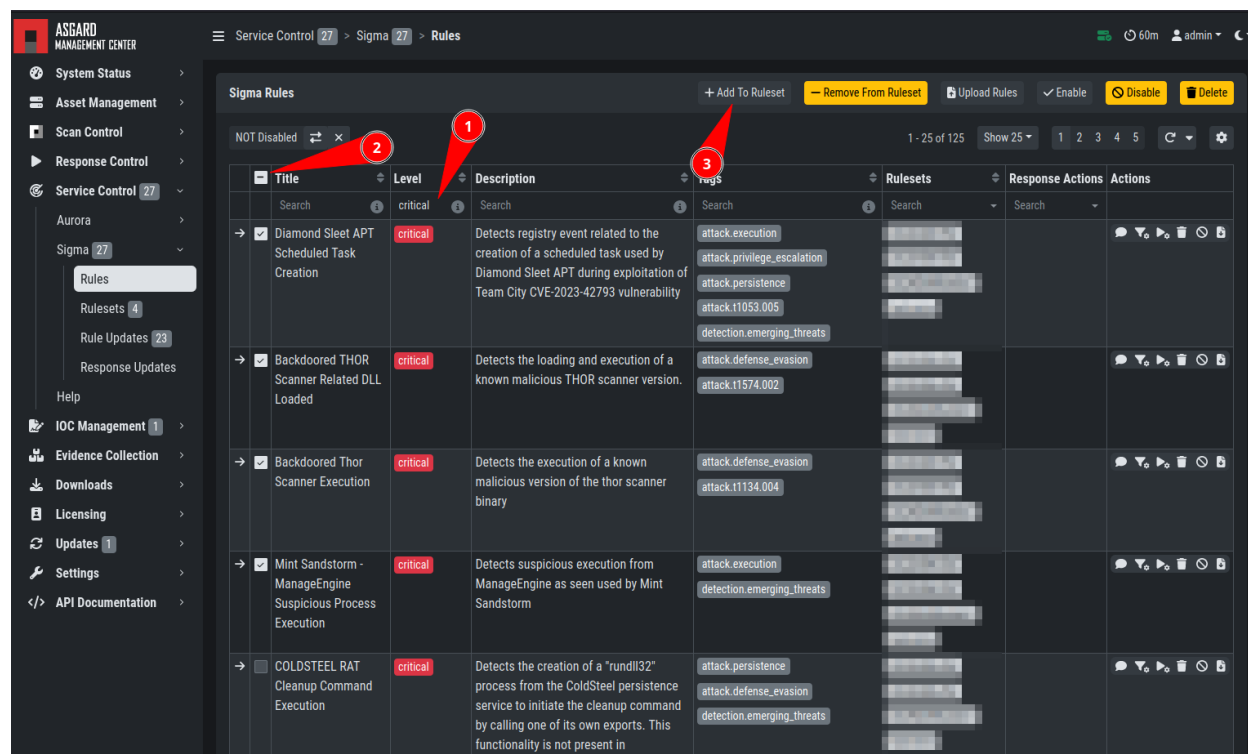


Fig. 50: Add All Critical Rules to a Ruleset

Another great way to pivot the Sigma rule database is the usage of MITRE ATT&CK® IDs.

Or you can just search the title or description field of the rules. You can also search the rule itself using the "Rule" column. (the "Rule" column is not shown by default and has to be added using the gear wheel button).

The screenshot shows the ASGARD Management Center interface with the 'Sigma Rules' section selected. The left sidebar contains navigation options like System Status, Asset Management, Scan Control, Response Control, Service Control, and more. The main panel displays a table of Sigma Rules. The 'Tags' column is highlighted with a red box, showing tags such as 't1543.003', 'attack.persistence', 'attack.privilege\_escalation', and 'attack.t1003'. The table includes columns for Title, Level, Description, Tags, Rulesets, Response Actions, and Actions.

Title	Level	Description	Tags	Rulesets	Response Actions	Actions
Search	critical	Search	t1543.003	Search	Search	
Malicious Service Installations	critical	Detects known malicious service installs that only appear in cases of lateral movement, credential dumping, and other suspicious activities.	attack.persistence, attack.privilege_escalation, attack.t1003, car.2013-09-005, attack.t1543.003, attack.t1569.002			
CobaltStrike Service Installations - System	critical	Detects known malicious service installs that appear in cases in which a Cobalt Strike beacon elevates privileges or lateral movement	attack.execution, attack.privilege_escalation, attack.lateral_movement, attack.t1021.002, attack.t1543.003, attack.t1569.002			
Moriya Rootkit - System	critical	Detects the use of Moriya rootkit as described in the securelist's Operation TunnelSnake report	attack.persistence, attack.privilege_escalation, attack.t1543.003			
Turla PNG Dropper Service	critical	This method detects malicious services mentioned in Turla PNG dropper report by NCC Group in November 2018	attack.persistence, attack.g0010, attack.t1543.003, detection.emerging_threats			
OilRig APT Registry Persistence	critical	Detects OilRig registry persistence as reported by Nyotron in their March 2018 report	attack.persistence, attack.g0049, attack.t1053.005, attack.s0111			

Fig. 51: Search by MITRE ATT&amp;CK® ID

The screenshot shows the ASGARD Management Center interface with the 'Sigma Rules' section selected. The left sidebar contains navigation options like System Status, Asset Management, Scan Control, Response Control, Service Control, and more. The main panel displays a table of Sigma Rules. The 'Title' column is highlighted with a red box. The table includes columns for Title, Level, Description, Tags, Rulesets, Response Actions, and Actions.

Title	Level	Description	Tags	Rulesets	Response Actions	Actions
exchange	critical	Search	Search	Search	Search	
Successful Exchange ProxyShell Attack	critical	Detects URP patterns and status codes that indicate a successful ProxyShell exploitation attack against Exchange servers	attack.initial_access, detection.emerging_threats			
CVE-2021-33766 Exchange ProxyToken Exploitation	critical	Detects the exploitation of Microsoft Exchange ProxyToken vulnerability as described in CVE-2021-33766	attack.initial_access, attack.t1190, cve.2021.33766, detection.emerging_threats			
CVE-2020-0688 Exchange Exploitation via Web Log	critical	Detects the exploitation of Microsoft Exchange vulnerability as described in CVE-2020-0688	attack.initial_access, attack.t1190, cve.2020.0688, detection.emerging_threats			
Exchange Exploitation CVE-2021-28480	critical	Detects successful exploitation of Exchange vulnerability as reported in CVE-2021-28480	attack.initial_access, attack.t1190, cve.2021.28480, detection.emerging_threats			
Certificate Request Export to Exchange Webserver	critical	Detects a write of an Exchange CSR to an untypical directory or with aspx name suffix which can be used to place a webshell	attack.persistence, attack.t1505.003			
Mailbox Export to Exchange Webserver	critical	Detects a successful export of an Exchange mailbox to untypical	attack.persistence			

Fig. 52: Search by Rule Title or Description

### 3.13.4 False Positive Tuning of Sigma Rules

Not every environment is the same. It is expected that some rules will trigger false positive matches in your environment. You have multiple options to tackle that issue.

1. If it is a general false positive, probably not only occurring in your environment, consider reporting it as a [Github issue](#) or e-mail to us at [rules@nextron-systems.com](mailto:rules@nextron-systems.com). We will take care of the tuning for you and your peers.
2. If the false positive is specific to your environment, you can tune single Sigma rules at **Service Control > Sigma > Rules**, filter for the rule in question and choose the "Edit false positive filters of this rule" action. Here you can do simple rule tunings on your own. By clicking the **Add False Positive Filter** button you can add single lines that filter the event for false positives (i.e. they are OR-connected meaning: "Do not match the event if any of those lines matches"). They are applied on top of the rule logic and persist automatic rule updates.

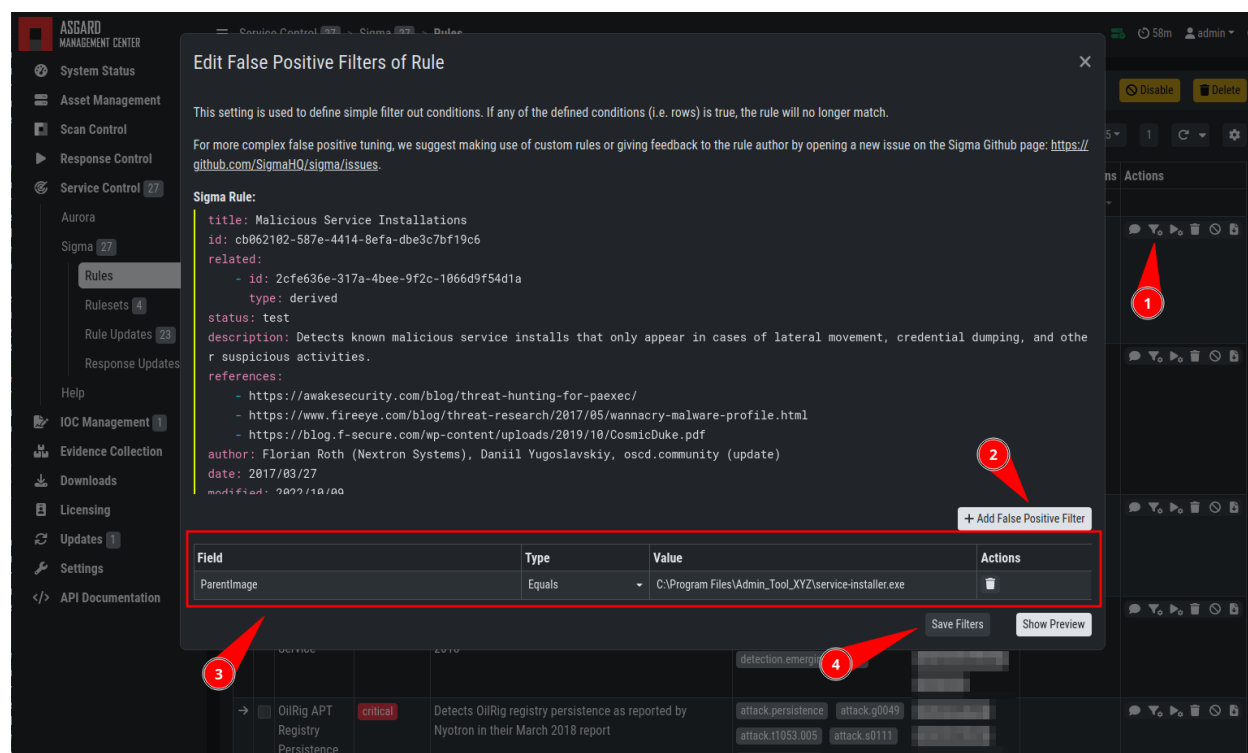


Fig. 53: Example of the false positive tuning of a Sigma rule

To see the resulting rule you can click the "Show Preview" button or look at the "Compiled Rule" row in the rule's drop down menu.

If you want to review the tuned rules: To filter for all rules containing a custom false positive tuning, you have to add the "Filters" column to your view (gear wheels icon) and show all non-empty rows by using the NOT - column filter.

3. If the rule is adding too much noise and tuning is not sensible, you can remove the rule from the ruleset for a subset of your machines (maybe you need to define and use a separate ruleset for that use-case) or you can disable the rule altogether. This is done using the **Disable this rule** action of the rule. Disabling the rule affects the rule in all rulesets.

After tuning a rule, the rulesets using that rule have to be re-compiled at **Service Control > Sigma > Rulesets**.

### 3.13.5 Adding Custom Rules

Custom rules can be added using the sigma format complying with the [specification](#). You can upload single files or a ZIP compressed archive. This can be done at Service Control > Sigma > Rules > Upload Rules.

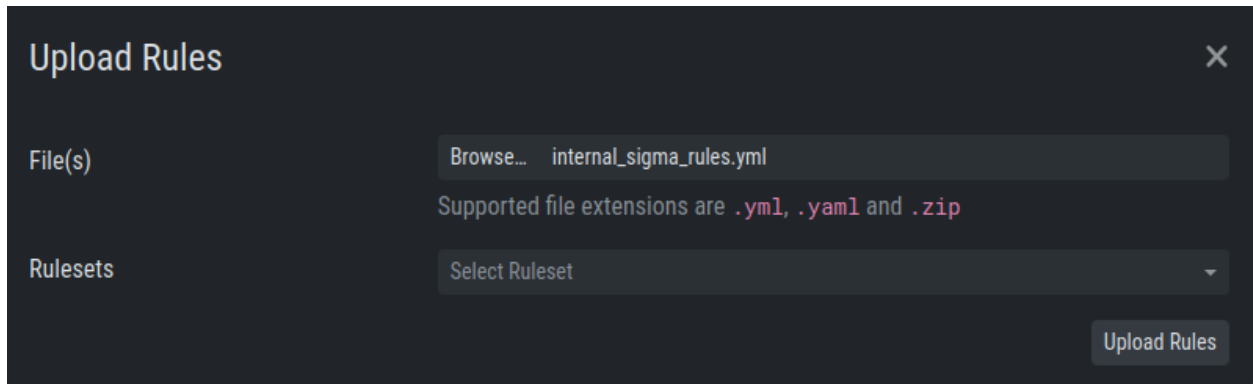


Fig. 54: Adding Custom Rules

### 3.13.6 Rule and Response Updates

If new rules or rule updates are provided by the Aurora signatures, the updates have to be applied by the user manually in order to be affecting Aurora agents managed by ASGARD. An indicator is shown in the WebUI and the rules changes can be reviewed and applied at Service Control > Sigma > Rule Updates.

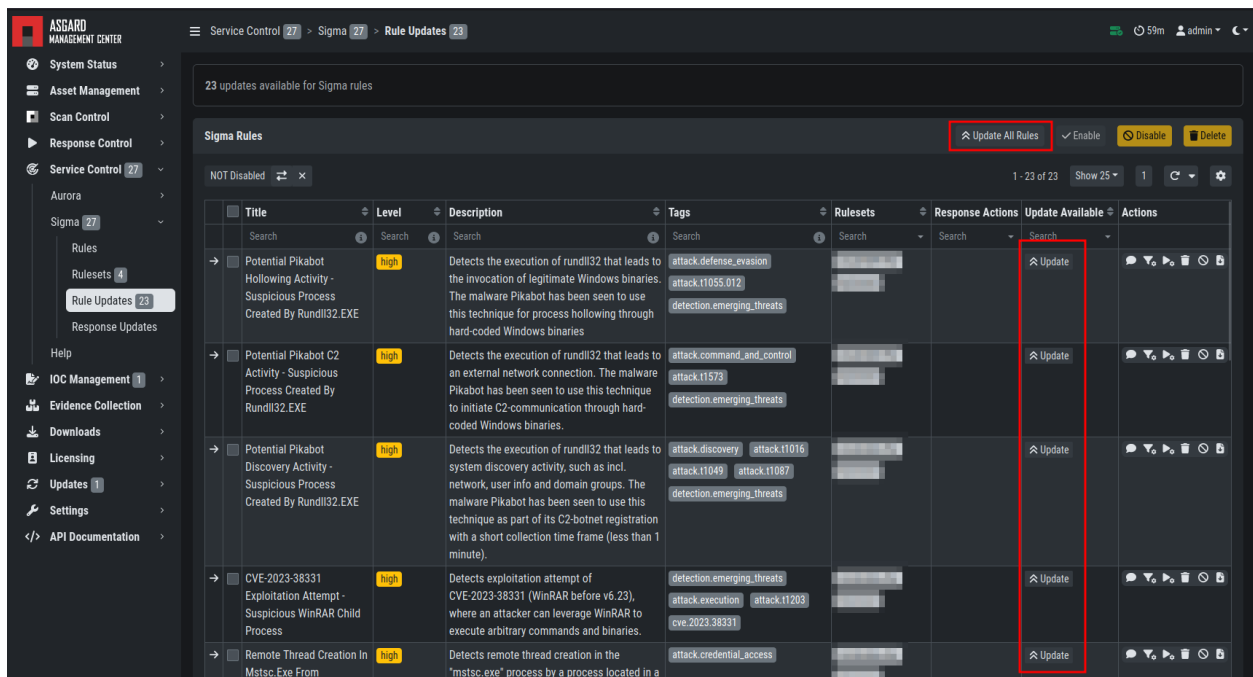


Fig. 55: Sigma Rule Updates for Aurora

Clicking on the Update button in the "Update Available" column opens a diff view in which the changes are shown and where the user can apply or discard the changes. If you do not need to review each single change, you can apply all changes using the Update All Rules button.

Analogous the updates of response actions can be viewed and applied at Service Control > Sigma > Response Updates.

### 3.13.7 How to activate Responses

As a fail safe and for administration purposes, responses are generally only simulated if not explicitly set to active. This has to be done on different levels:

- Service configuration level
- Ruleset configuration level (on updates)
- Ruleset rule level

If on one level a rule is simulated, it will not execute the response actions but only generate a log line that describes the action that would have been performed. You can see an overview of the state of all responses in the Service Control > Aurora > Configurations menu.

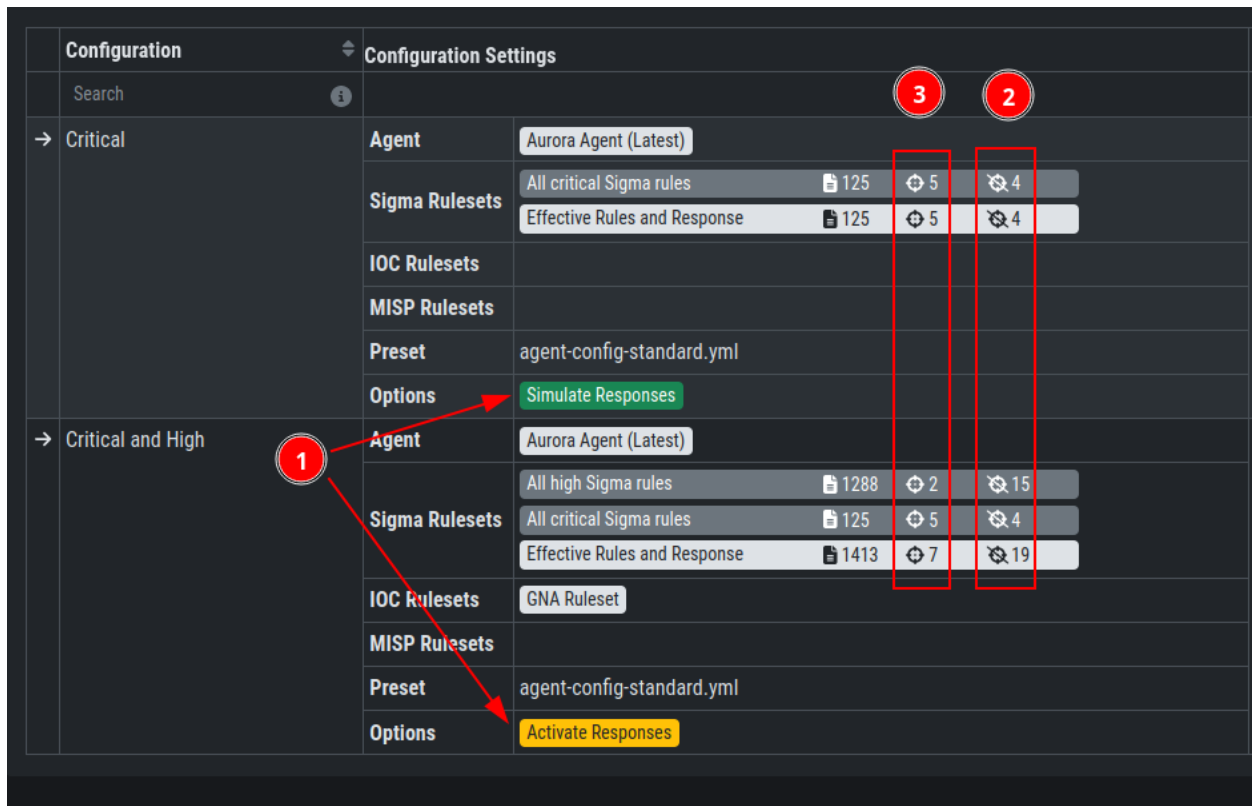


Fig. 56: Aurora Configuration Response Action Overview

- (1) indicates whether responses are activated on configuration level. Edit the configuration to change it.
- (2) indicates how many rules are only simulated in that ruleset (or in sum).
- (3) indicates how many rules have active responses in that ruleset (or in sum)

To change the status of a response in the ruleset click the ruleset link. You can view all simulated or all active responses. Use the checkbox and the button in the upper right to switch the response status of the rules between active and simulated.

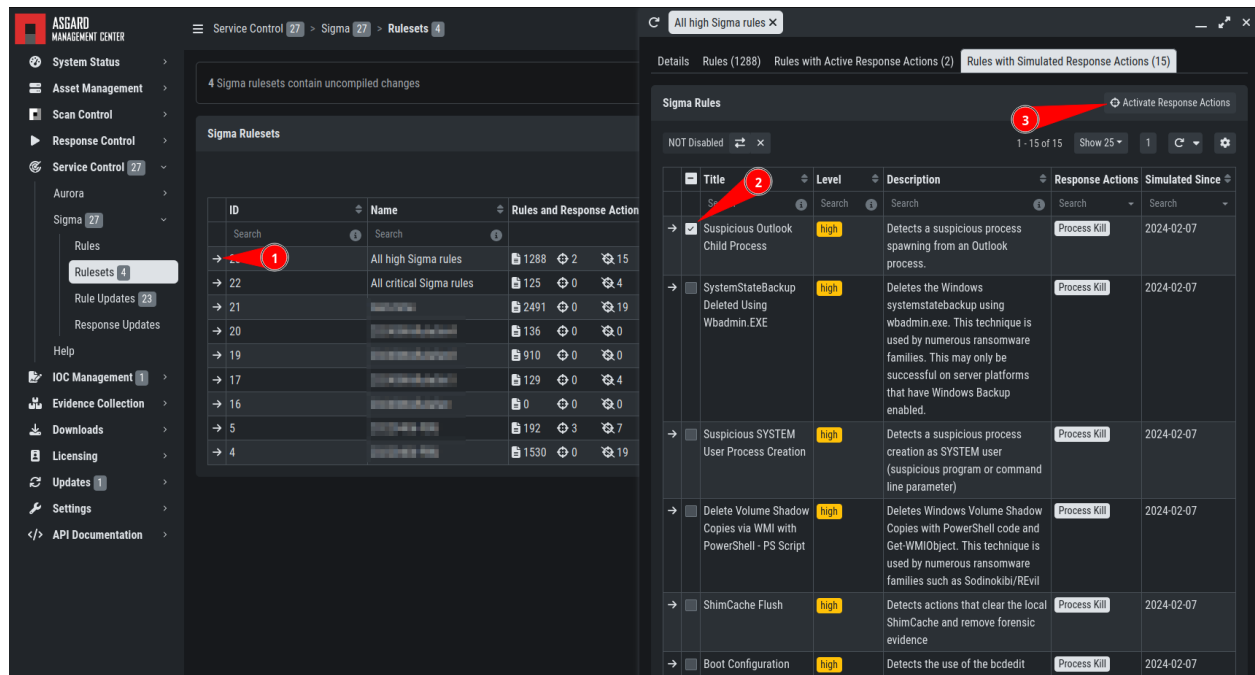


Fig. 57: Response Configuration in Rulesets

The default response mode of a ruleset is important for the behavior of response updates. It can be seen at Service Control > Sigma > Rulesets in the Default Response Mode column.

If "Simulation" is selected, response actions of new and updated rules will be put in simulation mode. If "Active" is selected, new rules will automatically be put in active mode and updated rules will not change their current response mode. We advise to leave the default response mode in "Simulation" mode.

## 3.14 IOC Management

### 3.14.1 Integrating Custom IOCs

The menu IOC Management gives you the opportunity to easily integrate custom signatures into your scans.

In order to create your own custom IOC Group, navigate to IOC Management > IOCs and click Add IOC Group in the upper right corner. Select a name and optionally a description for your IOC Group.

To add IOCs to this group, use the Show and edit IOCs in this IOC group action. A side pane opens where you can click the Import IOCs button to import your own signatures in any of THOR's IOC formats as files (e.g. files for keyword IOCs, YARA files and SIGMA files). Refer to the [THOR manual \(custom signatures\)](#) for a complete list and file formats. Browse to the file you want to add and click upload. This adds your IOC file to the default ruleset.

However, you can also click the Add IOC(s) button to add some IOCs interactively. Select the type, score and description, enter some values and click the Add IOC button.

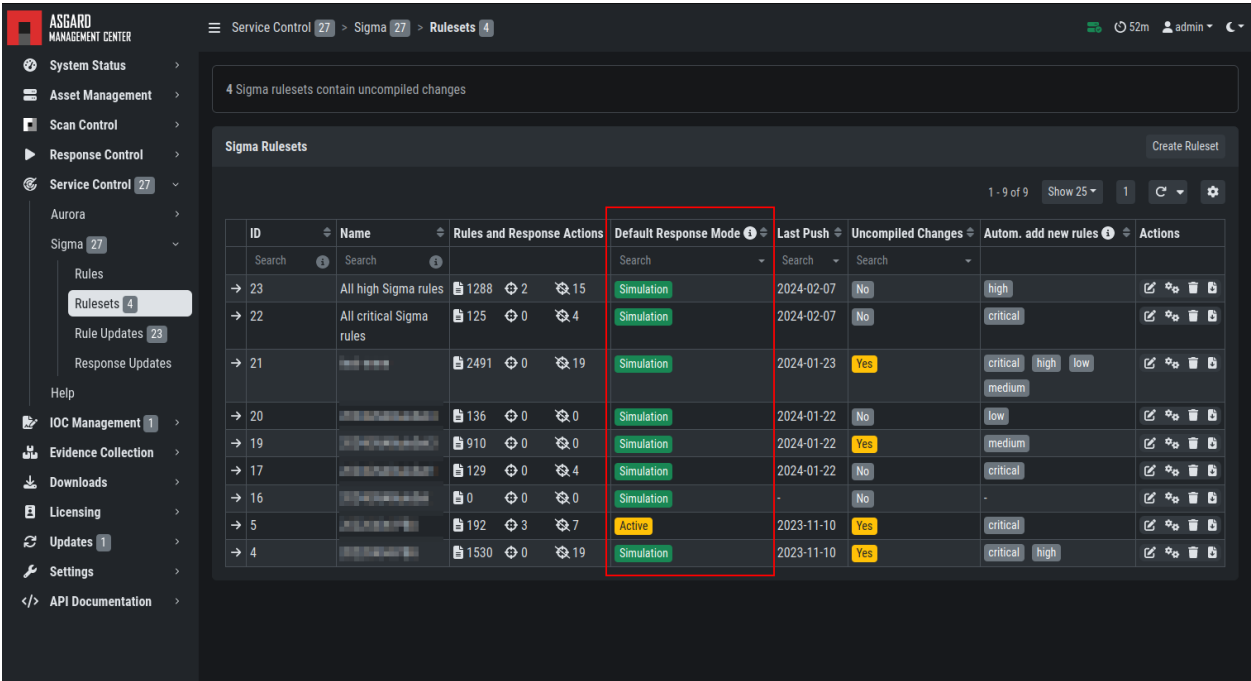


Fig. 58: Ruleset Default Response Mode

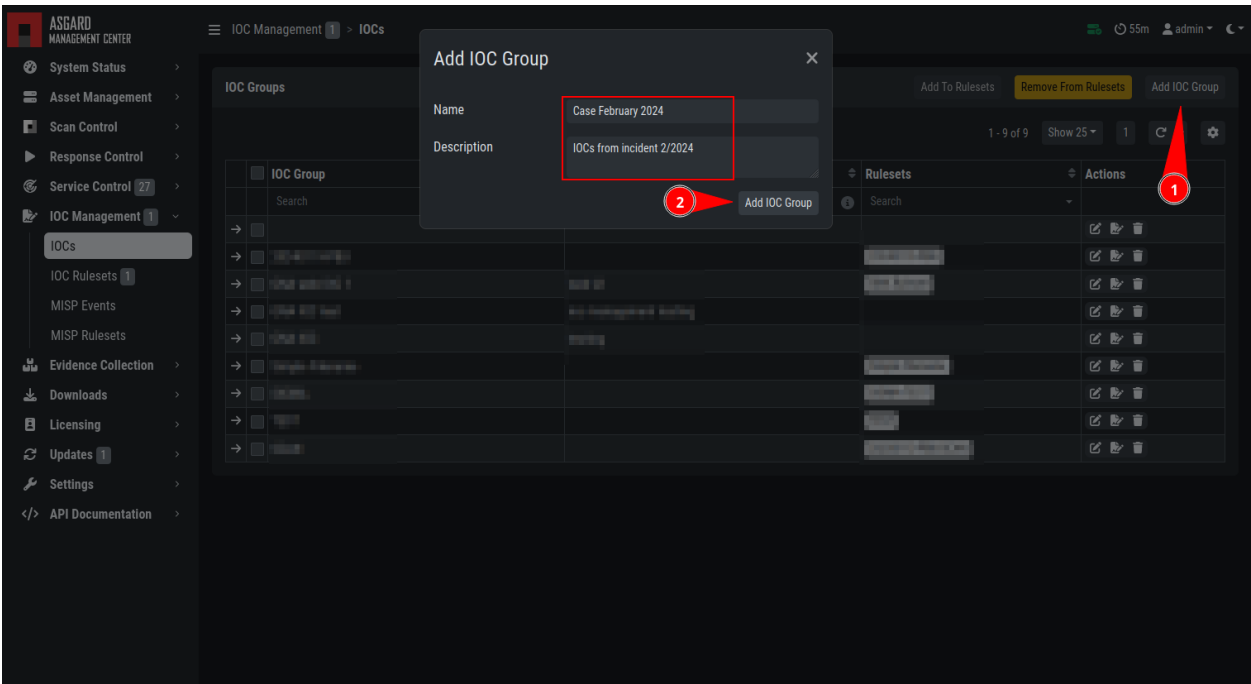


Fig. 59: Add IOC Group



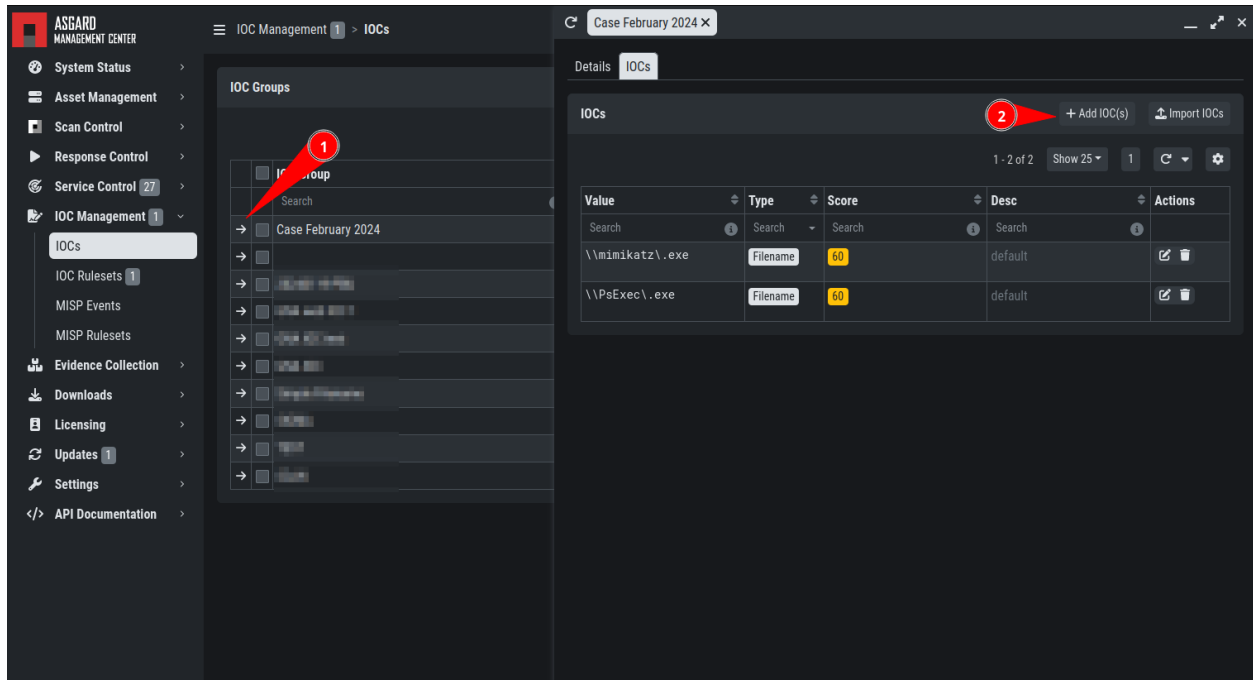


Fig. 60: Imported IOCs Overview

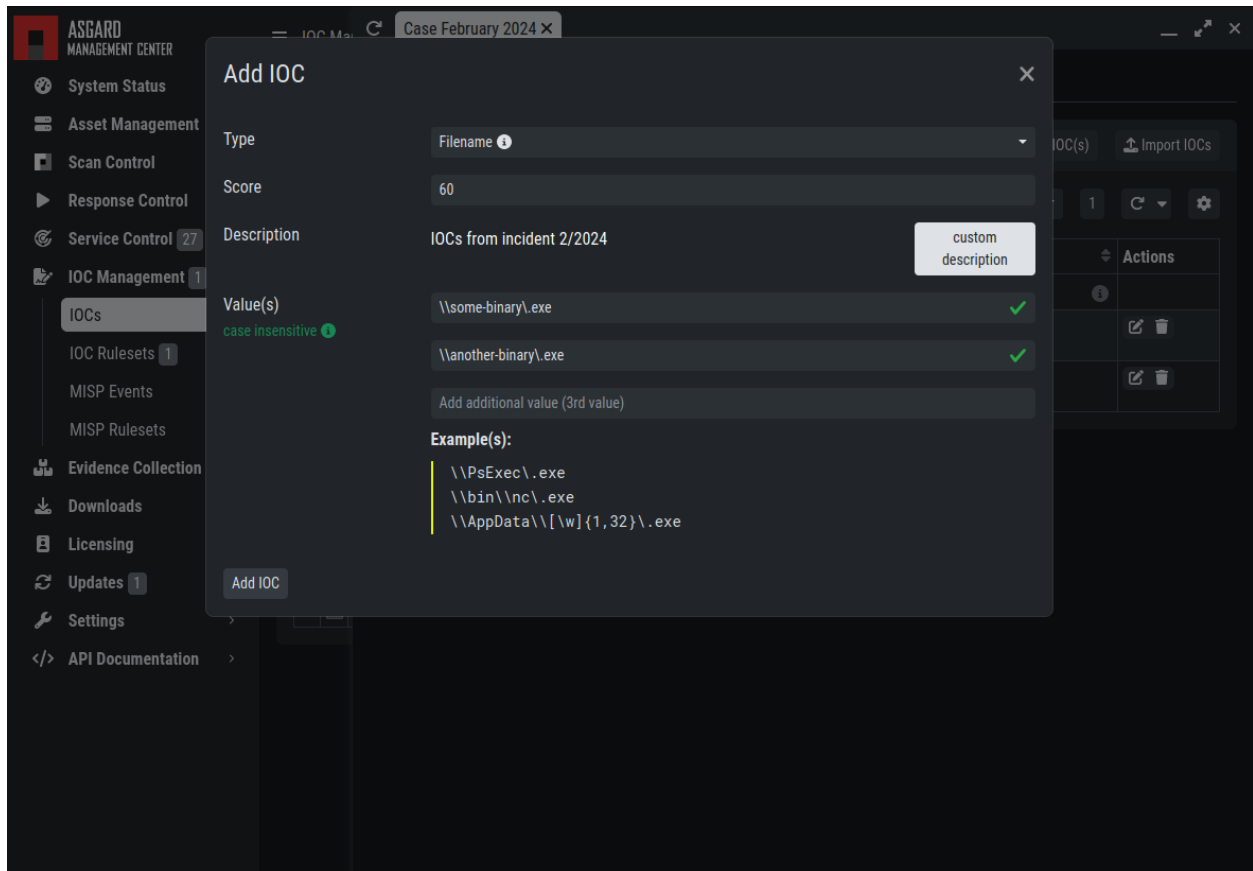


Fig. 61: Add IOCs

You can add those IOC Groups to IOC Rulesets which can be created in the IOC Management > IOC Rulesets tab by clicking the Add Ruleset button in the upper right corner. Select name and description and click the Add Ruleset button.

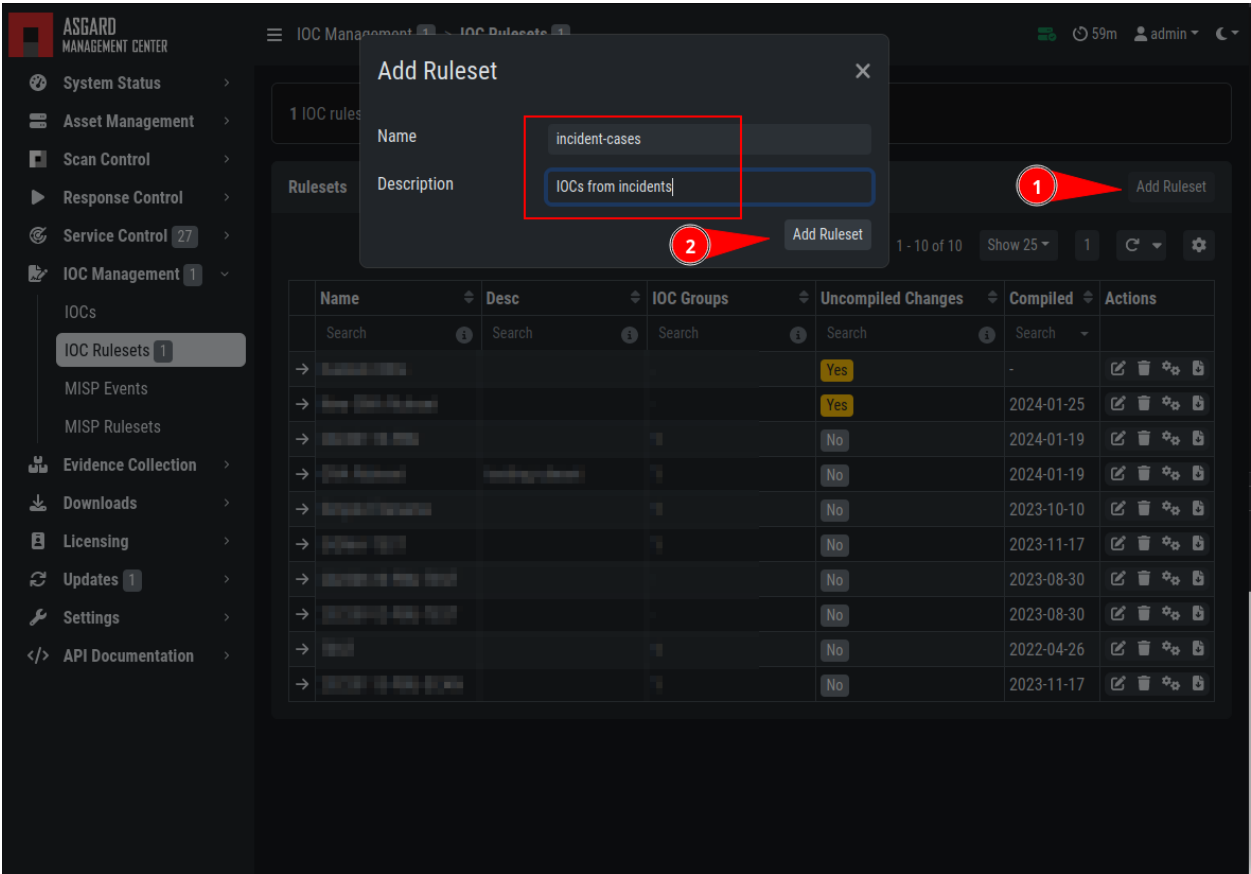


Fig. 62: Add Ruleset

After that, click on an entry in the table to expand it. There you get information about all IOC Groups which have been added to this ruleset. Additionally you can add or remove selected IOC Groups in IOC Management: IOCs by clicking one of the three buttons shown below.

