
ASGARD Management Center Manual

Stephan Kaiser, Florian Roth, Christian Burkard

Feb 21, 2024

CONTENTS:

1	Introduction	1
2	Before You Begin	3
2.1	Agent to ASGARD Communication	3
2.2	Performance Considerations	3
2.3	Using a Proxy between ASGARD Agent and ASGARD	3
2.4	Hardware Requirements	3
2.5	Agent Requirements	4
2.6	Network Requirements	4
2.7	Antivirus or EDR Exclusions	6
2.8	Verify the Downloaded ISO (Optional)	9
3	Setup Guide	11
3.1	Create a new ESX VM and Mount the ISO	11
3.2	Navigate through the installer	11
3.3	Network Configuration	11
3.4	Choosing a password	17
3.5	Partitioning the Hard Disk	17
3.6	Proxy Configuration	17
3.7	Install the ASGARD Management Center Services	17
3.8	Changing the IP-Address	22
3.9	First steps in the VM	22
4	Administration	25
4.1	License Management	25
4.2	System Status	25
4.3	ASGARD Agent Deployment	29
4.4	Asset Management	35
4.5	Scan Control	42
4.6	Response Control	54
4.7	Service Control	63
4.8	IOC Management	82
4.9	Evidence Collection	88
4.10	Generate Download Links	88
4.11	Licensing	92
4.12	Updates	92
4.13	User Management	95
4.14	Additional Settings	100
4.15	User Settings	111
4.16	Uninstall ASGARD Agents	114

4.17	Uninstall ASGARD Service Controller	115
5	MASTER ASGARD	117
5.1	Hardware Requirements for MASTER ASGARD	118
5.2	License Management	118
5.3	Setting up MASTER ASGARD	118
5.4	Link ASGARD Systems with MASTER ASGARD	118
5.5	Scan Control	119
5.6	Asset Management	119
5.7	IOC Management	121
5.8	Service Control	121
5.9	Evidence Collection	121
5.10	Download Section	122
5.11	Updates	122
5.12	User Management	122
5.13	MASTER ASGARD and Analysis Cockpit	124
5.14	MASTER ASGARD API	124
6	Maintenance	125
6.1	Log Rotation and Retention	125
6.2	Regain Disk Space	125
7	Advanced Configuration	127
7.1	Performance Tuning	127
7.2	Managing Logs	128
7.3	Agent and Agent Installer Update	130
7.4	Creating Custom Agent Installer	132
7.5	Backup and Restore	133
7.6	Disable Remote Console Globally	136
8	Troubleshooting	137
8.1	Diagnostic Pack	137
8.2	Agent Debugging	138
8.3	SSL Interception	140
8.4	Using Hostname instead of FQDN	140
8.5	ASGARD Errors	142
8.6	Resetting TLS/SSL Certificates	143
8.7	Admin User Password Reset	143
8.8	Reset Two Factor Authentication for a specific User	143
8.9	Scheduled Scans do not run at the correct time	145
8.10	Aurora is generating too many False Positives	146
9	Known Issues	147
9.1	AMC#015: THOR License not valid yet (timezone difference)	147
9.2	AMC#014: Edge Browser with translation, "removeChild" error	148
9.3	AMC#013: Master ASGARD custom IOCs in Scheduled Group Scan	148
9.4	AMC#012: Missing asgard2-agent.yaml	149
9.5	AMC#011: Context Deadline Exceeded	151
9.6	AMC#010: High number of duplicate assets	152
9.7	AMC#009: agent-access.log is not being rotated	153
9.8	AMC#008: Show Asset Timeline Fails	154
9.9	AMC#007: Sigma Rule Update Fails	154
9.10	AMC#006: Nested LDAP Groups not working	155
9.11	AMC#005: Basename Missing Operand after SSH Login	155
9.12	AMC#004: RPM Packages do not have a compatible architecture	156

9.13	AMC#003: Error on newly installed Management Center	158
9.14	AMC#002: Aurora False Positive Filters Cleared After Saving	158
9.15	AMC#001: API Documentation Curl Examples Not Working	159
10	Appendix	161
10.1	Installing ASGARD Agent via Powershell Script	161
10.2	Deploy ASGARD Agents via SCCM	162
10.3	Broken file and folder permissions	163
10.4	Installing ASGARD Agent on a Golden Image	164
10.5	Install TLS certificates on ASGARD and MASTER ASGARD	165
10.6	Agent Migration from ASGARD v1 to v2	184
11	Changelog	195
11.1	ASGARD Management Center	195
11.2	ASGARD Agent	215
11.3	ASGARD Service Controller	216
12	Indices and tables	219

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.

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 remote shells and other actions incident response specialists will find useful.

Moreover, ASGARD provides an easy to use interface for creation of custom multi-step response playbooks that can execute any command on endpoints and collect the respective outputs.

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

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

BEFORE YOU BEGIN

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 ASGARD 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.

2.2 Performance Considerations

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

Obviously, large 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 the result to show up. However, once open, the shell or the response tasks are very responsive – almost as if it is native on the system.

In order to adapt to specific requirements regarding responsiveness, the polling behavior can be modified. For details, refer to [Performance Tuning](#). The hardware requirements in the next chapter assume that the default polling interval is used.

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](#).

2.4 Hardware Requirements

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

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

2.5 Agent Requirements

The ASGARD Agent, which is installed on endpoints, uses up to 10MB of RAM. THOR uses up to 300 MB of RAM additionally when scanning is in progress.

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 system 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 and limits its CPU usage to a configurable percentage.

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

2.6 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.nexttron-systems.com/hosts/>.

2.6.1 From ASGARD Agent to ASGARD Server

Description	Ports
Agent / Server communication	443/tcp
Syslog Forwarder (optional)	514/tcp, 514/udp
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 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.

2.6.2 From Management Workstation to ASGARD Server

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

2.6.3 From ASGARD to SIEM

Description	Ports
Syslog forwarder	514/tcp, 514/udp

2.6.4 From ASGARD to Analysis Cockpit

Description	Ports
Asset Synchronization, Log- and Sample forwarding	7443/tcp
Syslog forwarder (optional)	514/tcp, 514/udp

2.6.5 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	update3.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).

2.6.6 From Master ASGARD to ASGARD

Direction	Port
From MASTER ASGARD v2 to ASGARD v2	5443/tcp
From MASTER ASGARD v2 to ASGARD v1	9443/tcp

You cannot manage ASGARD v2 systems from a MASTER ASGARD v1.

2.6.7 From Management Workstation to MASTER ASGARD

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

2.6.8 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.

2.6.9 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.

2.7 Antivirus or 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.

2.7.1 General Recommendation

We recommend using this list - include all sub folders:

Folder Exclusions including Subfolders	
Windows	%SYSTEMROOT%\System32\asgard2-agent\ %SYSTEMROOT%\Temp\asgard2-agent\
Linux	/usr/sbin/asgard2-agent-service /var/lib/asgard2-agent/ /var/tmp/asgard2-agent/
macOS	/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	
Windows	%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%\System32\asgard2-agent\services\bin\logwatcher.exe %SYSTEMROOT%\Temp\asgard2-agent\ (and all sub folders)
Especially And/Or	%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)
Especially And/Or	%SYSTEMROOT%\Temp\asgard2-agent-sc\aurora\[random]\aurora\aurora-agent.exe %SYSTEMROOT%\Temp\asgard2-agent-sc\aurora\[random]\aurora\aurora-agent-64.exe
Linux	/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 /var/lib/asgard2-agent/bin/update /var/tmp/asgard2-agent/[random]/thor/thor-linux /var/tmp/asgard2-agent/[random]/thor/thor-linux-64
macOS	/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).

2.7.2 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
Low Risk	thor.exe
	thor64.exe
	interrogate.exe
	generic.exe
	asgard2-agent.exe
	asgard2-agent-service.exe
	aurora-agent-64.exe
	aurora-agent.exe
Exclusions (include sub folders)	%SYSTEMROOT%\System32\asgard2-agent\
	%SYSTEMROOT%\Temp\asgard2-agent\
	%SYSTEMROOT%\Temp\asgard2-agent-sc\
Access Protection	thor.exe
	thor64.exe
	interrogate.exe
	generic.exe
	aurora-agent.exe
	aurora-agent-64.exe
	asgard2-agent.exe
	asgard2-agent-service.exe
	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
Network Flow	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
Trace	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
File Hashing	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*\

2.8 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](#).

2.8.1 Via Hash

Extract the ZIP and check the sha256 hash.