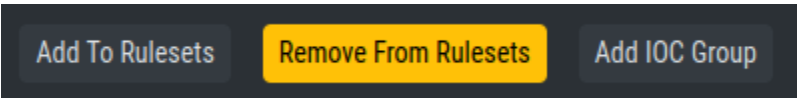


Fig. 63: Buttons to Add/Remove IOC Groups

You can now add your IOC Group to the newly created IOC Ruleset.  
This Ruleset can now be used in THOR scans.  
Anytime you add, remove or change IOCs within one of your IOC Groups, you have to recompile the IOC Ruleset. To do this, navigate to the IOC Rulesets page and click the "geard" icon in the Ruleset's row

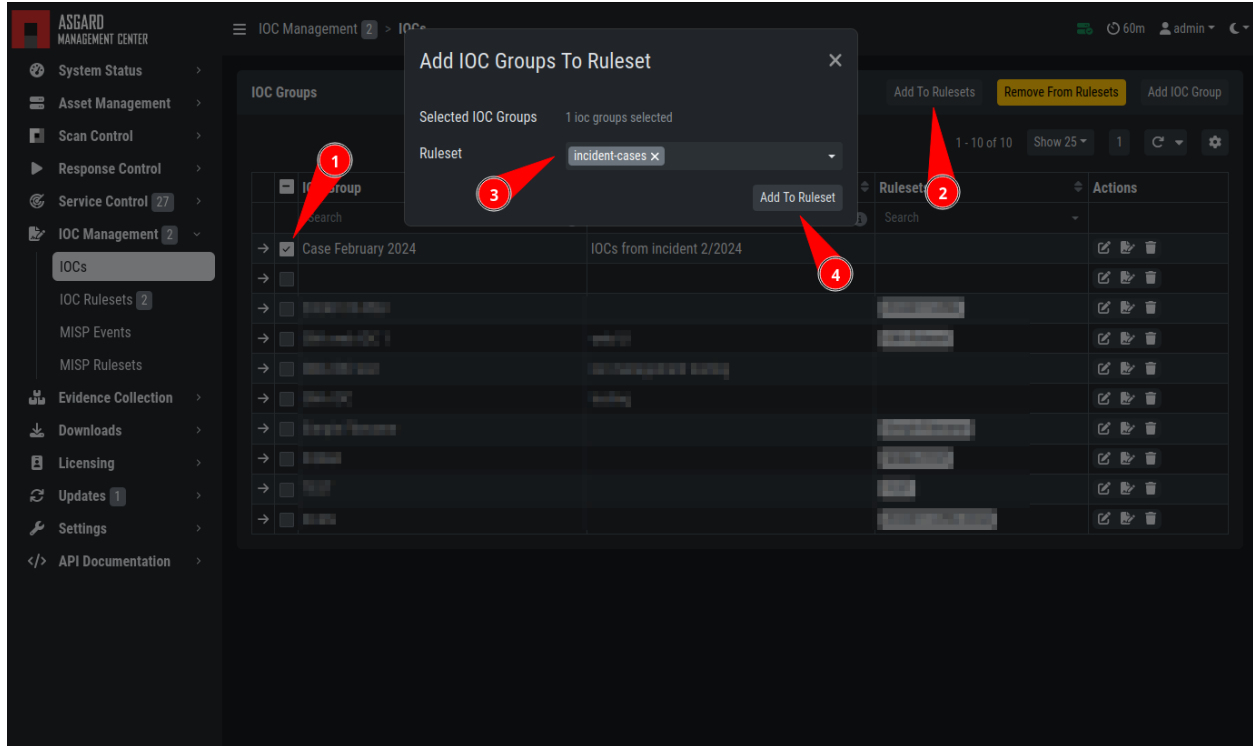


Fig. 64: Add IOC Group to Ruleset

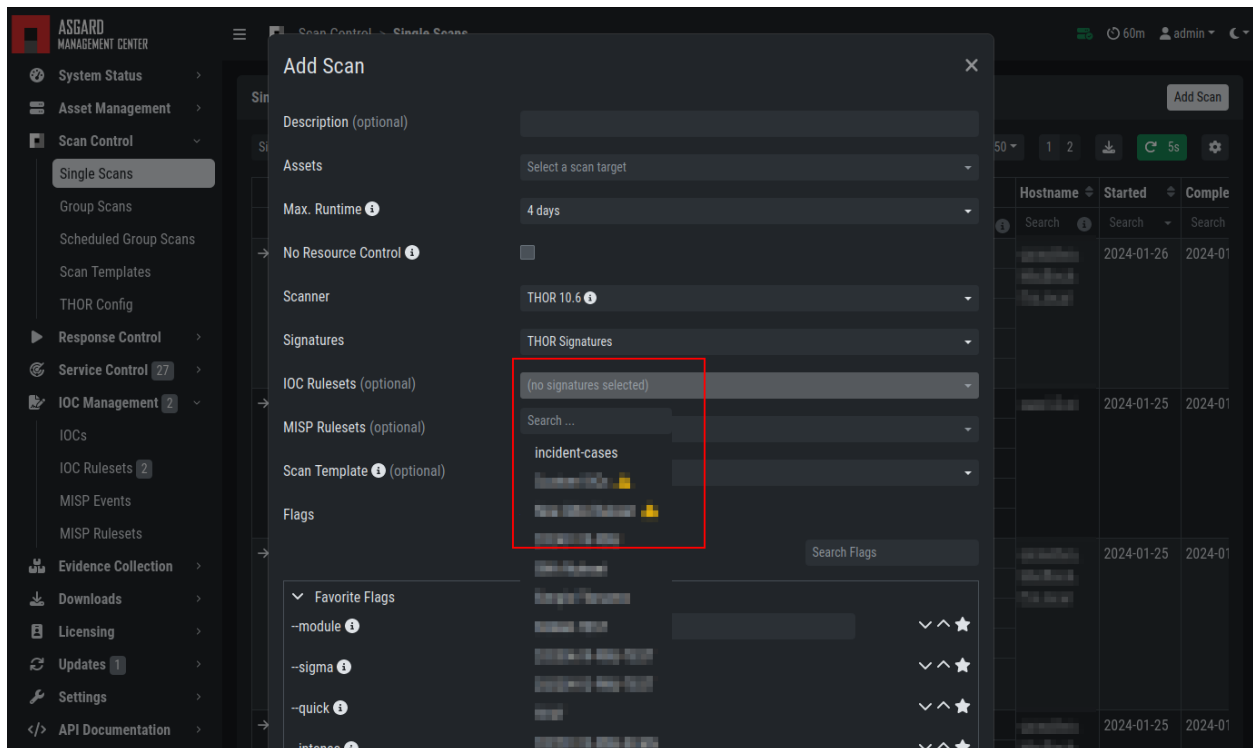


Fig. 65: IOC Ruleset in THOR Scan

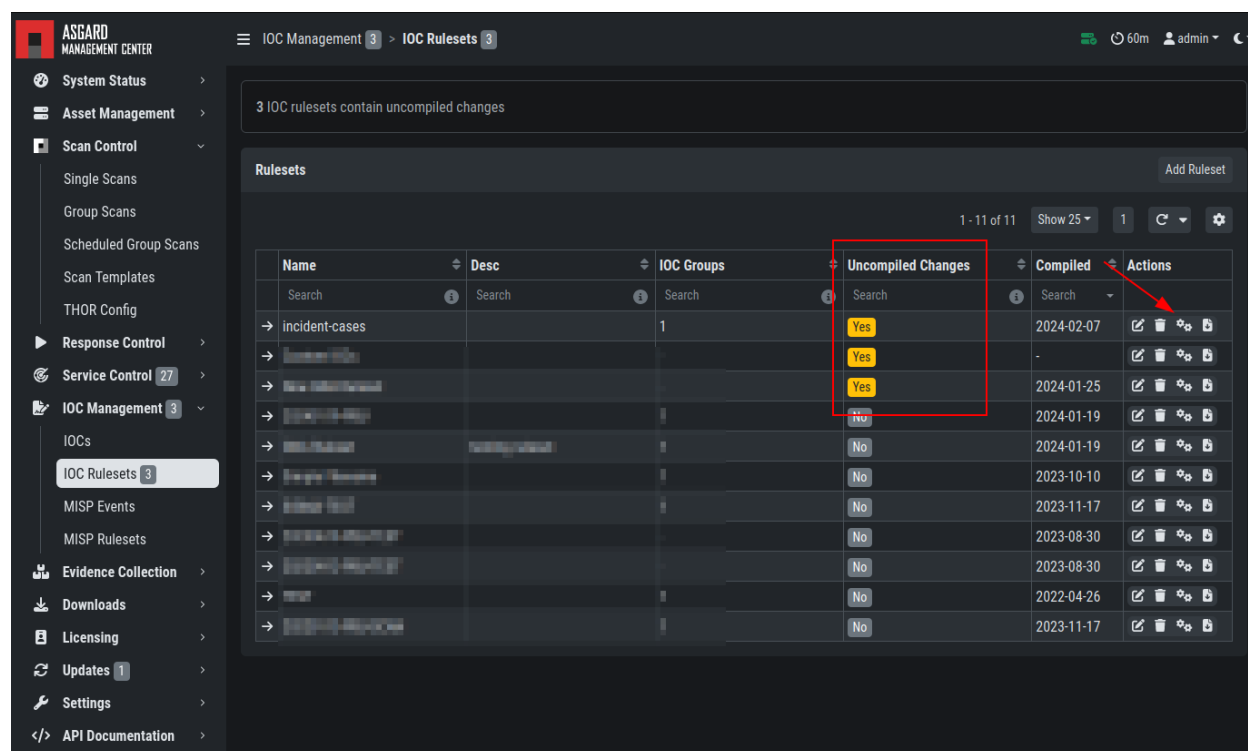


Fig. 66: Compile IOC Ruleset

### 3.14.2 Scan only with Custom IOCs

Those rulesets can be selected in the "IOC Rulesets" field while creating a new scan job. If a ruleset is selected, the scan will include all custom IOCs included in IOC Groups which have been added to this ruleset. You can also select more than one ruleset.

The THOR scan would be performed with the default settings and the custom ruleset, the default signatures would not be applied.

**Note:** To scan exclusively with the custom ruleset, the flag `--customonly` must be set. Please see [THOR Flags](#) for more information.

### 3.14.3 Integrating IOCs through MISP

**Note:** In order to use MISP events and their IOCs for scanning, you need to link your ASGARD with a MISP first. Please see [Link MISP](#) for reference.

ASGARD provides an easy to use interface for integrating IOCs from a connected MISP into THOR scans. In order to add rules from a MISP, navigate to **IOC Management > MISP > MISP Events**, select the IOCs and add them to the desired ruleset by using the button in the upper right corner.

There is no default ruleset for MISP. You must create at least one ruleset (see tab "MISP Rulesets") before you can add MISP rules.

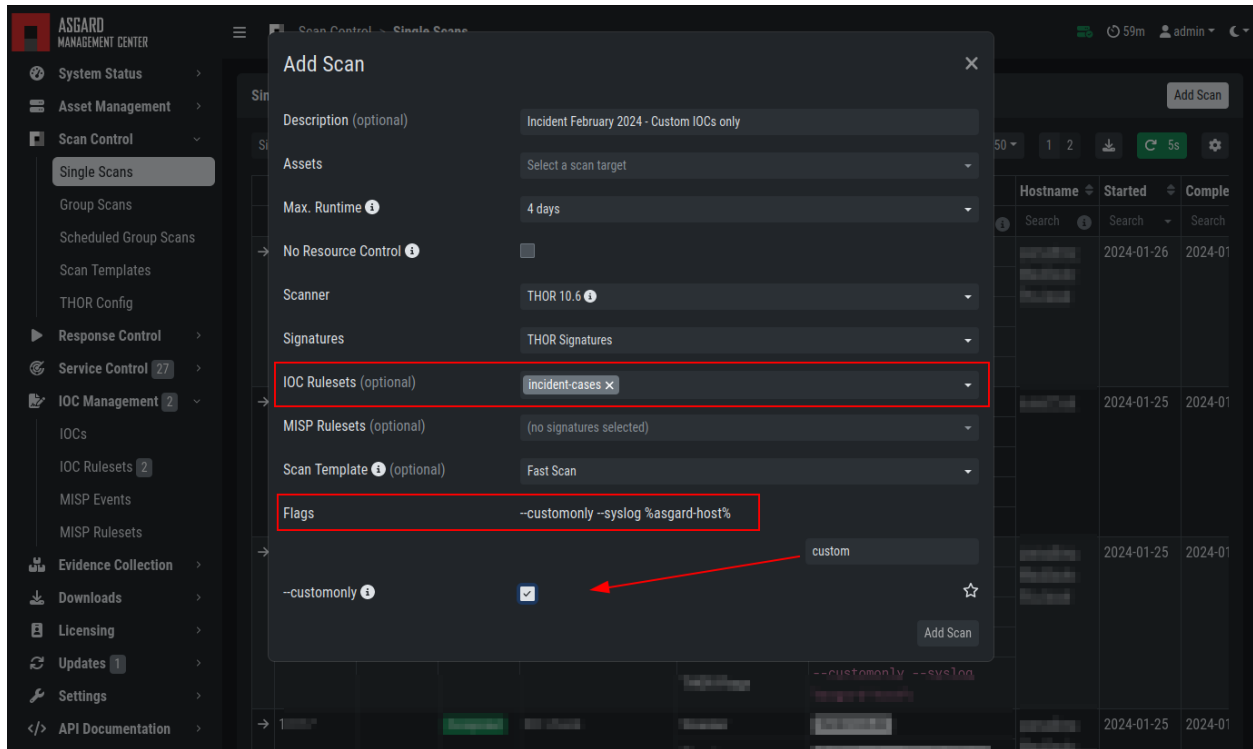


Fig. 67: Select Ruleset while creating a scan job

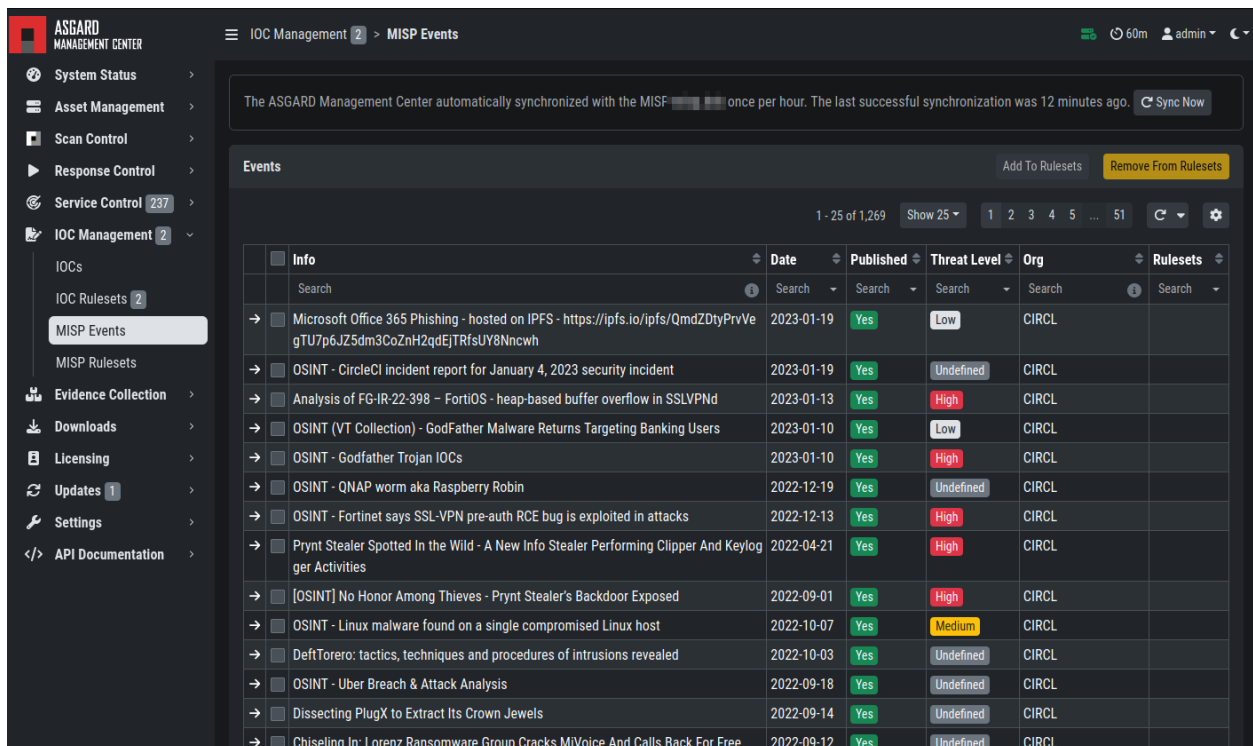


Fig. 68: MISP events

To create a new ruleset, click Add MISP Ruleset in the IOC Management > MISP > MISP Rulesets tab. Select a name and the type of IOCs you want to use in this ruleset. By default, all types are selected, but there may be reasons for deselecting certain categories. For example, filename IOCs tend to cause false positives and may be deselected for that reason. The picture below shows the dialogue for adding a MISP ruleset. Enable Auto Compile in order to automatically compile new MISP events into the ruleset, when they arrive.

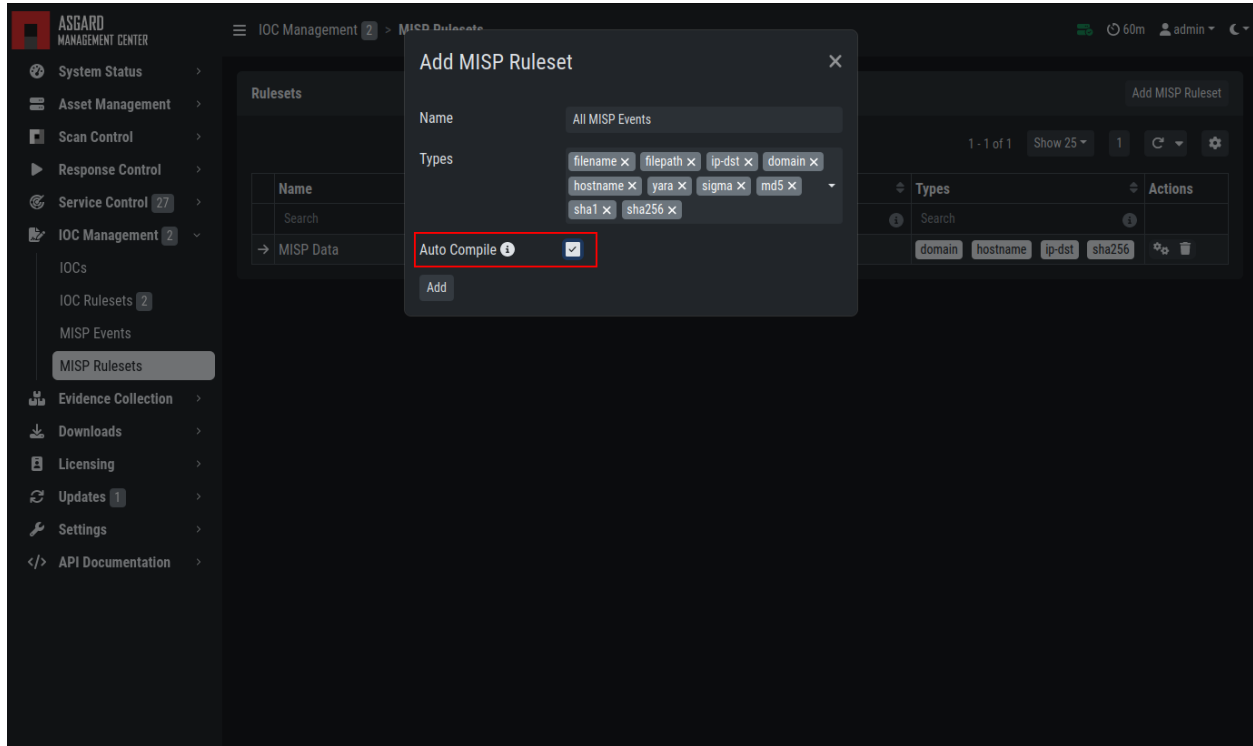


Fig. 69: Adding a new MISP ruleset

In order to use a MISP ruleset in a scan, add the ruleset in the MISP Signatures field when creating your scan.

### MISP Attributes used by ASGARD

Since not all the information and attributes in a MISP event are relevant to ASGARD and the THOR scanner, we provide a list of attributes which will be used by ASGARD:

- hostname
- ip-dst
- domain
- domain-ip>hostname
- domain-ip>ip-dst
- domain-ip>domain
- filename
- filepath
- file>filename
- file>filepath

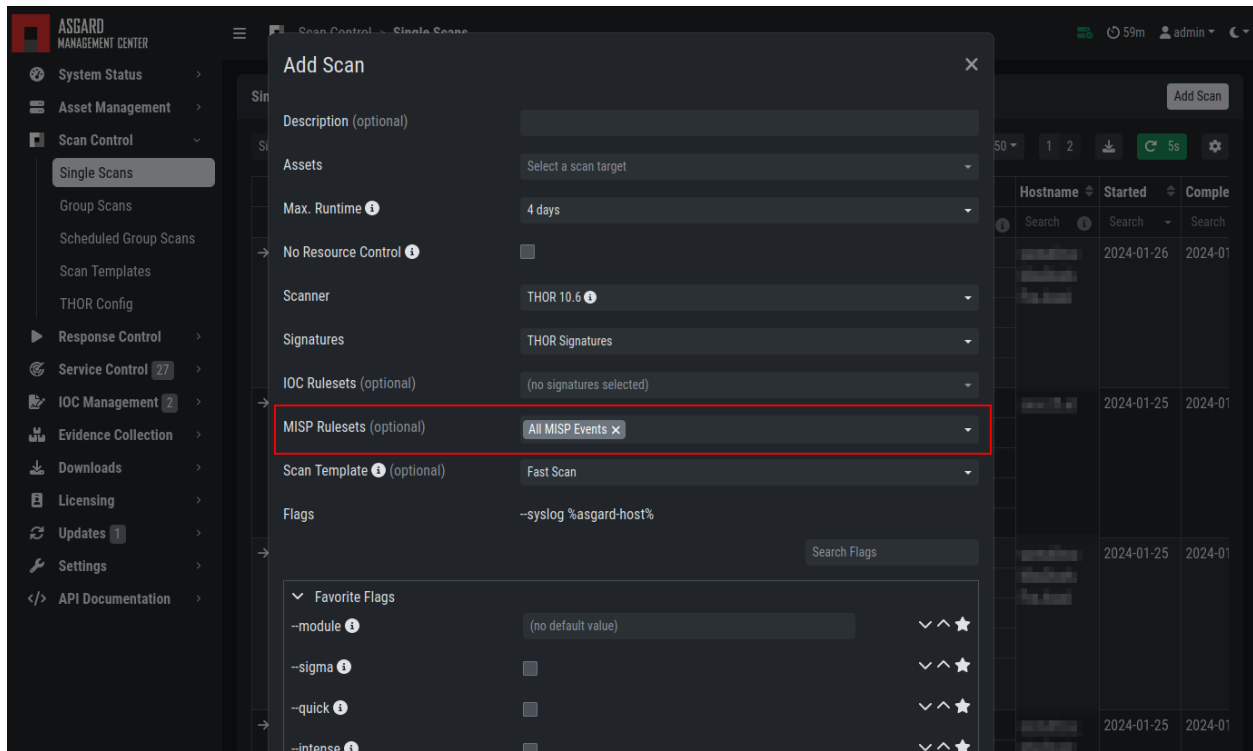


Fig. 70: Scanning with MISP Ruleset

- file>md5
- file>sha1
- file>sha256
- md5
- sha1
- sha256
- yara
- yara>yara
- sigma

**Warning:** Only attributes with the flag IDS set to true will be used by ASGARD. Please make sure that the flag is set if you are intending to use certain events/attributes.

## 3.15 Evidence Collection

### 3.15.1 Collected Evidences

ASGARD provides two forms of collected evidence:

1. Playbook output (file or memory collection, command output)
2. Sample quarantine (sent by THOR via Bifrost protocol during the scan)

All collected evidence can be downloaded in the **Collected Evidence** section.

Path	Size	Hostname	Type	SHA256	Actions
/root/.bash_history	5 KB		Bifrost	e2b17c49ee7c7d88550213ade1d4e267b83fea26d55d7f1d9b3a075c98ac1ac9	Download
/root/test.txt	6 B		Bifrost	521c38abbbb94536b928e06164a1557de83b7fd688c826f66551eccc7193ae	Download
/root/.bash_history	4 KB		Bifrost	35ea08f857a5e2c5a131a7149b6cbcb381bc6de067abda8bca92b6da3a5ccd05	Download
c:\Users\User\AppData\Local\ntuser.log1.txt	8 B		Bifrost	f7ef53d21502321eaecb78bb405b7ff266253b4a27d89b9b8c4da5847cdd1b9d	Download

Fig. 71: Collected Evidence List

### 3.15.2 Bifrost Quarantine

If Bifrost is used with your THOR scans, all collected samples show up here. You will need the "ResponseControl" permission in order to view or download the samples. See section [Roles](#) and [Rights](#) for details.



**Bifrost Quarantine**

1 - 4 of 4 Show 25 1 C ⚙

Name	Size	Hostnames	Type	SHA256	First Bytes	Reason	Actions
.bash_history	5 KB		UNKNOWN	e2b17c49ee7c7d88550213ade1d4e267b83fea26d55d7f1d9b3a075c98ac1ac9	64706b67202d69206772725f332e312e302e325f / d pkg -i grr_3.1.0.2_	Malware file found SCORE: 100 DESC: YARA rule TEST_CUSTOM_RULE / no description SUBSCORE: 100 REF: not set MATCHED: Str1: "Test!"	
test.txt	6 B		UNKNOWN	521c38abbbb94536b928e06164a1557de83b7fd688c826f66551eacca7193ae	54657374210a / Test!	Malware file found SCORE: 100 DESC: YARA rule TEST_CUSTOM_RULE / no description SUBSCORE: 100 REF: not set MATCHED: Str1: "Test!"	
.bash_history	4 KB		UNKNOWN	35ea08f857a5e2c5a131a7149b6cbcb381bc6de067abda8bca92b6da3a5ccd05	64706b67202d69206772725f332e312e302e325f / d pkg -i grr_3.1.0.2_	Malware file found SCORE: 100 DESC: YARA rule TEST_CUSTOM_RULE / no description SUBSCORE: 100 REF: not set MATCHED: Str1: "Test!"	
ntuser.log1.txt	8 B		UNKNOWN	f7ef53d21502321eaecb78bb405b7ff266253b4a27d89b9b8c4da5847cdd1b9d	7465737420313233 / test 123	Malware file found SCORE: 100 DESC: File Name Characteristics SUBSCORE: 100 REF: not set MATCHED: \\AppData\\Local\\ntuser.log1	

Fig. 72: Bifrost Collections

## 3.16 Download Links

The Downloads section lets you create and download a full THOR package including scanner, custom IOCs and MISP rulesets along with a valid license for a specific host. This package can then be used for systems that cannot be equipped with an ASGARD agent for some reason. For example, this can be used on air gapped networks. Copy the package to a flash drive or CD ROM and use it where needed.

You can choose to disable the download token altogether using **Disable Download Token**. If disabled, anyone with network access can download and issue licenses, which may lead to unwanted exhaustion of the ASGARD license pool. You can reset the download token by disabling and then re-enabling it using **New Download Token**.

While selecting different options in the form, the download link changes.

After you have generated a download token and have selected the correct scanner, operating system and target hostname (not FQDN), you can copy the download link and use it to retrieve a full scanner package including a license file for that host. These download links can be sent to administrators or team members that don't have access to ASGARD management center. Remember that the recipients of that link still need to be able to reach ASGARD's web server port (443/tcp). The token can be used to download THOR or a THOR license without an ASGARD account. Attention: If you disable the token, anybody can download THOR from this ASGARD or can generate licenses.

**Note:** The scanner package will not contain a license file if you don't set a hostname in the **Target Hostname** field. If you have an Incident Response license, you must provide it separately.

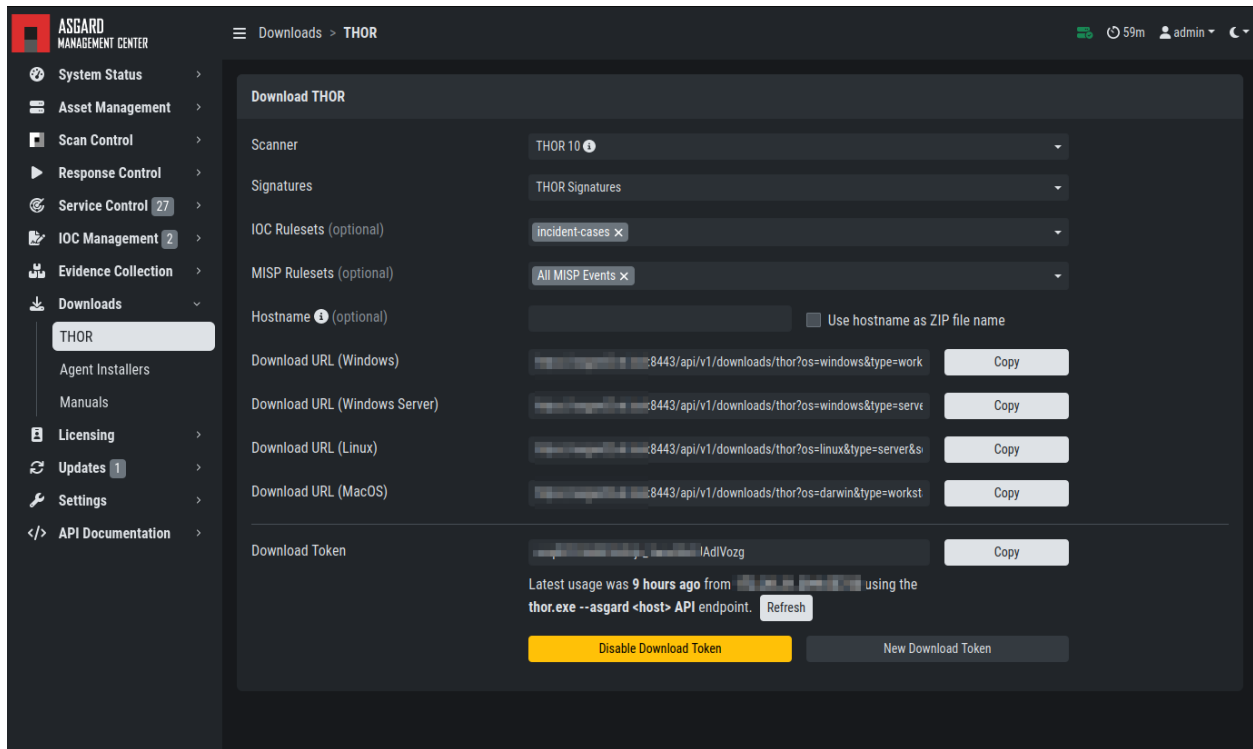


Fig. 73: Download THOR package and license workstation named 'WIN-CLI-DE-1234'

### 3.16.1 Use Case 1 - Share th URL without Hostname

You can generate download links without an included license by leaving the *hostname* field empty. A valid license (e.g. "Incident Response") must be placed in the program folder after the download and extraction.

### 3.16.2 Use Case 2 - Share th URL with Hostname

By including the hostname in the form, a license will be generated and included in the download package. You can copy the final download link and send it to anyone, who can use this link to download a package and run scans on a host with that name.

You or the recipient can change the name in that URL to make it usable on other systems.

Note that you may have to adjust the *type* field to get the correct license type (*client* for workstations, *server* for servers) and the THOR version (*win*, *linux*, *osx*) to generate a correct URL.

```
.../thor?os=windows&type=server&scanner=thor10%40latest&hostname=mywinserver...
.../thor?os=windows&type=workstation&scanner=thor10%40latest&hostname=mywinwks1...
.../thor?os=linux&type=server&scanner=thor10%40latest&hostname=mylinuxsrv1...
```

### 3.16.3 Use Case 3 - Use the URL in Scripts

By default, the generated download link is protected with a token that makes it impossible to download a package or generate a license without knowing that token. This token is specific to every ASGARD instance.

You can use that URL in Bash or PowerShell scripts to automate scans on systems without an installed ASGARD agent.

```
$Type = "server"
$Download_Url = "https://asgard2.nexttron:8443/api/v1/downloads/thor?os=windows&type=$((
↪$Type)&scanner=thor10%4010.6&signatures=signatures&hostname=$((Hostname)&token=$((
↪Token)"
```

## 3.17 Licensing

ASGARD requires an Issuer-License in order to scan systems. The Issuer-License contains the number of asset-, server- and workstation systems that can be scanned with ASGARD Management Center as well as the Aurora service licenses.

ASGARD will automatically issue a valid single-license for a particular system during its initial THOR scan.

The screenshot below shows the licensing section of an ASGARD.

Status	Starts	Expires	Asset Lic.	Server Lic.	Workstation Lic.	Aurora Server Lic.	Aurora Workstation Lic.	Owner	Actions
Valid	2024-02-07	2025-01-09	0 / unlimited	0 / 19484	0 / 500	0 / 500	0 / 500	Private Network (Private)	
Valid	2023-10-30	2024-10-21	0 / unlimited	0 / 10	0 / 10	0 / 0	0 / 0	Private Network (Private)	
Valid	2023-04-26	2024-04-26	18 / unlimited	23 / 19994	8 / 1510	4 / 1500	3 / 1500	Private Network (Private)	

Fig. 74: ASGARD licensing

In addition, ASGARD can create single-licenses that can be used for agent-less scanning. In this case the license is generated and downloaded through the Web frontend.

The following systems require a workstation license in order to be scanned:

- Windows 7 / 8 / 10 / 11
- Mac OS

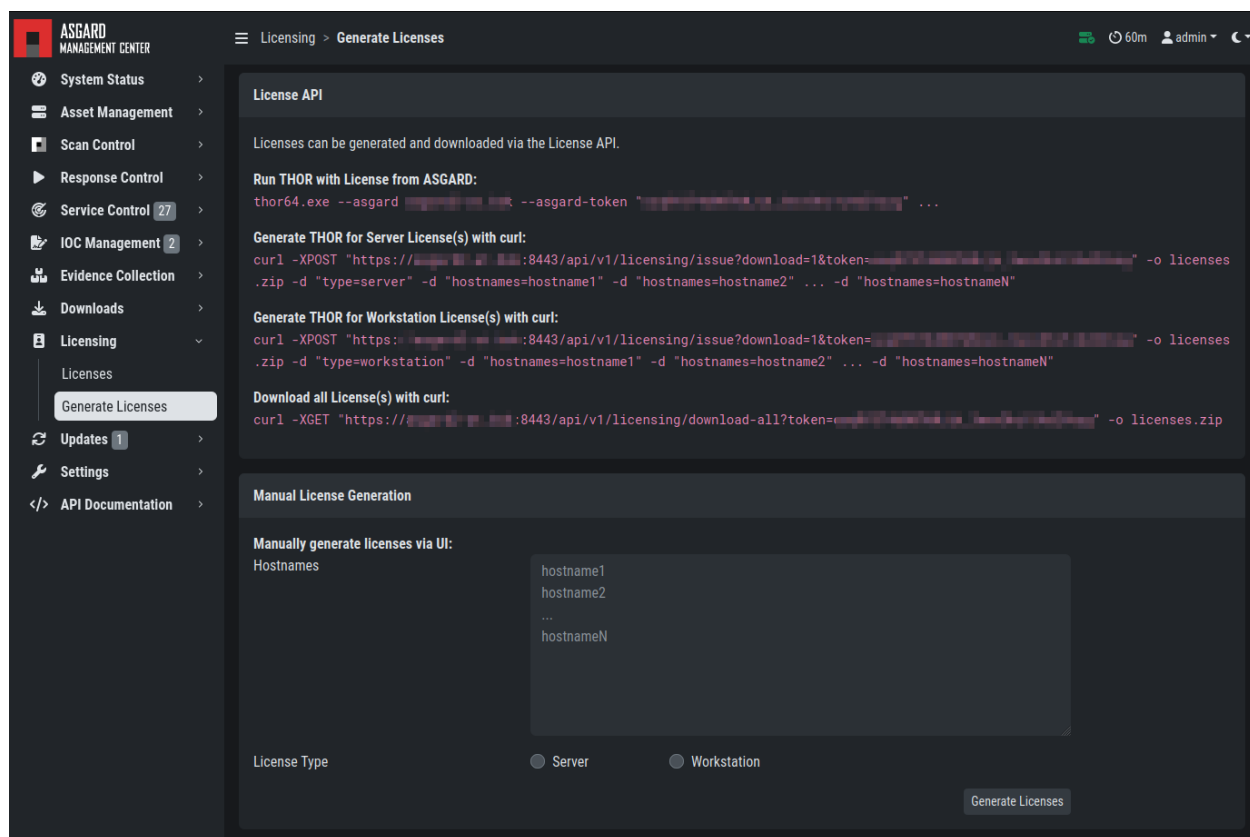


Fig. 75: Generate licenses

The following systems require a server license in order to be scanned:

- All Microsoft Windows server systems
- All Linux systems

The licenses are hostname based except for asset licenses. Asset licenses are issued for each accepted asset as soon as a response action is performed (playbook or remote console access).

## 3.18 Updates

### 3.18.1 ASGARD Updates

ASGARD will search for ASGARD updates on a daily basis. Available updates will automatically be shown in the section Updates.

As soon as an ASGARD update is available, a button Upgrade from ... to ... appears. Clicking this button will start the update process. The ASGARD service will be restarted and the user will be forced to re-login. Generally update MASTER ASGARD before the connected ASGARDs.

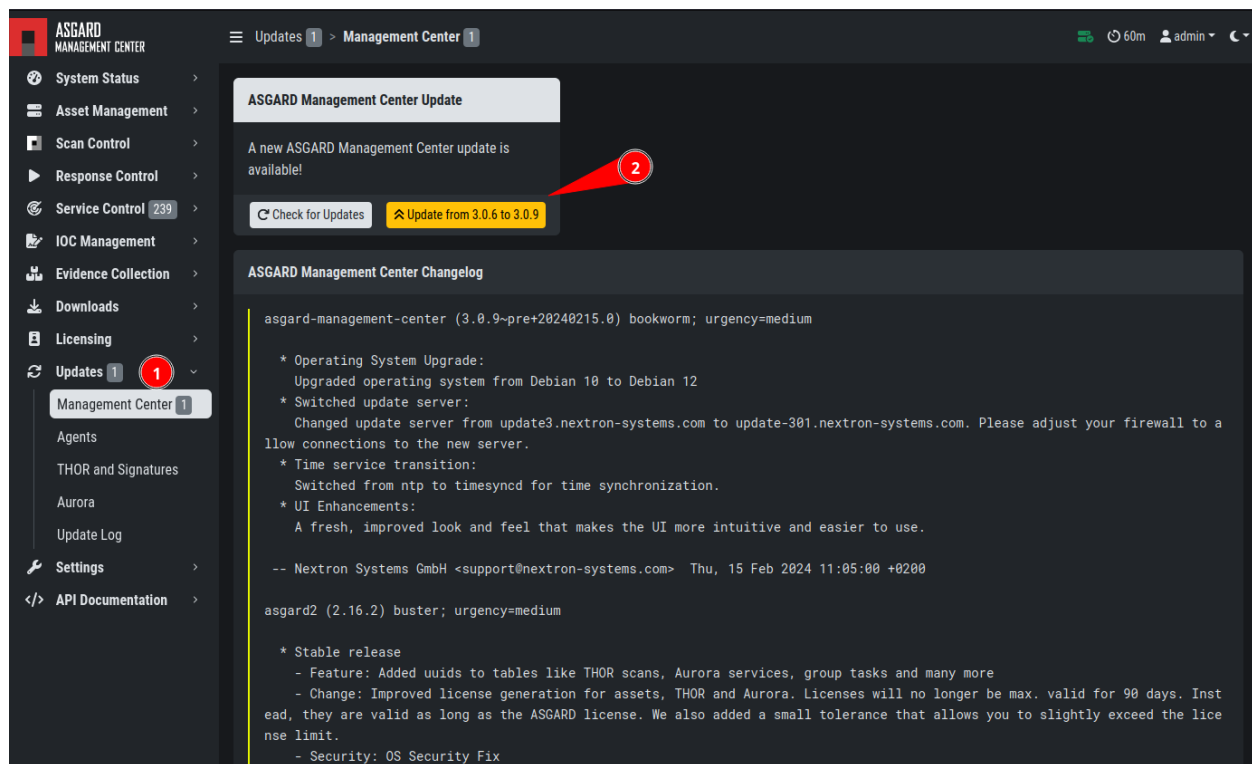
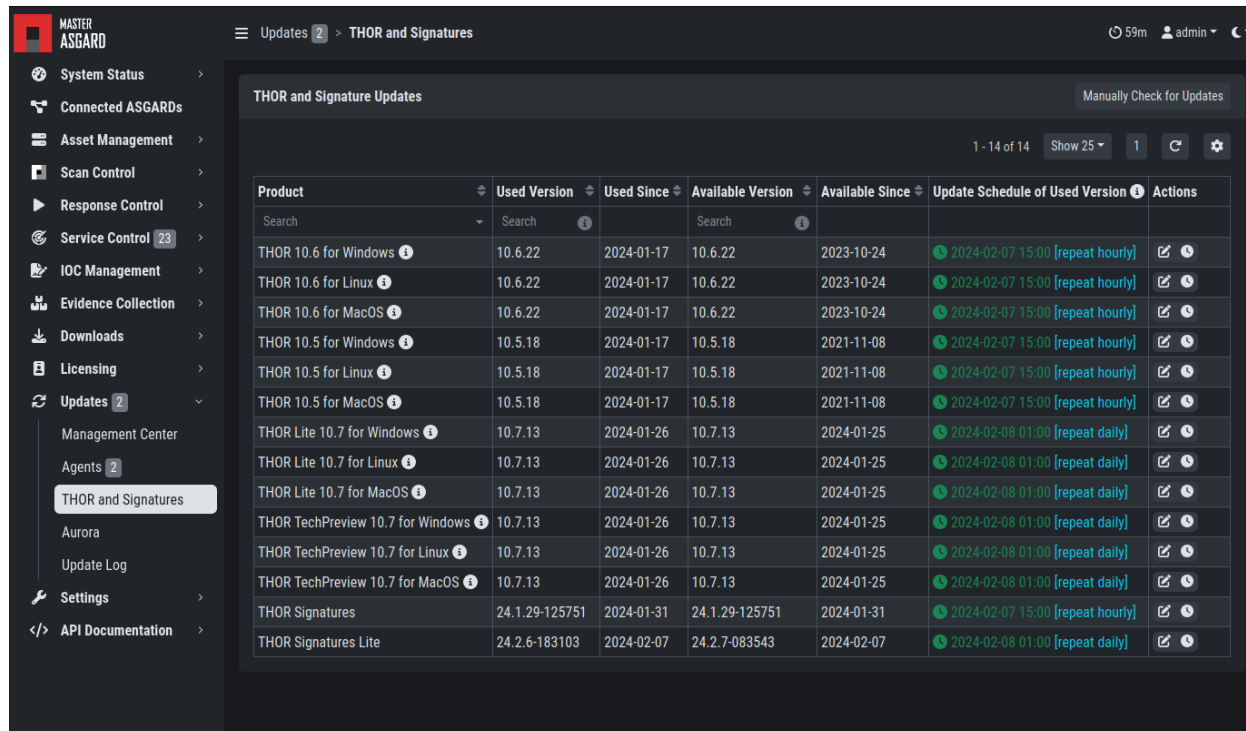


Fig. 76: Updating ASGARD

### 3.18.2 Updates of THOR and THOR Signatures

By default, ASGARD will search for signature updates and THOR updates on an hourly basis. These updates will be set to active automatically. Therefore, a triggered scan will always employ the current THOR version and current signature version. You may disable or modify the automatic THOR and Signature updates by deleting or modifying the entries in this section.



Product	Used Version	Used Since	Available Version	Available Since	Update Schedule of Used Version	Actions
THOR 10.6 for Windows	10.6.22	2024-01-17	10.6.22	2023-10-24	2024-02-07 15:00 [repeat hourly]	[Edit] [Clock]
THOR 10.6 for Linux	10.6.22	2024-01-17	10.6.22	2023-10-24	2024-02-07 15:00 [repeat hourly]	[Edit] [Clock]
THOR 10.6 for MacOS	10.6.22	2024-01-17	10.6.22	2023-10-24	2024-02-07 15:00 [repeat hourly]	[Edit] [Clock]
THOR 10.5 for Windows	10.5.18	2024-01-17	10.5.18	2021-11-08	2024-02-07 15:00 [repeat hourly]	[Edit] [Clock]
THOR 10.5 for Linux	10.5.18	2024-01-17	10.5.18	2021-11-08	2024-02-07 15:00 [repeat hourly]	[Edit] [Clock]
THOR 10.5 for MacOS	10.5.18	2024-01-17	10.5.18	2021-11-08	2024-02-07 15:00 [repeat hourly]	[Edit] [Clock]
THOR Lite 10.7 for Windows	10.7.13	2024-01-26	10.7.13	2024-01-25	2024-02-08 01:00 [repeat daily]	[Edit] [Clock]
THOR Lite 10.7 for Linux	10.7.13	2024-01-26	10.7.13	2024-01-25	2024-02-08 01:00 [repeat daily]	[Edit] [Clock]
THOR Lite 10.7 for MacOS	10.7.13	2024-01-26	10.7.13	2024-01-25	2024-02-08 01:00 [repeat daily]	[Edit] [Clock]
THOR TechPreview 10.7 for Windows	10.7.13	2024-01-26	10.7.13	2024-01-25	2024-02-08 01:00 [repeat daily]	[Edit] [Clock]
THOR TechPreview 10.7 for Linux	10.7.13	2024-01-26	10.7.13	2024-01-25	2024-02-08 01:00 [repeat daily]	[Edit] [Clock]
THOR TechPreview 10.7 for MacOS	10.7.13	2024-01-26	10.7.13	2024-01-25	2024-02-08 01:00 [repeat daily]	[Edit] [Clock]
THOR Signatures	24.1.29-125751	2024-01-31	24.1.29-125751	2024-01-31	2024-02-07 15:00 [repeat hourly]	[Edit] [Clock]
THOR Signatures Lite	24.2.6-183103	2024-02-07	24.2.7-083543	2024-02-07	2024-02-08 01:00 [repeat daily]	[Edit] [Clock]

Fig. 77: Automatic Scanner and Signature Updates

It is possible to intentionally scan with an old scanner version by clicking on the pencil icon and selecting the respective version from the drop-down menu.

Please be aware, that this is a global setting and will affect all scans!

**Hint:** You can trigger a Manual Check and download new THOR packages by clicking **Manually Check for Updates**. This can also be used in new ASGARD installations, as sometimes it takes a while until ASGARD does this automatically.

### 3.18.3 Agent Updates

If an asset or an agent can be update, there will be a notice shown in the Updates > Agents tab.

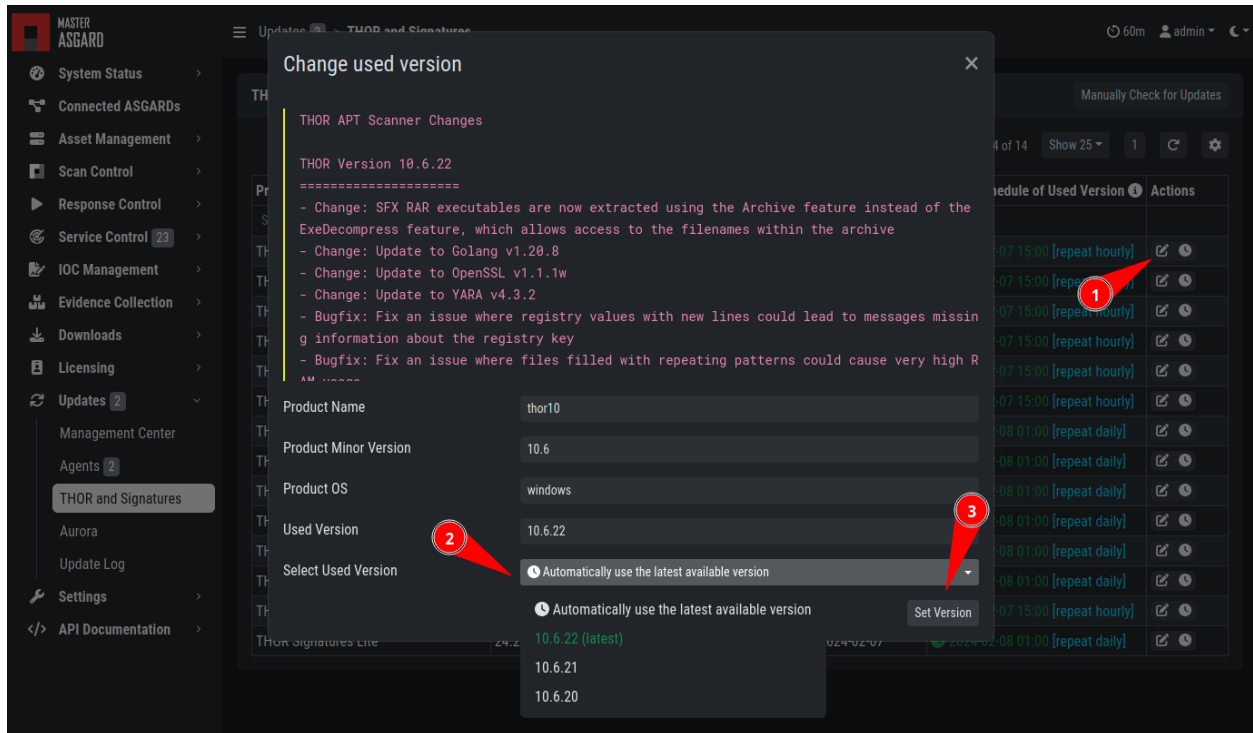


Fig. 78: Selecting a Scanner Version manually

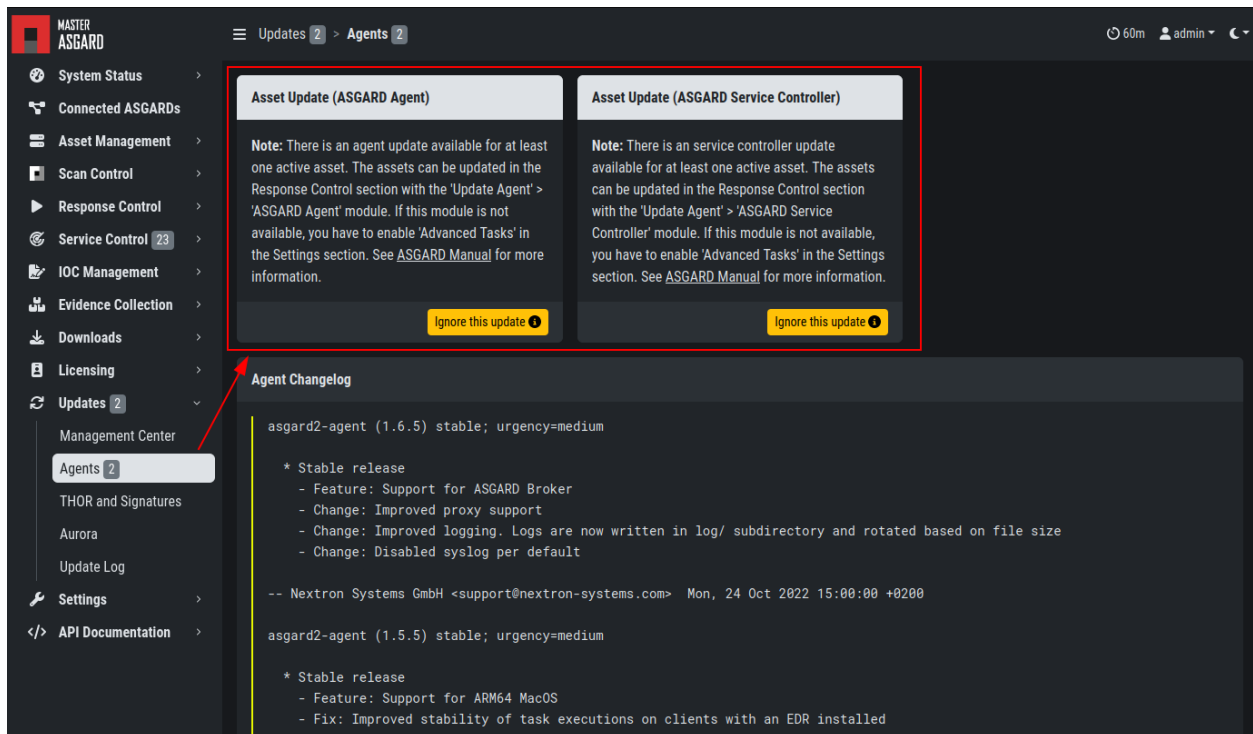


Fig. 79: Update Agent

## 3.19 User Management

Access user management via **Settings > Users**. This section allows administrators to add or edit user accounts.

The field **2FA** in the overview indicates if a user has **Two Factor Authentication** enabled or not.

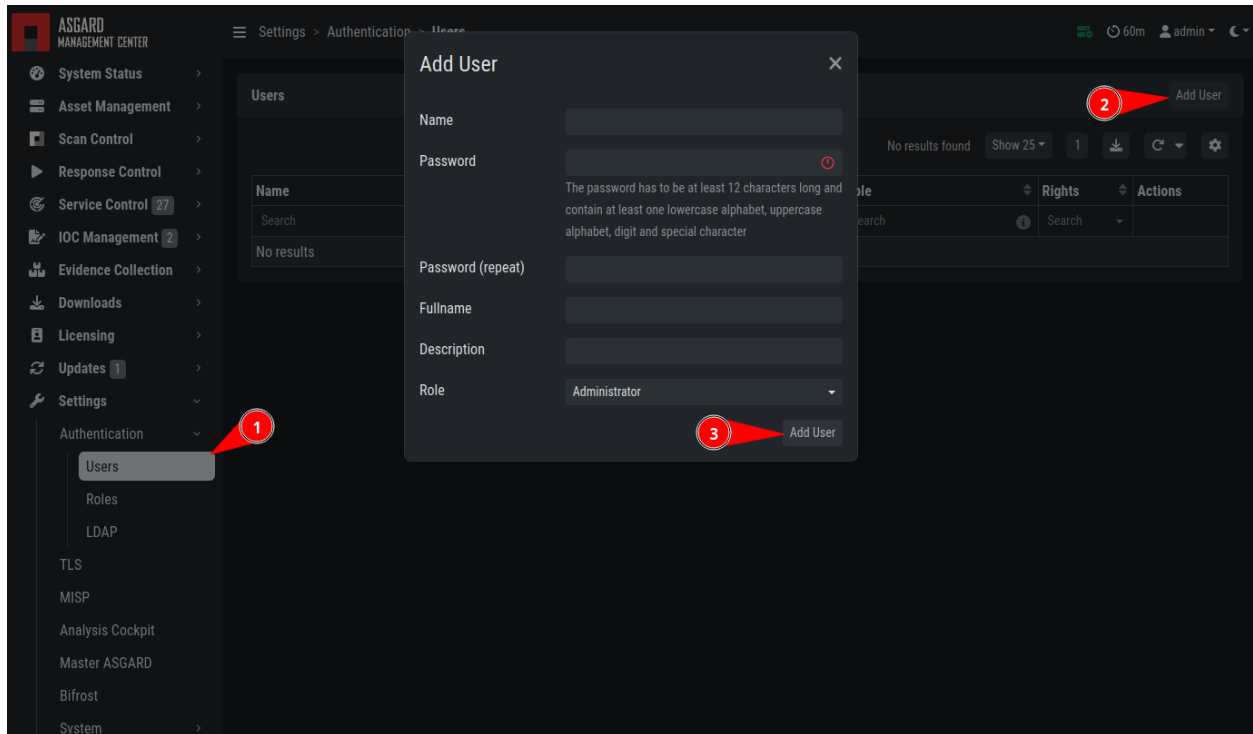


Fig. 80: Add User Account

Editing a user account does not require a password although the fields are shown in the dialogue. An initial password has to be provided for user creation, though.

Access the user roles in **Settings > Roles**.

You can download a list of all users in CSV format.

### 3.19.1 Roles

By default, ASGARD ships with the following pre-configured user roles. The pre-configured roles can be modified or deleted. The ASGARD role model is fully configurable.

Note that all users except users with the right **Readonly** have the right to run scans on endpoints.

The following section describes these predefined rights and restrictions that each role can have.



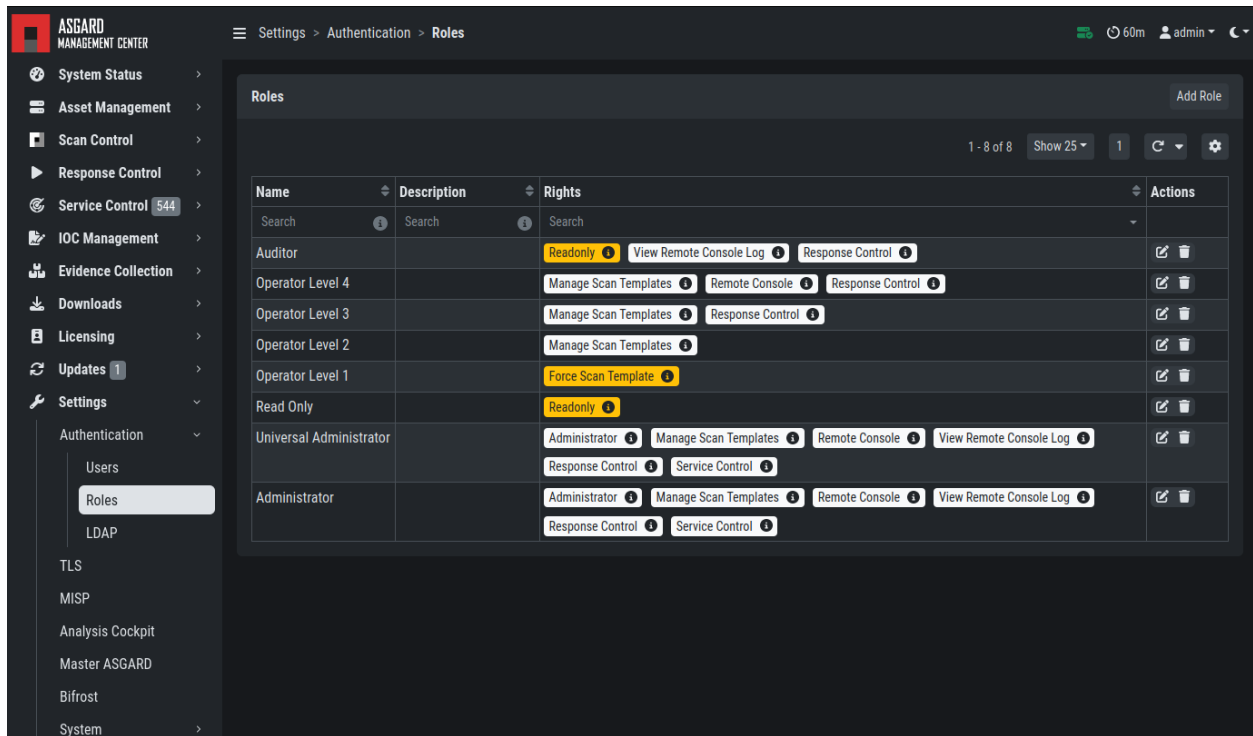


Fig. 81: User Roles – Factory Defaults

### 3.19.2 Rights

Role	Permissions
Administrator	Unrestricted
Manage Scan Templates	Allows scan templates management
Remote Console	Connect to endpoints via remote console
View Remote Console Log	Review the recordings of all remote console sessions
Response Control	Run playbooks, including playbooks for evidence collection, to kill processes or isolate an endpoint
Service Control	User can manage services on endpoint, e.g. Aurora

### 3.19.3 Restrictions

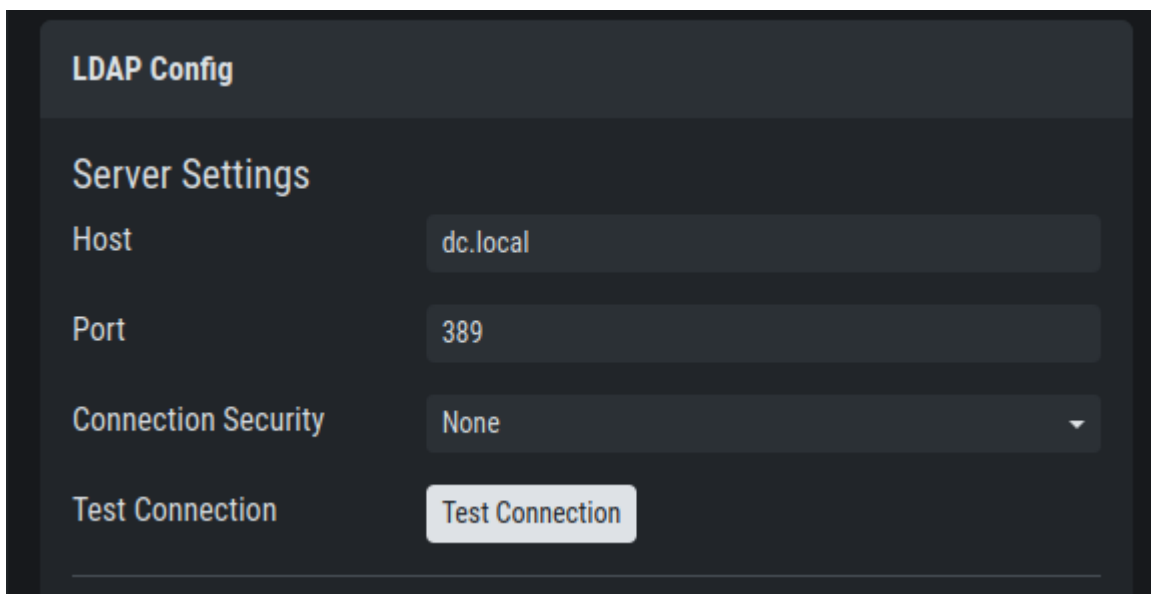
Role	Restrictions
Force Scan Template <sup>2</sup>	Force user to use predefined scan templates that are not restricted
No Inactive Assets <sup>Page 103, 2</sup>	Cannot view inactive assets in asset management.
No Task Start <sup>2</sup>	Cannot start scans or task (playbooks)
Readonly <sup>2</sup>	Can't change anything, can't run scans or response tasks. Used to generate read-only API keys

<sup>2</sup> Restricted Roles have a yellow font in the UI

### 3.19.4 LDAP Configuration

In order to configure LDAP, navigate to **Settings > LDAP**. In the left column you can test and configure the LDAP connection itself. In the right column, the mapping of LDAP groups to ASGARD groups (and its associated permissions) is defined.

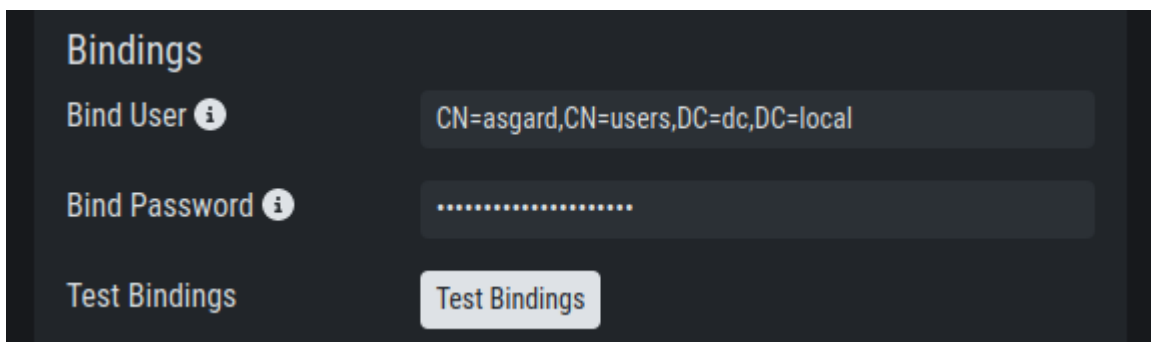
First check if your LDAP server is reachable by ASGARD by clicking "Test Connection".



The screenshot shows the 'LDAP Config' window with a 'Server Settings' section. It contains four fields: 'Host' with the value 'dc.local', 'Port' with the value '389', 'Connection Security' with a dropdown menu set to 'None', and a 'Test Connection' button.

Fig. 82: Configure the LDAP Server

Then check the bind user you want to use for ASGARD. Read permissions on the bind user are sufficient. To find out the distinguished name you can use an LDAP browser or query using the PowerShell AD module command `Get-ADUser <username>`.



The screenshot shows the 'Bindings' section of the configuration interface. It includes a 'Bind User' field with the value 'CN=asgard,CN=users,DC=dc,DC=local', a 'Bind Password' field with masked characters (dots), and a 'Test Bindings' button.

Fig. 83: Configure the LDAP Bind User

Next configure the LDAP filters used to identify the groups and users and their preferred attributes in your LDAP structure. A default for LDAP and AD in a flat structure is given in the "**Use recommended filters**" drop-down menu, but you can adapt it to your liking. The test button shows you if a login with that user would be successful and which groups ASGARD identified and could be used for a mapping to ASGARD groups.

If you need to adapt the recommended configuration or want to customize it, we recommend an LDAP browser such as [ADExplorer](#) from Sysinternals to browse your LDAP structure. As an example you

Base

Base ⓘ DC=dc,DC=local

Users and Groups

Use recommended filters Microsoft Active Directory ▼

User Filter ⓘ (&(objectClass=user)(objectCategory=user)(sAMAccountName=%s))

Group Filter ⓘ (&(objectCategory=group)(objectClass=group)(member=%s))

User UID ⓘ dn

Group GID ⓘ cn

Test Users and Groups asgard ..... Test Login

Update LDAP Config

Fig. 84: Configure the LDAP User and Group Filters

could use your organization's e-mail address as a user login name if you change the "User Filter" to (&(objectClass=user)(objectCategory=user)(userPrincipalName=%s))

**Note:** You need to save the configuration by clicking **Update LDAP Config**. Using the test buttons only uses the data in the forms, but does not save it, so that you can use it for testing purposes anytime, without changing your working configuration.

After the LDAP configuration is set up, you need to provide role mapping from LDAP groups to ASGARD groups. This is done in the right column by using the **Add LDAP Role** feature.

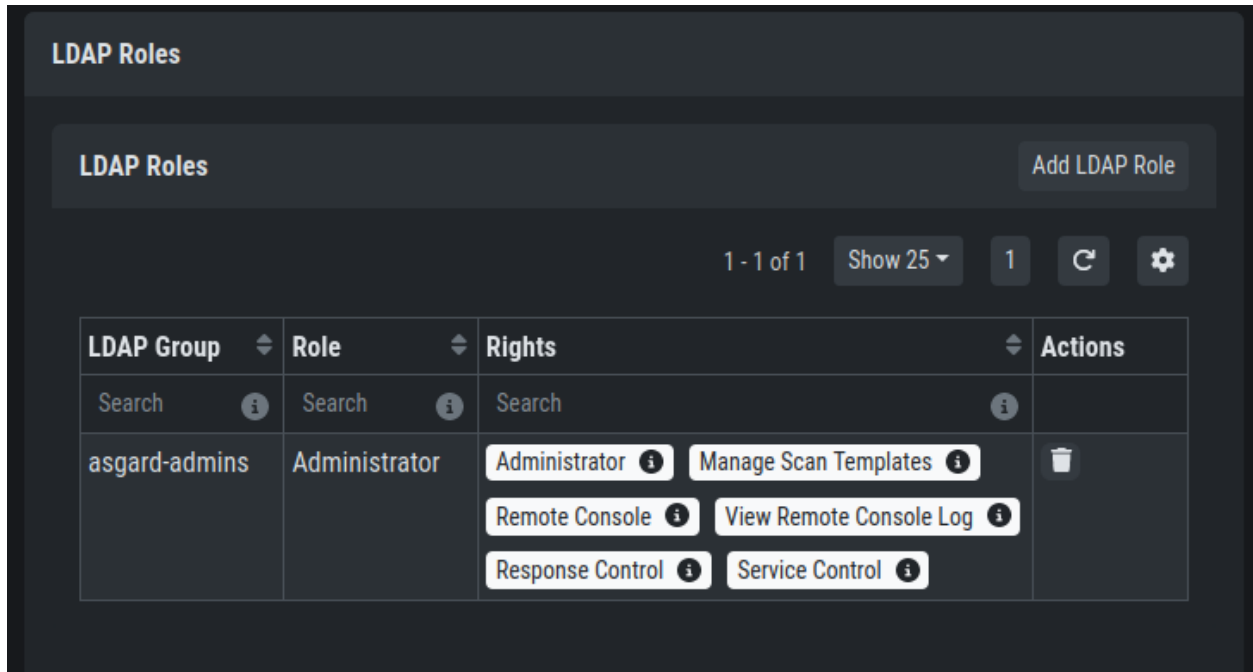


Fig. 85: LDAP Group to ASGARD Role Mapping

## 3.20 Additional Settings

### 3.20.1 Rsyslog Forwarding

Rsyslog forwarding can be configured in **Settings > System > Rsyslog**. To add a forwarding configuration for local log sources, click **Add Rsyslog Forwarding**.

The following log sources can be forwarded individually:

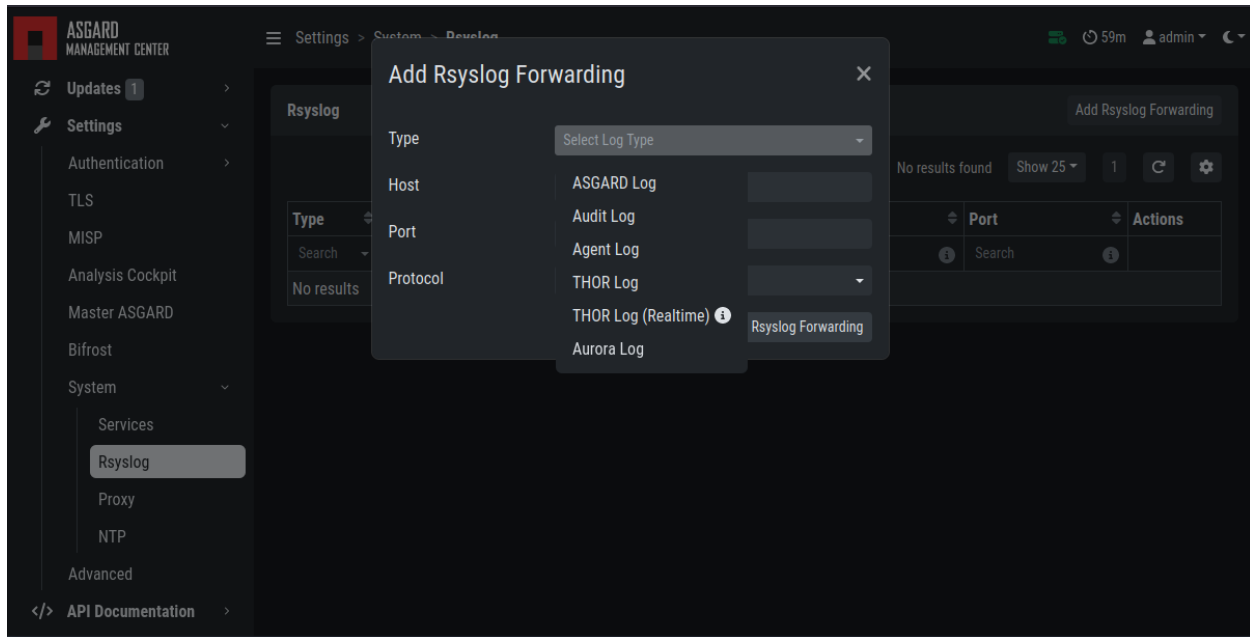


Table 1: Available Log Sources

Log	Description
ASGARD Log	Everything related to the ASGARD service, processes, task and scan jobs
ASGARD Audit Log	Detailed audit log of all user activity within the system
Agent Log	All ASGARD agent activities
THOR Log	THOR scan results
Thor Log (Realtime)	The THOR (Realtime) logs are the same logs as THOR logs, except that they are collected via udp syslog instead of https. To forward THOR logs in realtime, you have to configure your scans to forward syslog to ASGARD, see <a href="#">Syslog Forwarding</a> ). Make sure the necessary firewall rules are in place to allow the asset to communicate with the ASGARD.
Aurora Log	Aurora Logs

### 3.20.2 TLS Certificate Installation

Instead of using the pre-installed self-signed TLS Certificate, users can upload their own TLS Certificate for ASGARD.

In order to achieve the best possible compatibility with the most common browsers, we recommend using the system's FQDN in both fields **Common Name** AND **Hostnames**.

Please note that generating a CSR on the command line is not supported.

The generated CSR can be used to generate a TLS Certificate. Subsequently, this TLS Certificate can be uploaded in the **Settings > TLS** section.

**Note:** Please see [Install TLS certificates on ASGARD and MASTER ASGARD](#) for a guide on how to sign the CSR and install it in your ASGARD.

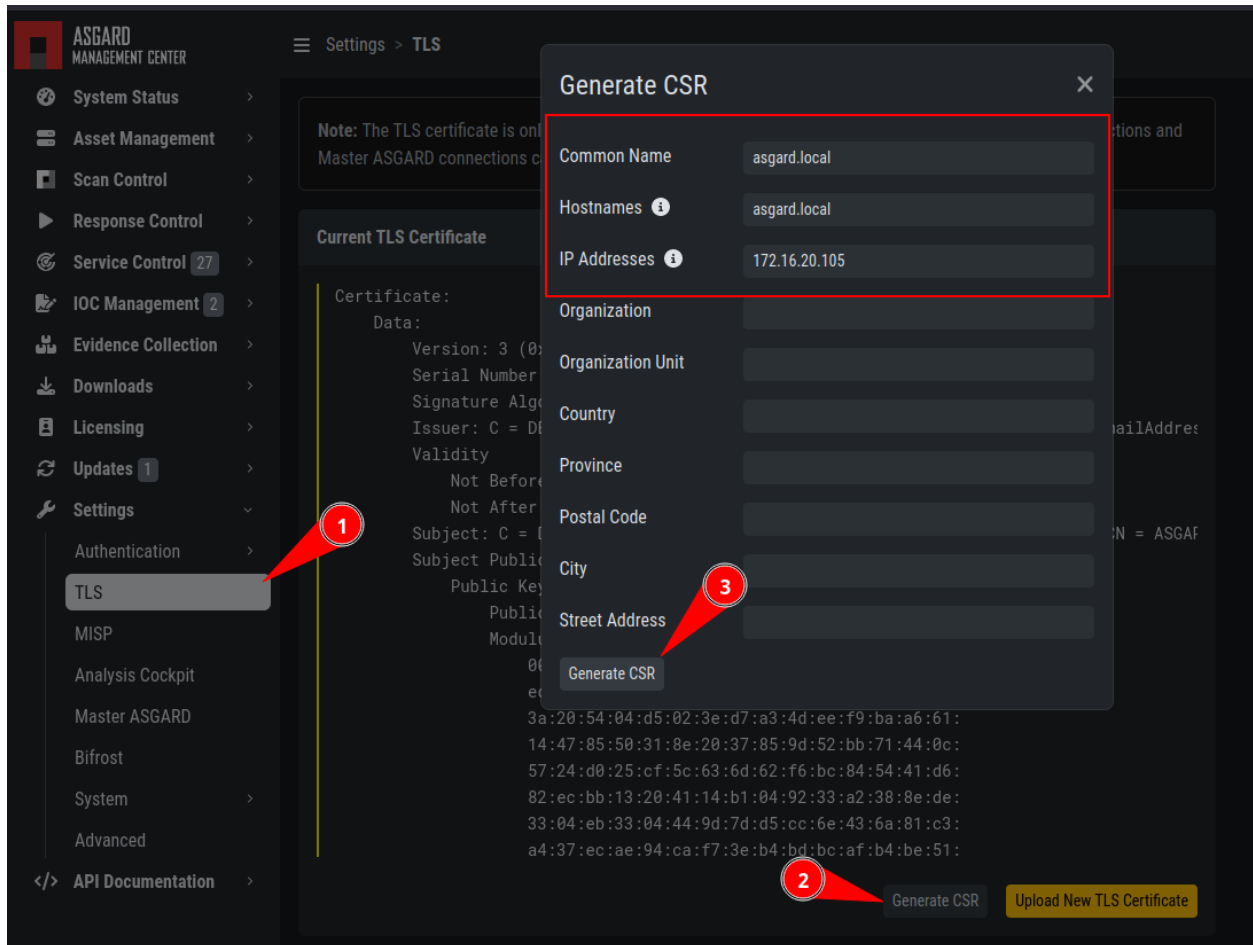


Fig. 86: Generate a Certificate Signing Request (CSR)

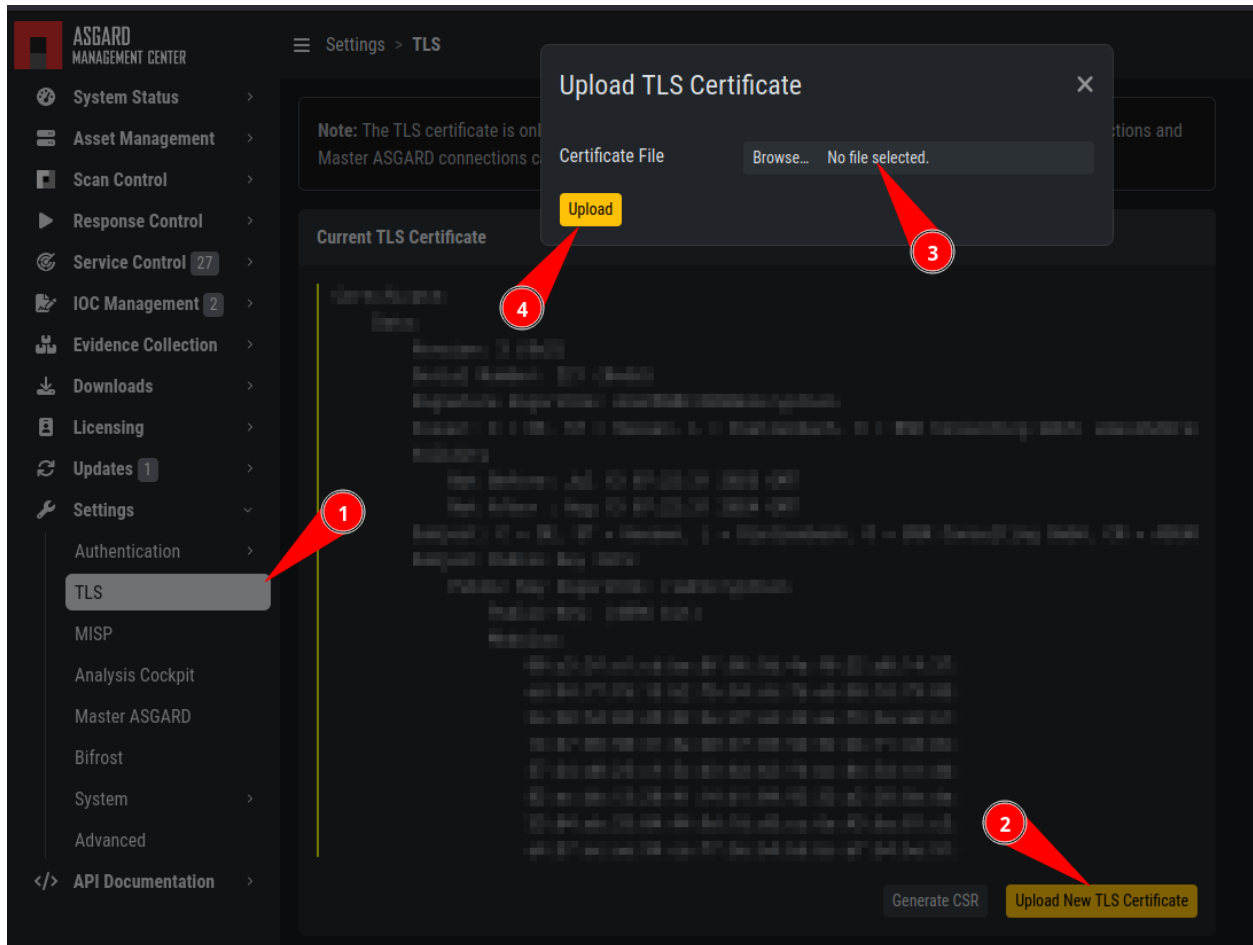


Fig. 87: Upload a TLS Certificate

### 3.20.3 Manage Services

The individual ASGARD services can be managed in **Settings > System > Services**. The services can be stopped or restarted with the respective buttons in the **Actions** column.