Linux:

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

Windows command prompt:

```
C:\Users\user\Desktop\asgard2-installer>type nextron-universal-installer.iso.sha256
efccb4df0a95aa8e562d42707cb5409b866bd5ae8071c4f05eec6a10778f354b nextron-universal-
↵installer.iso
C:\Users\user\Desktop\asgard2-installer>certutil -hashfile nextron-universal-installer.
↵iso SHA256
SHA256 hash of nextron-universal-installer.iso:
efccb4df0a95aa8e562d42707cb5409b866bd5ae8071c4f05eec6a10778f354b
CertUtil: -hashfile command completed successfully.
```

Powershell:

```
PS C:\Users\user\Desktop\asgard2-installer>type .\nextron-universal-installer.iso.sha256
efccb4df0a95aa8e562d42707cb5409b866bd5ae8071c4f05eec6a10778f354b nextron-universal-
↪installer.iso
PS C:\Users\user\Desktop\asgard2-installer>Get-FileHash .\nextron-universal-installer.iso

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

2.8.2 Via Signature (Recommended)

Extract the ZIP, [download the public signature](#) and verify the signed ISO:

Linux:

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

Powershell:

```
PS C:\Users\user\Desktop\asgard2-installer>Invoke-WebRequest -Uri https://www.nextron-
↪systems.com/certs/codesign.pem -OutFile codesign.pem
PS C:\Users\user\Desktop\asgard2-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

3.1 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 10 (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.

3.2 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.

3.3 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.

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:

Guest OS Version:

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

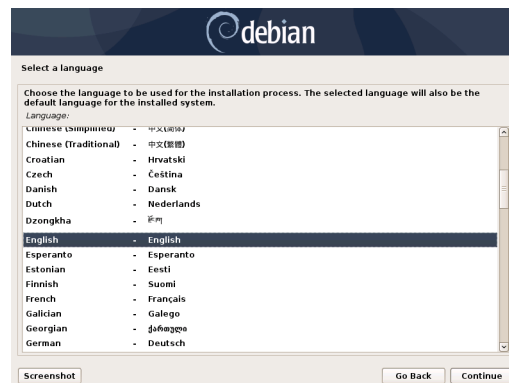
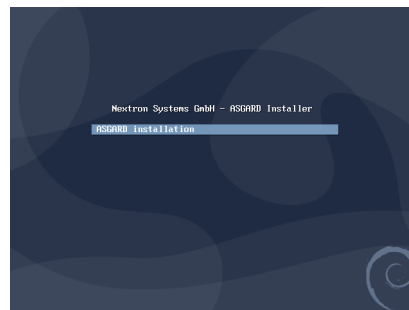
> CPU *	1		
> Memory *	16	GB	
> New Hard disk *	100	GB	
> New SCSI controller *	VMware Paravirtual		
> New Network *	VM Network		<input checked="" type="checkbox"/> Connect...
> New CD/DVD Drive *	Datastore ISO File		<input checked="" type="checkbox"/> Connect...
> Video card *	Specify custom settings		
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






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




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




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:

Carriata	- en_US.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



Configure the network

 **Network autoconfiguration failed**

Your network is probably not using the DHCP protocol. Alternatively, the DHCP server may be slow or some network hardware is not working properly.



Configure the network

From here you can choose to retry DHCP network autoconfiguration (which may succeed if your DHCP server takes a long time to respond) or to configure the network manually. Some DHCP servers require a DHCP hostname to be sent by the client, so you can also choose to retry DHCP network autoconfiguration with a hostname that you provide.

Network configuration method:

Retry network autoconfiguration

Retry network autoconfiguration with a DHCP hostname

Configure network manually

Do not configure the network at this time

Screenshot

Go Back

Continue



Configure the network

The IP address is unique to your computer and may be:

- * four numbers separated by periods (IPv4);
- * blocks of hexadecimal characters separated by colons (IPv6).

You can also optionally append a CIDR netmask (such as /24).

If you don't know what to use here, consult your network administrator.

IP address:

Screenshot

Go Back

Continue



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



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

3.4 Choosing a password

3.5 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".

3.6 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.

3.7 Install the ASGARD Management Center Services

Use SSH to connect to the appliance using the user `nextron` and the password you specified during the installation (if you were using an old ISO to install the base system, the password is `nextron`). Now you can run the following command:

```
sudo nextronInstaller -asgard (caution: upper case "i" in the middle). This will install ASGARD.
```

After installation is complete type `sudo systemctl status asgard2`.

The output should look like the screenshot below with status **Active**.



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:

Screenshot

Go Back 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



Installation is complete, you are ready to log into the web-based GUI.

3.7.1 Changing Proxy Configuration

If you have to change your proxy configuration before you run the `nexttronInstaller` script, you can do so with the following command:

```
nexttron@asgard:~$ sudoedit /etc/apt/apt.conf.d/proxy
```

The format of the proxy in this configuration file is as follows:

```
Acquire::http::Proxy "http://<user>:<password>@<proxyfqdn>:<port>";
Acquire::https::Proxy "http://<user>:<password>@<proxyfqdn>:<port>";
```

Example:

```
Acquire::http::Proxy "http://proxyuser:mySecurePassword123@proxy.internal.domain:8080";
Acquire::https::Proxy "http://proxyuser:mySecurePassword123@proxy.internal.domain:8080";
```

[illegible]

```

root@nexusfire-asg2-2:~# sudo systemctl status asg2d
● asg2d.service - ASGv80 R Management Center
   Loaded: loaded (/lib/systemd/system/asg2d.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2020-02-05 15:58:09 CET; 22s ago
 Main PID: 21843 (run_asg2d.sh)
 Tasks: 7 (limit: 65537)
 Memory: 67.9K
 CGroup: /system.slice/asg2d.service
        └─21843 /usr/bin/asg2d --start --no-run-asg2d --no-run-asg2d.sh
            └─21844 /usr/bin/asg2d

Feb 05 15:58:11 asg2d.asg2d[21843]: [GIN-debug] POST   /api/v0/misp/events/rulesets/action... → git
Feb 05 15:58:11 asg2d.asg2d[21843]: [GIN-debug] GET    /api/v0/misp/rulesets/datasets       → git
Feb 05 15:58:11 asg2d.asg2d[21843]: [GIN-debug] DELETE /api/v0/misp/rulesets/delete/ruleid → git
Feb 05 15:58:11 asg2d.asg2d[21843]: [GIN-debug] POST   /api/v0/misp/rulesets/generate/ruleid → git
Feb 05 15:58:11 asg2d.asg2d[21843]: [GIN-debug] POST   /api/v0/misp/rulesets/get/ruleid     → git
Feb 05 15:58:11 asg2d.asg2d[21843]: [GIN-debug] PUT    /api/v0/misp/rulesets/info/ruleid    → git
Feb 05 15:58:11 asg2d.asg2d[21843]: [LEVEL] "Info" MESSAGE: "Starting background tasks." MODUL
Feb 05 15:58:11 asg2d.asg2d[21843]: [LEVEL] "Info" MESSAGE: "Starting client API." MODULE "I
Feb 05 15:58:11 asg2d.asg2d[21843]: [LEVEL] "Warning" MESSAGE: "could not load licenses." MODU

```

3.8 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:~$ sudo vi /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`