The screenshot shows the ASGARD Management Center interface. The left sidebar contains navigation options: Response Control, Service Control (27), IOC Management (2), Evidence Collection, Downloads, Licensing, Updates (1), and Settings. The Settings menu is expanded, showing sub-options: Authentication, TLS, MISP, Analysis Cockpit, Master ASGARD, Bifrost, System, Services (selected), Rsyslog, Proxy, NTP, and Advanced. The main content area is titled 'Services' and shows a table of services. The table has columns: Service, Description, Active, Active Since, Auto Start, and Actions. The table lists four services: asgard-management-center, mariadb, rsyslog, and systemd-timesyncd. All services are active (Yes) and have auto-start enabled (Yes). The Actions column contains a refresh icon for each service.

Service	Description	Active	Active Since	Auto Start	Actions
Search	Search	Search	Search	Search	
asgard-management-center	ASGARD Management Center	Yes	Thu 2024-01-18 16:18:21 CET	Yes	Refresh
mariadb	MariaDB Database	Yes	Thu 2024-01-18 16:17:14 CET	Yes	Refresh
rsyslog	Log processing	Yes	Thu 2024-01-18 16:16:43 CET	Yes	Refresh
systemd-timesyncd	Clock synchronization	Yes	Mon 2024-01-22 12:08:38 CET	Yes	Refresh

Fig. 88: Manage Services

### 3.20.4 NTP Configuration

The current NTP configuration can be found **Settings > System > NTP**.

You can add or delete NTP servers by adding/changing the values in the text fields. After you are done with your changes, click **Save** and **Restart NTP** to save your changes.



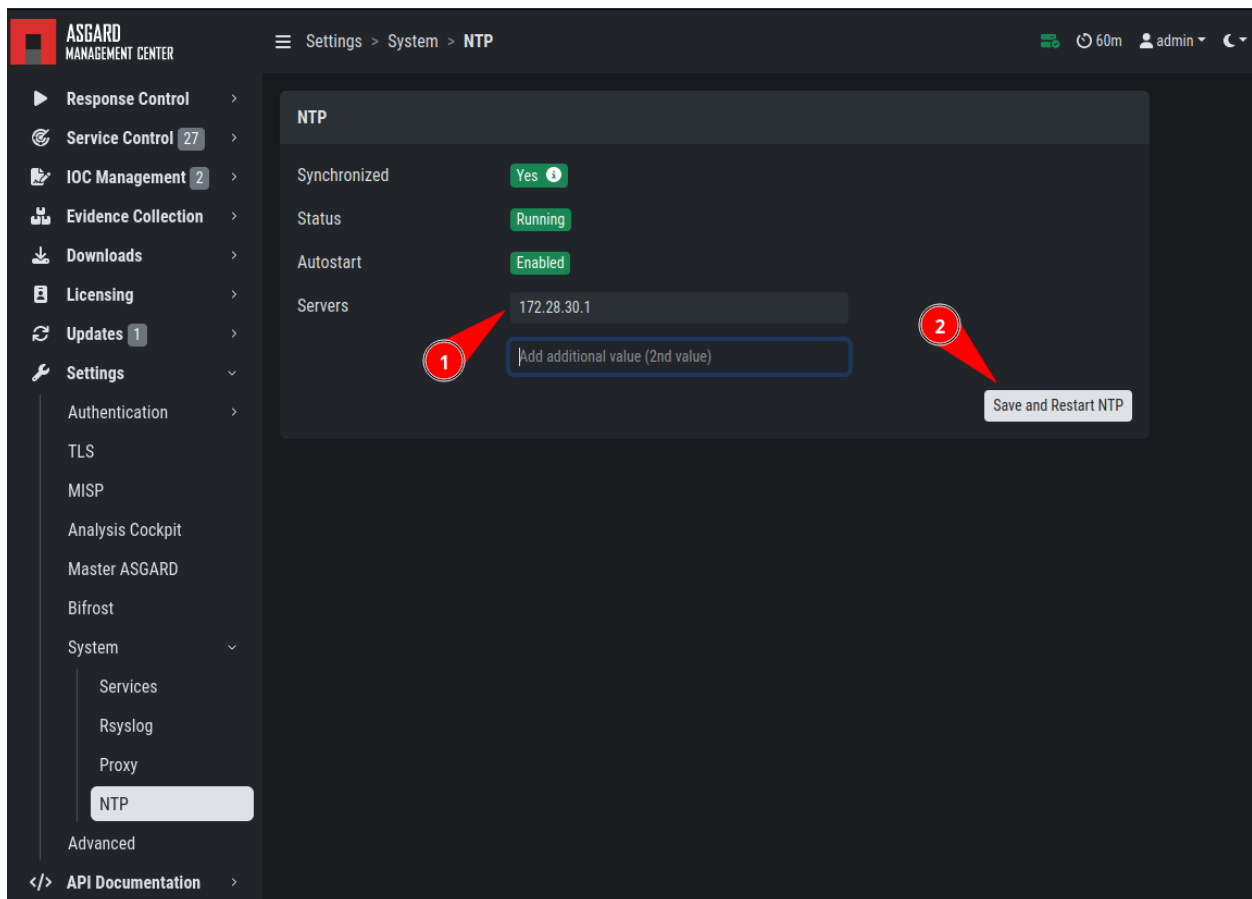


Fig. 89: NTP configuration

### 3.20.5 Settings for Bifrost

Bifrost allows you to automatically upload suspicious files to your ASGARD during a THOR scan. If an Analysis Cockpit is connected, these files get automatically forwarded to the Analysis Cockpit in order to drop them into a connected Sandbox system. However, the collected files will stay on ASGARD for the amount of time specified in Retention time (0 days represent an indefinite amount of time).

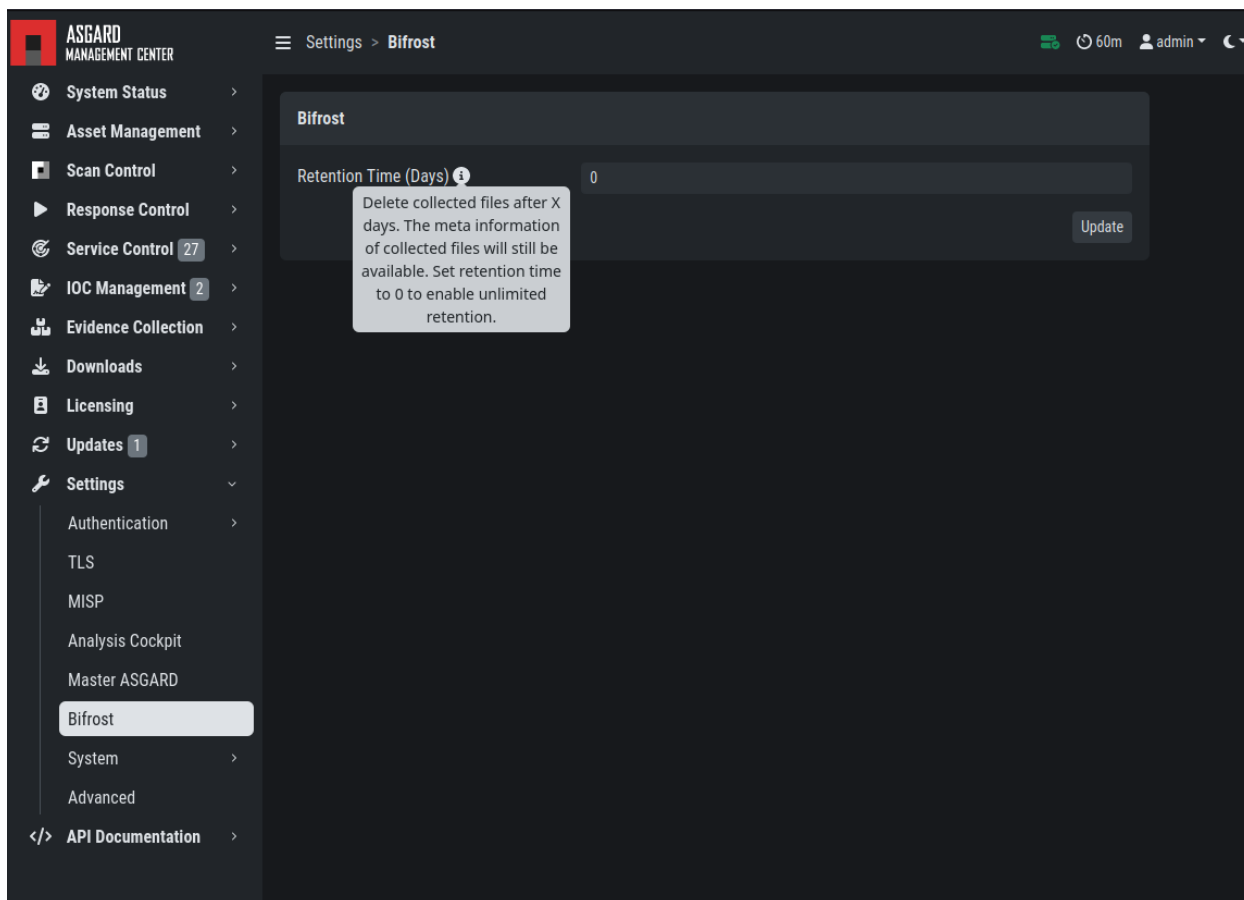


Fig. 90: Settings for Bifrost

The collected files can be downloaded in the Evidence Collection section. All files are zip archived and password protected with the password infected.

In order to automatically collect suspicious files, you have to create a scan with Bifrost enabled. Check the Send Suspicious Files to ASGARD option to send samples to the system set as bifrost2Server. Use the placeholder %asgard-host% to use the hostname of you ASGARD instance as the Bifrost server.

This will collect all files with a score of 60 or higher and make them available for download in ASGARDs Collected Files section.

For Details on how to automatically forward to a sandbox system please refer to the [Analysis Cockpit Manual](#).

Flags

--bifrost2Server %asgard-host% --syslog %asgard-host%

bifrost

--bifrost2Server ⓘ

☒ Send Suspicious Files to ASGARD

%asgard-host%

Add Scan

Fig. 91: Scan option for Bifrost

### 3.20.6 Link Analysis Cockpit

In order to connect to an Analysis Cockpit, enter the respective hostname of the Analysis Cockpit (use the same FQDN used during installation of the Analysis Cockpit) in the field FQDN, enter the one-time code, choose the type and click Update Analysis Cockpit.

ASGARD MANAGEMENT CENTER

Settings > Analysis Cockpit

58m admin

Analysis Cockpit Settings

FQDN ⓘ analysis.local

One-Time Code .....

Type Analysis Cockpit 4

Update Analysis Cockpit

System Status >

Asset Management >

Scan Control >

Response Control >

Service Control 27 >

IOC Management 2 >

Evidence Collection >

Downloads >

Licensing >

Updates 1 >

Settings >

Authentication >

TLS

MISP

Analysis Cockpit

Master ASGARD

Bifrost

System >

Fig. 92: Linking the Analysis Cockpit

The Cockpit's API key can be found at Settings > Link Products > Management Center.

ASGARD must be able to connect to the Analysis Cockpit on port 443/TCP for a successful integration. Once connected, the Cockpit will show up in ASGARD's System Status > Overview section together with the other connectivity tests.

Please wait up to five minutes for the status to change on ASGARD's system status page. It will change from Not linked to Online.

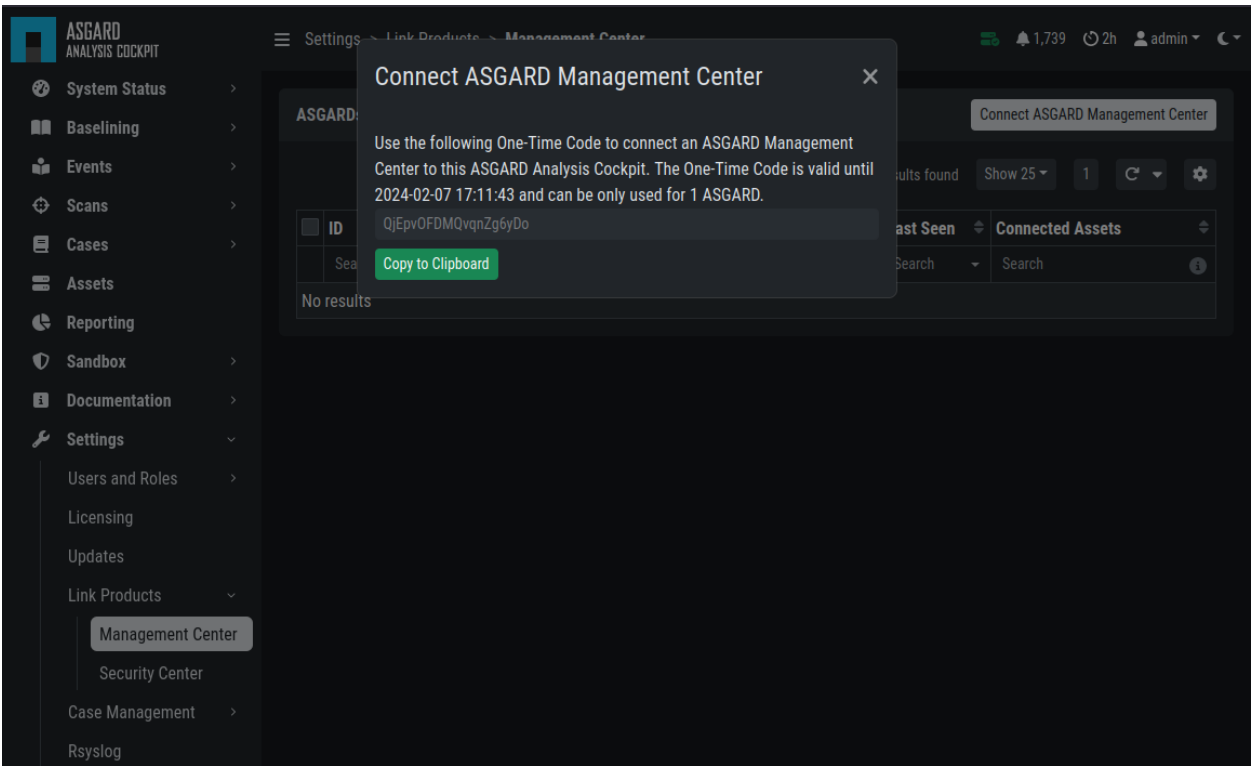


Fig. 93: Analysis Cockpit API Key

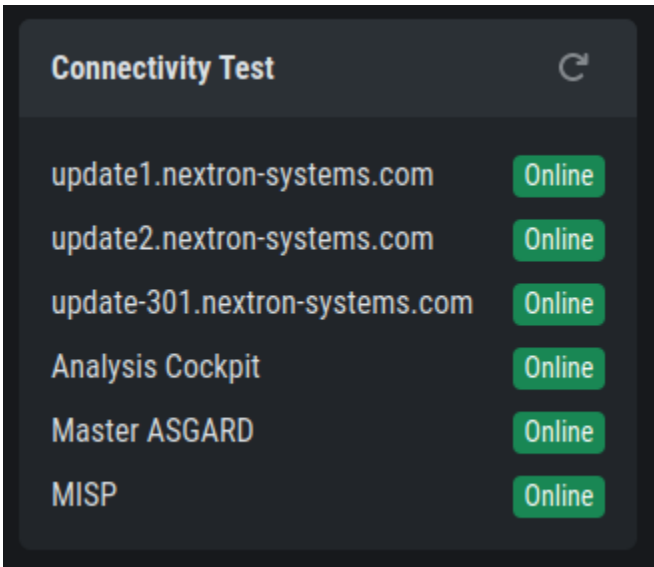


Fig. 94: Connectivity Test

### 3.20.7 Link MASTER ASGARD

In order to control your ASGARD with a MASTER ASGARD, you must generate a One-Time Code and use it in the "Add ASGARD" dialogue within the MASTER ASGARD frontend.

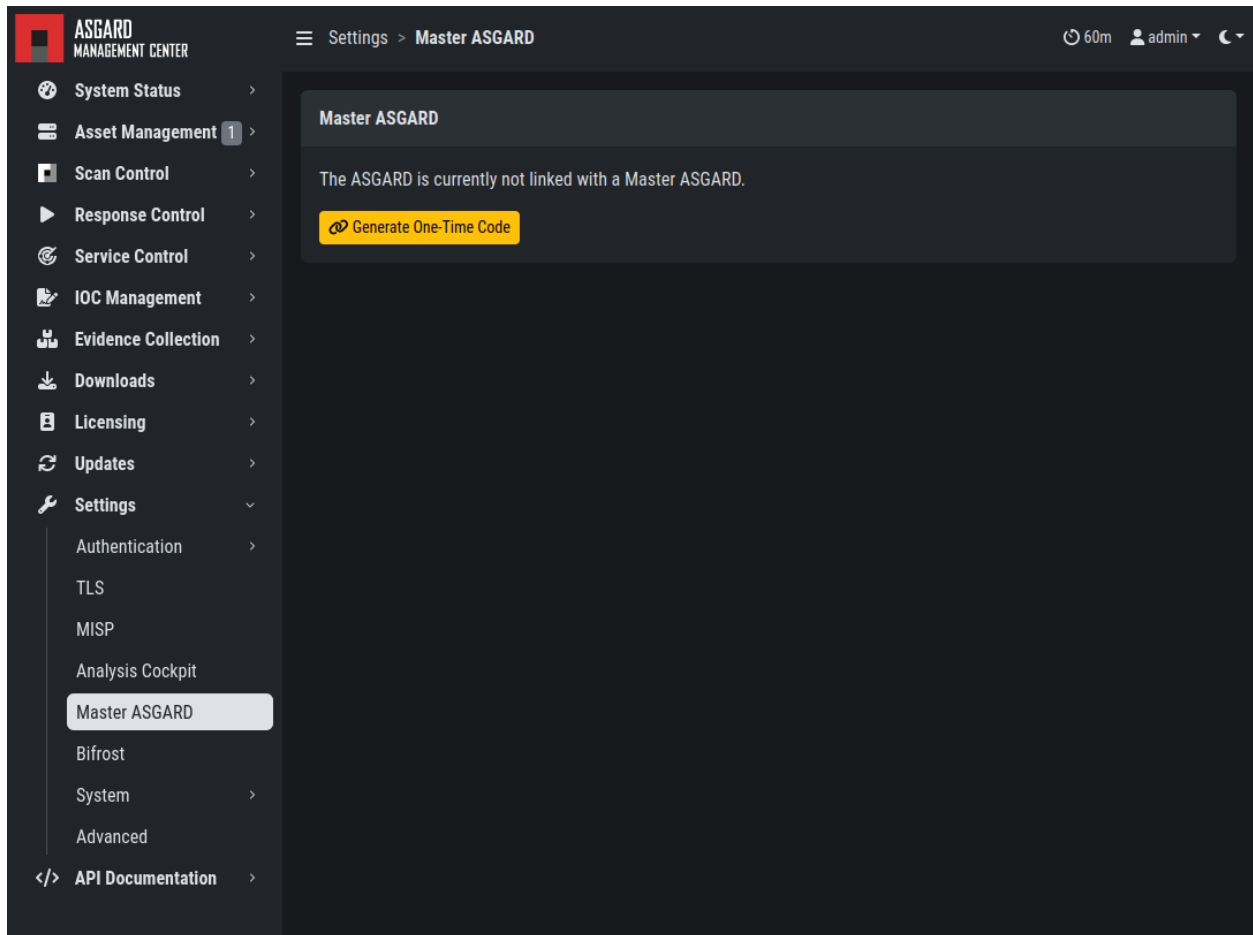


Fig. 95: Link MASTER ASGARD

Please see [Link ASGARD Systems with Master ASGARD](#) for more information.

### 3.20.8 Link MISP

In order to connect to a MISP with your ASGARD Management Center, navigate to Settings > MISP. Insert the MISP's address, along with the API Key and click Test and Link MISP.

The MISP connectivity status is shown in the Overview section. Please allow five minutes for the connection status to indicate the correct status, and also MISP rules to be downloaded and shown in IOC Management > MISP > MISP Events.

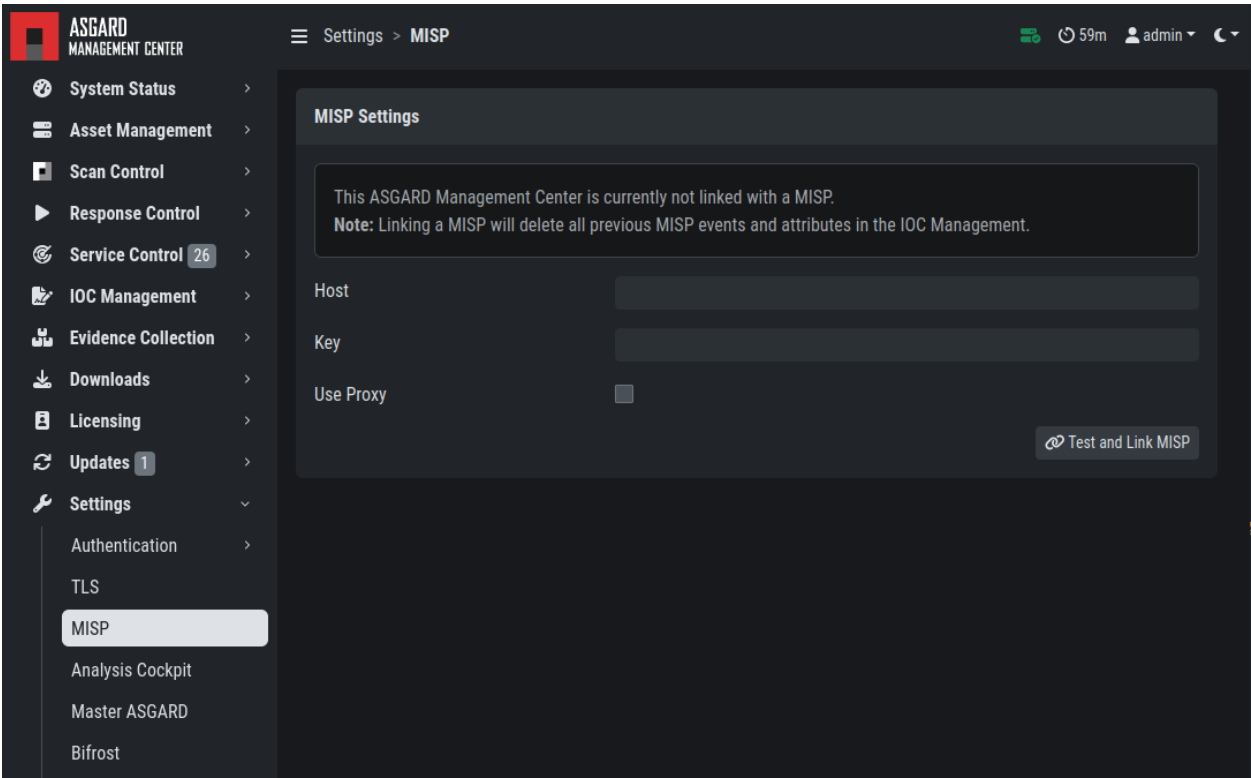


Fig. 96: Linking a MISP to ASGARD

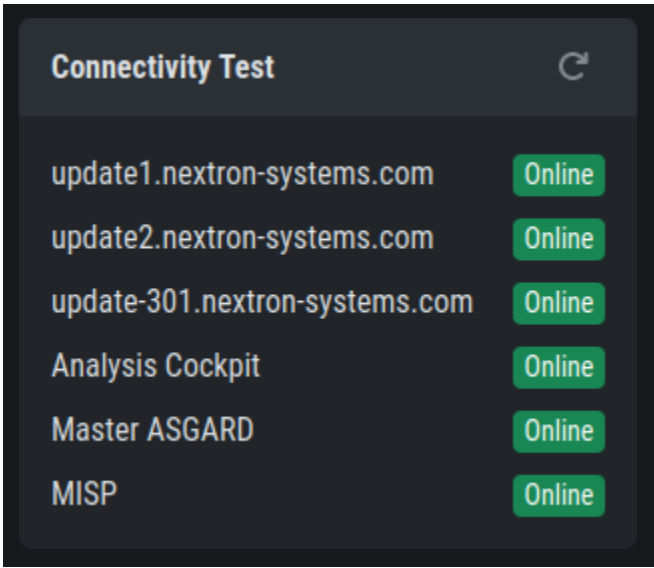


Fig. 97: MISP connectivity status

### 3.20.9 Change Proxy Settings

In this dialogue, you can add or modify ASGARDe proxy configuration. Please note, you need to restart the ASGARD service (Tab Services) afterwards.

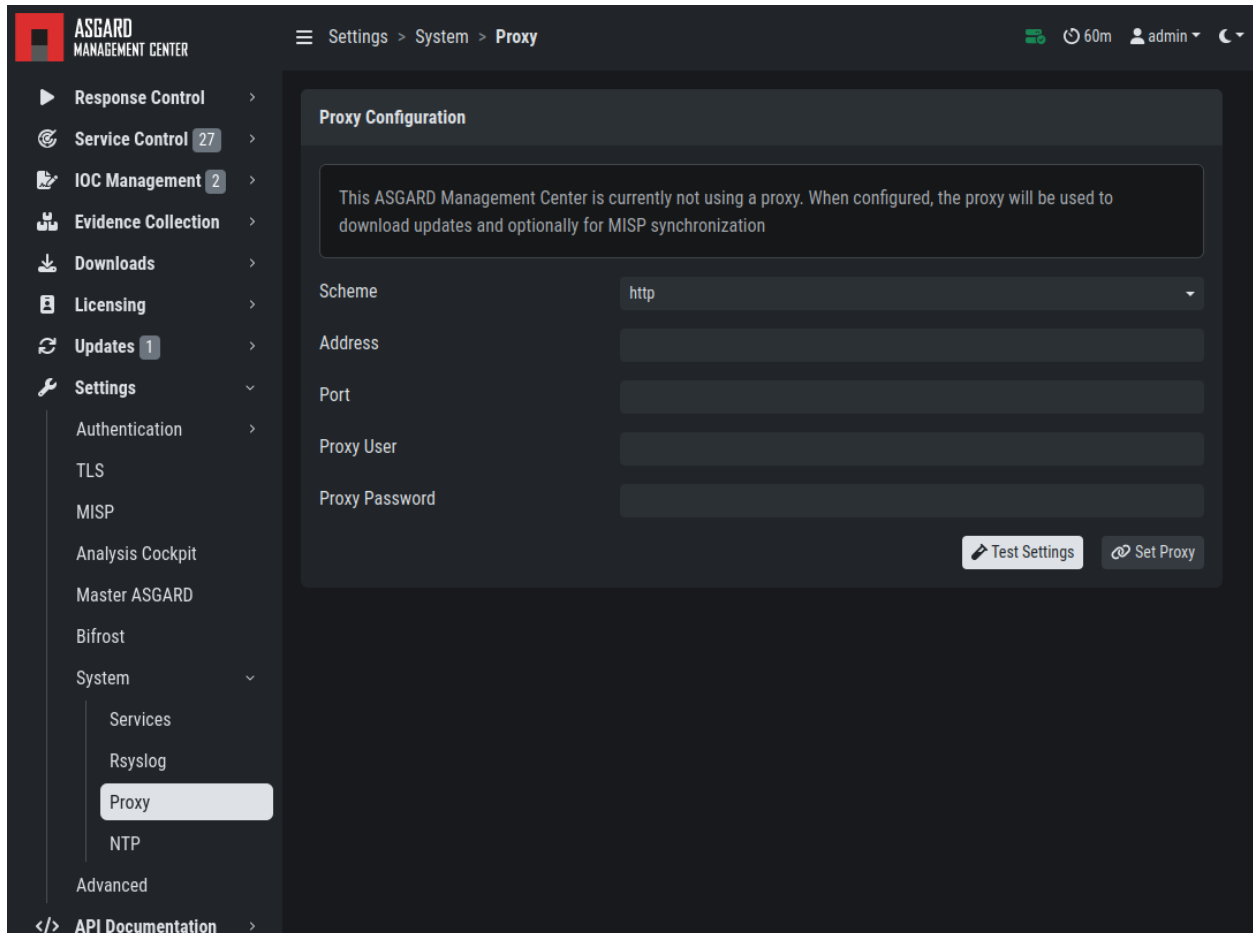


Fig. 98: Change Proxy Settings

## 3.21 Advanced Settings

The Advanced tab lets you specify additional global settings. The session timeout for web-based UI can be configured. Default is one hour. If Show Advanced Tasks is set, ASGARD will show system maintenance jobs (e.g. update ASGARD Agent on endpoints) within the response control section.

Inactive assets can be hidden in the Asset Management Section by setting a suitable threshold for Hide inactive Assets.

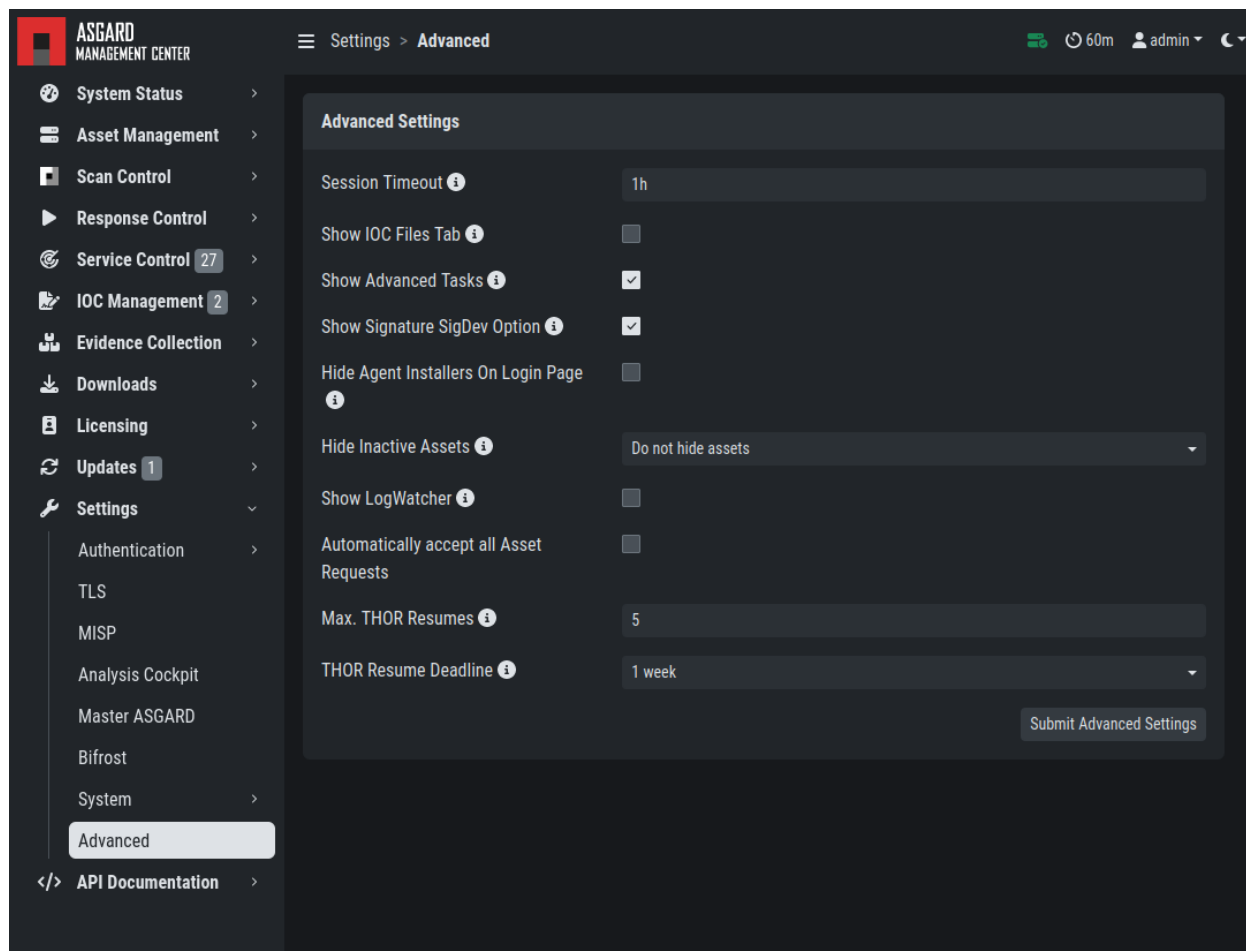


Fig. 99: Advanced Settings



## 3.22 User Settings

The following settings will only affect the currently logged in user.

### 3.22.1 Changing your password

To change your password, click your username in the top right corner and click **User Settings**. This will lead you to the personal user settings.

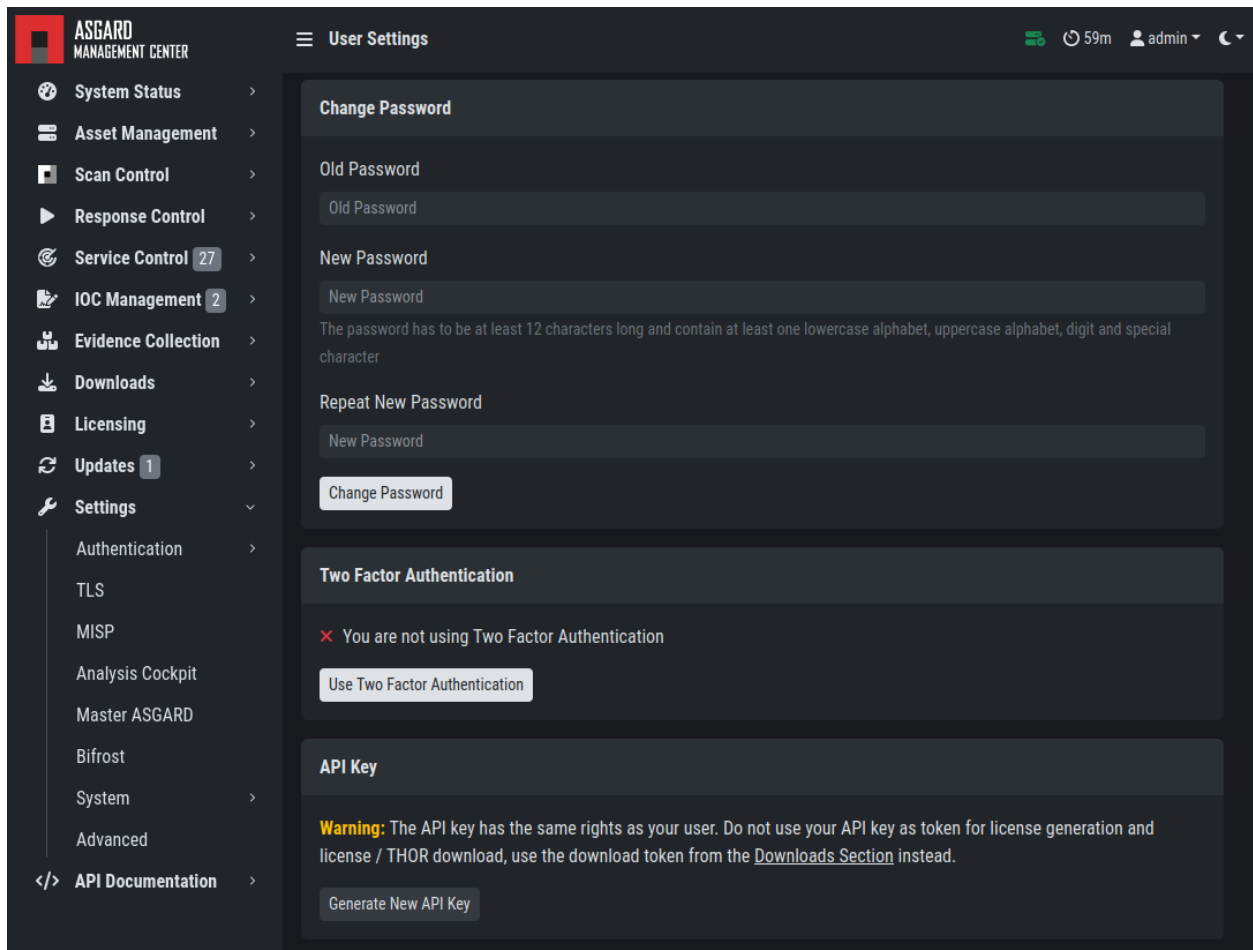


Fig. 100: Changing your password

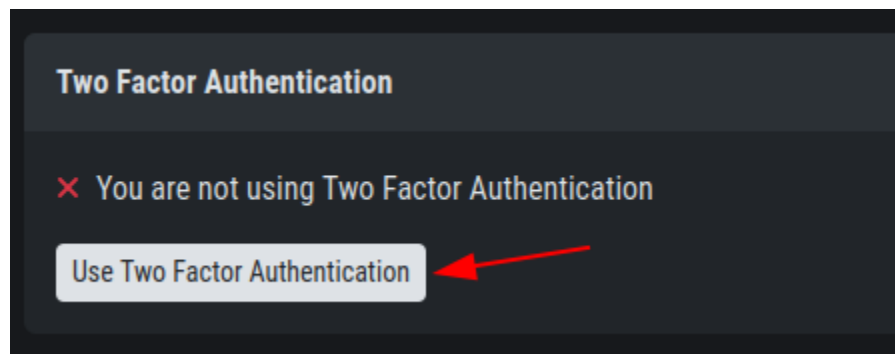
### 3.22.2 Two Factor Authentication

We are currently using the Time-based One-time Password (TOTP) algorithm for two factor authentication. We recommend one of the following mobile apps for 2FA:

- Google Authenticator
- Microsoft Authenticator
- Twilio Authy
- iOS built-in Password Manager (iOS 15 or newer)

#### Enable Two Factor Authentication

To enable Two Factor Authentication, click **Use Two Factor Authentication** in your User Settings and follow the instructions on the screen.



After clicking the button, you will be presented with a QR code for your authenticator app of your choice. Alternatively, you can use the secret key. You will need to verify the 6-digit token and click **Validate Two Factor Authentication** to enable 2FA.

---

**Note:** You will be logged out of your current session if the validation was successful.

---

#### Disable Two Factor Authentication

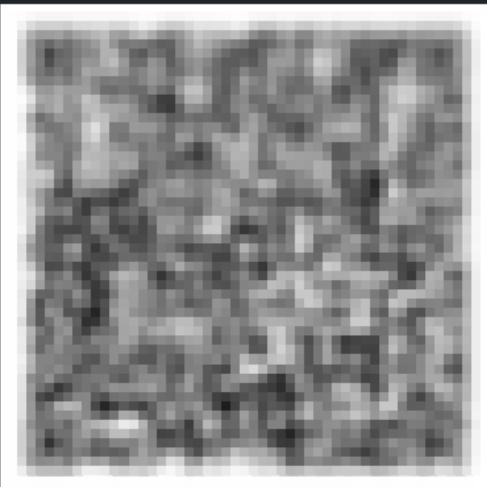
To disable 2FA, navigate to **User Settings > Two Factor Authentication** and click **Deactivate Two Factor Authentication**.

---

**Note:** If a user is unable to log into ASGARD to disable their own 2FA, follow the instructions at [Resetting Two Factor Authentication](#)

---

**Two Factor Authentication**



Use the above QR Code to import the Two Factor Authentication Secret in your Authentication App.  
Then enter the 6-digit token from your App below to validate activation.

6-digit token

Validate Two Factor Authentication

Cancel

**Two Factor Authentication**

✓ You are currently using Two Factor Authentication

Deactivate Two Factor Authentication

### 3.22.3 API Key

To generate an API Key, navigate to **User Settings > API Key**.

This page allows you to set an API key. If an API key was previously set, a new key will be generated. You will only be able to see your new API key once after it has been generated.

---

**Note:** Currently an API key always has the access rights of the user context in which it has been generated. If you want to create a restricted API key, add a new restricted user and generate an API key in the new user's context.

---

**Warning:** The API key has the same rights as your user. Do not use your API key as token for license generation and license / THOR download. Instead, use the download token from the Downloads menu ([Download Links](#)).

## MASTER ASGARD

The Master ASGARD is a single central management console that can control all of your ASGARD systems. It is meant to centrally manage controlled scans on all your ASGARD systems. MASTER ASGARD also provides one central point of management for your Response Playbooks, Evidence Collection and IOC Management. A special license for this is needed.

---

**Note:** Please note that the Master ASGARD is a completely separate system from your existing Management Center. This means a new server/vm and a special license are required.

---

### 4.1 Installation

Master ASGARD is a single central management console that can control all of your ASGARD systems. It is meant to centrally manage controlled scans on all your ASGARD systems. Master ASGARD also provides one central point of management for your Response Playbooks, Evidence Collection and IOC Management. A special license for this is needed.