3.8.1 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
```

3.9 First steps in the VM

3.9.1 Change the Command Line Password

Login to ASGARD and type `passwd` in order to change the password for the default user `nexttron`. The default password is `nexttron`.

Warning: This step is not necessary if you used the new installer ISO, since the password will be already set during installation (see *Choosing a password*)

3.9.2 Change the Web Password

Login to the ASGARD Web interface with user `admin` and password `admin`.

The admin user has limited/restricted access to some sections to ensure the correct audit of certain actions. In order to access restricted functions which require an audit please create an user with the corresponding rights under **Settings > Users**.

Click on **User Settings** and update your password.

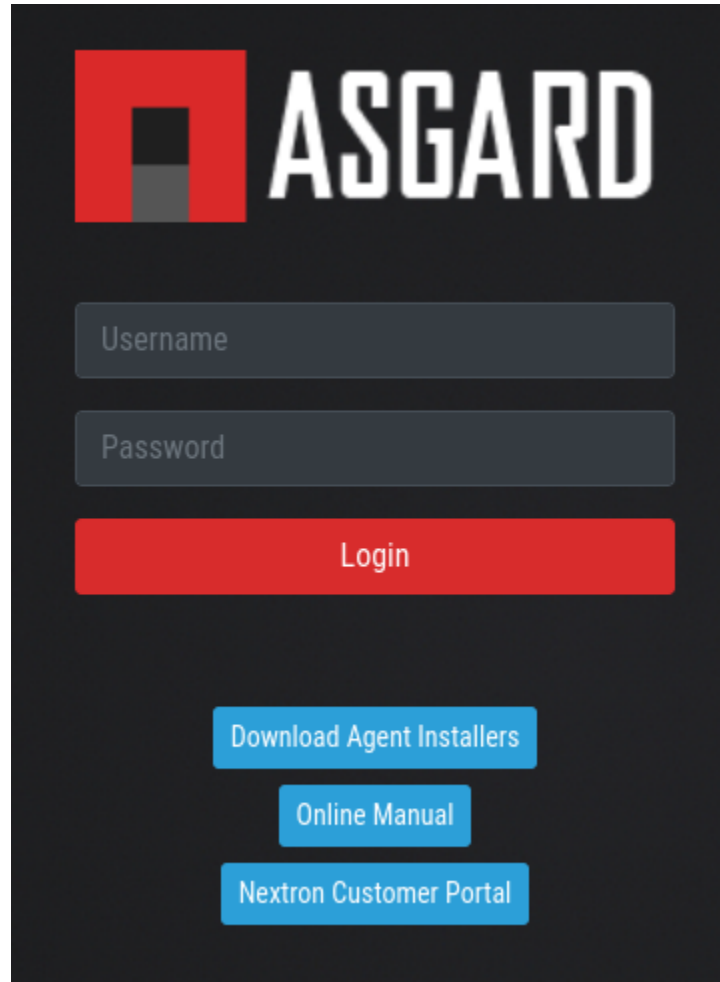


Fig. 2: Login Screen

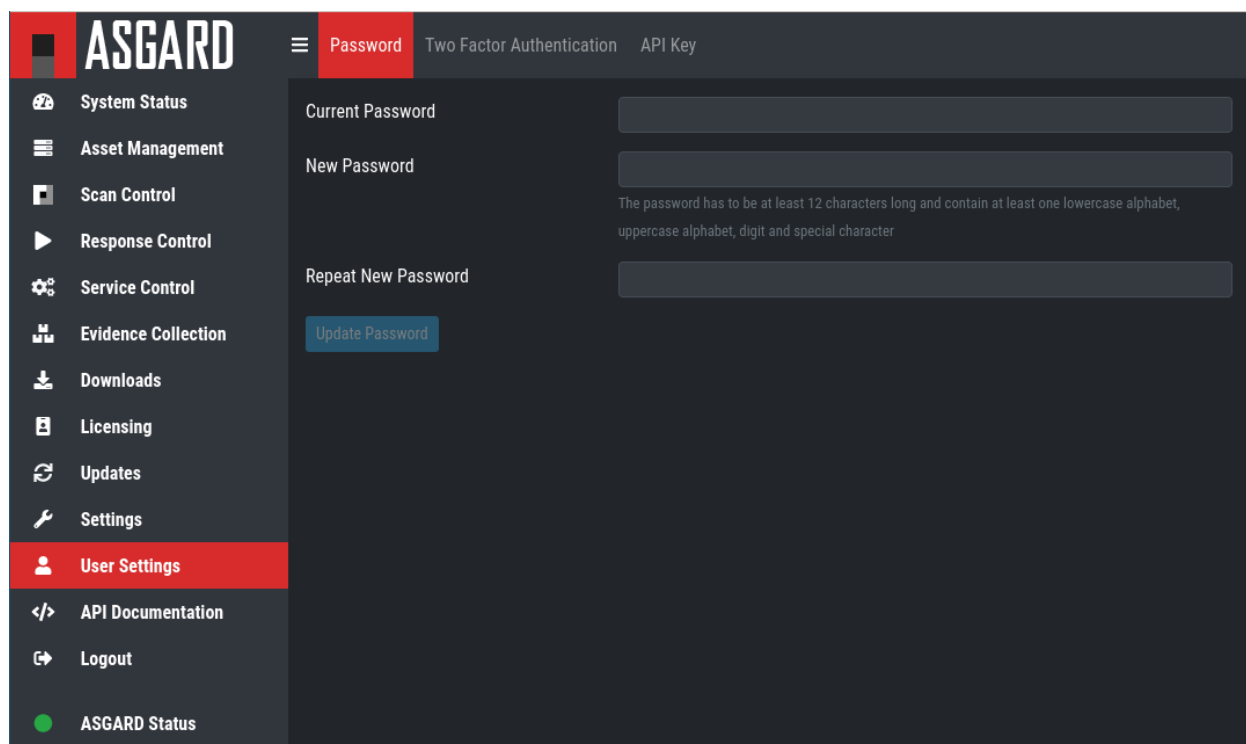


Fig. 3: Changing the Password

ADMINISTRATION

4.1 License Management

Login to ASGARD, navigate to Licensing, click Upload ASGARD Management Center License and upload a valid license.

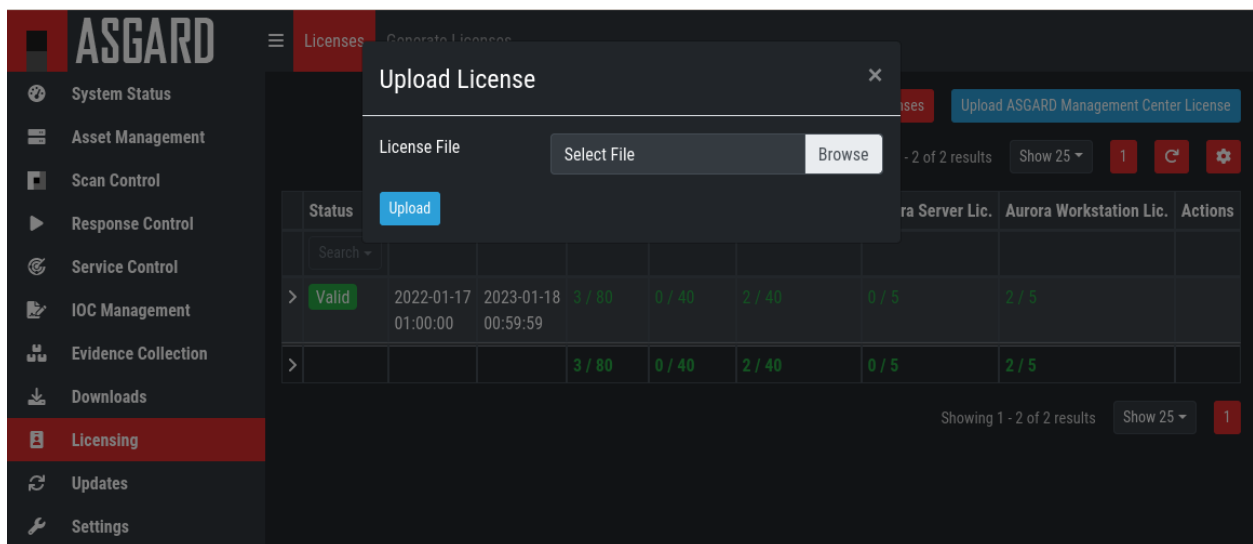


Fig. 1: Install a license

After uploading, the license details are displayed.

4.2 System Status

4.2.1 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 ASGARD software version along with available versions of THOR. Additionally, the connection status to the update servers, MASTER ASGARD and Cockpit are shown with a graph that shows 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. THOR is downloaded automatically after the installation and should show up not later than one hour after installation.



Fig. 2: Overview Top Half

4.2.2 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 traffic light on the left menu always shows if any of those checks failed by showing a warning or error (i.e. yellow or red light) and you can click the status to view the diagnostics page as a pop-up.

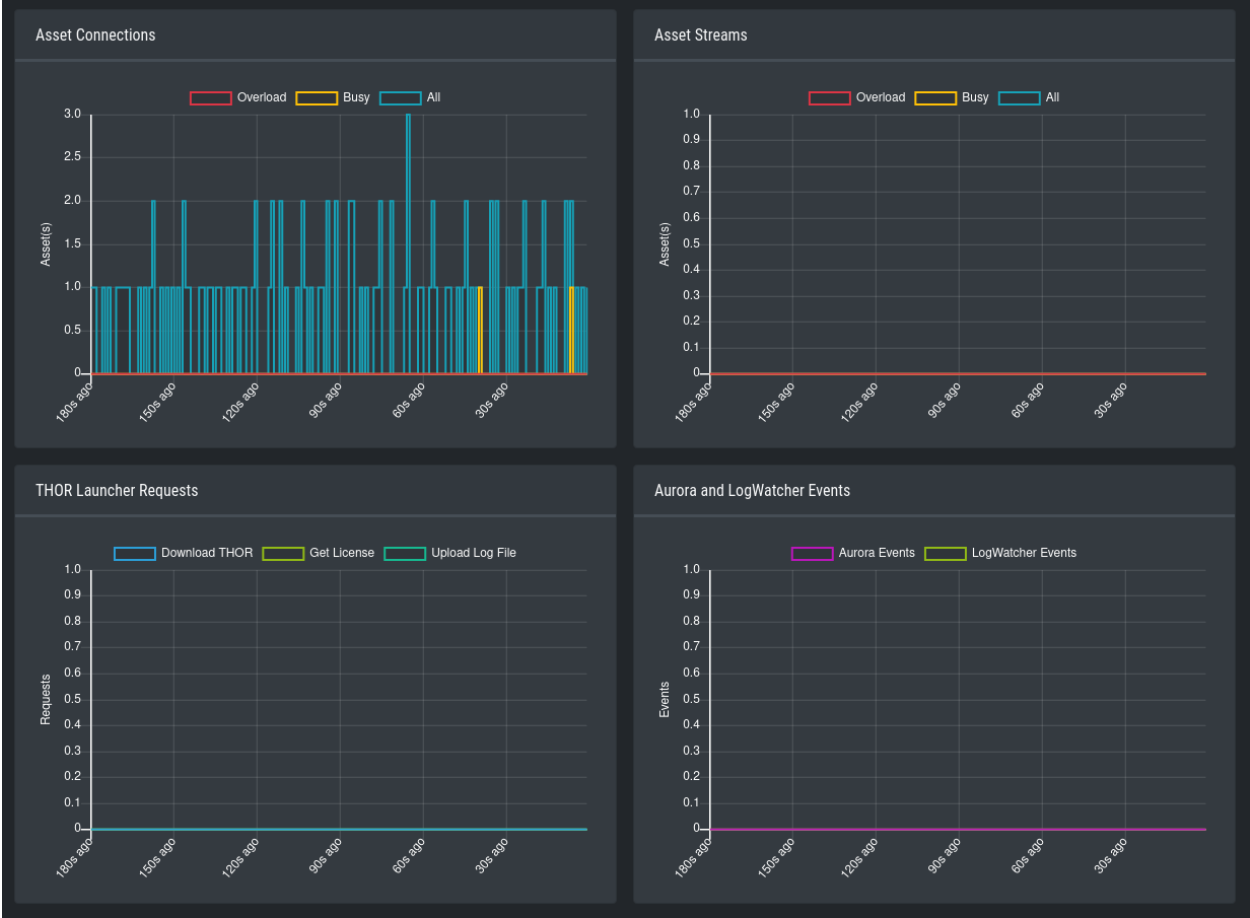
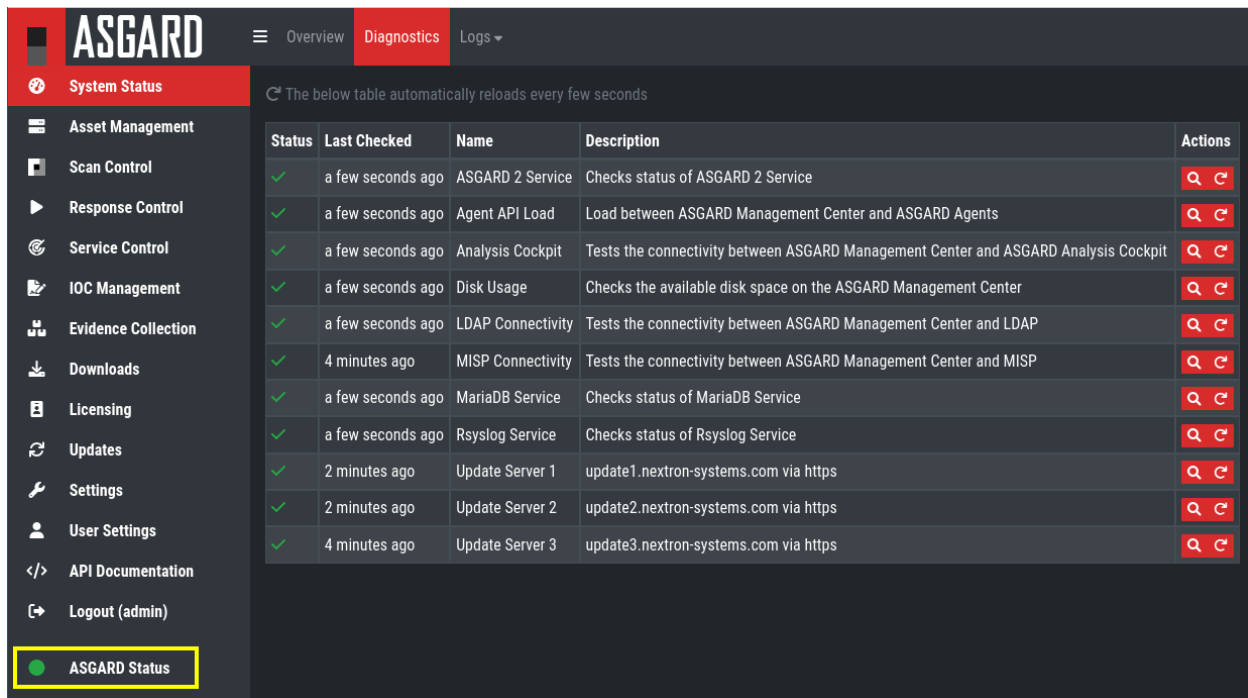


Fig. 3: Overview Bottom Half



Status	Last Checked	Name	Description	Actions
✓	a few seconds ago	ASGARD 2 Service	Checks status of ASGARD 2 Service	Q C
✓	a few seconds ago	Agent API Load	Load between ASGARD Management Center and ASGARD Agents	Q C
✓	a few seconds ago	Analysis Cockpit	Tests the connectivity between ASGARD Management Center and ASGARD Analysis Cockpit	Q C
✓	a few seconds ago	Disk Usage	Checks the available disk space on the ASGARD Management Center	Q C