To install a Master ASGARD, you can use our Nextron Universal Installer. Please follow the instructions in the following chapter: *Install the ASGARD Management Center Service*.

### 4.2 Hardware Requirements for Master ASGARD

The Master ASGARD has the following hardware requirements:

Component	Value
System Memory	16 GB
Hard Disk	1 TB
CPU Cores	8

## 4.3 License Management

Once you connect your ASGARD Management Centers to your Master ASGARD, the licensing sections on connected ASGARD Management Centers become inactive. The local ASGARD license will be replaced with the Master ASGARD license. Every ASGARD can issue scanning licenses to assets as long as the total number of scanned servers and workstations does not exceed the number of systems in the Master license.

## 4.4 Setting up Master ASGARD

The setup procedure for Master ASGARD is identical to the setup procedure for ASGARD Management Center, see *Setup Guide*. The only difference is that you need to provide a Master ASGARD license file.

## 4.5 Link ASGARD Systems with Master ASGARD

On your ASGARD server, go to Settings > Master ASGARD, generate a one-time code and copy it.

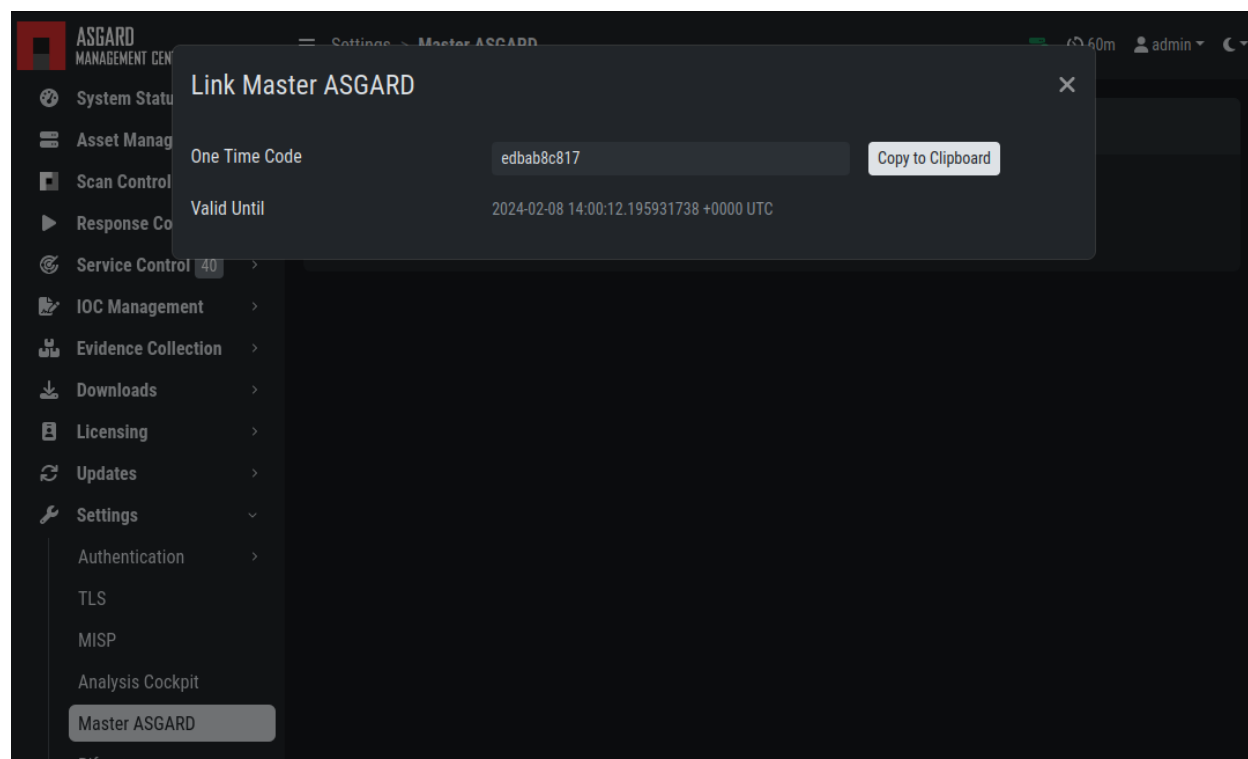


Fig. 1: Generate One Time Token on ASGARD

In Master ASGARD go to Connected ASGARDS, click the Add ASGARD button in the upper right corner, and use the hostname and one-time token to connect that ASGARD system. You can use a description to provide more information on that ASGARD server, e.g. DMZ 1 or Region EMEA - HQ 1.

**Note:** You don't have to provide a port in the hostname field. Don't use a URL like `https://`, just the FQDN. Remember that Master ASGARD must be able to reach ASGARD v2 systems on port 5443/tcp and ASGARD v1 systems on

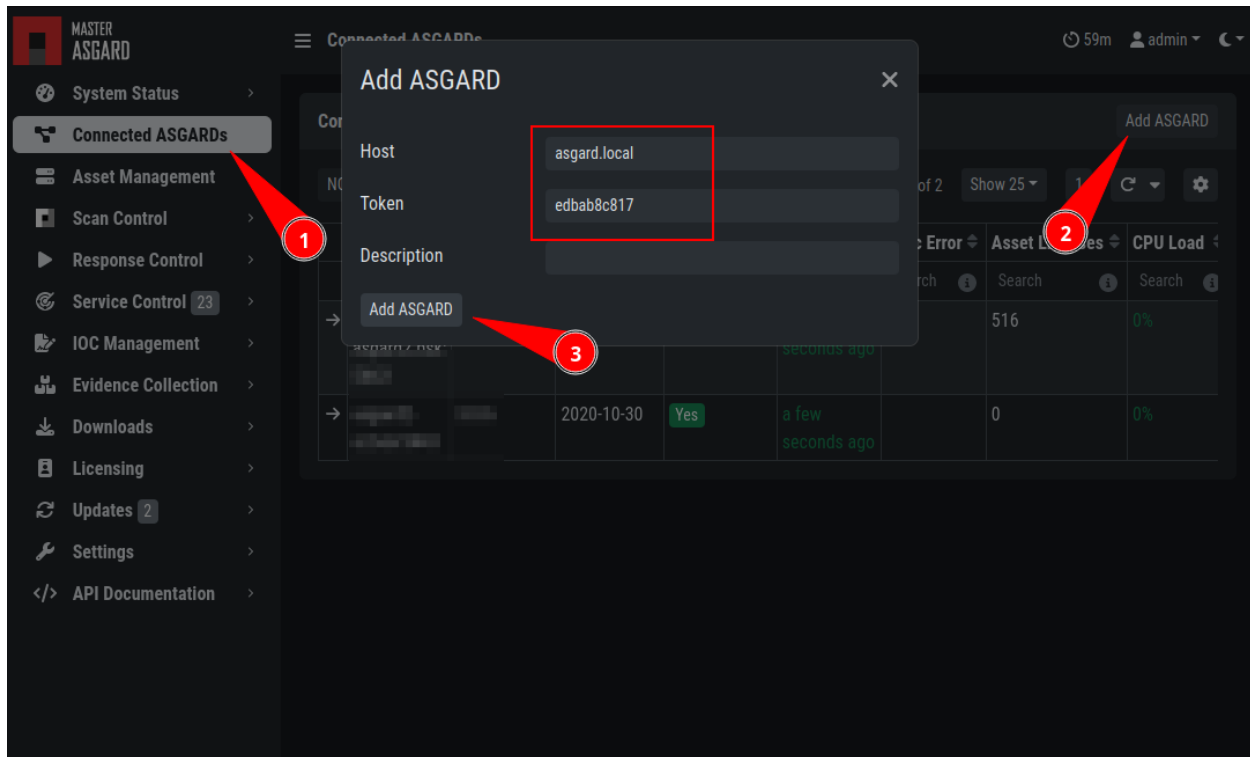


Fig. 2: Link ASGARD in Master ASGARD

port 9443/tcp. Also make sure that the Master ASGARD system is able to resolve the FQDN of the ASGARD system.

## 4.6 Scan Control

Scan Control in Master ASGARD looks the same as in an ASGARD server. The only difference is that you can select an ASGARD Server or "All ASGARDs" to run the scans on.

## 4.7 Asset Management

Asset Management in Master ASGARD is very similar to the asset management in ASGARD.

The only differences are:

- ASGARD column shows to which ASGARD system the endpoint is connected
- Only CSV export is allowed (asset labeling via CSV import is unavailable)

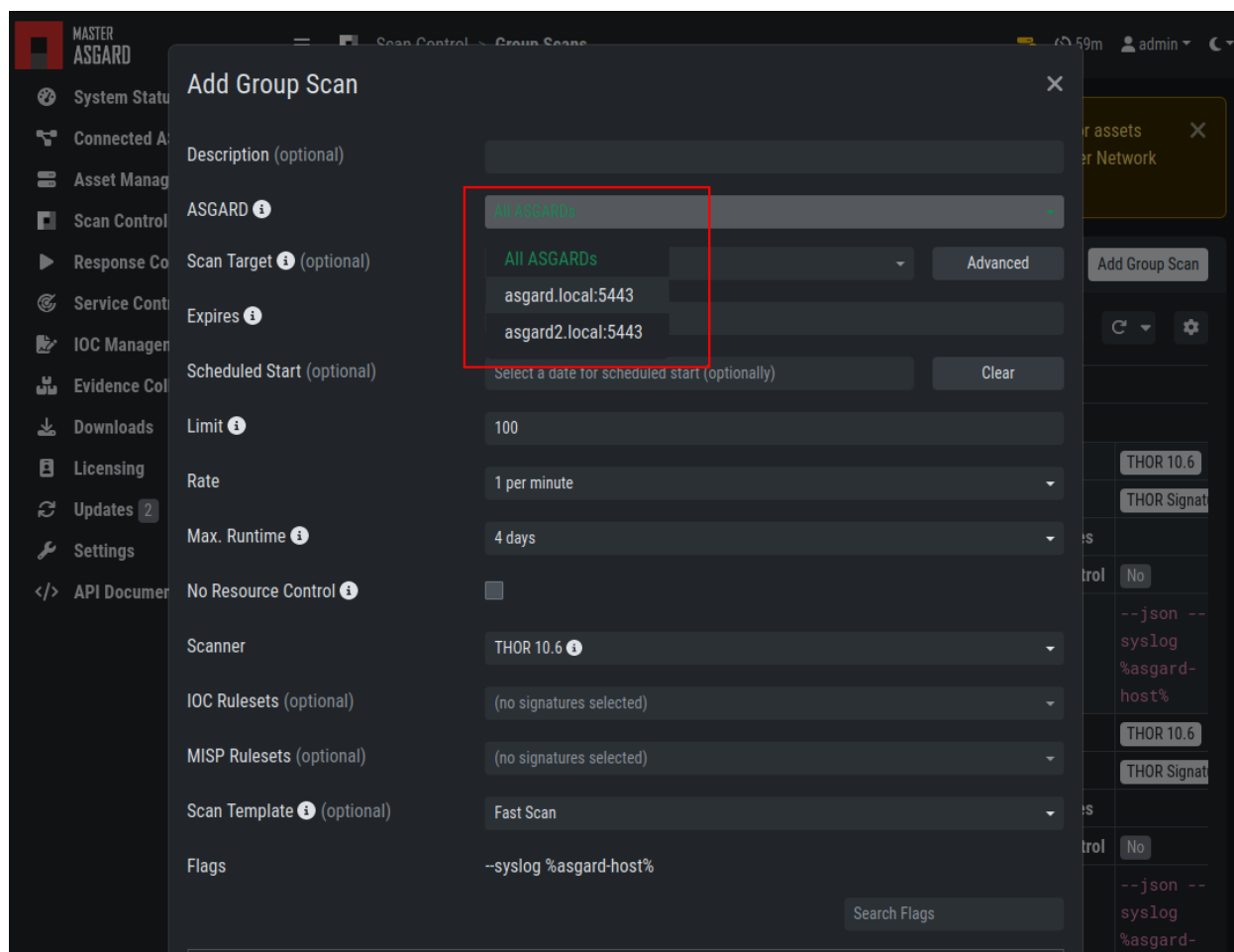


Fig. 3: Scan Control in Master ASGARD - Add Group Task



## 4.8 IOC Management

On Master ASGARD you can manage IOCs exactly like on ASGARD. The only limitation is that IOCs in Master ASGARD and ASGARD are isolated. That means if you want to use the IOCs from Master ASGARD, you need to initiate the scan from Master ASGARD and if you want to use the IOCs from ASGARD, you need to initiate the scan from ASGARD. In general we suggest to manage IOCs in Master ASGARD for maximum flexibility.

## 4.9 Service Control

Service Control lists the asset with an installed service controller. An asset is either managed by Master ASGARD or its connected ASGARD, not by both. If an asset is managed by Master ASGARD it can still be viewed by the connected ASGARD (and vice versa). If Master ASGARD or ASGARD edits a configuration of an asset it will take over the "leadership" over this asset, no matter by which it was managed beforehand.

## 4.10 Evidence Collection

All collected evidence is available in Master ASGARD's **Evidence Collection** section.

## 4.11 Download Section

The **Downloads** section of Master ASGARD allows to generate and download Agent Installers on all your connected ASGARs. This allows for a central management of the Installers.

## 4.12 Updates

The **Updates** section contains a tab in which upgrades for ASGARD can be installed.

The menu **THOR** and **Signatures** gives you an overview of the used scanner and signature versions on all connected ASGARs.

This view is identical to a standalone ASGARD Management Center installation (see *Updates of THOR and THOR Signatures*)

The view in your connected ASGARD Management Centers however will be different:

It is possible to set a certain THOR and Signatures version for each connected ASGARD. However, if automatic updates are configured, this setting has only effect until a new version gets downloaded.

Customers use this feature in cases where they want to test a certain THOR version before using it in production. In this use case the ASGARD system that runs the test scans is set to automatic updates, while the ASGARD systems in production use versions that administrators set manually after successful test runs.

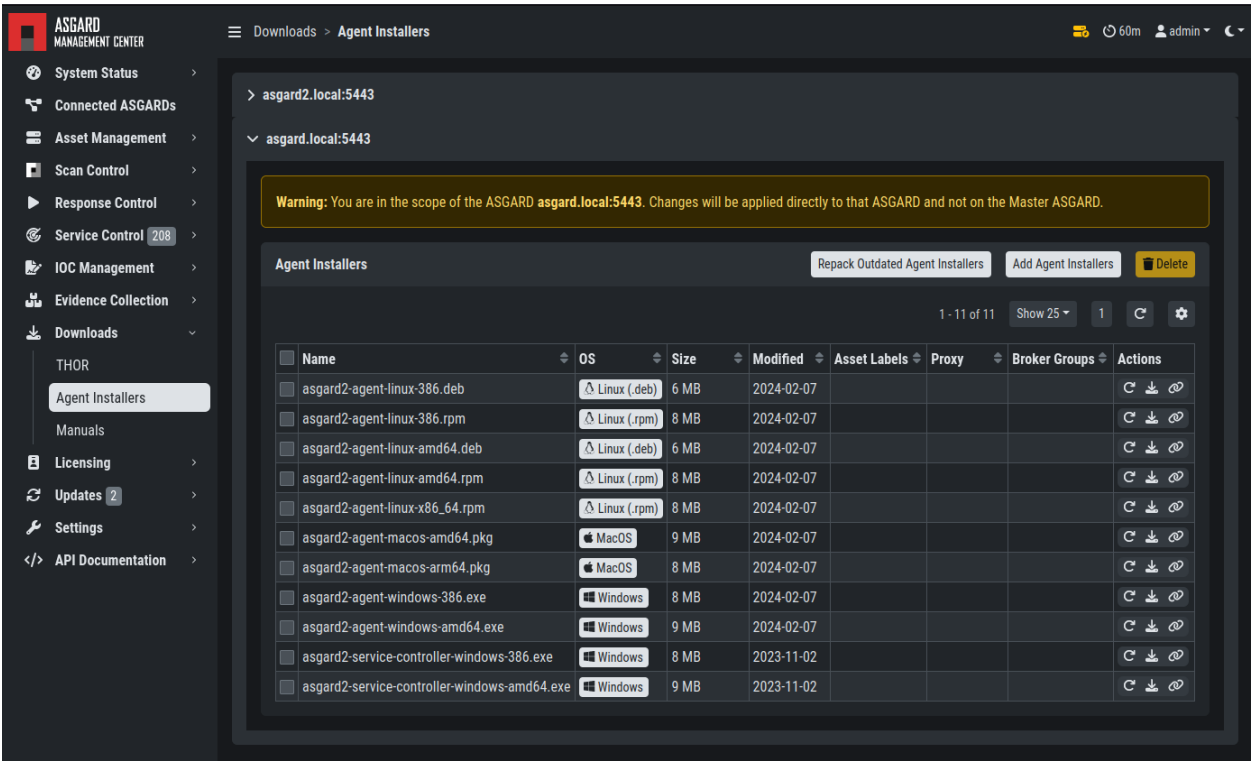


Fig. 4: Example: Download Section in ASGARD but managed by Master ASGARD

4.13 User Management

Master ASGARD offers no central user and role management for all connected ASGARD servers. Since Master ASGARD and ASGARD allow to use LDAP for authentication, we believe that complex and centralized user management should be based on LDAP.

4.14 Master ASGARD and Analysis Cockpit

It is not possible to link a Master ASGARD with an Analysis Cockpit and transmit all scan logs via Master ASGARD to a single Analysis Cockpit instance. Each ASGARD has to deliver its logs separately to a connected Analysis Cockpit.

4.15 Master ASGARD API

The Master ASGARD API is documented in the API Documentation section and resembles the API in ASGARD systems.

However, many API endpoints contain a field in which users select the corresponding ASGARD (via ID) or all ASGARDs (ID=0)

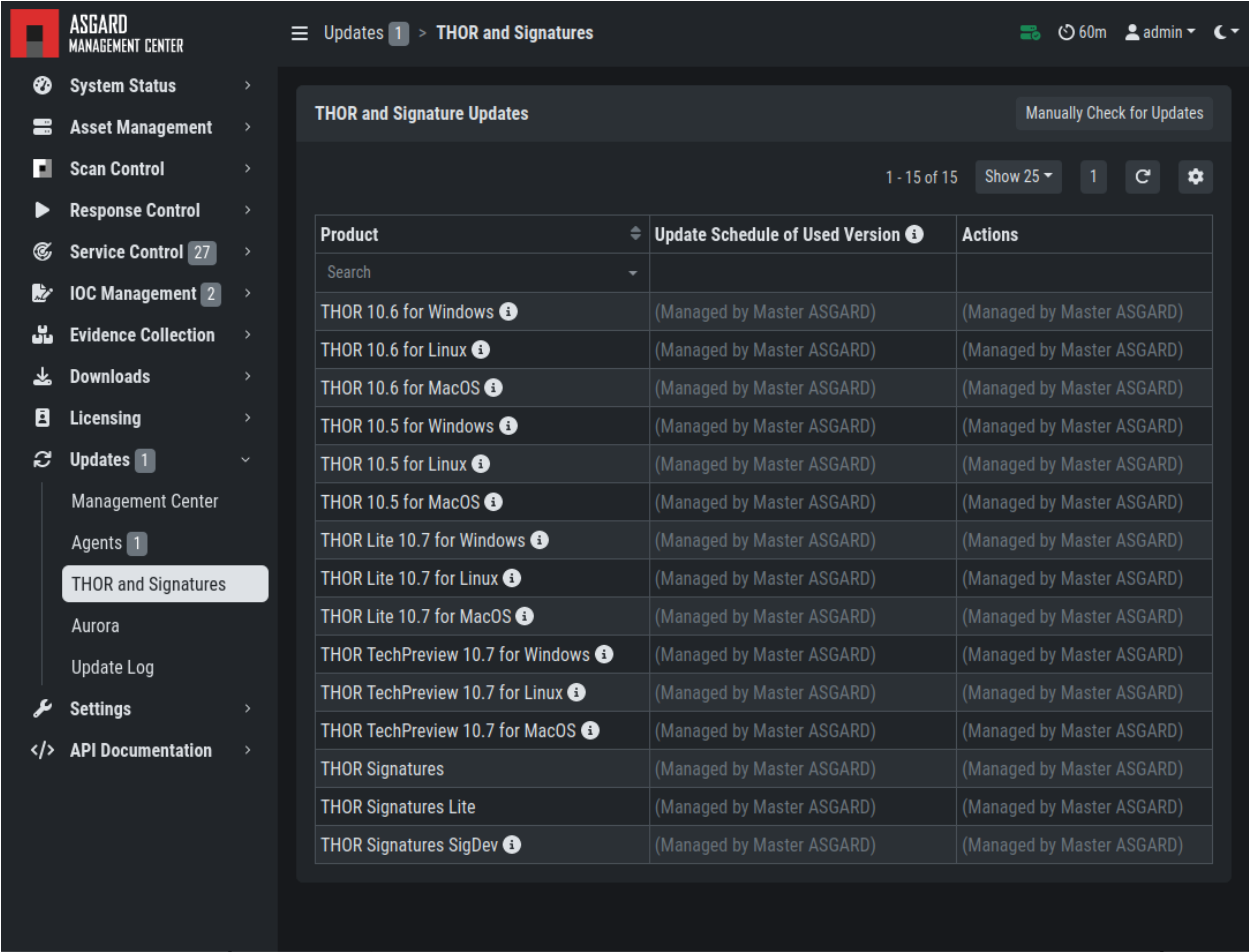


Fig. 5: ASGARD THOR and Signatures Update view when connected to a Master ASGARD

Name	Description
asgard	
integer	(Master ASGARD only): Only create the scheduled group task / scan on one connected ASGARD instead of all.
(formData)	
	asgard

Fig. 6: Master ASGARD API Peculiarity



## MAINTENANCE

This chapter contains basic maintenance tasks you can perform on your Management Center.

### 5.1 Log Rotation and Retention

ASGARD is rotating logs automatically at a set time interval. It is important to keep in mind how long logs will be stored on the system before they get purged. All logs will be rotated and zipped into one file monthly, for up to 14 months.

To get a better understanding of how the log rotation is handled, you can inspect `/etc/logrotate.d/asgard-management-center`.

#### 5.1.1 Syslog Logs

ASGARD will store all logs under `/var/lib/asgard-management-center/log`. This does not include the Scan Logs, as those are handled separately.

If you require a longer retention period, please copy the oldest log packages to another directory or to a dedicated log server. Do not modify the built-in rotation settings as this might interfere with ASGARD updates!

Log	Name
Audit	asgard-audit.log
ASGARD Management Center	asgard.log
ASGARD Agent and Service Controller	agent.log
ASGARD Agent Access	agent-access.log
THOR via Syslog	scan.log
THOR via Syslog (Scan Start, Licensing, Completion only)	subscan.log
Aurora	aurora-service.log

If you want to forward those logs automatically to a dedicated server, you can set up [Rsyslog Forwarding](#). Forwarded logs will still reside on ASGARD.

## 5.2 Regain Disk Space

If your disk usage is growing too fast and free disk space is running out, you have several options:

1. Increase the size of your disk
2. Delete files that are not needed for operation (i.e. safe to delete)
3. Delete files that are used by MC but might be unneeded / dated

### 5.2.1 Safe-to-Delete Files

The following files are safe to delete. They are not needed for ASGARD to operate.

- `/var/lib/asgard-management-center/log/*.gz`

They are only kept on the system if needed for further processing. E.g. saving/sending the log files to another system. If you do not need or plan to use those, they can be deleted. If you are unsure make a copy to another system before deleting them.

- `/var/lib/asgard-management-center/downloads/*` (except current day)

The files in this folder are only generated for temporary downloading files from the UI and are not needed after the download has finished. The directory has a sub structure of `year/month/day`. It is safe to delete any files older than the current day.

### 5.2.2 Potentially Unneeded / Dated Files

- Bifrost quarantined files

If you use Bifrost, the collected files are not deleted by default. If dated files are no longer needed, you can define a retention period at **Settings > Bifrost**.

- `/var/lib/asgard-management-center/scan-results/*.gz`
- `/var/lib/asgard-management-center/generic-results/*`
- `/var/lib/asgard-management-center/remote-console/protocol/*.gz`

The listed files are the results of THOR scans (scan-results), Tasks except Scans (generic-results) and the sessions of remote consoles (remote-console). They are not needed for ASGARD to function, but the data is viewed and available for download in ASGARD. This means deleting these files will not break ASGARD, but you lose the information provided by the files. If you need the disk space and cannot increase the disk, we suggest to delete these files older than a given date, that you no longer need. This can be done with a find-remove combination using the command line:

```
root@asgard:~# find /var/lib/asgard-management-center/<directory> -mtime +<days> -print0
↪ | xargs -0 -r rm
```

Where `<directory>` is one of `scan-results/*.gz`, `generic-results/*` or `remote-console/protocol/*` and `<days>` the number of days you want to keep. Files and folders older than `<days>` days will be deleted.

## ADVANCED CONFIGURATION

This chapter contains advanced configuration options, which can be helpful in different scenarios. Please have a look if some options could be helpful for your environment.

### 6.1 Performance Tuning

The ASGARD agents poll the Management Server server frequently for new tasks to execute. The default polling interval depends on the number of connected endpoints. In larger environments the polling interval increases dynamically up to 10 minutes for a configuration with 25.000 endpoints connected to a single ASGARD.

Additionally, ASGARD is configured to serve a maximum of 100 concurrent asset connections and 25 concurrent asset streams. Asset connections are short polls from the agent such as answering the question "do you have a new task for me?". Asset streams are intense polls such as downloading THOR to the agent or uploading scan results back to ASGARD.

Requests that exceed the limits will receive an answer from ASGARD to repeat the request after N seconds, where N is calculated based on the current load.

This factory preset behavior insures your ASGARD stays stable and responsive even if your ASGARD's system resources are limited. Furthermore, you most likely can't overload your network or firewalls with high numbers of requests or downloads.

In order to modify ASGARDs performance settings edit `/etc/asgard-management-center/asgard.conf` and restart the ASGARD service.

The default values are:

Value	Description
LoadConnMax=100	Max. concurrent „Busy Connections"
LoadStreamMax=25	Max. concurrent „Busy Streams"
PingRateMin=10	Polling Rate with 0 connected Assets (seconds)
PingRateMax=600	Polling Rate with 25000 connected Assets (seconds)
PingRateFast=5	Polling Rate for Assets in Fast Ping Mode (seconds)

These values should work fine in most scenarios – regardless of the size of the installation. However, you may want to decrease PingRateMax in order to achieve a better responsiveness of your ASGARD infrastructure.

### 6.1.1 Overloading ASGARD

While temporary stream overloads are quite normal, connection overloads should not happen. If they do, either adjust your PingRateMax, your LoadConnMax or both.

ASGARD will indicate an overload with the "Connection Overload line" and the "Stream Overload line" within the graphs in the overview section (see picture below). If an ASGARD is in an overload situation it will postpone connections and streams but will not lose or drop tasks or be harmed in any way. ASGARD will recover to normal load automatically.

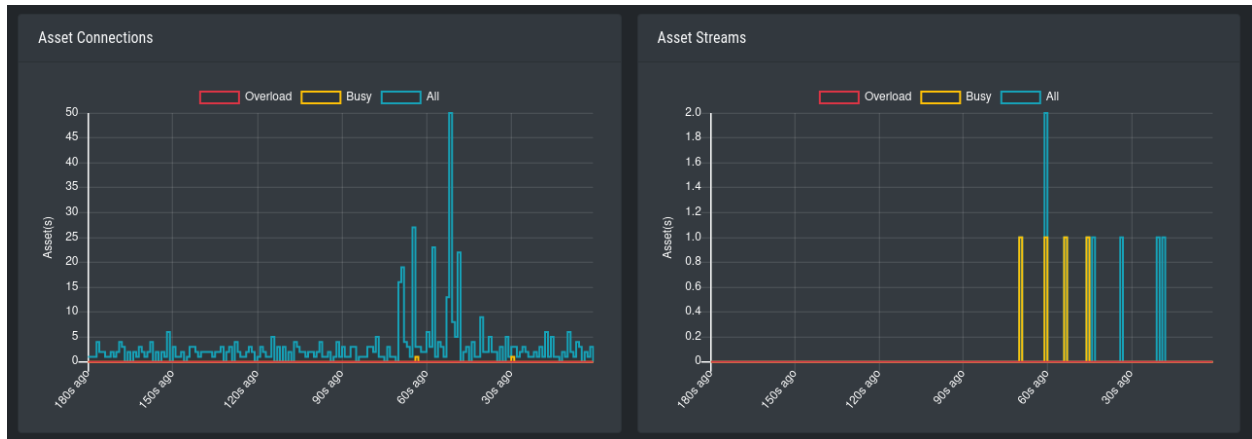


Fig. 1: Asset Connections and Asset Streams

Stream overloads can happen temporarily (e.g. if you schedule a grouped scan or grouped task with an unlimited rate). The picture below shows such a normal overload situation that was caused by starting a grouped scan with an unlimited rate. This is the expected behavior. ASGARD will manage the load automatically and postpone streams until the load has returned to normal.

The "Busy Streams" line indicates the number of streams currently active. As you might have guessed, the picture above was taken on an ASGARD in default configuration where the number of concurrent streams is set to the default value of 25.

## 6.2 Managing Logs

ASGARD will store all logs under `/var/lib/asgard-management-center/log`

All logs in this directory will be rotated and automatically cleared after 14 months, please see [Log Rotation and Retention](#) for more information.

Please copy the oldest log packages to another directory or to a dedicated log server in case you require longer retention periods. **Do not modify the built-in rotation settings** as this might interfere with ASGARD updates!



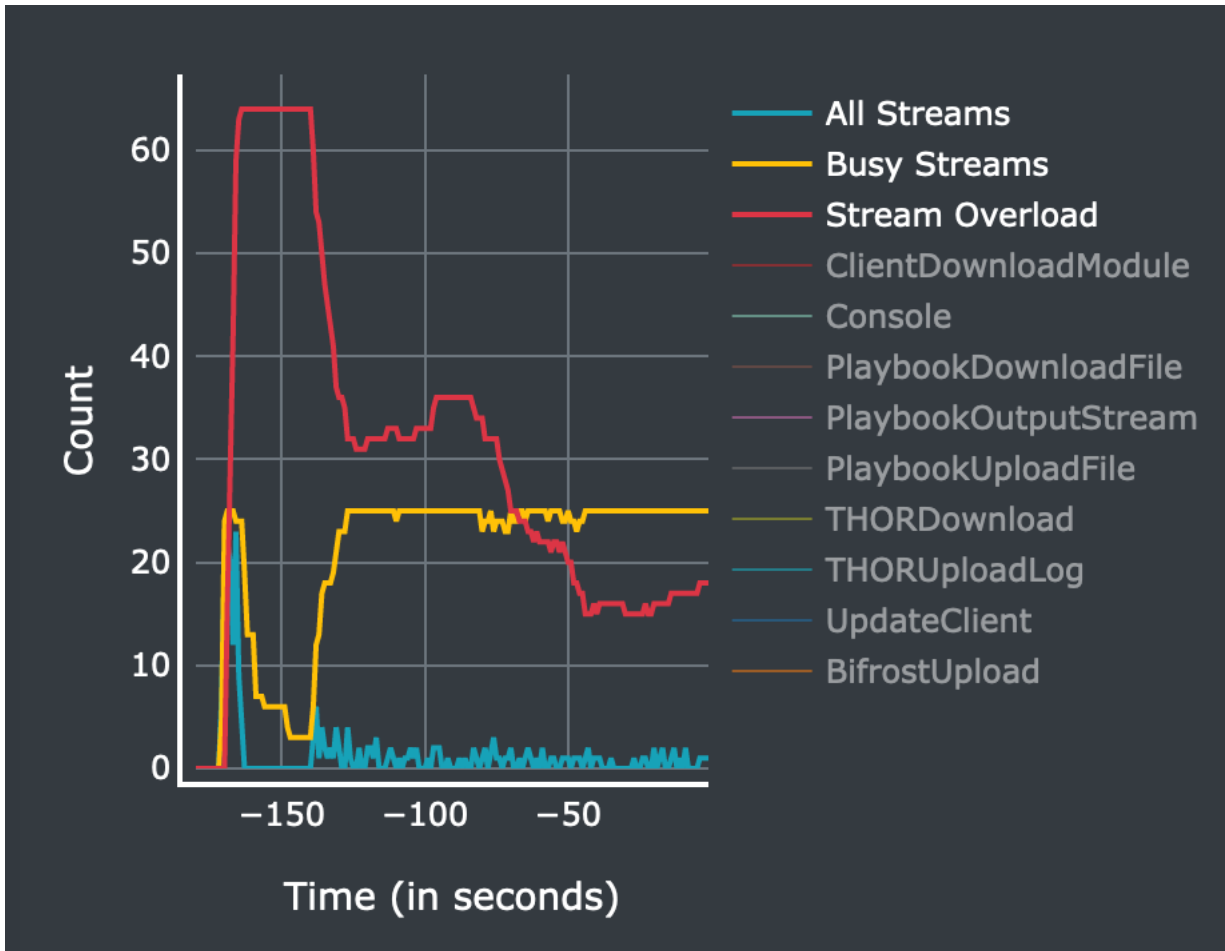


Fig. 2: Asset Streams in an overload situation

Log	Name	Rsyslog
Audit	asgard-audit.log	Audit Log <sup>1</sup>
ASGARD Management Center	asgard.log	ASGARD Log <sup>Page 136, 1</sup>
ASGARD Agent and Service Controller	agent.log	Agent Log <sup>1</sup>
ASGARD Agent Access	agent-access.log	
THOR via Syslog	scan.log	THOR Log <sup>1</sup>
THOR via Syslog (Scan Start, Licensing, Completion only)	subscan.log	THOR Log <sup>1</sup>
Aurora	aurora-service.log	

The logs will always be stored here, even if you have *Rsyslog Forwarding* activated.

## 6.2.1 Scan Logs

ASGARD will store all scan logs under `/var/lib/asgard-management-center/scan-results`

All Scans will generate two files, `thor-<ID>.txt.gz` and `thor-report-<ID>.html.gz`. The first file will be the raw THOR Scan Log(s) and the second file will be the HTML Report(s). The numeric value in the file name is the Scan-ID, which can be found in the the Scan Control view. Please make sure to enable the ID column, since it is not enabled in the default view.

For Scans which were started with the `--json` flag, log files are additionally placed in the scan-results directory and are named `thor-<ID>.json.gz`. Please keep in mind, those JSON log files are not being transferred to any connected Analysis Cockpit.

## 6.3 Agent and Agent Installer Update

When ASGARD has a new agent version available you can see an indicator on the **Update** menu item as well as on the sub menu **Update > Agents**. There are two tasks to perform, updating the agents on your assets and updating the agent installer for all future asset deployments.

### 6.3.1 Agent Update

If this is the first agent update performed on this ASGARD you might need to enable the **Update Agent** module under **Settings > Advanced > Show Advanced Tasks**.

Then you need to run the **Update Agent** module. You can do this on a per asset basis by running a playbook from **Asset Management** or create a **New Group Task** from **Response Control**, which is the preferred way. You can roll-out the update in batches by providing labels for each stage or not select any label to perform the update on all assets.

---

**Note:** The **Update Agent** module is not shown by default under (Group) Tasks. To show the group task or single tasks (also inside the group task) you need to select the **Update Agent** module from the **Module** column. You may need to select the **Module** column from **Column visibility** first, if not shown.

---

<sup>1</sup> This is the **Type** you can select in *Rsyslog Forwarding*.

Add Group Task

Description (optional)

Task Target

Simple

Include Labels ⓘ (optional)
OR ⓘ

Exclude Labels ⓘ (optional)
OR ⓘ

ASGARD Query ⓘ (optional)

system = "windows"

Test Query

Expires ⓘ

2024-02-15 14:00:00

Scheduled Start (optional)

Select a date for scheduled start (optionally)

Clear

Limit ⓘ

100

Rate

10 per minute

Task

Maintenance

Max. Runtime ⓘ

3 hours

Maintenance Type

Upgrade Agent

Add Group Task

Add and Activate Group Task

Fig. 3: Example Group Task for Agent Update

### 6.3.2 Agent Installer Update

You need to update the agent installer as well, so that newly added assets will directly use the current agent version. This is a manual task you have to perform once a new version is available. Navigate to **Downloads > Agent Installers** and click **Repack Outdated Agent Installers**. Please note that this process might take a while to finish.

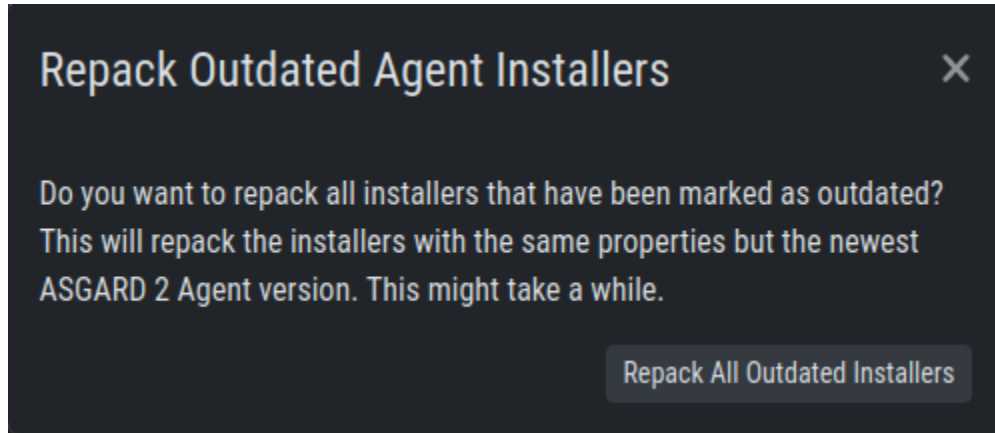


Fig. 4: Repack Agent Installers

## 6.4 Creating Custom Agent Installer

ASGARD supports creation of custom installers. Custom installers can be configured in a way so that agents show up with a preset label or with a preset proxy configuration.

Go to **Downloads > Agent Installers > Add Agent Installer**. Edit the properties of the desired installer and generate the installer by clicking **Add Agent Installers**. The installers are available at the downloads page besides the default installers, so best use an affix as distinction.

---

**Note:** If a new version of the agent installer is available, you will see a notice that agent installers need repacking. You can press the **Repack Outdated Agent Installers** button and wait for the process to finish. This guarantees that newly downloaded installers use the newest version.

---

## 6.5 Backup and Restore

All of our ASGARD servers come with predefined backup and restore scripts. You can use them to keep a backup available in case something stops working.

**Warning:** If you are using a Management Center and Analysis Cockpit together, it is advised to create the backups at the same time. This avoids potential data inconsistencies across the two platforms. You can do this via a cronjob on both systems or with an automation tool like Ansible, Terraform, etc.

The same should be kept in mind when restoring your backups. You should always restore the backups on all servers, to avoid getting problems in the future.

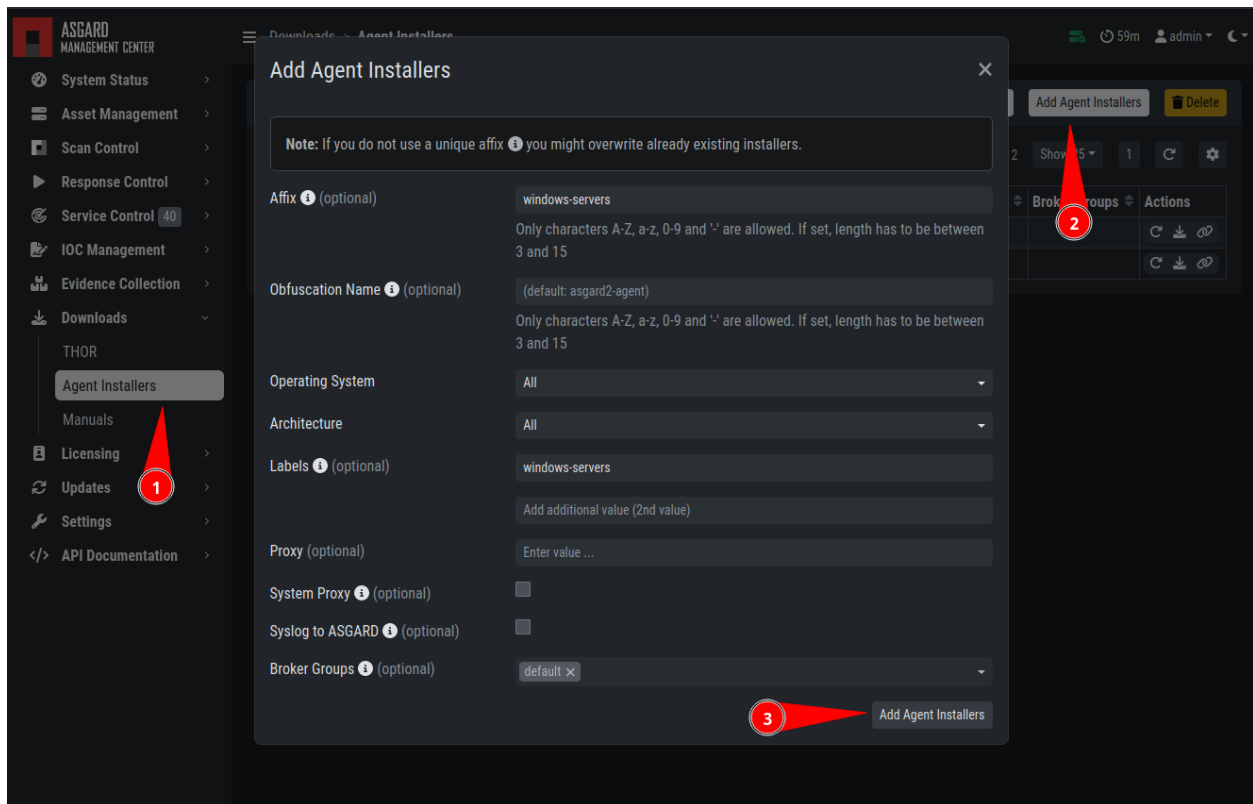


Fig. 5: Custom Agent Installer from the WebUI

## 6.5.1 Backup

We create a script which can be used to generate a backup of all configurations, assets, tags, user accounts, tasks etc., except:

- Log files (ASGARD, THOR)
- Playbook results (collected evidence)
- Quarantined samples (Bifrost)

```
nexttron@asgard:~$ sudo /usr/share/asgard-management-center/scripts/backup.sh
Writing backup to '/var/lib/asgard-management-center/backups/20240209-1110.tar'
tar: Removing leading '/' from member names
tar: Removing leading '/' from hard link targets
Removing old backups (keeping the 5 most recent files)...
done.
```

If you want to transfer the backup to a different system, make sure to copy the .tar file to the home directory of the nexttron user and change the permissions:

```
nexttron@asgard:~$ sudo cp /var/lib/asgard-management-center/backups/20240209-1110.tar /
→home/nexttron
nexttron@asgard:~$ sudo chown nexttron:nexttron /home/nexttron/20240209-1110.tar
nexttron@asgard:~$ ls -l
total 205560
-rw-r--r-- 1 nexttron nexttron 210493440 Feb  9 11:17 20240209-1110.tar
```

After this is done, you can use scp or any other available tool to transfer the backup file to a different system.

**Hint:** Our recommendation is to run the backup as a cronjob during a time, when no tasks are running or are scheduled to run. The reason for this is that our sample script will stop the ASGARD service before the backup to avoid any inconsistency with the data.

Here is an example script and cronjob entry to create backups on a schedule:

Listing 1: Example backup script, e.g. /root/backup.sh

```
1  #!/bin/bash
2  BACKUPDIR="/var/lib/asgard-management-center/backups"
3  NEWDIR="/home/nexttron/backups"
4  date
5
6  echo "checking for destination folder"
7  if ! [ -d "$NEWDIR" ]; then
8      mkdir $NEWDIR
9      chown -R nexttron: $NEWDIR
10 fi
11
12 echo "stopping asgard-management-center.service"
13 if ! systemctl stop asgard-management-center.service; then
14     echo "could not stop asgard-management-center.service, exiting script"
15     exit 1
16 fi
```

(continues on next page)

(continued from previous page)

```

17
18 sleep 3
19 echo "running backup script"
20 /usr/share/asgard-management-center/scripts/backup.sh
21
22 sleep 3
23 echo "starting asgard-management-center.service"
24 if ! systemctl start asgard-management-center.service; then
25     echo "could not start asgard-management-center.service, needs manual debugging"
26     exit 1
27 fi
28
29 echo "moving backup files to destination"
30 mv $BACKUPDIR/*.tar $NEWDIR
31 chown -R nextron: $NEWDIR
32
33 echo "backup created successfully"
34 echo ""
35 echo ""
36 exit 0

```

The following crontab entry could be created to run the script every day at 2am. You can edit the crontab of the root user with the following commands:

```

nextron@asgard:~$ sudo su
[sudo] password for nextron:
root@asgard:~# crontab -e

```

```

0 2 * * * /bin/bash /root/backup.sh >> /root/backup.log

```

**Warning:** Please keep in mind that the backup.sh script is only keeping 5 backups in place. If you want to change this, you have to change the value GENERATIONS in the file /usr/share/asgard-management-center/scripts/backup.sh to a different value.

## 6.5.2 Restore

You can use the restore.sh script to restore a backup.

```

nextron@asgard:~$ sudo /usr/share/asgard-management-center/scripts/restore.sh
Usage: /usr/share/asgard-management-center/scripts/restore.sh <BACKUPFILE>
nextron@asgard:~$ sudo /usr/share/asgard-management-center/scripts/restore.sh /var/lib/
↳ asgard-management-center/backups/20240209-1110.tar
Stopping services... Removed "/etc/systemd/system/multi-user.target.wants/asgard-
↳ management-center.service".
done.
etc/asgard-management-center/
etc/asgard-management-center/broker.conf
etc/asgard-management-center/server_cert_ext.cnf.in
etc/asgard-management-center/rsyslog-thor.conf.20240208142245.bak

```

(continues on next page)

(continued from previous page)

```
...
1+0 records in
1+0 records out
24 bytes copied, 0.000126177 s, 190 kB/s
Starting services... Created symlink /etc/systemd/system/multi-user.target.wants/asgard-
management-center.service → /lib/systemd/system/asgard-management-center.service.
done.
```

---

**Note:** The version of the ASGARD were the backup will be restored should be the same as the version which was present while the backup was created. If you need an older version of ASGARD, please contact our support team.

---

## 6.6 Disable Remote Console Globally

Remote Console on connected endpoints can be disabled centrally by creating the following file.

```
nexttron@asgard:~$ sudo touch /etc/asgard-management-center/disable_console
```

To re-enable Remote Console simply remove the created file

```
nexttron@asgard:~$ sudo rm /etc/asgard-management-center/disable_console
```



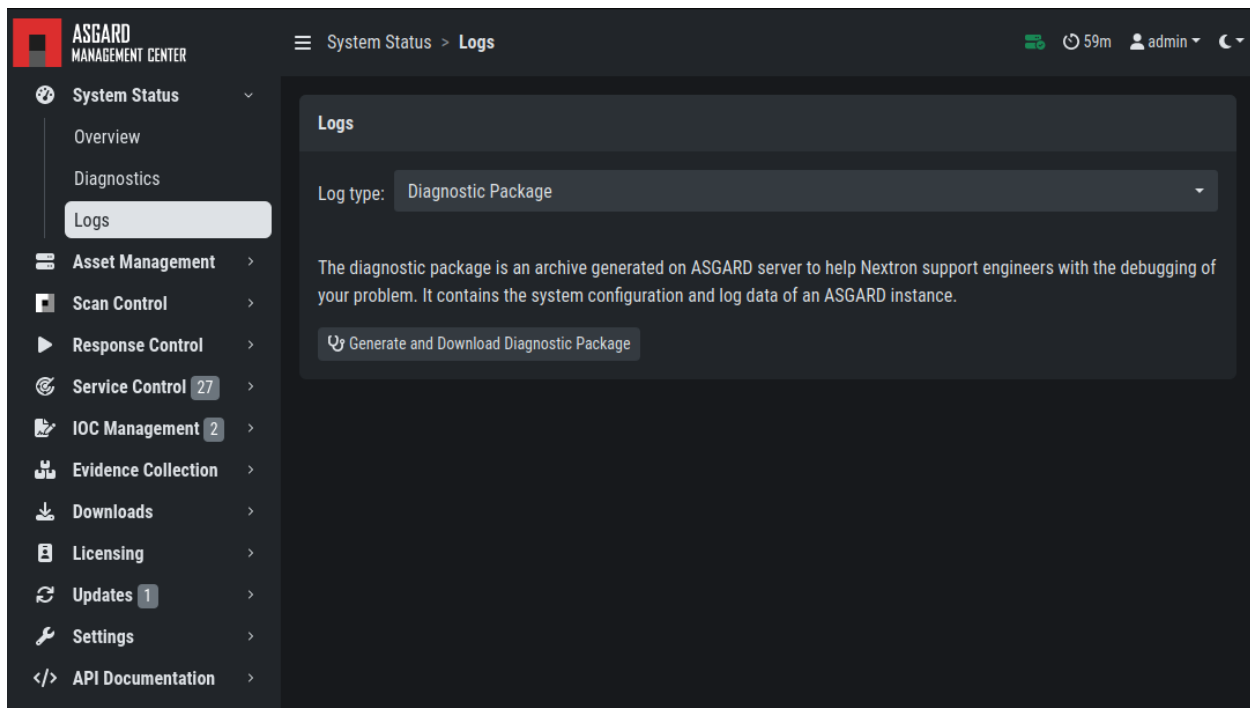
## TROUBLESHOOTING

This chapter contains information to help with debugging and troubleshooting potential problems with your Management Center.

### 7.1 Diagnostic Pack

The diagnostic package is an archive generated on ASGARD server to help Nextron support engineers with the debugging of your problem. It contains the system configuration and log data of an ASGARD instance.

You can generate a Diagnostic Package in Systems Status > Logs > Diagnostics Package.



The package can have a size that cannot be shared via Email. In this case you can either

1. ask us for an upload link (secure file sharing) or
2. remove big log files from the package (e.g. the file `/var/lib/asgard-management-center/log/agent-access.log` is often responsible for 97% of the package size)

## 7.2 Agent Debugging

### 7.2.1 Internal Agent Debugging

Edit the file `asgard2-agent.yaml` and set the value of `write_log` to `true`. The file can be found in `C:\Windows\System32\asgard2-agent\` or `/var/lib/asgard2-agent/` for Windows and Linux/macOS, respectively.

```
write_log: true
```

After making these changes, restart the ASGARD service. You can then find log entries and possible error messages in the file `asgard2-agent.log` in the same directory as the configuration file.

Note: The value is set to `false` by default, because the agent doesn't rotate or compress these logs. Leaving that value on `true` could cause that file to grow very big and use a significant amount of disk space. We recommend resetting it after the debugging session.

### 7.2.2 Go Debug Logging

On Windows, open the `cmd.exe` as Administrator. Set some environment variables.

```
C:\Windows\system32>set GRPC_GO_LOG_SEVERITY_LEVEL=info
C:\Windows\system32>set GODEBUG=http2debug=2
```

Navigate into the agent's program directory and start it to see all output messages.

```
C:\Windows\system32>sc stop asgard2-agent
C:\Windows\system32>cd C:\Windows\system32\asgard2-agent\
C:\Windows\system32\asgard2-agent>asgard2-agent.exe
```

Interrupt the agent with CTRL+C. Don't forget to start the Windows service after the debugging session.

```
C:\Windows\system32\asgard2-agent>sc start asgard2-agent
```

On Linux, open a shell as root (`sudo`).

```
nextron@asgard:~$ sudo su -
[sudo] password for nextron:
root@asgard:~#
root@asgard:~# export GRPC_GO_LOG_SEVERITY_LEVEL=info
root@asgard:~# export GODEBUG=http2debug=2
```

Navigate into the agent's program directory and start it to see all output messages.

```
root@asgard:~# systemctl stop asgard2-agent
root@asgard:~# cd /var/lib/asgard2-agent/
root@asgard:/var/lib/asgard2-agent# ./asgard2-agent
```

Interrupt the agent with CTRL+C. Don't forget to start the Linux service after the debugging session.

```
root@asgard:/var/lib/asgard2-agent# systemctl start asgard2-agent
```

## 7.2.3 Aurora Diagnostics Pack

If Aurora does not behave like it should, e.g. using more resources than you expected, you can create a diagnostics pack for our support to help in troubleshooting the issue. This can be conveniently done using the playbook [Default] Create and Collect Aurora Agent Diagnostics Pack (Windows).

It can be run from Asset Management > Response Action (Play button) or from Response Control > Tasks > Add Task or if needed as a group task. The resulting diagnostics.zip can be downloaded from the third step in the Playbook Result tab of the expanded task.

## 7.2.4 Duplicate Assets Remediation

If you are seeing the Duplicate Assets view in your Asset Management, you need to fix the issue to avoid unwanted behavior of this asset. To fix the issue, you need to uninstall the current ASGARD agent, delete the configuration files, and redeploy a fresh copy.

The screenshot shows the ASGARD Management Center interface. The sidebar on the left contains navigation links: System Status, Asset Management (selected), Asset Requests, Duplicate Assets (1), Scan Control, Response Control, Service Control (40), IOC Management, Evidence Collection, Downloads, Licensing, Updates, Settings, and API Documentation. The main content area is titled 'Duplicate Assets' and shows a table with the following data:

Asset ID	Addresses
14	192.168.0.130:42112 192.168.0.120:49556

A warning message at the top of the main content area states: 'The table below shows assets that are connected with multiple addresses simultaneously. This indicates that this asset is running on multiple endsystems that might be caused by cloning a system with an already installed ASGARD 2 Agent. Undesirable side effects of duplicate assets are alternating hostname and tasks that fail immediately.'

Fig. 1: Troubleshooting Duplicate Assets

- To uninstall the ASGARD agent, please follow the instructions in [Uninstall ASGARD Agents](#).
- To delete the configuration files, make sure that the following folder is deleted before installing a new agent:
  - Windows: C:\Windows\System32\asgard2-agent\

– Linux: `/var/lib/asgard2-agent/`

- To install the ASGARD agent, please follow the instructions in [ASGARD Agent Deployment](#).

It is also recommended to redeploy the ASGARD Service Controller.

- To uninstall the ASGARD Service Controller, please follow the instructions in [Uninstall ASGARD Service Controller](#).
- To install the ASGARD Service Controller, please follow the instructions in [Service Controller Installation](#). You need to wait a few minutes until the asset is connected to your ASGARD before you continue with this step. Please note that you might need to accept the Asset Request.

## 7.3 SSL Interception

Using a web proxy with TLS/SSL interception will break the installation routine and shows this error:

```
Certificate verification failed: The certificate is NOT trusted. The certificate issuer
is unknown. Could not handshake: Error in the certificate verification.
```

Solution: Disable TLS/SSL interception for our update servers.

- `update-301.nextron-systems.com`

Used for THOR updates:

- `update1.nextron-systems.com`
- `update2.nextron-systems.com`

We do not support setups in which the CA of the intercepting proxy is used on our ASGARD appliances.

## 7.4 Using Hostname instead of FQDN

The most common error is to define a simple hostname instead of a valid FQDN during installation. This happens if no domain name has been set during the setup step [Network Configuration](#) (Domain name).

This leads to a variety of different problems.

The most important problem is that ASGARD Agents that install on endpoints will never be able to resolve and connect to the ASGARD server.

### 7.4.1 Errors that appear in these cases

```
Apr 23 12:07:12 debian10-dev/10.10.30.118 ASGARD_AGENT: Error:
could not run: rpc error: code = Unavailable desc = connection
error: desc = "transport: authentication handshake failed: x509:
certificate is valid for wrong-fqdn, not asgard.nextron.internal"
```

## 7.4.2 How to Fix a non-existing or wrong FQDN

The FQDN is set at installation time and is composed by the hostname and the domain name. The ASGARD Agents require a resolvable FQDN to correctly operate and connect to the ASGARD Server. One of the processes which are executed at installation time include the integration of the FQDN - which should be set during installation - into the ASGARD agents. If we incorrectly set the FQDN or leave any of those values empty, the agents will fail to connect to ASGARD.

With this fix we will set a new FQDN for the ASGARD Management Center, recreate the internal certificates, and rebuild the agents.

**Warning:** The used FQDN in this manual is just an example. Please use the FQDN of your domain. make sure the FQDN is resolvable via your DNS server.

### Set a valid FQDN

To set a valid FQDN for your ASGARD Management Center server, follow the steps below. We are assuming that your local DNS server already has an A-Record assigned, so your clients can resolve the new hostname/FQDN of your ASGARD Management Center.

Connect via SSH to the ASGARD Management Center:

```
user@somehost:~$ ssh nextron@asgard-mc.example.org
```

Edit the hosts file. Please be careful with the changes in this file, as this might make your system unusable!

```
nextron@asgard-mc:~$ sudoedit /etc/hosts
[sudo] password for nextron:
```

You need to change the following line (**do not change the IP-Address!**):

```
1 127.0.0.1      localhost
2 172.16.0.20   asgard-mc
3
4 # The following lines are desirable for IPv6 capable hosts
5 ::1          localhost ip6-localhost ip6-loopback
6 ff02::1      ip6-allnodes
7 ff02::2      ip6-allrouters
```

To this (values are examples, please change accordingly!)

```
1 127.0.0.1      localhost
2 172.16.0.20   asgard-mc.example.org asgard-mc
3
4 # The following lines are desirable for IPv6 capable hosts
5 ::1          localhost ip6-localhost ip6-loopback
6 ff02::1      ip6-allnodes
7 ff02::2      ip6-allrouters
```

**Note:** If you did not set a static IP-Address for your ASGARD Management Center server, your IP-Address in the second line of the file might be 127.0.1.1. This is due to your server using DHCP. It is advised that you are using a static IP-Address. To change this, please see [Changing the IP-Address](#).

You can verify if the changes worked. Run the following commands and see the difference in the output:

```
nextron@asgard-mc:~$ hostname --fqdn
asgard-mc.example.org
nextron@asgard-mc:~$ hostname
asgard-mc
```

If the first command shows the FQDN and the second one the hostname without domain, your changes were set up correctly and you can continue to the next step.

### Recreate the TLS Certificate

We need to recreate the TLS certificate to make the Agent to ASGARD communication possible again. Create a new file which will contain the script with the fix. In this example we'll use nano as the text editor. Make sure that the system has a valid FQDN.

```
nextron@asgard-mc:~$ nano fix-fqdn.sh
```

Insert the following content into the text editor:

```
1 #!/bin/bash
2 export FQDN=$(hostname --fqdn)
3
4 sed "s/\${FQDN}/${FQDN}/" /etc/asgard-management-center/server_cert_ext.cnf.in > /etc/
5 ↪ asgard-management-center/server_cert_ext.cnf
6 openssl req -new -nodes -subj "/O=Nextron Systems GmbH/CN=${FQDN}" -key /etc/asgard-
7 ↪ management-center/client-service.key -out /etc/asgard-management-center/client-service.
8 ↪ csr
9 openssl x509 -req -in /etc/asgard-management-center/client-service.csr -CA /etc/asgard-
10 ↪ management-center/ca.pem -CAkey /etc/asgard-management-center/ca.key -CAcreateserial -
11 ↪ days 36500 -out /etc/asgard-management-center/client-service.pem -extfile /etc/asgard-
12 ↪ management-center/server_cert_ext.cnf
13 systemctl restart asgard-management-center.service
14 asgard-agent-repacker -host $FQDN
```

After changing the variables to the desired values, save the file. In nano this can be done in by pressing CTRL + X and confirming the changes with y.

Give the created script execution permissions and execute it:

```
nextron@asgard-mc:~$ chmod +x fix-fqdn.sh
nextron@asgard-mc:~$ sudo ./fix-fqdn.sh
```

You should now be able to reach the ASGARD Server via the new FQDN. Navigate to `https://<YOUR-FQDN>:8443`, which reflects the FQDN we set earlier.

At this point you have to install the ASGARD agents on your endpoints again. Remember to review the network requirements section to ensure all needed ports are open to the ASGARD Management Center from your endpoints. See [Network Requirements](#)

## 7.5 ASGARD Errors

### 7.5.1 ASGARD noticed that the THOR scan failed

In some cases THOR fails to complete its scan and ASGARD reports the following error.

```
ASGARD noticed that the THOR scan failed

could not remove temp directory: remove C:\Windows\Temp\asgard2-agent\12fa35a6762a\thor\
↳ signatures\sigma\windows\file_event_win_webshell_creation_detect.yms:
The process cannot access the file because it is being used by another process. exit.
↳ status 1
(scan result does not exist)
```

The most likely reason for this error is an Antivirus interaction. The Antivirus killed the THOR process and still holds a handle to one of the signature files. The "THOR Launcher" can only report that the process was terminated and that it isn't able to remove all files because the Antivirus process still has that open handle on the file.

Solution:

Configure an Antivirus exclusion for THOR. See *Antivirus and EDR Exclusions* for more details.

## 7.6 Resetting TLS/SSL Certificates

### 7.6.1 Web GUI: Regenerate the Self-Signed Certificate

ASGARD ships with a self-signed certificate for its web interface that expires after 182 days. If you do not use your own CA infrastructure and want to renew the certificate or want to revert from a broken state, you can recreate a self-signed certificate. To do so log in using SSH and execute:

```
nexttron@asgard:~$ sudo openssl req -new -newkey rsa:4096 -days 182 -nodes -x509 -subj "/
↳ O=Nexttron Systems GmbH/CN=$(hostname --fqdn)" -keyout /etc/asgard-management-center/
↳ server.key -out /etc/asgard-management-center/server.pem
```

You need to restart ASGARD in order for the changes to take effect.

```
nexttron@asgard:~$ sudo systemctl status asgard-management-center.service
```

### 7.6.2 Regenerate ASGARD Server Certificate Agent Communication

Please see chapter *Using Hostname instead of FQDN*.

## 7.7 Admin User Password Reset

If you've lost the password of the local admin user (Web GUI) but still have access the system via SSH, you can reset it via command line using the following command.

```
nexttron@asgard:~$ sudo mysql asgard-management-center -e "UPDATE users SET password = 'YmIc6P_6jdbEEL0HY4xIcpYstmM' WHERE name = 'admin';"
```

This resets the password to admin. You should then change that password immediately.

## 7.8 Resetting Two Factor Authentication

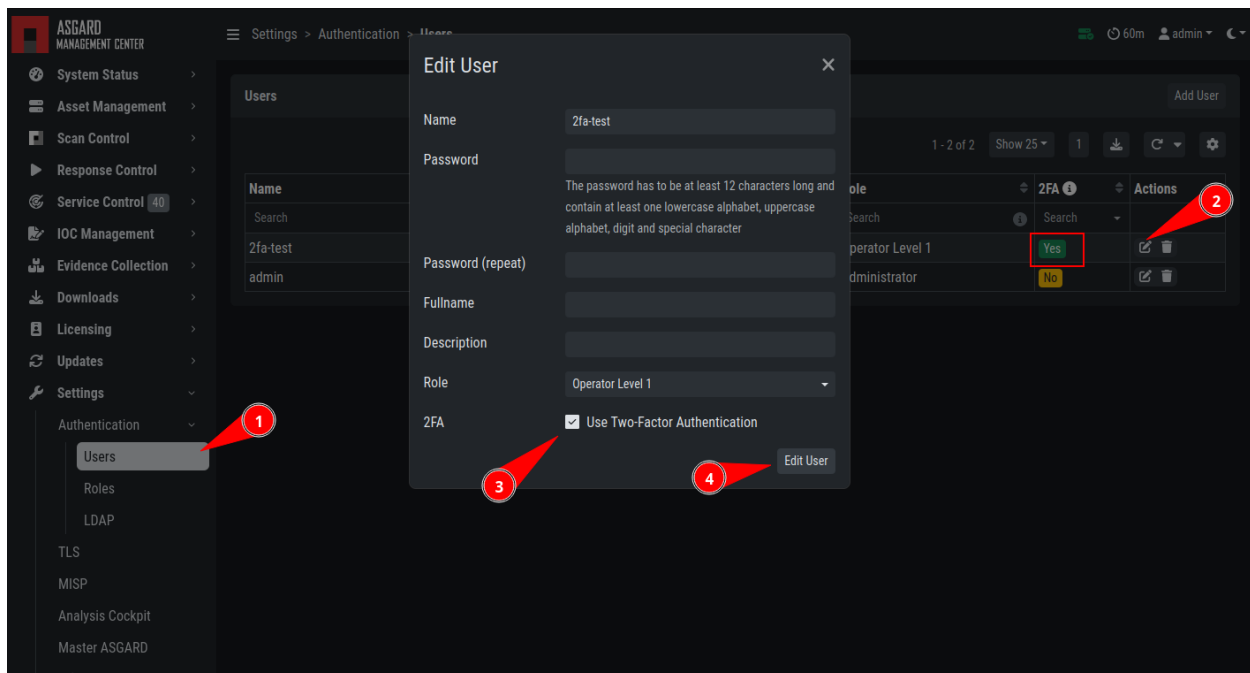
If you or another user lost their second factor (2FA) to log into the ASGARD Web UI, you have to reset the users MFA Settings. If you cannot access the Web UI, use the Command Line method.

There are two possible ways to reset Two Factor Authentication for a specific user. We recommend to use the first option via the WebUI.

### 7.8.1 Using the Web UI

Log into ASGARDs Web UI as a user with administrative privileges.

Navigate to **Settings > Authentication > Users** and edit the user you want to reset 2FA for. On the bottom of the modal you will see that the 2FA option is enabled. Disable the option and click **Edit User** (Leave everything else as it is; do not fill in a new password if not necessary).



After you edited the user, the Two Factor Authentication will be disabled and the user can log into ASGARD without 2FA.



## 7.8.2 Using the Command Line Interface

**Note:** This method needs SSH access to the Management Center.

Log into your ASGARD via SSH. You can reset the users MFA Settings with the following command (in this example we assume that the user is called john):

```
nexttron@asgard:~$ sudo mysql asgard-management-center --execute "UPDATE users SET tfa_
↪valid = 0 WHERE name = 'john';"
```

**Warning:** This will disable the 2FA settings directly in the database. Please make sure the command and especially the username is correct.

If you don't know the exact username for a user, you can use the following command to get all the usernames and the 2FA status from ASGARD (if tfa\_valid has a value of 1, this means the user has Two Factor Authentication enabled).

```
nexttron@asgard:~$ sudo mysql asgard-management-center --execute "select name,tfa_valid,
↪from users;"
```

name	tfa_valid
admin	1
john	0
rickroll	1

This command will also allow you to verify if the UPDATE command was successful (tfa\_valid should be 0).

## 7.9 Scheduled Scans have incorrect time

In some cases the timezone during the installation of the server image might not be correct. To see if you have this problem in your current installation, please log into your server and execute the following command:

```
nexttron@asgard:~$ timedatectl
      Local time: Mon 2022-10-24 09:52:03 BST
     Universal time: Mon 2022-10-24 08:52:03 UTC
          RTC time: Mon 2022-10-24 08:52:04
        Time zone: Europe/London (BST, +0100)
System clock synchronized: no
          NTP service: inactive
      RTC in local TZ: no
```

If you see that the **Time zone** is incorrect, follow the next steps to correct it.

List all the timezones with `timedatectl list-timezones`. If you want to search for a specific Country/City, you can use `grep`, e.g. `timedatectl list-timezones | grep Prague`.

Now that you have the correct timezone you can set it the following way:

```
nexttron@asgard:~$ sudo timedatectl set-timezone Europe/Prague
nexttron@asgard:~$ timedatectl
          Local time: Mon 2022-10-24 10:56:45 CEST
          Universal time: Mon 2022-10-24 08:56:45 UTC
            RTC time: Mon 2022-10-24 08:56:46
            Time zone: Europe/Prague (CEST, +0200)
System clock synchronized: no
            NTP service: inactive
          RTC in local TZ: no
```

Please reboot the system after the changes have been made.

**Warning:** This might cause problems with existing Scheduled Scans!

## 7.10 Aurora has too many False Positives

In some environments, Aurora might generate a high amount of False Positives. This should never be the case, since Aurora should only alert on very few and mostly important findings. Most likely a rule is matching on the environment and generates too many false positives. To circumvent this, you can disable the rule and set a filter later on. For Tuning, please see *False Positive Tuning of Sigma Rules*.

## KNOWN ISSUES

You can find a list of known issues in this section.

### 8.1 Known Issues

#### 8.1.1 AMC#008: could not generate csr

This bug will prevent you from generating a new CSR in the TLS Section of the Settings. The error message will look like this:

```
Error - could not generate csr
Could not read private key
```

Introduced Version	Fixed Version
<= 3.0.11	3.0.12

This bug will only occur if you upgraded your ASGARD Management Center from version 2.x to 3.x. The issue is caused by the `controller.key` file not being present in the `/etc/asgard-management-center` directory. If you installed a fresh ASGARD Management Center 3.x, with the new web based installer, this issue will not occur.

#### AMC#008: Workaround

To work around this issue, you can run the following command:

```
nextron@asgard:~$ sudo -u asgard-management-center ln -s /etc/asgard-management-center/
↪server.key /etc/asgard-management-center/controller.key
[sudo] password for nextron:
```

This will create a symbolic link from the `server.key` to the `controller.key` file. After that, you should be able to generate a new CSR in the TLS Section of the Settings.

### 8.1.2 AMC#007: curl: (58) could not load PEM client certificate

This bug only affects the asgard-updater helper tool, which is used to update your ASGARD Management Center from version 2.x to 3.x

Introduced Version	Fixed Version
<= 1.0.20	1.0.21

There is a bug in older versions of the asgard-updater tool which is used to update your ASGARD Management Center from version 2.x to 3.x. When using start-asgard-update, you might encounter the below error in rare cases.

```
curl: (58) could not load PEM client certificate, OpenSSL error error:0909006C:PEM_
↳ routines:get_name:no start line, (no key found, wrong pass phrase, or wrong file_
↳ format?)
```

This error will appear if the following conditions are met:

- the directory /etc/nextron/asgard2 contains multiple licenses files (.lic)
- one of the licenses is older than April 2023
- one of the old licenses is the last in an alphabetical order (based on the MD5 Hash)

#### AMC#007: Workaround

There are two workarounds, with the first being the easier one:

1. Install the newest version of the asgard-updater

```
nexttron@asgard:~$ sudo apt update
nexttron@asgard:~$ sudo apt install asgard-updater
```

2. Remove the old license files (you might need to change to default license view to "All Licenses" in your Management Center). You can compare the MD5 value of the license with the filename of all licenses in the /etc/nextron/asgard2 directory and delete expired or old licenses.

### 8.1.3 AMC#006: THOR License not valid yet (timezone difference)

Introduced Version	Fixed Version
<= 2.16.3	N/A

There is currently a bug in the ASGARD Management Center which can cause problems during THOR license generation. This happens if the following conditions are given:

- An asset which is located in a different timezone to your ASGARD Management Center
- The difference between the two timezones is greater than 8 hours.

If this is the case for a few assets of yours, you will encounter the following error in your THOR scan:

```
REASON: license not valid yet
```

## AMC#006: Workaround

The current workaround is to avoid issuing THOR licenses on your ASGARD Management Center during a specific time window. We take the time difference between your asset and your Management Center and subtract 8 hours. The resulting time is the time window, beginning at 00:00 AM local time of your Management Center, from which you should avoid issuing licenses. Below are two examples:

- ASGARD Management Center timezone: UTC +11
- Asset timezone: UTC -3

This results in a time difference of 14 hours. We subtract 8 hours from that and are left with 6 hours. That means you should avoid issuing new licenses during the following time:

00:00 AM until 06:00 AM of the ASGARD Management Center local time.

If you have the following scenario, you will not encounter the problem:

- ASGARD Management Center timezone: UTC +2
- Asset timezone: UTC -3

The timezone difference is smaller than 8.

### 8.1.4 AMC#005: Edge Browser with translation, "removeChild" error

Introduced Version	Fixed Version
N/A	N/A

Microsoft's Edge Browser is changing DOM objects on web pages, when the translator is activated. This leads to the following error on some of our pages:

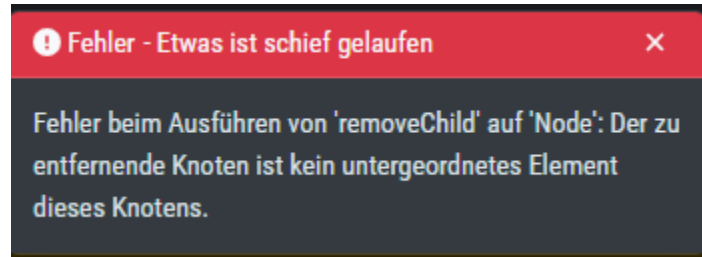


Fig. 1: removeChild Error with Edge translation

Since this is an issue with Microsoft Edge, we can not fix this. You have to disable the translation tool of Edge to make the pages functional.

### 8.1.5 AMC#004: Missing asgard2-agent.yaml

Introduced Version	Fixed Version
asgard2-agent (1.6.5)	Planned end of April 2023

Due to a bug in the installer of our ASGARD Agent, there is a possibility that the configuration file (`asgard2-agent.yaml`) gets renamed but not replaced by a more current version. This usually happens if the agent installer is being run a second time, after the agent is already installed. In some rare cases this can also happen when the agent is being updated via your ASGARD. All together, this leaves the agent in an undesirable state, which will cause no tasks/jobs to be executed due to the missing config file (task will be in Pending state or return an error).

You will find errors in the agent log (`C:\Windows\System32\asgard2-agent\log\agent.log`) and also observe that the installer directory only contains `asgard2-agent.yaml.old` and not the correct `asgard2-agent.yaml` config file.

Listing 1: Errors in the asgard.log file

```
2023/03/29 23:34:26 ASGARD_THOR: Error: could not load config: open C:\Windows\System32\
↪asgard2-agent\asgard2-agent.yaml: The system cannot find the file specified.
2023/03/29 23:34:26 ASGARD_AGENT: Error: task 1350 done with error: exit status 1
```

Another indicator is the `asgard2-agent-install.log` file located at `C:\Windows\System32\asgard2-agent\`. This almost always means the installer was executed multiple times. See the two highlighted lines below, a normal install would only contain the first line. Re-running the installer will produce lines 2 and 3, which indicate that the agent might be in the faulty state.

Listing 2: Errors in the asgard2-agent-install.log file

```
1 2023/03/30 16:13:14 installer arguments: asgard2-agent.exe -install
2 2023/03/30 16:13:14 could not open dst file C:\Windows\System32\asgard2-agent\asgard2-
↪agent-service.exe: open C:\Windows\System32\asgard2-agent\asgard2-agent-service.exe:
↪The process cannot access the file because it is being used by another process.
3 2023/03/30 16:13:14 could not copy files from executable path . to install path C:\
↪Windows\System32\asgard2-agent: open C:\Windows\System32\asgard2-agent\asgard2-agent-
↪service.exe: The process cannot access the file because it is being used by another
↪process.
```

#### AMC#004: Workaround

To get the agent up and running again, you need to rename the config file to its original name and restart the `asgard2-agent` service. We wrote a little batch script you can use, alternatively you can write your own and deploy it. Administrative rights on the endpoint are needed.

```
1 @ECHO OFF
2
3 IF EXIST "C:\Windows\System32\asgard2-agent\asgard2-agent.yaml" GOTO noFix
4 IF EXIST "C:\Windows\System32\asgard2-agent\asgard2-agent.yaml.old" GOTO fixConfig
5
6 :noFix
7 echo config file exists, nothing to do
8 GOTO commonExit
9
```

(continues on next page)

(continued from previous page)

```

10 :fixConfig
11 echo stopping asgard2-agent service
12 sc stop asgard2-agent
13 timeout /t 5
14
15 echo config file in renamed state, fixing
16 copy "C:\Windows\System32\asgard2-agent\asgard2-agent.yaml.old" "C:\Windows\System32\
   ↳ asgard2-agent\asgard2-agent.yaml"
17 timeout /t 2
18
19 echo starting asgard2-agent service
20 sc start asgard2-agent
21 timeout /t 5
22
23 echo service should be in state RUNNING
24 sc query asgard2-agent | findstr STATE
25
26 GOTO commonExit
27
28 :commonExit
29 exit

```

**Hint:** If you are seeing a second asset with the same hostname in your ASGARD, the issue was most likely caused by re-installing the agent over an already installed agent. Try to avoid running the installer a second time on systems which already have an agent installed. You can find information when the installer was being run in the installer log C:\Windows\System32\asgard2-agent\asgard2-agent-install.log.

### 8.1.6 AMC#003: Context Deadline Exceeded

Introduced Version	Fixed Version
N/A	Ongoing

When debugging GRPC connectivity issues between your components (for example Management Center to Analysis Cockpit), you might encounter an error similar to the following one:

```

1 {
2   "LEVEL": "Warning",
3   "MESSAGE": "could not dial grpc",
4   "MODULE": "api",
5   "REQUEST_IP": "172.16.30.20",
6   "TIME": "2023-03-06T12:35:37Z",
7   "USER": "admin",
8   "error": "context deadline exceeded",
9   "host": "cockpit3.domain.local:7443"
10 }

```

### AMC#003: Workaround

There is no workaround for this type of error. The error usually occurs because one of the following things are preventing proper communication between your components:

- Firewall is using TLS Inspection
- Proxy is using TLS Inspection
- DNS Issues

---

**Note:** Your components expect specific certificates from each other when communicating. If a device is trying to inspect TLS traffic, the certificate will change and you receive the above error.

---

To help you figuring out what is causing the problem, you can try the following. You can use openssl on your source system to see which certificate is presented by the destination host (change the host and port values as needed).

```
nexttron@asgard2:~$ openssl s_client -host cockpit3.domain.local -port 7443
CONNECTED(000000005)
depth=0 0 = Nextron Systems GmbH, CN = cockpit3.domain.local
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 0 = Nextron Systems GmbH, CN = cockpit3.domain.local
verify error:num=21:unable to verify the first certificate
verify return:1
write W BLOCK
---
Certificate chain
 0 s:0 = Nextron Systems GmbH, CN = cockpit3.domain.local
  i:0 = Nextron Systems GmbH, CN = Analysis Cockpit 3
---
Server certificate
-----BEGIN CERTIFICATE-----
```

The marked lines show you the certificate which is presented by the destination host. If this certificate is different from the one you installed, then the problem might be a device trying to do TLS Inspection.

We are currently working on improving the presented error message, to give a better understanding what might be the issue at hand.

### 8.1.7 AMC#002: High number of duplicate assets

Introduced Version	Fixed Version
N/A	N/A

In some edge cases within restricted endpoint configurations, you can encounter a problem which causes some agents to send a lot of asset requests. This is mostly caused by hardened systems, where the asgard agent is not able to write to its own configuration file. One example is SELinux prohibiting write access to the needed YAML file.



## AMC#002: Workaround

The asgard-agent process needs write access to the configuration file.

Make sure the following condition is present to avoid multiple asset requests from the same endpoint:

Process	File	Permissions
/var/lib/asgard2-agent/asgard2-agent	/var/lib/asgard2-agent/asgard2-agent.yaml	Read/Write

Make sure to disable `Automatically accept all Asset Requests` in the *Advanced Settings* Settings in the meantime, to avoid cleaning up after the changes to the endpoints have been made.

## 8.1.8 AMC#001: Nested LDAP Groups not working

Introduced Version	Fixed Version
2.0.0	Open

Using nested groups in your LDAP/AD will result in no users because the query will fail.

## AMC#001: Workaround

Change your LDAP GroupFilter to the following:

```
(&(objectCategory=group)(objectClass=group)(member:1.2.840.113556.1.4.1941:=%s))
```



## APPENDIX

This chapter contains random scripts and tips for various tasks you might encounter. Please keep in mind that we want to provide guidance with the scripts in this chapter, and you should still try to understand what they do and modify them accordingly to your needs.