✓	a few seconds ago	LDAP Connectivity	Tests the connectivity between ASGARD Management Center and LDAP	Q C
✓	4 minutes ago	MISP Connectivity	Tests the connectivity between ASGARD Management Center and MISP	Q C
✓	a few seconds ago	MariaDB Service	Checks status of MariaDB Service	Q C
✓	a few seconds ago	Rsyslog Service	Checks status of Rsyslog Service	Q C
✓	2 minutes ago	Update Server 1	update1.nextron-systems.com via https	Q C
✓	2 minutes ago	Update Server 2	update2.nextron-systems.com via https	Q C
✓	4 minutes ago	Update Server 3	update3.nextron-systems.com via https	Q C

Fig. 4: Overview Over Periodic Diagnostic Checks

4.2.3 Logs

The logs section shows the latest and most relevant logs. Complete logs can be found at `/var/lib/nextron/asgard2/log`.

Available logs and their content:

- Audit: Containing user login/-off, changes done over the UI.
- ASGARD Management Center: Overall status of the MC, general errors and warnings.
- ASGARD Agent and Service Controller: Status of the agents deployed on assets.
- THOR via Syslog: Received syslog events of THOR scans. Partial results if a scan did not complete.
- Aurora: All Aurora events:
- Aurora Event Producers: The top 10 of 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.
- LogWatcher: All LogWatcher events.
- Diagnostic Pack: Button for generating and downloading a diagnostic pack that may be asked for by support.

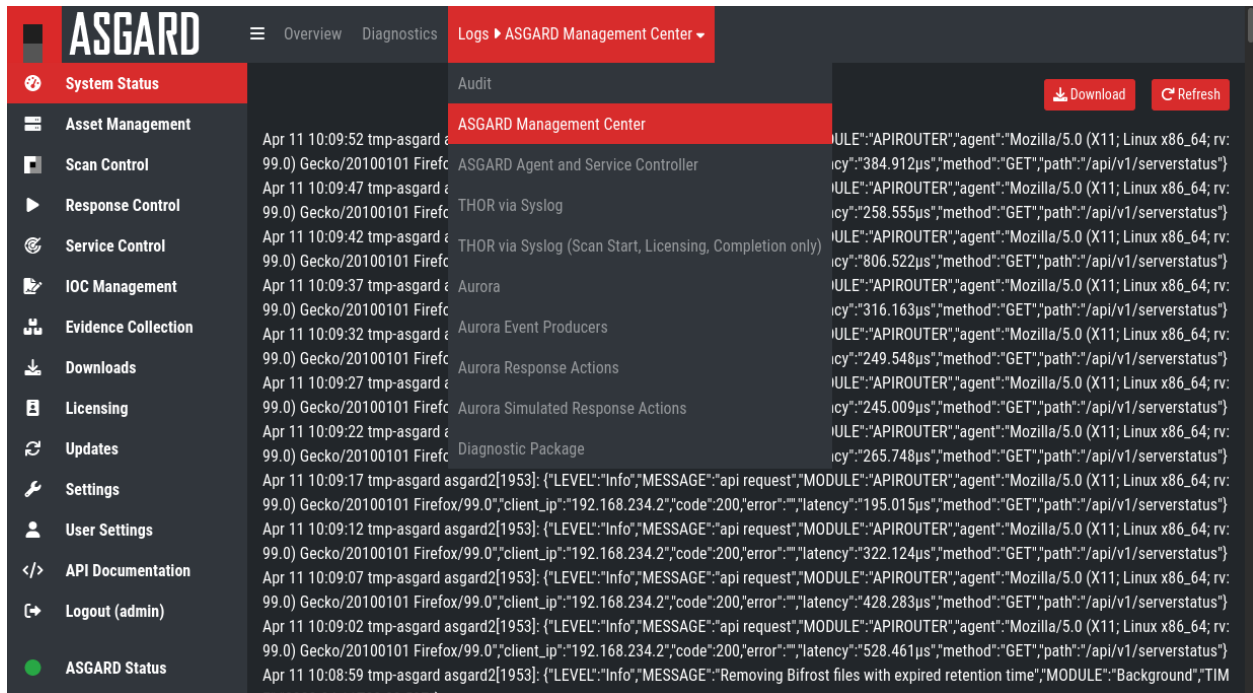


Fig. 5: Logs Section

4.3 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 ASGARD login screen through the button **Download Agent Installers**. A list of available agents for various operating systems appears.

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

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

In the requests tab, select the agents you want ASGARD to manage and click **Accept**. After that, the endpoint shows up in the asset tab and is now ready to be managed or scanned.

A registered agent will poll to the ASGARD Management Center at a given interval between 10 seconds and 600 seconds – depending on the number of connected endpoints (see [Performance Tuning](#) for details). If ASGARD has scheduled a task for the endpoint (for example: run THOR scan) it will be executed directly after the poll.

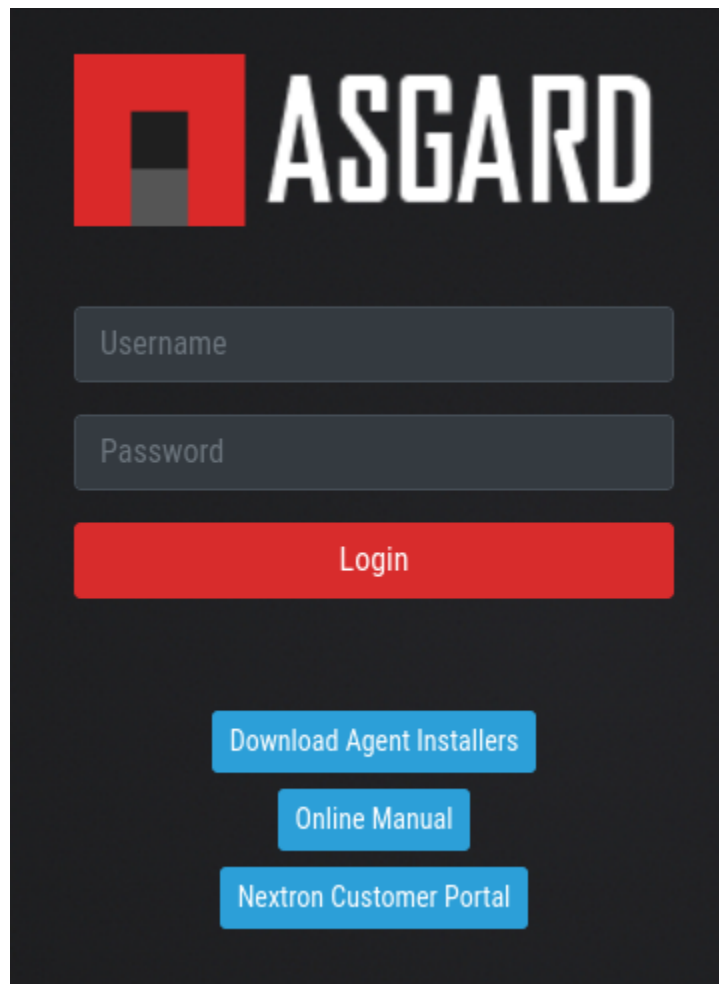
























Fig. 6: Download Agent Installers from Login Screen

Agent Installers			
Name	Asset Labels	Proxy	Actions
> asgard2-agent-linux-386.deb			 
> asgard2-agent-linux-386.rpm			 
> asgard2-agent-linux-amd64.deb			 
> asgard2-agent-linux-amd64.rpm			 
> asgard2-agent-macos-amd64.pkg			 
> asgard2-agent-macos-arm64.pkg			 
> asgard2-agent-rand-windows-amd64.exe	Windows Client R&D		 
> asgard2-agent-windows-386.exe			 
> asgard2-agent-windows-amd64.exe			 
> asgard2-service-controller-windows-386.exe			 
> asgard2-service-controller-windows-amd64.exe			 



Showing 1 - 11 of 11 results Show 25 1 

Fig. 7: Agents Overview



Assets

Asset Requests 1

System Status

Asset Management 1

Scan Control

Response Control

Service Control

IOC Management




Evidence Collection

Downloads

Accept Asset Requests

Deny Asset Requests

Apply Actions from CSV

Showing 1 - 1 of 1 results Show 25 1   

<input checked="" type="checkbox"/>	Hostname	First Seen	Last Seen	OS	Labels	Denied
> <input checked="" type="checkbox"/>	rhel.local	2022-04-11 10:27:08	2022-04-11 10:27:08	linux		No

Showing 1 - 1 of 1 results Show 25 1

Fig. 8: Accepting ASGARD Agent Requests

4.3.1 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.

4.3.2 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.

4.3.3 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 on installation time and making it unique for each new installation, it's 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 their 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 always keep in mind to check your systems 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 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:

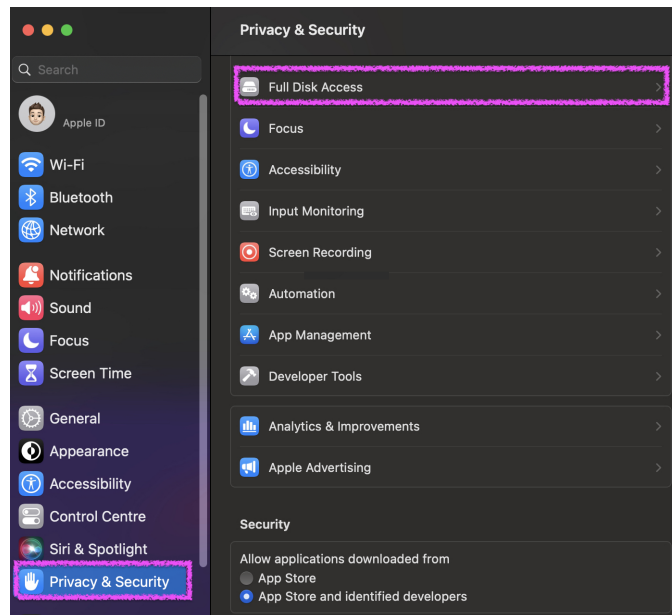
```
MacBook-Pro:~ nexttron$ spctl --status
assessments enabled
```

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

macOS Full Disk Access

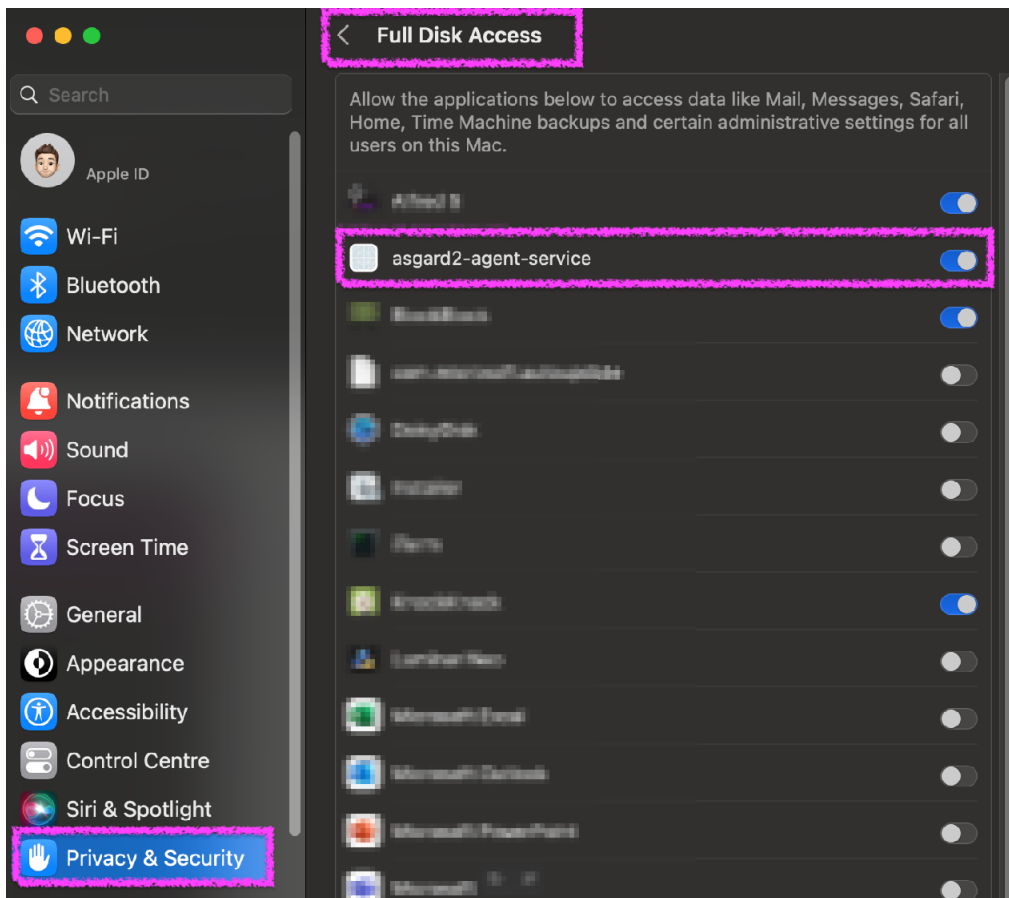
Since macOS version 13 (Ventura) the ASGARD Agent needs full disk access to function properly. After you have deployed the ASGARD Agent, you need to grant the service the required access permissions. Please keep in mind that administrative privileges on the machine are needed to perform this change.

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 version 10.14 (Mojave), you need to grant the same permissions if you want to scan removable volumes.



4.4 Asset Management

In the Asset Management 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](#)).

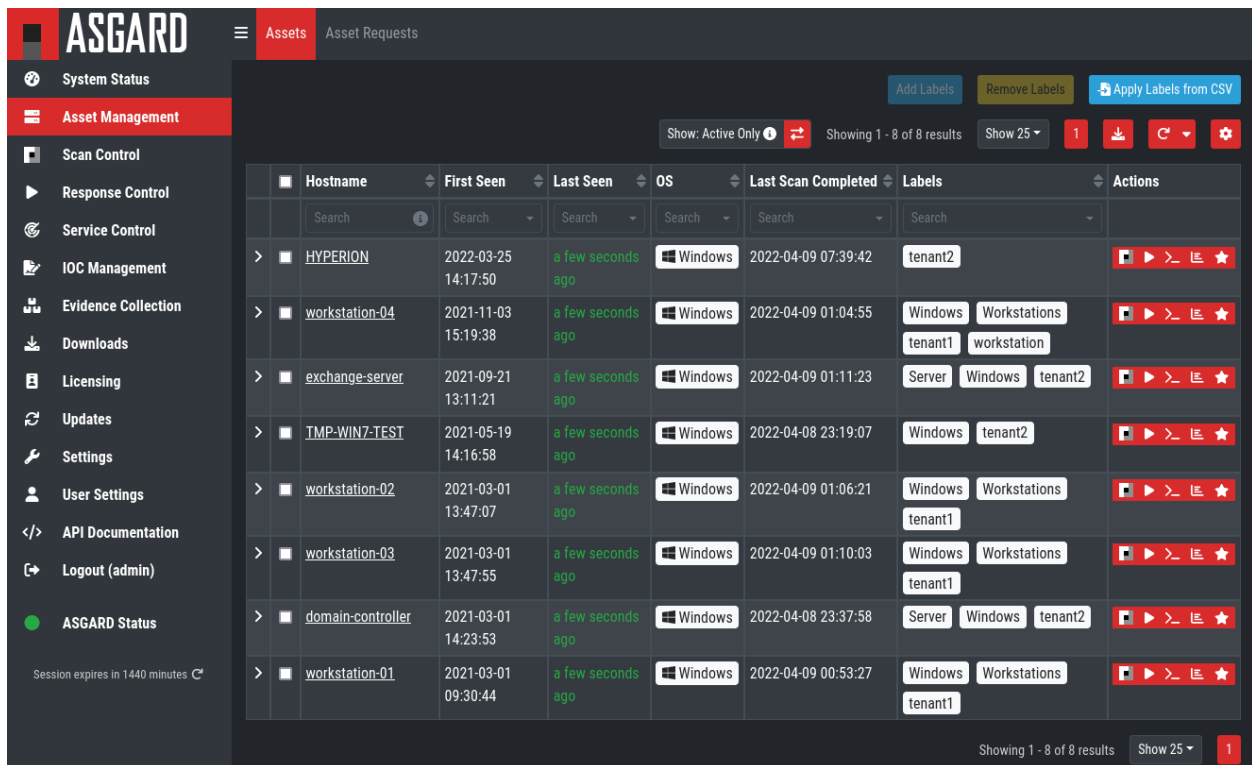
If the Duplicate Assets view is visible, you should try to remediate the issues in a timely manner, since this might cause unwanted side effects on the duplicate hosts.

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 2 Agent. Undesirable side effects of duplicate assets are alternating hostnames and tasks that fail immediately.