## 9.1 Installing ASGARD Agent via Powershell Script

You can find a simple script to install the ASGARD Agent via Powershell. Place the installer and script in the same folder. Change the script as needed.

```
1  # Setting vars
2  $scriptpath = $MyInvocation.MyCommand.Path
3  $dir = Split-Path $scriptpath
4  $installer = "asgard2-agent-windows-amd64.exe"
5  $servicename = "asgard2-agent"
6
7  # Checking if ASGARD Agent is already installed
8  if (Get-Service -Name $servicename -ErrorAction SilentlyContinue) {
9      Write-Host "ASGARD Agent already installed, exiting"
10     exit 0
11 } else {
12     Write-Host "ASGARD Agent not found, trying to install..."
13
14     # Install ASGARD Agent
15     Start-Process -Wait -FilePath "$dir\$installer" -WorkingDirectory $dir -WindowStyle_
↵Hidden -PassThru
16
17     # Timeout just to make sure the service is up and running
18     Timeout /T 15
19
20     # Checking service to see if agent was installed
21     if (Get-Service -Name $servicename -ErrorAction SilentlyContinue) {
22         Write-Host "Installed ASGARD Agent successfully"
23         exit 0
24     } else {
25         $Host.UI.WriteLine("Could not install ASGARD Agent")
26         exit 1
27     }
28 }
```

## 9.2 Deploy ASGARD Agents via SCCM

To deploy the ASGARD Agent (or any other .exe installer) via SCCM, you have to write a Powershell script with a few conditions to mark an installation correctly as successful or failed.

Please refer to Microsoft's [Create applications in Configuration Manager](#) .

```

1  # Get current directory
2  $scriptpath = $MyInvocation.MyCommand.Path
3  $dir = Split-Path $scriptpath
4
5  # Run the installer
6  $installer = "asgard2-agent-windows-amd64.exe"
7  Start-Process -Wait -FilePath "$dir\$installer" -WorkingDirectory $dir -WindowStyle_
   ↪ Hidden -PassThru
8
9  # Timeout just to make sure the service is up and running
10 Timeout /T 15
11
12 # If the service exists, the script writes console output and exits with code 0
13 # If the service does not exist, the script writes an error output and exits with code 1
14 # See https://learn.microsoft.com/en-us/mem/configmgr/apps/deploy-use/create-applications
   ↪ #about-custom-script-detection-methods
15
16 $servicename = "asgard2-agent"
17 if (Get-Service -Name $servicename -ErrorAction SilentlyContinue) {
18     Write-Host "ASGARD Agent installed"
19     exit 0
20 } else {
21     $Host.UI.WriteLine("ASGARD Agent not installed")
22     exit 1
23 }

```

**Warning:** This is just an example script which should work with SCCM. If you encounter any problems, refer to the link provided above for additional information.

SCCM Applications can also use a script to detect the Deployment. You can use this part of the script to detect if the installation was successful:

```

1  $servicename = "asgard2-agent"
2  if (Get-Service -Name $servicename -ErrorAction SilentlyContinue) {
3      Write-Host "ASGARD Agent installed"
4      exit 0
5  } else {
6      $Host.UI.WriteLine("ASGARD Agent not installed")
7      exit 1
8  }

```

## 9.3 Broken file and folder permissions

The ASGARD Agent folder has in a normal installation specific permissions set. The ASGARD Agent checks regularly for broken permissions and tries to fix them. If for some reason this process fails, you have to check and change the permissions manually.

```
2023/03/31 12:02:35 ASGARD_THOR: Error: failed to repair permissions: set security info:
↪Access is denied.
```

To do this we wrote a little PowerShell script which can help you with this process. Please test the script before you deploy it in your environment. To do this, you can leave the `-WhatIf` flag to see what the script would do if the permissions are broken. If you are content with the potential changes, remove the `-WhatIf` arguments. The script needs administrative permissions.

```
1 $asgardAgent = "C:\Windows\System32\asgard2-agent"
2 $asgardAgentTemp = "C:\Windows\Temp\asgard2-agent"
3
4 if (Get-Item -Path $asgardAgent | Get-Acl | where {$_.Access.IsInherited -eq $false}) {
5     Write-Host "ASGARD Agent folder permission broken. Trying to fix: $asgardAgent"
6     # Set the new Access Rule to inherit permissions
7     $newAcl = Get-Acl -Path $asgardAgent
8     $newAcl.SetAccessRuleProtection($false, $true)
9     Set-Acl $asgardAgent -AclObject $newAcl -WhatIf
10 }
11 if (Get-Item -Path $asgardAgentTemp | Get-Acl | where {$_.Access.IsInherited -eq $false}
12 ↪) {
13     Write-Host "ASGARD Agent folder permission broken. Trying to fix: $asgardAgentTemp"
14     # Set the new Access Rule to inherit permissions
15     $newAcl = Get-Acl -Path $asgardAgentTemp
16     $newAcl.SetAccessRuleProtection($false, $true)
17     Set-Acl $asgardAgentTemp -AclObject $newAcl -WhatIf
18 }
19 get-childitem -path $asgardAgent -Recurse -Depth 1 | Get-Acl | where {$_.Access.
20 ↪IsInherited -eq $false} | % {
21     $fullPath = Convert-Path $_.Path
22     Write-Host "ASGARD Agent folder permission broken. Trying to fix: $fullPath"
23     # Set the new Access Rule to inherit permissions
24     $newAcl = Get-Acl -Path $_.Path
25     $newAcl.SetAccessRuleProtection($false, $true)
26     Set-Acl $_.Path -AclObject $newAcl -WhatIf
27 }
```

**Tip:** After you changed the permissions of the asgard2-agent folder, the agent might correct the permissions again and set them accordingly. Only use this script if the agent is showing errors that permissions can not be set.

## 9.4 Installing ASGARD Agent on a Golden Image

If you want to implement the ASGARD Agent into your Golden Image, you can do this by following the steps in this section. Make sure to download the right Agent Installer package from your ASGARD.

You have two options to deploy an Agent on your Golden Image, with the first one being the easier method.

### 9.4.1 Offline Installation

**Note:** Before continuing, make sure the host can't reach your ASGARD.

In this method we make sure that the host system, which is being prepared for the Golden Image, is either offline or can't reach the ASGARD. Go ahead and install your ASGARD agent as you do normally. Once the installation is done, you can stop the `asgard2-agent` service.

Windows (administrative command prompt):

```
C:\Windows\system32>sc stop asgard2-agent
```

Linux:

```
user@golden:~$ sudo systemctl stop asgard2-agent.service
```

You ASGARD Agent should be ready now. You have to make sure that the Agent is not communicating with your ASGARD during the whole process. If the agent is for some reason communicating with the ASGARD and creating an Asset Request, make sure that you stop the `asgard2-agent` service again and inspect the following file:

- Windows: `C:\Windows\System32\asgard2-agent\asgard2-agent.yaml`
- Linux: `/var/lib/asgard2-agent/asgard2-agent.yaml`

The file should not contain the marked lines in the next example. If both lines exist, make sure you delete them and save the file. Make also sure to deny the Asset Request in your ASGARD to avoid confusion:

```
1 host: yourasgard.domain.local:443
2 token: +uW6HrF3kxmLNZYqKTKuZt [...]
3 registered: true
4 proxy: []
5 system_proxy: false
6 labels: []
7 write_log: false
```

**Warning:** Your Golden Image will not work if the two lines in the `asgard2-agent.yaml` file exist, it instead will create a Duplicate Asset. So make sure that they are not present when you are creating the Golden Image!

## 9.4.2 Online Installation

If for some reason you can not prevent your host, which is being used for the Golden Image, to communicate with your ASGARD, then follow the next steps. Go ahead and install your ASGARD agent as you do normally. Once the installation is done, you can stop the `asgard2-agent` service.

Windows (administrative command prompt):

```
C:\Windows\system32>sc stop asgard2-agent
```

Linux:

```
user@golden:~$ sudo systemctl stop asgard2-agent.service
```

Once the service is stopped, we have to alter the configuration file of the agent. This is necessary because your agent will have communicated with your ASGARD by now, thus having generated an `token`, which should be unique. If you would create your Golden Image now, you would have the systems, installed with the Golden Image, appear as Duplicate Asset (see [Duplicate Assets Remediation](#)).

Open the `asgard2-agent.yaml` file and delete the marked lines in our example.

- Windows: `C:\Windows\System32\asgard2-agent\asgard2-agent.yaml`
- Linux: `/var/lib/asgard2-agent/asgard2-agent.yaml`

```
1 host: yourasgard.domain.local:443
2 token: +uW6HrF3kxmLNZYqKTKuZt [...]
3 registered: true
4 proxy: []
5 system_proxy: false
6 labels: []
7 write_log: false
```

After you deleted the two lines and saved the file, your host is ready. Make sure those two lines are not present, as well as your `asgard2-agent` service is still not running. We delete the `token` because it is unique to ASGARD. If two agents are presenting the same token, they will be flagged as duplicate assets. The `registered` value tells the agent if it has to send a new asset request or not. Once it is set to `true` it would not send a new request.

---

**Hint:** Make sure to deny the Asset Request, which we just created while installing the agent on our host, in ASGARD. This is to avoid confusion down the road.

---

## 9.5 Install TLS certificates on ASGARD and MASTER ASGARD

There are several methods to sign the ASGARD generated CSR request. This section describes the two most common procedures.

## 9.5.1 Use Case 1 - CSR Signing with a Microsoft Based CA

Open the Certificate Authority snap-in within Windows Server

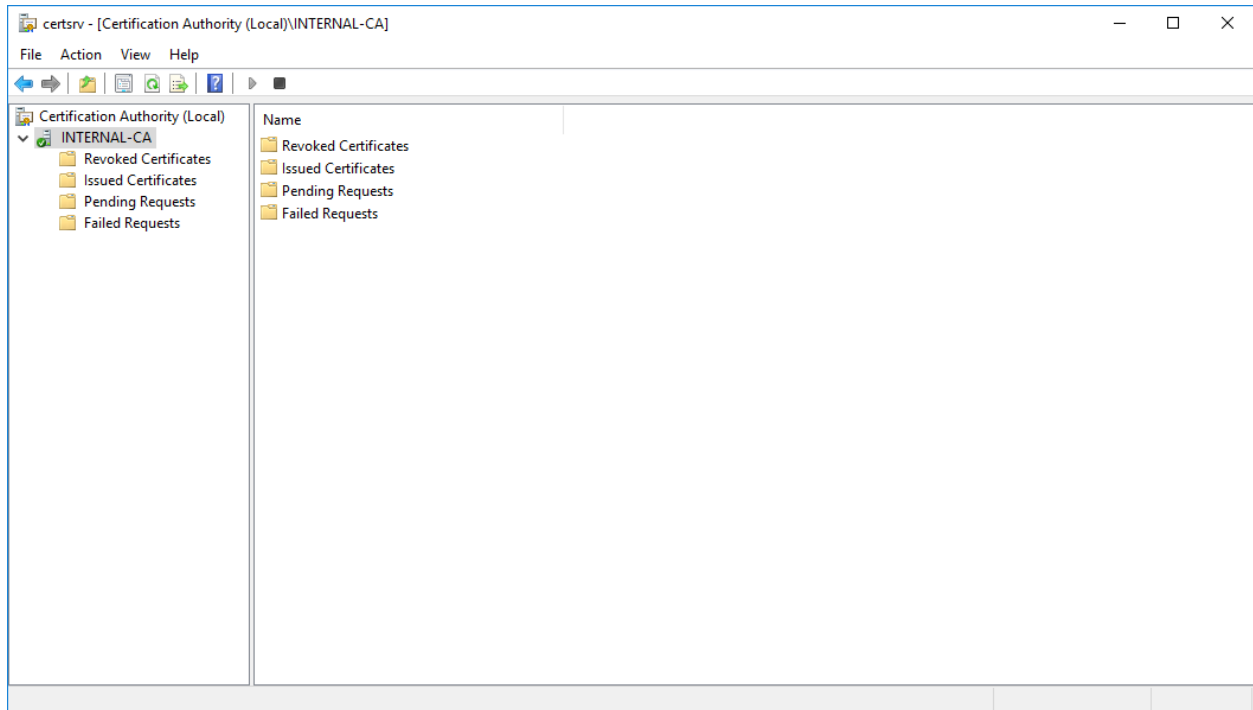


Fig. 1: certsrv – Microsoft Certification Authority Main Page

Right click your CA >> All Tasks >> Submit new request

Locate and open the signing request file we've saved in previous steps

Navigate to the "Pending Requests" within your CA snap-in and right click the imported CSR >> All Tasks >> Issue

Once the certificate has been issued, it will be located under "Issued Certificates"

Right click on the issued certificate and click open

Inspect the information of the Certificate and continue to the next step, if the presented data is correct.

Check that the generated certificate has a status of OK

Navigate to the Details tab and click "Copy to File..."

On the Certificate Export Wizard – click Next

Select Base-64 encoded X.509(.CER) and click Next

Choose an output location and click Next

Click Finish - Once the confirmation message box pops up, click OK

Navigate to Settings >> TLS.

On the bottom of the page click Upload TLS Certificate and select the exported certificate from the previous step.

If all steps were followed, a message box should pop up indicating that the certificate was successfully installed.

Navigate to Settings >> Services and restart the ASGARD 2 Service by clicking Restart button.

Please take into consideration that it could take a few minutes until the ASGARD Service is restarted successfully.



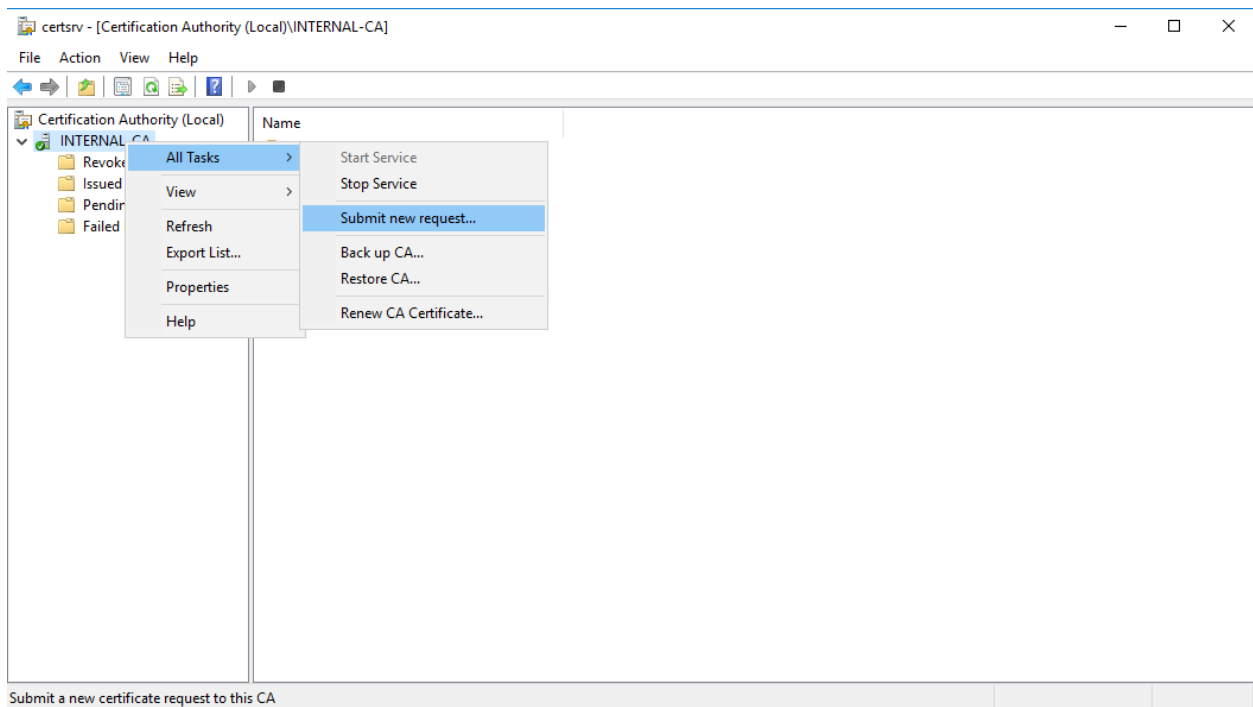


Fig. 2: certsrv – Submit new request

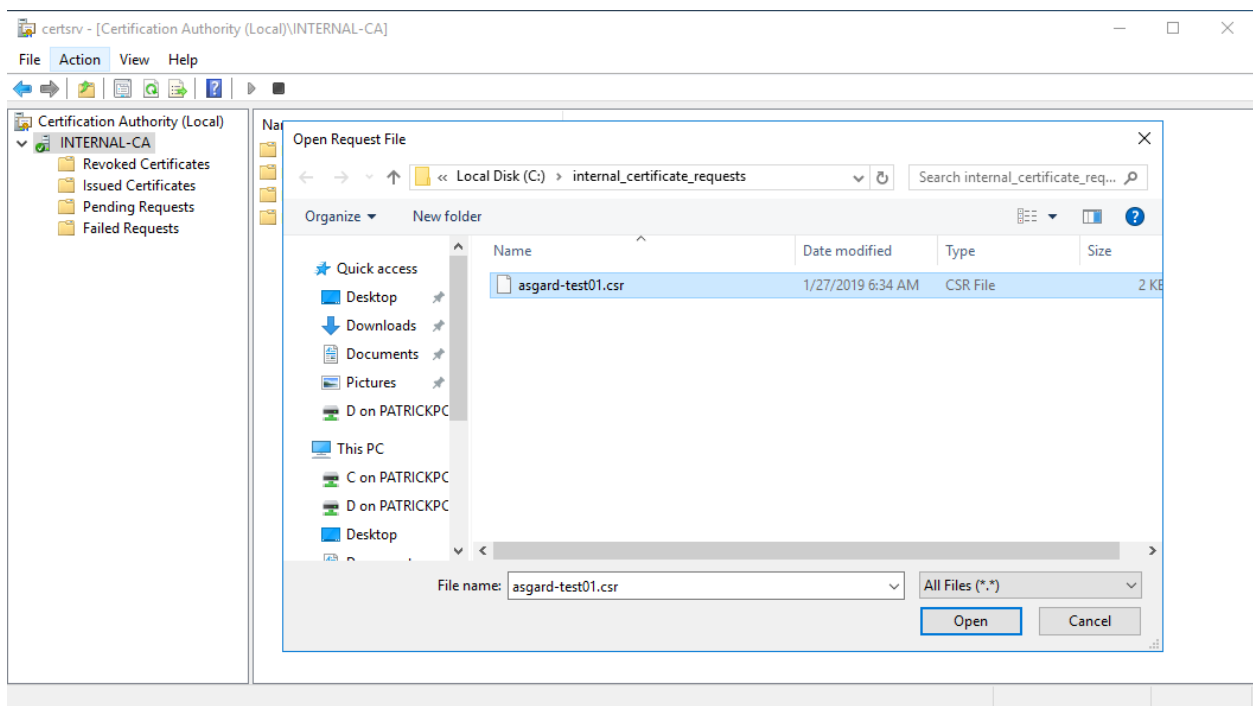


Fig. 3: certsrv – Locate the CSR to be signed

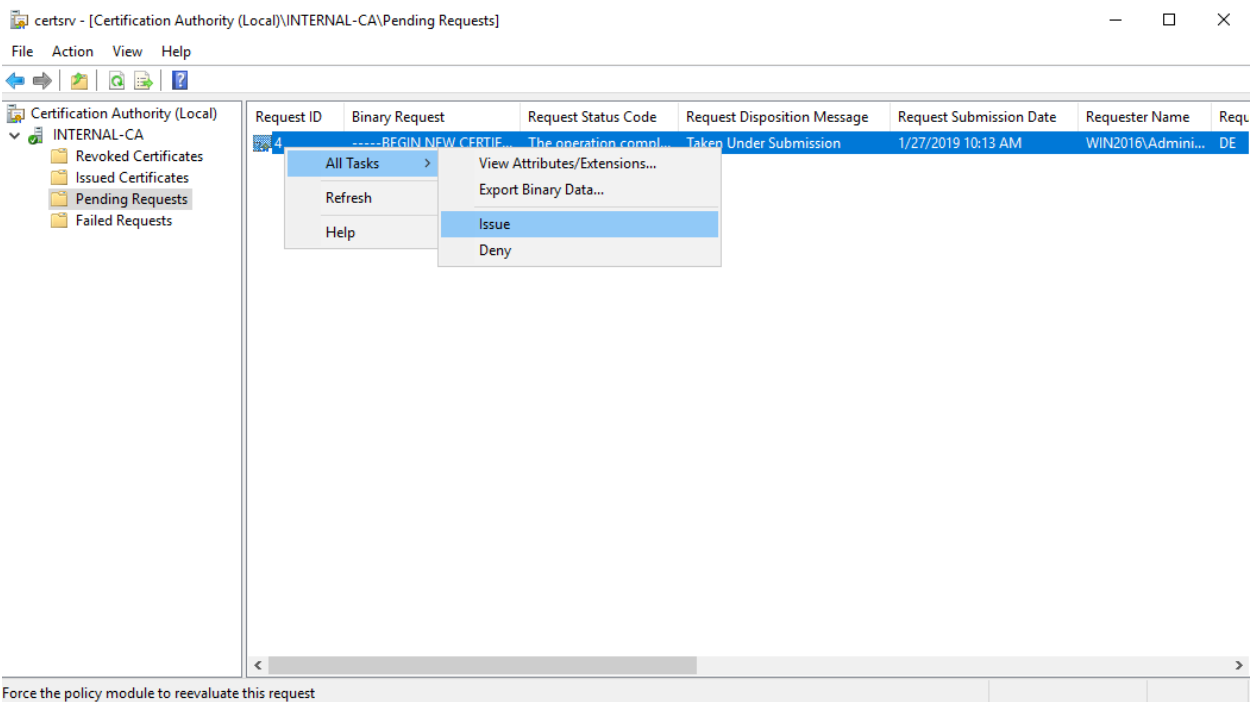


Fig. 4: certsrv – Issue the certificate

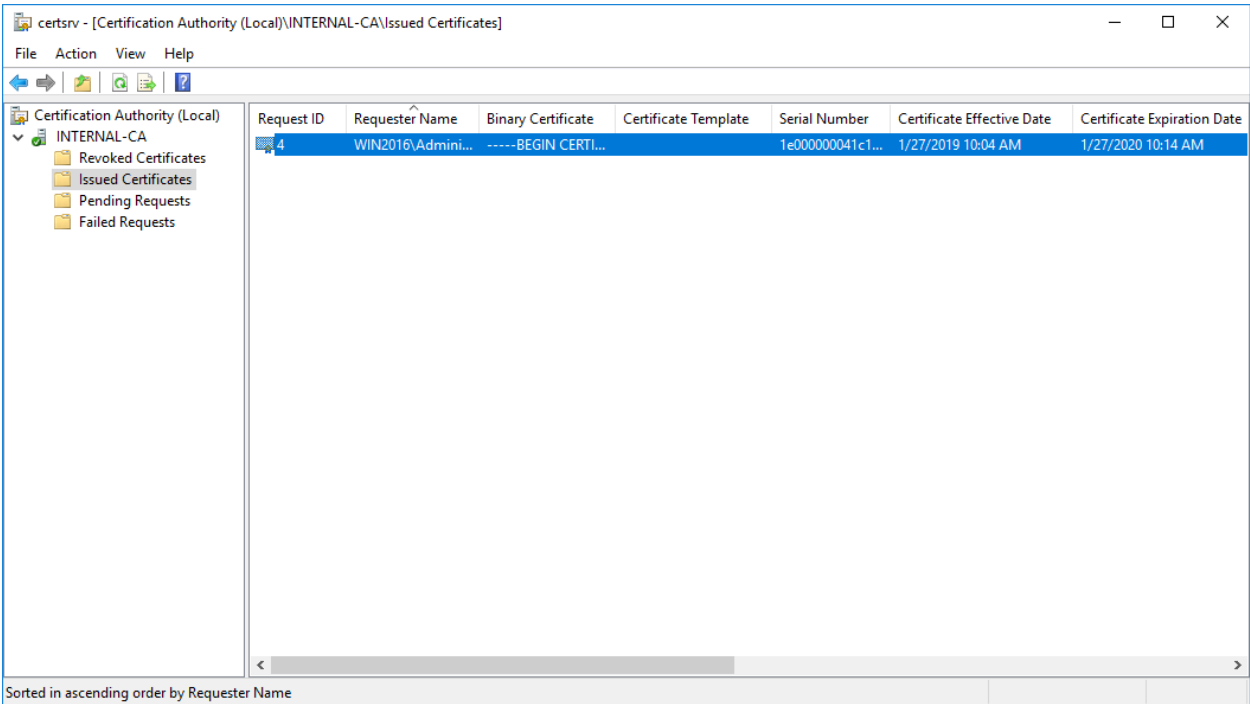


Fig. 5: certsrv – Locate issued certificate

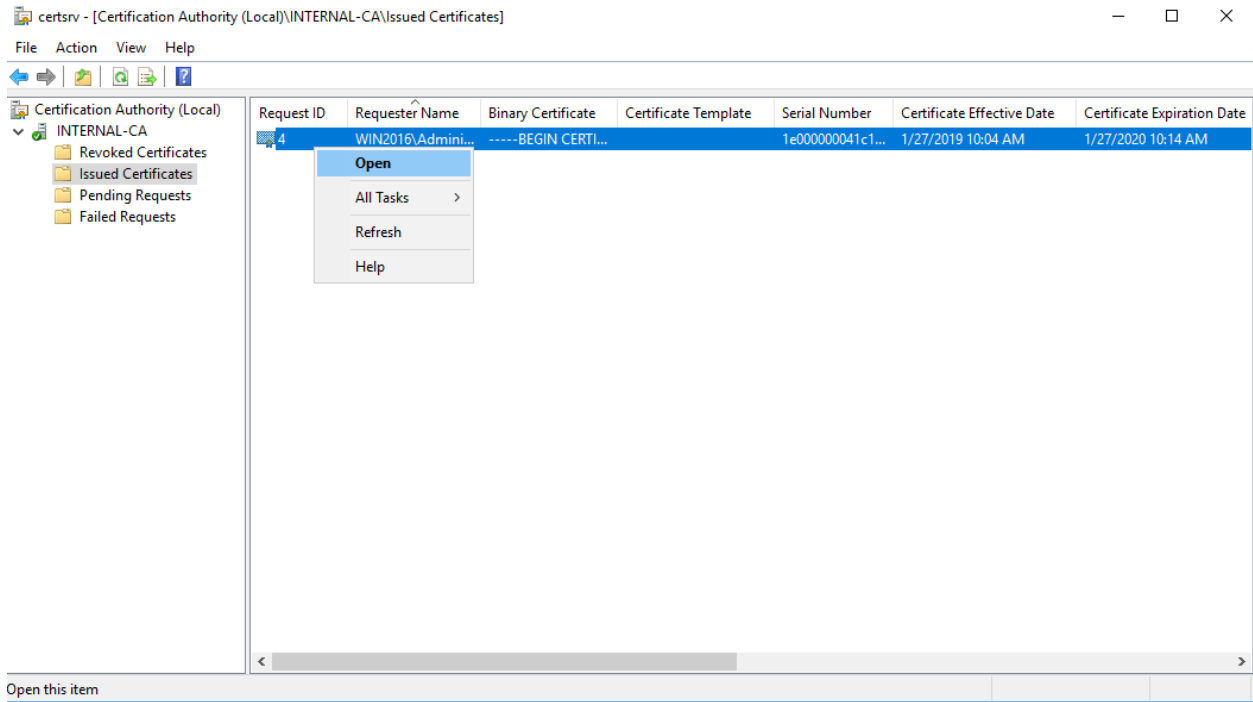


Fig. 6: certsrv – Export certificate

After the service has been successfully restarted, the installed certificate will be used by your Management Center.

## 9.5.2 Use Case 2 - CSR Signing with an OpenSSL Based CA

**Warning:** In order to avoid security warnings<sup>1</sup> on some browsers, the CA signing process needs to ensure to copy all Subject Alternative Name (SAN) from the CSR to the signed Certificate.

There are two ways of doing this while signing the CSR via openssl.

**The first method** of including all extensions from the CSR to the new certificate, is via the `openssl.cnf` file, by uncommenting the `copy_extensions` attribute.

The location of the `openssl.cnf` file depends on your system. On our test system, this file was located at `/etc/pki/tls/openssl.cnf`.

**Warning:** Please make sure to comment the line out again once you are done with signing your CSR.

Example:

```
#####
[ CA_default ]
```

(continues on next page)

<sup>1</sup> These security warnings are a result of an incomplete signing process, where requested attributes from the CSR are not included in the signed certificates (subjectAltName).