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

4.4.1 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.



	Hostname	First Seen	Last Seen	OS	Last Scan Completed	Labels	Actions
>	HYPERION	2022-03-25 14:17:50	a few seconds ago	Windows	2022-04-09 07:39:42	tenant2	[Stop] [Refresh] [Close] [Star]
>	workstation-04	2021-11-03 15:19:38	a few seconds ago	Windows	2022-04-09 01:04:55	Windows Workstations tenant1 workstation	[Stop] [Refresh] [Close] [Star]
>	exchange-server	2021-09-21 13:11:21	a few seconds ago	Windows	2022-04-09 01:11:23	Server Windows tenant2	[Stop] [Refresh] [Close] [Star]
>	TMP-WIN7-TEST	2021-05-19 14:16:58	a few seconds ago	Windows	2022-04-08 23:19:07	Windows tenant2	[Stop] [Refresh] [Close] [Star]
>	workstation-02	2021-03-01 13:47:07	a few seconds ago	Windows	2022-04-09 01:06:21	Windows Workstations tenant1	[Stop] [Refresh] [Close] [Star]
>	workstation-03	2021-03-01 13:47:55	a few seconds ago	Windows	2022-04-09 01:10:03	Windows Workstations tenant1	[Stop] [Refresh] [Close] [Star]
>	domain-controller	2021-03-01 14:23:53	a few seconds ago	Windows	2022-04-08 23:37:58	Server Windows tenant2	[Stop] [Refresh] [Close] [Star]
>	workstation-01	2021-03-01 09:30:44	a few seconds ago	Windows	2022-04-09 00:53:27	Windows Workstations tenant1	[Stop] [Refresh] [Close] [Star]

Fig. 9: Asset View

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:



Fig. 10: Available Actions (left to right): Run Scan, Run Task, Connect To Remote Console, Show Timeline, Enable/Disable Fast Poll Mode

- 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.

4.4.2 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.

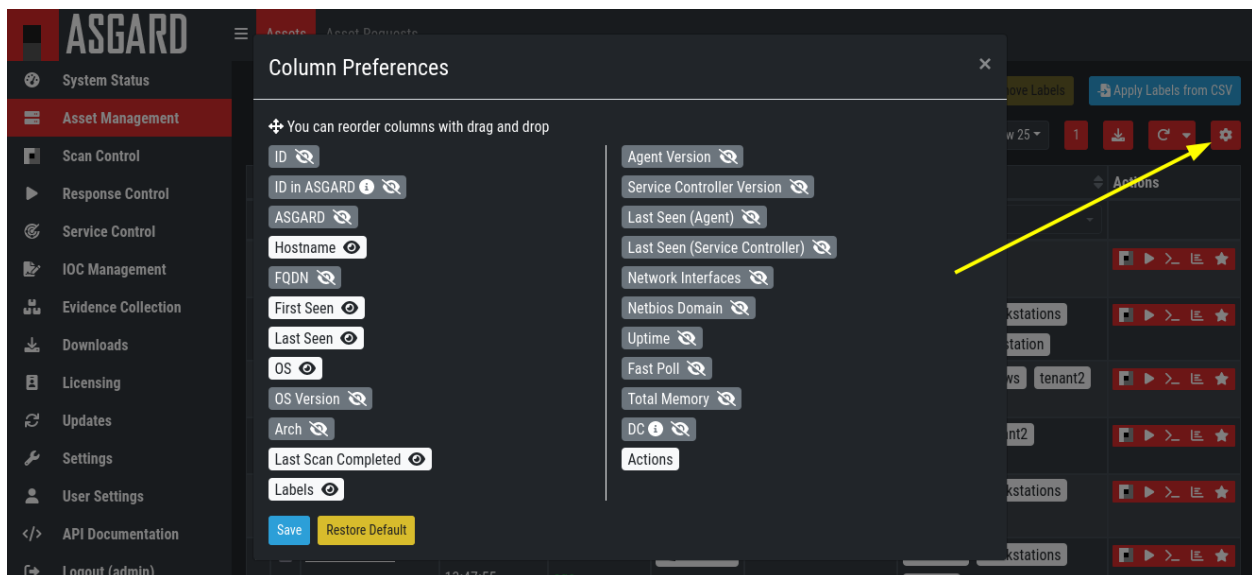


Fig. 11: Available columns in Asset Management

4.4.3 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 Analysis Cockpit, exports / imports or other underlying legacy functions.

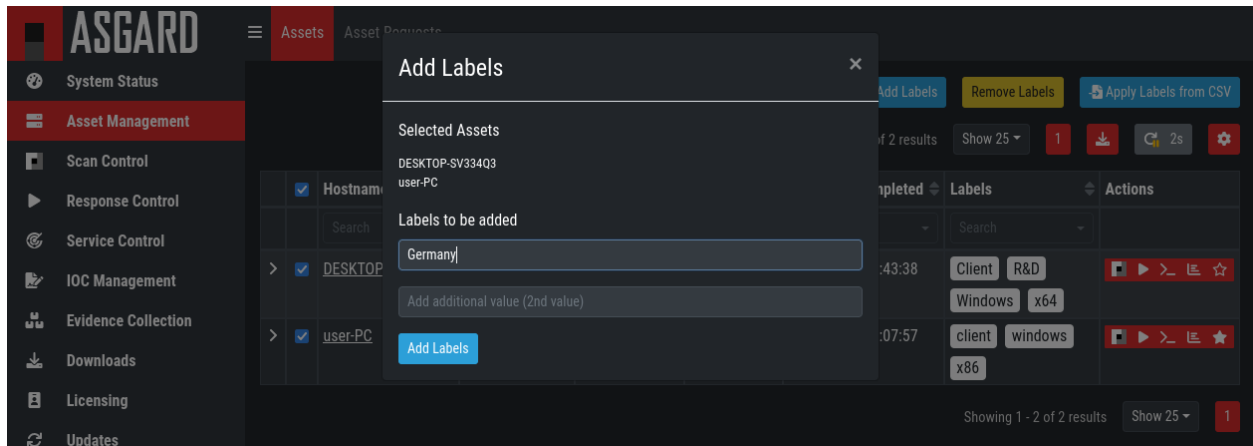


Fig. 12: Add labels

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.

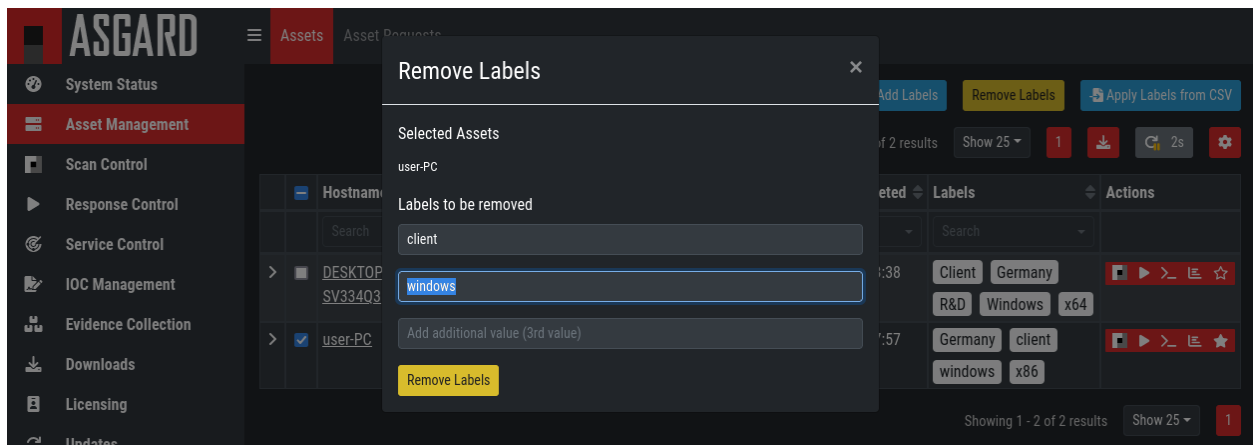


Fig. 13: Remove labels

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.

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:a	windows,x,x64,y		
5										

Fig. 14: Asset Labeling via CSV

4.4.4 ASGARD Query

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

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

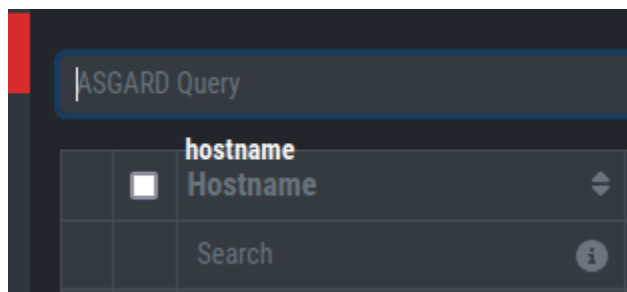
```
(system = "linux" and interfaces = "172.28.30.0/24") or (system = "windows" and
interfaces = "172.28.50.0/24")
```

```
(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:



4.4.5 Asset Migration

You can move an asset from one ASGARD to another via the Maintenance Module of Response Control. To do this, navigate to **Asset Management** 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 ASGARD. In this case, the asset will

Add Task

Description (optional)

Assets

cd3123b5b49a

Module

Maintenance

Max. Runtime ⓘ

1 hour

Maintenance Type

Move asset to another ASGARD

Agent Installer ⓘ

Select Installer

Browse

Add Task

remain on the ASGARD which issued the migration task. Only the asset will be migrated (it shows up as a brand new asset on your new ASGARD), no scan or response tasks and also no logs will be migrated.

4.4.6 Delete Assets

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

To delete an asset, go to the **Asset Management 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 asset.

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.

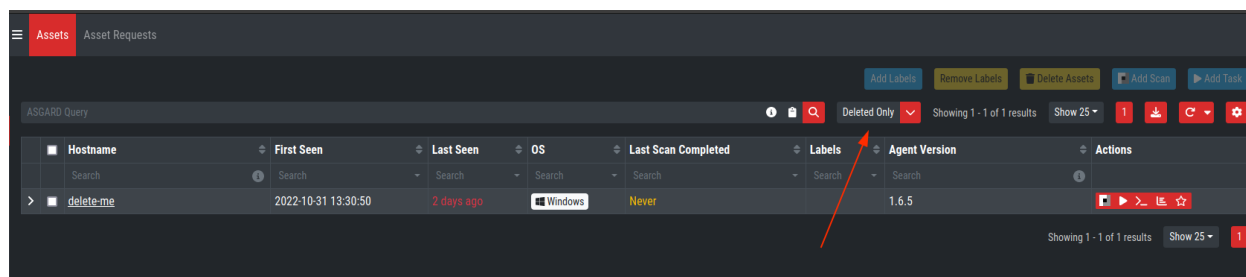


Fig. 15: Deleted Assets View

4.5 Scan Control

The Scan Control in your ASGARD 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 the different options don't need to be configured for every new scan. False-Positive Filters can be set to exclude certain files from scan results, or even whole directories can be excluded.

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

4.5.1 Managing Scan Templates

Scan templates are the most convenient way to make use of THOR's rich set of scan options. Starting with ASGARD 1.10, 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.