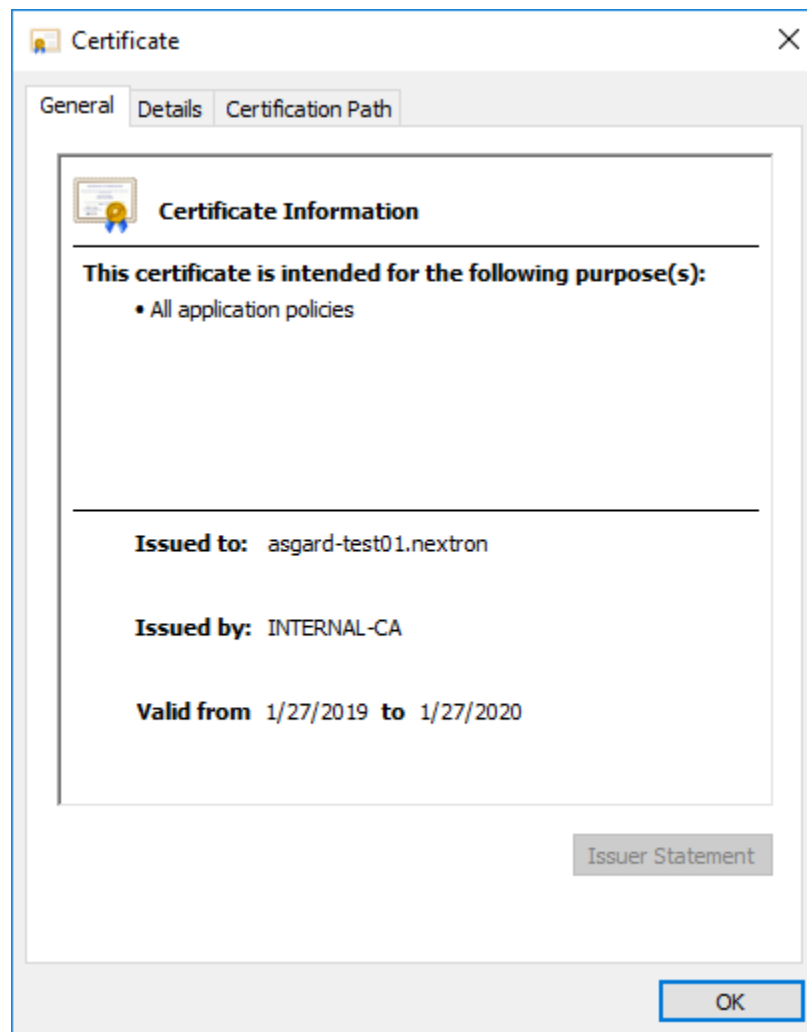


Fig. 7: certsrv – Export certificate

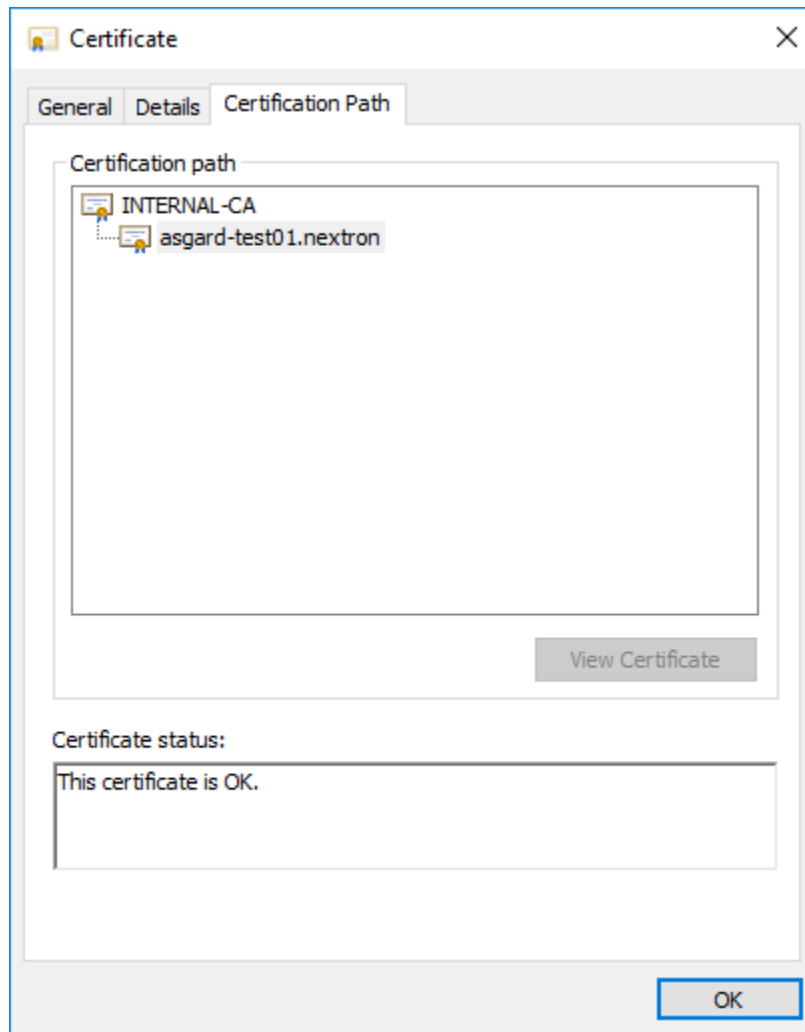


Fig. 8: certsrv – Export certificate

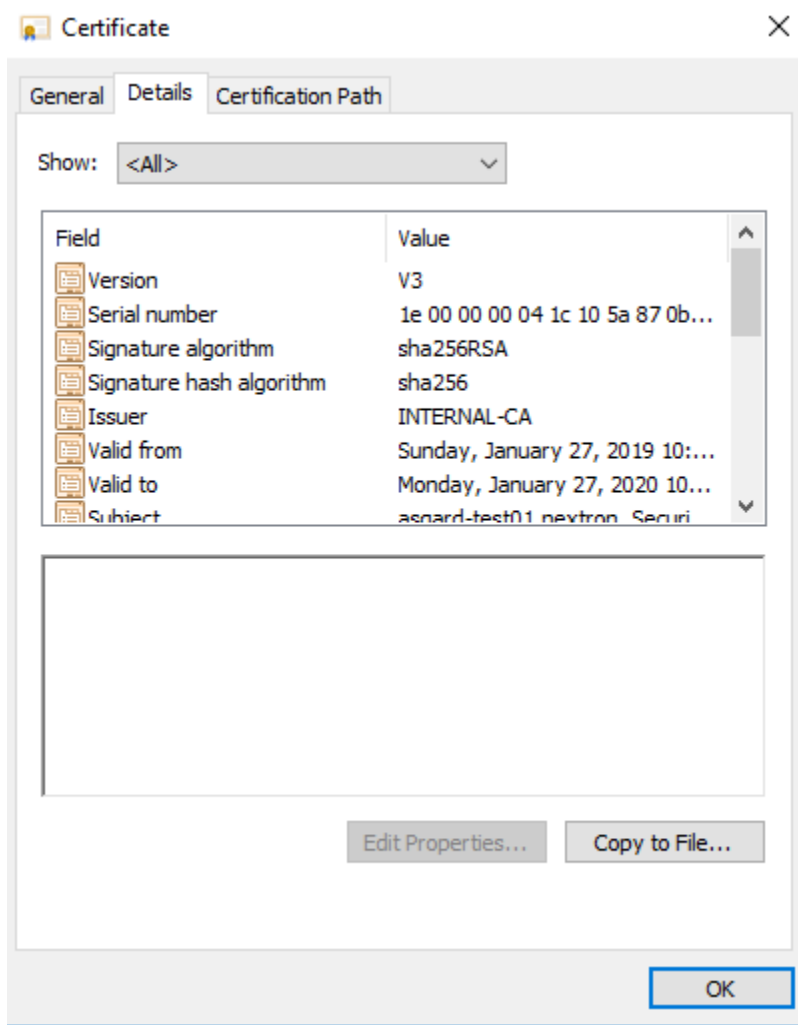


Fig. 9: certsrv – Export certificate

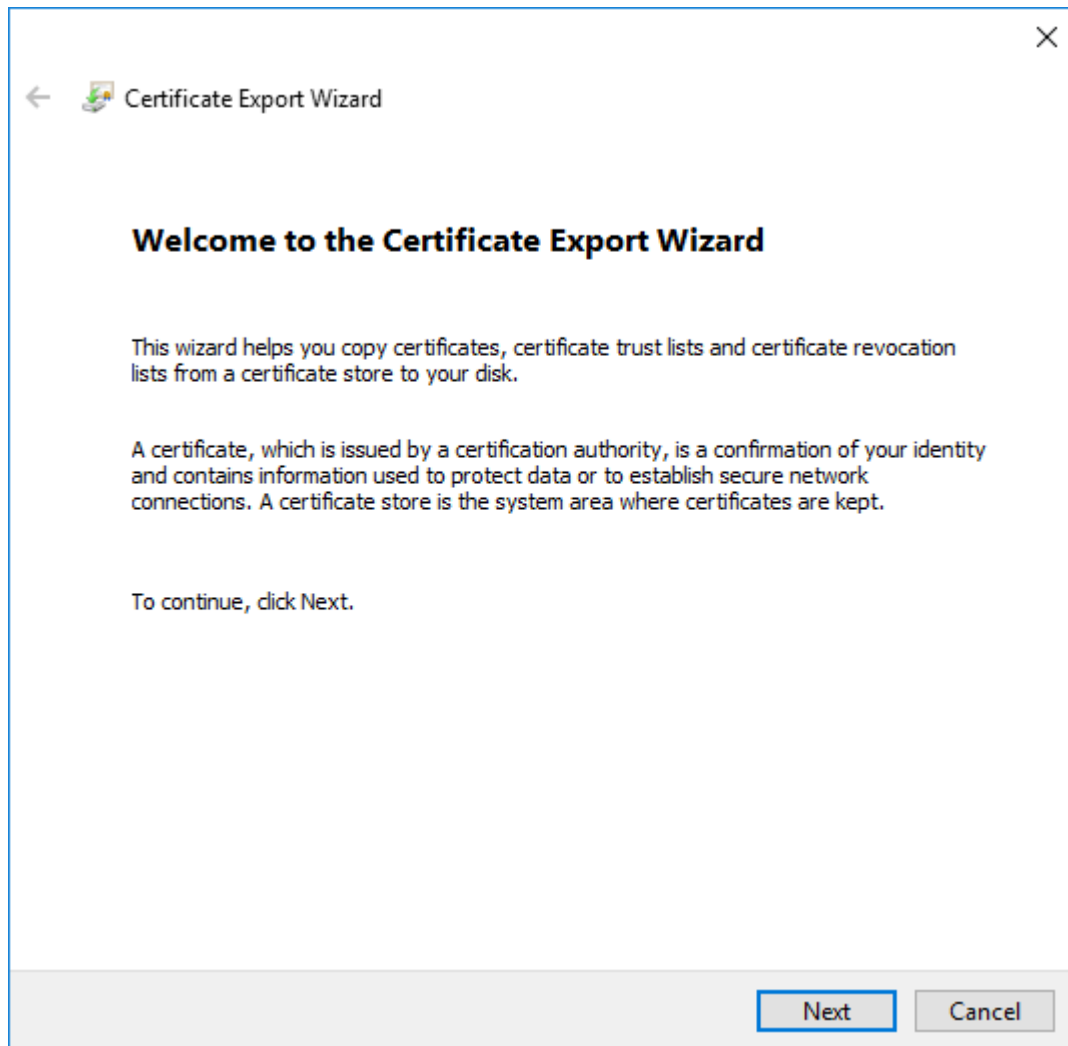


Fig. 10: certsrv – Export certificate

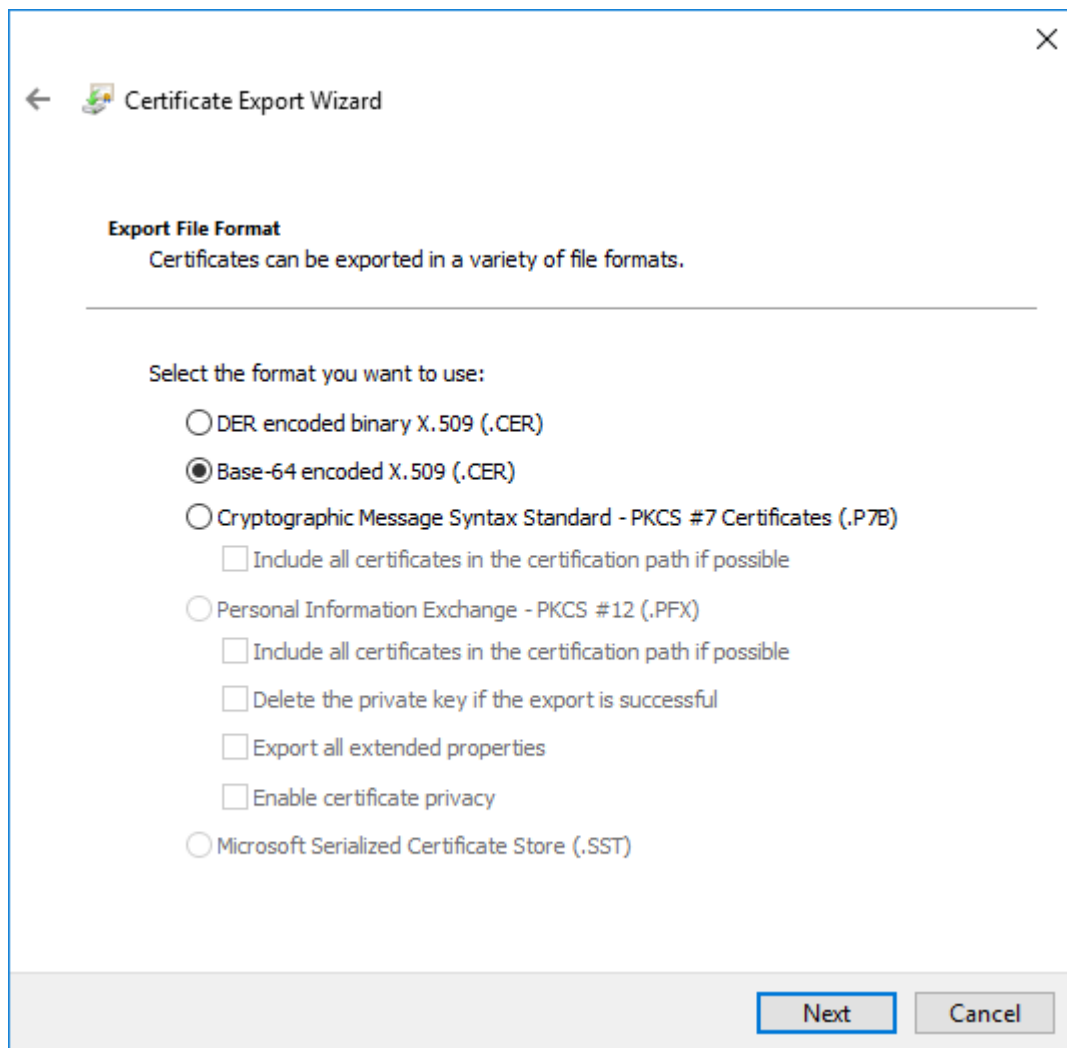


Fig. 11: certsrv – Export certificate



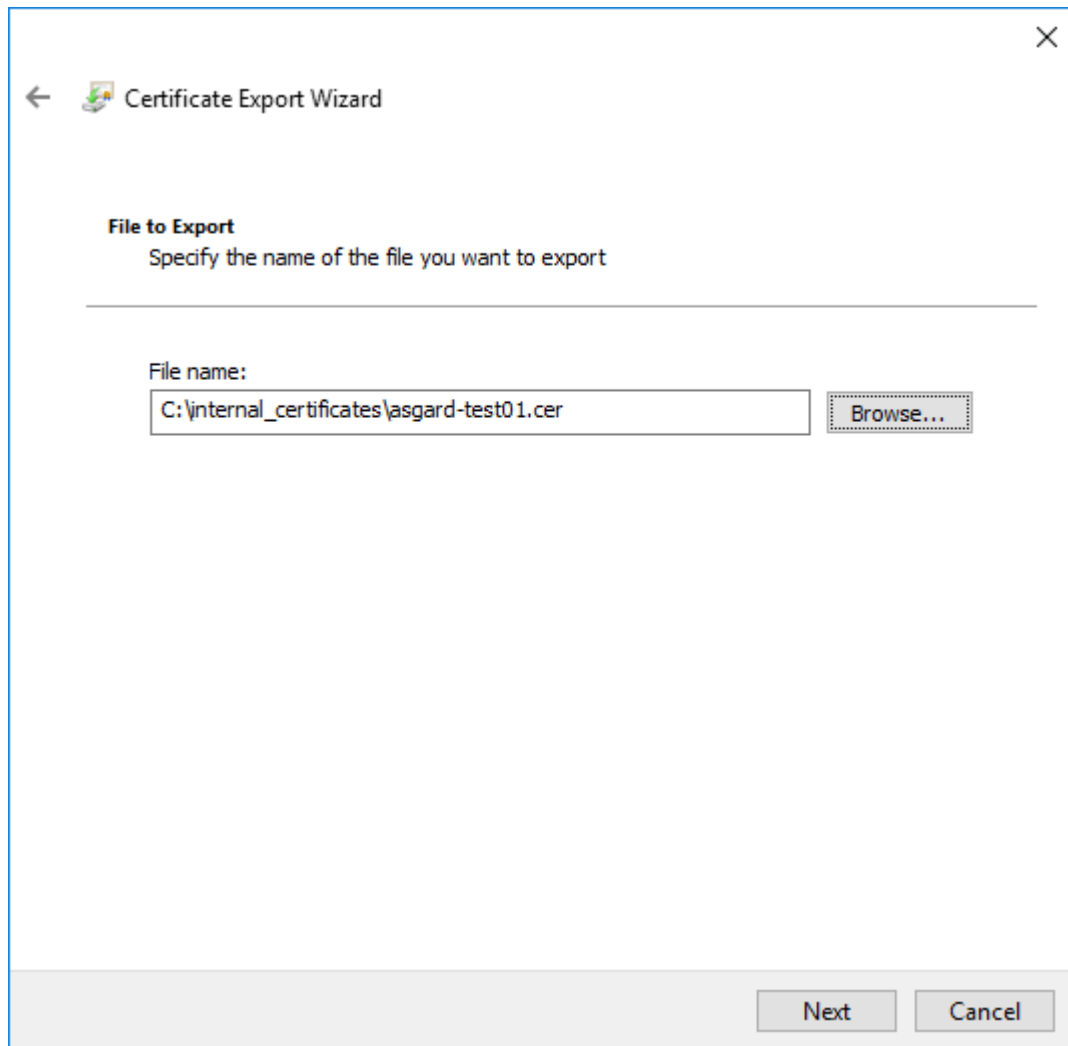


Fig. 12: certsrv – Export certificate

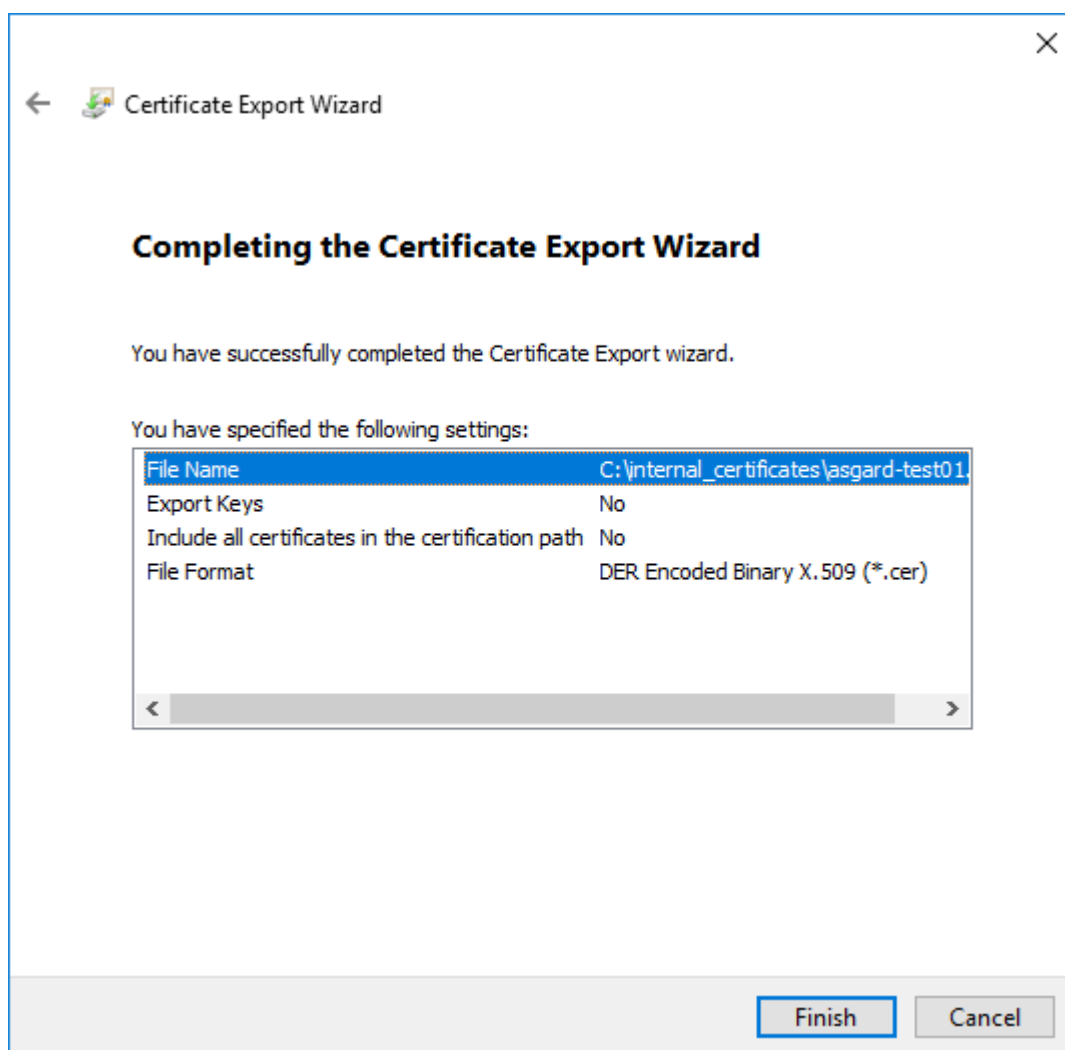


Fig. 13: certsrv – Export certificate

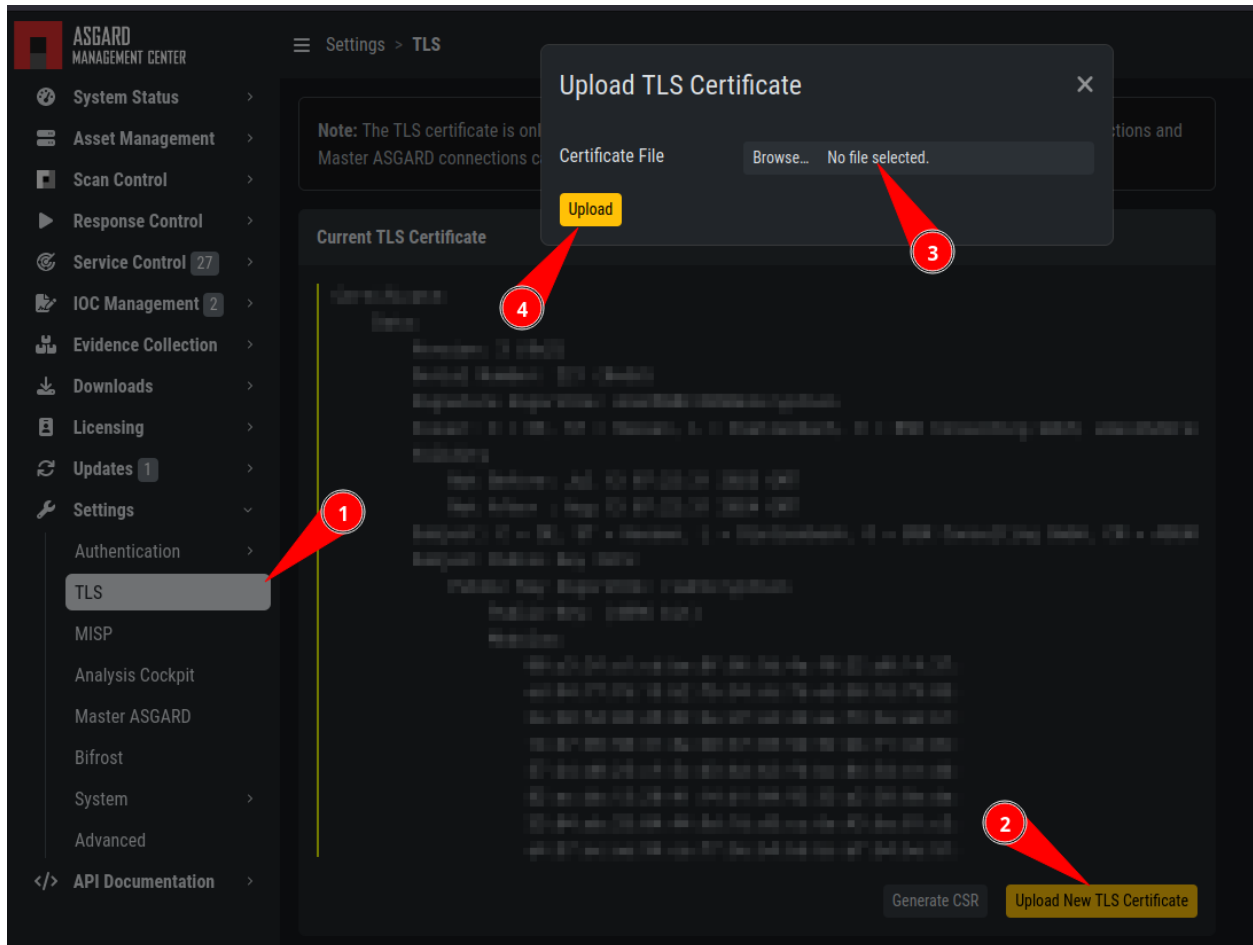


Fig. 14: ASGARD Certificate Import

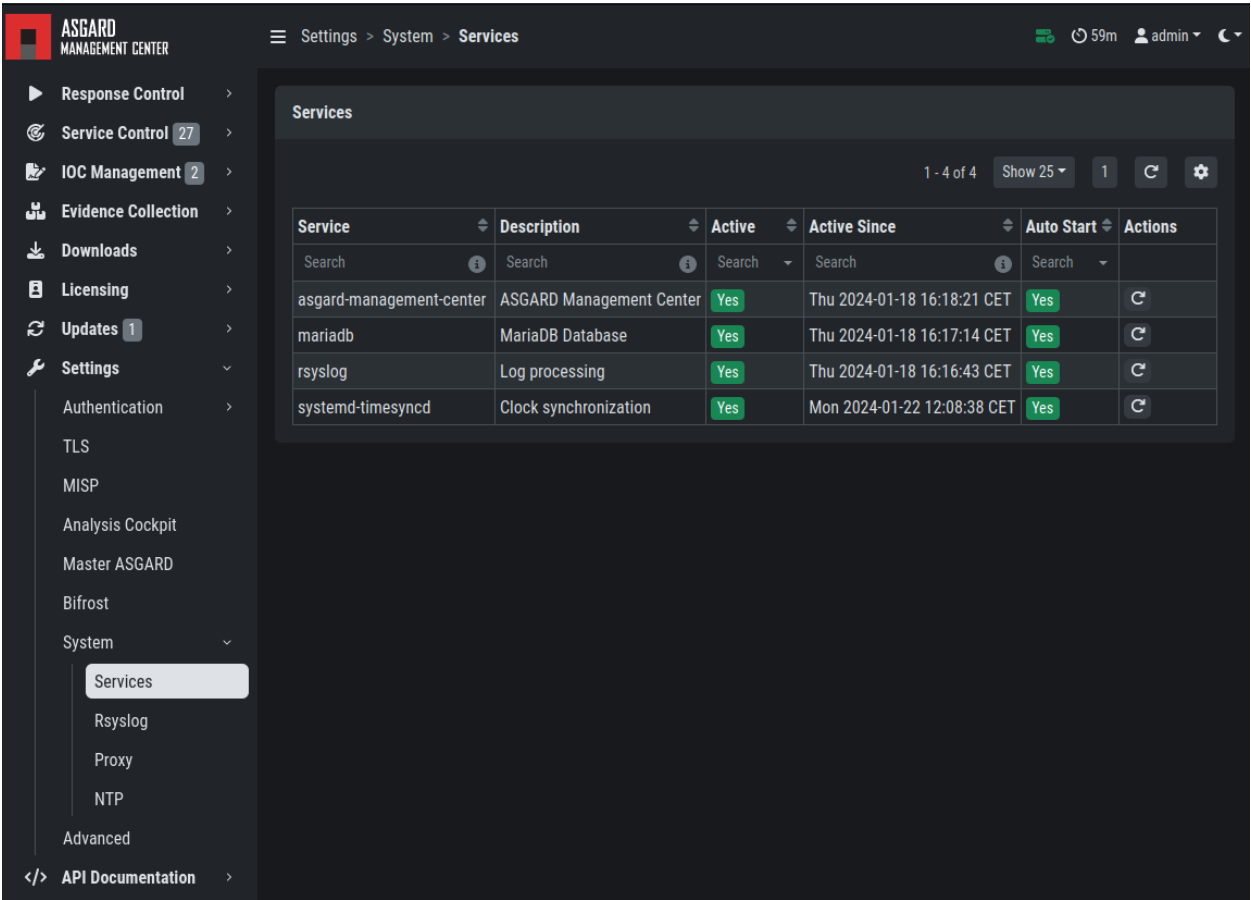


Fig. 15: ASGARD service restart

(continued from previous page)

```

83 dir          = ./demoCA          # Where everything is kept
84 certs        = $dir/certs        # Where the issued certs are kept
85 crl_dir       = $dir/crl         # Where the issued crl are kept
86 database      = $dir/index.txt    # database index file.
87 #unique_subject = no              # Set to 'no' to allow creation of
88                                     # several certs with same subject.
89 new_certs_dir  = $dir/newcerts    # default place for new certs.
90
91 certificate    = $dir/cacert.pem  # The CA certificate
92 serial        = $dir/serial       # The current serial number
93 crlnumber      = $dir/crlnumber    # the current crl number
94                                     # must be commented out to leave a V1 CRL
95 crl           = $dir/crl.pem      # The current CRL
96 private_key    = $dir/private/cakey.pem # The private key
97
98 x509_extensions = usr_cert        # The extensions to add to the cert
99
100 # Comment out the following two lines for the "traditional"
101 # (and highly broken) format.
102 name_opt       = ca_default       # Subject Name options
103 cert_opt       = ca_default       # Certificate field options
104
105 # Extension copying option: use with caution.
106 copy_extensions = copy
107
108 [...]
    
```

**The second method** of including all extensions from the CSR to the new certificate, is via an extension file (for example asgard-test01.ext) containing all your subjectAltName entries. This tells openssl to use a extension for signing the CSR. In our case the extension contains a list of subjectAltName values.

To do this, place a file with your subjectAltName entries in the same folder of your CSR. The contents of this file look something like the following example. Values after subjectAltName = should be equal to the values of your CSR:

```

root@ca:~# cat asgard-test01.ext
subjectAltName = DNS:asgard-test01.nextron, IP Address:172.28.28.101
    
```

The content should be identical to the values you set in your CSR. You can inspect those with the following command:

```

root@ca:~# openssl req -in asgard-test01.csr -noout -text
↳ [31/
↳ 146]
Certificate Request:
Data:
  Version: 1 (0x0)
  Subject: C = DE, ST = Hesse, O = Nextron, OU = Security IT, CN = asgard-test01.
↳ nextron
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    Public-Key: (4096 bit)
    Modulus:
      00:cb:74:c9:ed:4e:4d:db:39:7b:e0:dc:bb:55:d6:
      [...]
    
```

(continues on next page)

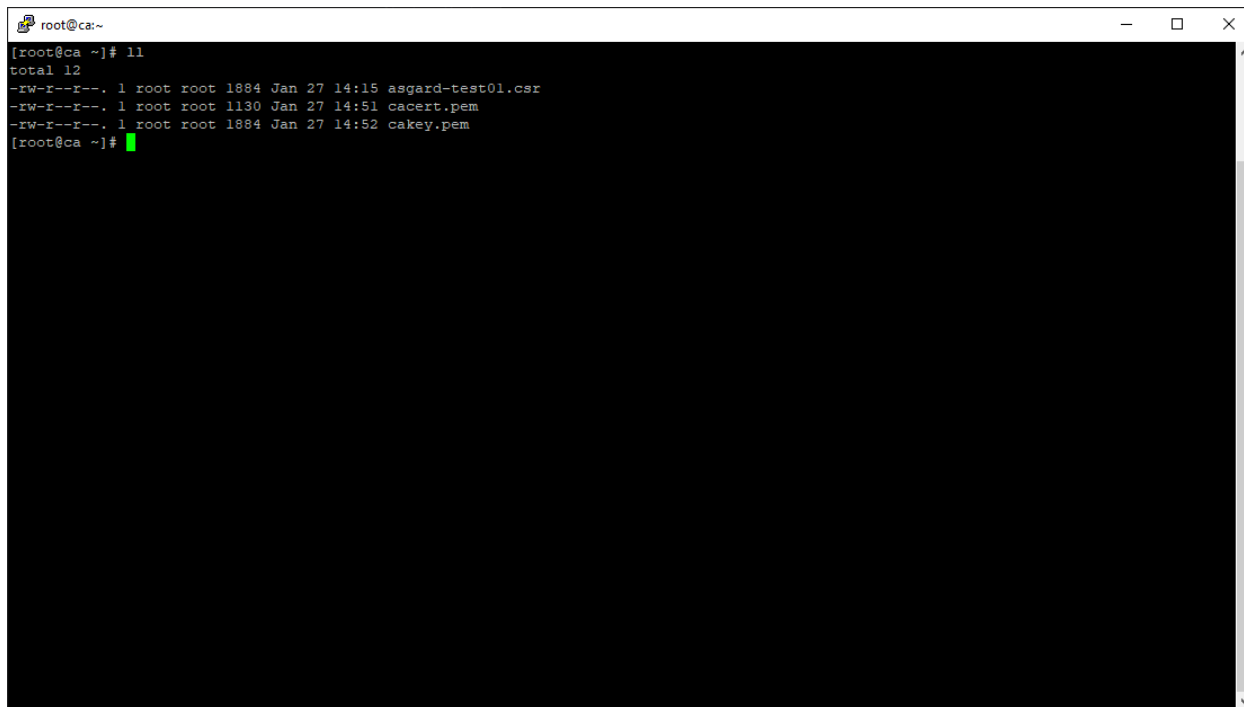
(continued from previous page)

```

c2:9f:69
Exponent: 65537 (0x10001)
Attributes:
  Requested Extensions:
    X509v3 Subject Alternative Name:
      DNS:asgard-test01.nexttron, IP Address:172.28.28.101

```

Prepare the CA certificate, CA private key and the certificate signing request (and optionally your extension file, if you chose method 2).



```

root@ca:~
[root@ca ~]# ll
total 12
-rw-r--r--. 1 root root 1884 Jan 27 14:15 asgard-test01.csr
-rw-r--r--. 1 root root 1130 Jan 27 14:51 cacert.pem
-rw-r--r--. 1 root root 1884 Jan 27 14:52 cakey.pem
[root@ca ~]#

```

Fig. 16: CSR and signing Certificates preparation

Execute/adapt the following command depending on the method you chose before:

**First method:**

```

root@ca:~# openssl ca -cert cacert.pem -keyfile cakey.pem -in asgard-test01.csr -out
↳ asgard-test01.crt -days 3650
Using configuration from /etc/pki/tls/openssl.conf
Enter pass phrase for cakey.pem:

```

**Second method:**

```

root@ca:~# openssl ca -cert cacert.pem -keyfile cakey.pem -in asgard-test01.csr -out
↳ asgard-test01.crt -days 3650 -extfile asgard-test01.ext
Using configuration from /etc/pki/tls/openssl.conf
Enter pass phrase for cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:

```

(continues on next page)

```

root@ca:~# ll
total 12
-rw-r--r--. 1 root root 1884 Jan 27 14:15 asgard-test01.csr
-rw-r--r--. 1 root root 1130 Jan 27 14:51 cacert.pem
-rw-r--r--. 1 root root 1884 Jan 27 14:52 cakey.pem
[root@ca ~]# openssl ca -cert cacert.pem -keyfile cakey.pem -in asgard-test01.csr -out asgard-test01.crt -days 3650
Using configuration from /etc/pki/tls/openssl.cnf
Enter pass phrase for cakey.pem:

```

Fig. 17: Certificate signing command

(continued from previous page)

```

Serial Number: 1 (0x1)
Validity
    Not Before: Feb 23 09:58:10 2023 GMT
    Not After : Feb 20 09:58:10 2033 GMT
Subject:
    countryName           = DE
    stateOrProvinceName   = Hesse
    organizationName       = Nextron
    organizationalUnitName = Security IT
    commonName             = asgard-test01.nextron
X509v3 extensions:
    X509v3 Subject Alternative Name:
        DNS:asgard-test01.nextron IP Address:172.28.28.101
Certificate is to be certified until Feb 20 09:58:10 2033 GMT (3650 days)

```

Enter the passphrase for your CA's private key

Confirm that the data contained in the CSR is accurate and confirm the signing of the request to the CA.

Once confirmed commit the changes to your local DB.

As a result, the signed certificate will be available with the indicated filename.

As a last step, the generated certificate can be imported following the [TLS Certificate Installation](#) steps.

```

root@ca:~
[root@ca ~]# ll
total 12
-rw-r--r--. 1 root root 1884 Jan 27 14:15 asgard-test01.csr
-rw-r--r--. 1 root root 1130 Jan 27 14:51 cacert.pem
-rw-r--r--. 1 root root 1884 Jan 27 14:52 cakey.pem
[root@ca ~]# openssl ca -cert cacert.pem -keyfile cakey.pem -in asgard-test01.csr -out asgard-test01.crt -days 3650
Using configuration from /etc/pki/tls/openssl.cnf
Enter pass phrase for cakey.pem:

```

Fig. 18: Signing procedure

```

root@ca:~
[root@ca ~]# vi /etc/pki/CA/index.txt
[root@ca ~]# openssl ca -cert cacert.pem -keyfile cakey.pem -in asgard-test01.csr -out asgard-test01.crt -days 3650
Using configuration from /etc/pki/tls/openssl.cnf
Enter pass phrase for cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
    Serial Number: 2 (0x2)
    Validity
        Not Before: Jan 27 19:58:58 2019 GMT
        Not After : Jan 24 19:58:58 2029 GMT
    Subject:
        countryName           = DE
        stateOrProvinceName   = Hessen
        organizationName      = Nextron
        organizationalUnitName = Security IT
        commonName            = asgard-test01.nextron
    X509v3 extensions:
        X509v3 Basic Constraints:
            CA:FALSE
        Netscape Comment:
            OpenSSL Generated Certificate
        X509v3 Subject Key Identifier:
            E3:Cl:DB:5D:7E:39:CD:A2:DA:4F:E9:79:3D:55:76:A6:53:0E:EF:B4
        X509v3 Authority Key Identifier:
            keyid:85:16:A7:9B:FB:D1:B2:CB:A4:75:FE:55:37:D5:99:BD:F5:67:97:D1

        X509v3 Subject Alternative Name:
            DNS:asgard-test01.nextron, IP Address:172.28.28.101
Certificate is to be certified until Jan 24 19:58:58 2029 GMT (3650 days)
Sign the certificate? [y/n]y

1 out of 1 certificate requests certified, commit? [y/n]y

```

Fig. 19: Signing procedure – Checking data is accurate



```

root@ca:~
[root@ca ~]# vi /etc/pki/CA/index.txt
[root@ca ~]# openssl ca -cert cacert.pem -keyfile cakey.pem -in asgard-test01.csr -out asgard-test01.crt -days 3650
Using configuration from /etc/pki/tls/openssl.cnf
Enter pass phrase for cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
  Serial Number: 2 (0x2)
  Validity
    Not Before: Jan 27 19:58:58 2019 GMT
    Not After : Jan 24 19:58:58 2029 GMT
  Subject:
    countryName           = DE
    stateOrProvinceName   = Hessen
    organizationName       = Nextron
    organizationalUnitName = Security IT
    commonName             = asgard-test01.nextron
  X509v3 extensions:
    X509v3 Basic Constraints:
      CA:FALSE
    Netscape Comment:
      OpenSSL Generated Certificate
    X509v3 Subject Key Identifier:
      E3:C1:DB:5D:7E:39:CD:A2:DA:4F:E9:79:3D:55:76:A6:53:0E:EF:B4
    X509v3 Authority Key Identifier:
      keyid:85:16:A7:9B:FB:D1:B2:CB:A4:75:FE:55:37:D5:99:BD:F5:67:97:D1
    X509v3 Subject Alternative Name:
      DNS:asgard-test01.nextron, IP Address:172.28.28.101
Certificate is to be certified until Jan 24 19:58:58 2029 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]:y
Write out database with 1 new entries
Data Base Updated
[root@ca ~]#
    
```

Fig. 20: Signing procedure – Committing changes

```

root@ca:~
[root@ca ~]# ll
total 20
-rw-r--r--. 1 root root 5976 Jan 27 14:59 asgard-test01.crt
-rw-r--r--. 1 root root 1884 Jan 27 14:15 asgard-test01.csr
-rw-r--r--. 1 root root 1130 Jan 27 14:51 cacert.pem
-rw-r--r--. 1 root root 1884 Jan 27 14:52 cakey.pem
[root@ca ~]#
    
```

Fig. 21: Signing procedure – Locating the generated certificate



## UPGRADE FROM MANAGEMENT CENTER V2 TO V3

This Chapter contains instructions on how to upgrade your running Management Center version 2.17.2 to the newest version 3.

We developed an update program which helps you through the upgrade by automating the process as much as possible.

---

**Note:** If you are using the **Broker Network** functionality, please consider updating the components as well. You can find the instructions in the **Broker Network Manual** in the section [Major Updates](#).

---

**Warning:** Due to a bug in our updater tool, a small chance exists that the upgrade will encounter an error. Make sure you have the latest version of the updater tool installed. For more information, please perform the steps in [Management Center Upgrade](#) carefully to install the latest version of the updater.

For information regarding the issue, please see the KB entry [AMC#007: curl: \(58\) could not load PEM client certificate](#).

### 10.1 Upgrade

This chapter guides you through the upgrade process of your Management Center version 2.17.2 to version 3.x.

It is important to follow the steps carefully. We advise you to create a snapshot of the Management Center itself before starting your upgrade.

If you are using a Master ASGARD in your environment, we advise you to upgrade it first.

#### 10.1.1 Preparation

To prepare for your upgrade, we compiled a list of tasks you should follow:

Task	Description
Snapshot of your Management Center	For disaster recovery
Management Center running version 2.17.2	Prerequisite for the Major Upgrade
Connection to our new update servers	New update server infrastructure

For details regarding some of the above tasks, see the next section in this manual.

With the new version of your Management Center, we also made changes to our update servers. Please make sure that all your components can reach the following servers:

Server	Port	Description
update3.nexttron-systems.com	tcp/443	Old update server
update-301.nexttron-systems.com	tcp/443	New update Server

The old update server is needed to fetch the updater and other prerequisites. The new update server is needed to upgrade your servers to Debian 12 and also to install any new packages, which are needed for your Management Center v3.

You can find the corresponding IP-Addresses to the above FQDNs here: <https://www.nexttron-systems.com/hosts/>.

### Management Center running version 2.17.2

To check if your Management Center is running on the correct version you can navigate to Settings and Updates. The page should look like this:

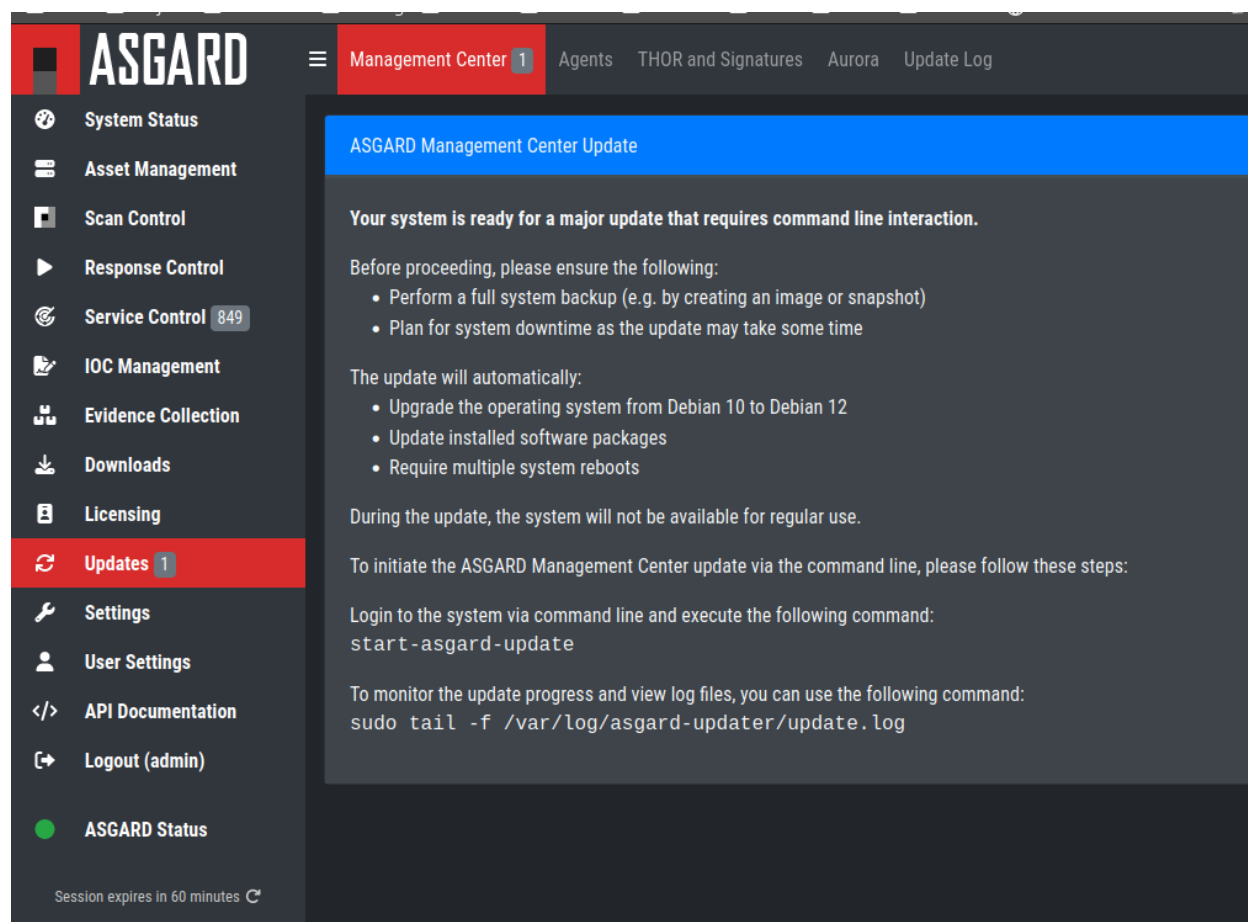


Fig. 1: Update Section

## 10.1.2 Performing the upgrade

In this section we will perform the actual upgrade of the Management Center.

### Management Center Upgrade

To start your upgrade, connect to your Management Center via SSH. We will utilize `asgard-updater` to perform the upgrade. First we need to check if a newer version of the `asgard-updater` is available. If you get the highlighted output, you have already the newest version installed (the version might differ from the output here):

```
nexttron@asgard:~$ sudo apt update
nexttron@asgard:~$ sudo apt install asgard-updater
Reading package lists... Done
Building dependency tree
Reading state information... Done
asgard-updater is already the newest version (1.0.15).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

You can now run the `asgard-updater` with the following command:

```
nexttron@asgard:~$ start-asgard-update
```

The server running your Management Center will now restart multiple times. It is important to not interrupt the upgrade process and let the server do all the tasks. You can, however, see if any errors occurred during the upgrade or just observe at what stage the upgrade is.

Run the following command to see the status of your upgrade:

```
nexttron@asgard:~$ sudo tail -f /var/log/asgard-updater/update.log
```

**Note:** Since the upgrade is downloading many packages of the debian base system, the process will take a while. The web interface of your Management Center might be available throughout the upgrade, but we still advise to use it until the upgrade is finished.

The update is finished if you are seeing the following lines:

```
nexttron@asgard:~$ sudo tail -f /var/log/asgard-updater/update.log
2024-01-16T14:20:54.253032+01:00 asgard asgard-updater[667]: Upgrade finished.
↪Deactivating service...
2024-01-16T14:20:54.259176+01:00 asgard asgard-updater[667]: Removed "/etc/systemd/
↪system/multi-user.target.wants/asgard-updater.service".
```

Your upgrade is now finished, and you can use your Management Center with the newest version.



## CHANGELOG

This chapter contains a list of all changes. Those changes are only related to the Management Center version 3 and its components.

### 11.1 Management Center v3

This chapter contains all the changes of the ASGARD Management Center.

#### 11.1.1 Management Center 3.0.12

Release Date
Thu, 28 Mar 2024 11:46:00 +0200

Type	Description
Bugfix	Improved performance of the asset table and the task statistics
Bugfix	Fixed non-working API key generation for read-only users
Bugfix	Fixed non-working CSR generation for HTTPS TLS certificate
Bugfix	Removed some major upgrade leftovers from the diagnostics pack

#### 11.1.2 Management Center 3.0.11

Release Date
Wed, 28 Feb 2024 09:19:00 +0200

Type	Description
Bugfix	Fixed non-working diagnostics pack generation on some Management Centers

### 11.1.3 Management Center 3.0.10

Release Date
Tue, 20 Feb 2024 13:01:00 +0200

Type	Description
Operating System Up-grade	Upgraded operating system from Debian 10 to Debian 12
Switched update server	Changed update server from update3.nexttron-systems.com to update-301.nexttron-systems.com. Please adjust your firewall to allow connections to the new server.
Time service transition	Switched from ntp to timesyncd for time synchronization.
UI Enhancements	A fresh, improved look and feel that makes the UI more intuitive and easier to use.



## INDICES AND TABLES

- search



# INDEX

## A

- Additional Settings, 106
- Admin User Password Reset, 149
- Administration, 29
- Advanced Configuration, 132
- Advanced Settings, 117
- Agent and Agent Installer Update, 136
- Agent Debugging, 143
- Agent Requirements, 4
- Antivirus and EDR Exclusions, 7
- Appendix, 159
- ASGARD Agent Deployment, 34
- ASGARD Errors, 148
- Asset Management, 41
- Aurora, 70
- Aurora too many False Positives, 152

## B

- Backup and Restore, 138
- Before you begin, 3

## C

- Changelog, 187
- Configure the OS, 24
- Creating Custom Agent Installer, 138

## D

- Diagnostic Pack, 143
- Disable Remote Console Globally, 142
- Download Links, 94

## E

- ESXi, 15
- Evidence Collection, 93

## G

- Golden Image, 163
- Group Scan, 54

## H

- Hardware Requirements, 4

- Helpful scripts, 161

- Home, 1

## I

- Install Service, 25
- Install TLS certificates on ASGARD and MASTER ASGARD, 165
- Installer, 15
- Introduction, 3
- IOC Management, 85

## K

- Known Issues, 152

## L

- Licensing, 97
- Log Rotation and Retention, 131

## M

- Maintenance, 128
- Management Center Major Upgrade, 185
- Managing Logs, 134
- Master ASGARD, 122, 123

## N

- Network Configuration, 15
- Network Requirements, 5

## O

- Other Installer Steps, 22

## P

- Performance Tuning, 133

## R

- Regain Disk Space, 131
- Requirements, 1
- Resetting TLS/SSL Certificates, 149
- Resetting Two Factor Authentication, 150
- Response Control, 61

## S

- Scan Control, [48](#)
- Scheduled Scan, [58](#)
- Scheduled Scans have incorrect time, [151](#)
- Service Control, [69](#)
- Setup, [13](#)
- Sigma, [76](#)
- Single Scan, [52](#)
- SSL Interception, [146](#)
- Syslog Forwarding, [59](#)
- System Status, [31](#)

## T

- Troubleshooting, [142](#)

## U

- Uninstall ASGARD Agents, [38](#)
- Updates, [99](#)
- Upgrade from Management Center v2 to v3, [181](#)
- User Management, [100](#)
- User Settings, [117](#)
- Using Hostname instead of FQDN, [146](#)

## V

- Verify the ISO, [11](#)