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 ASGARD 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 for a reason.

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

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

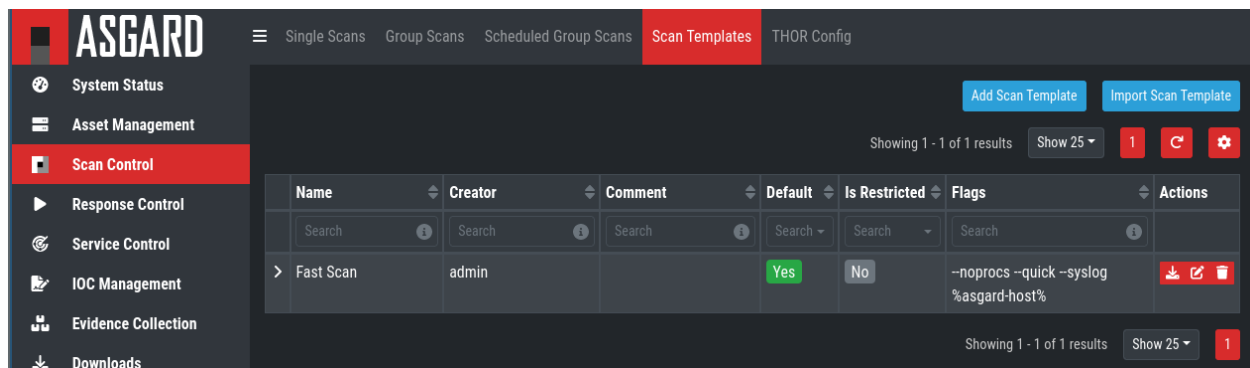


Fig. 16: Scan Templates Overview

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.

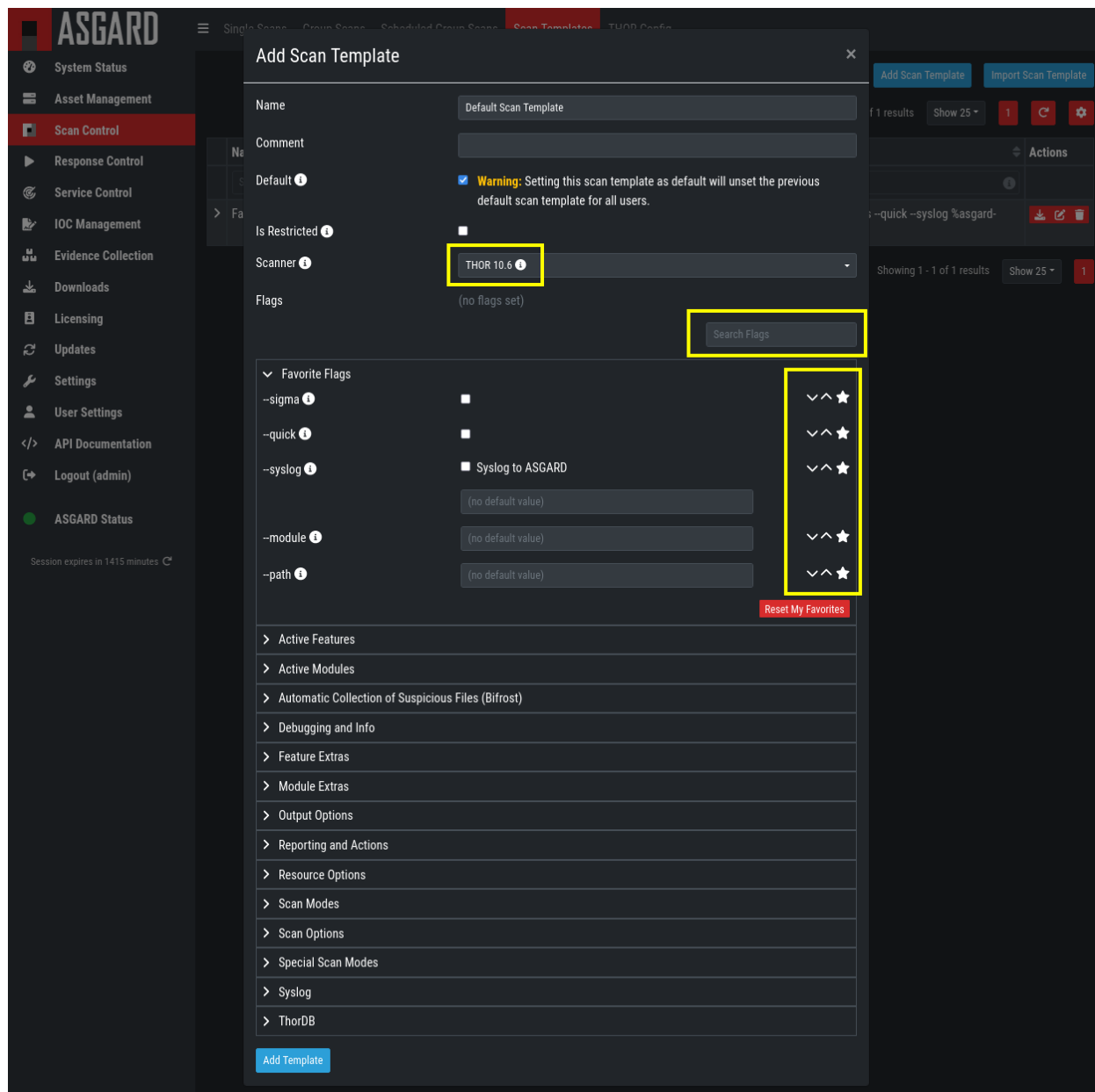


Fig. 17: Scan Flags

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 "ForceStandardArgs" restriction set. (By default this are all users who are not member of the group "Operator Level 1"). After clicking the "Add Template" button on the bottom of the template page, an overview of all existing scan templates is shown.

4.5.2 Scan a Single System

Create a Single Scan

The creation of a scan is performed within the Asset Management. There is a button for each asset to create a new scan and to show all past scans.

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

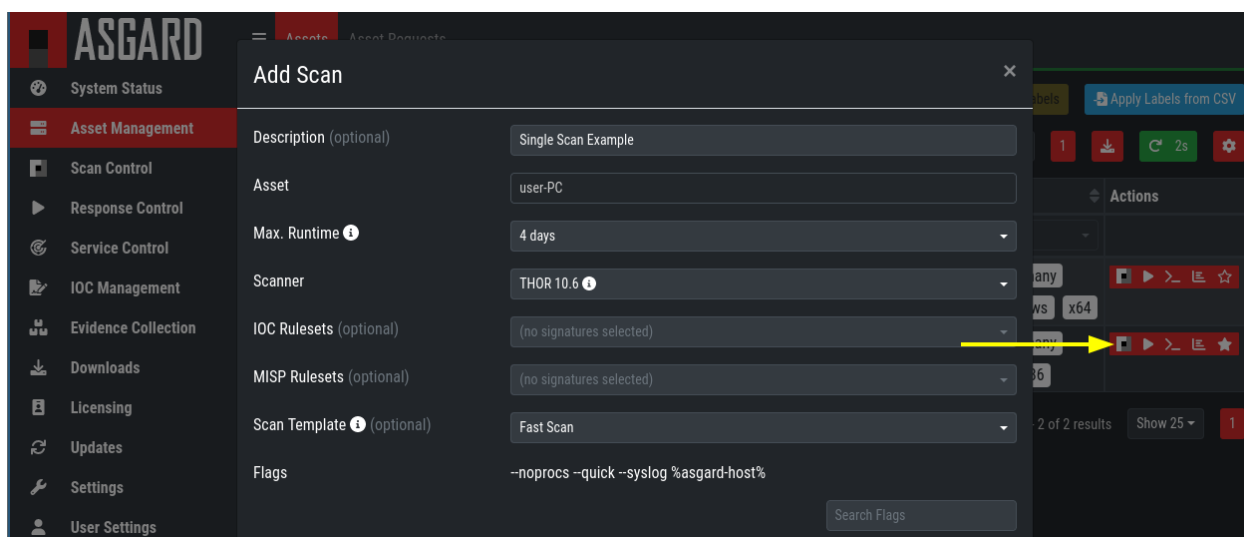


Fig. 18: Scan Control - Scan Creation

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

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

Create a Single Scan for multiple Assets

If you want to run a Single Scan - instead of a Group Scan - on multiple Assets, you can do this by navigating to the Asset Management View and select the assets you want to scan.

Click the Add Scan button in the top right corner and fill in the scan options. This will create a Single Scan for each asset.

Add Scan

Description (optional)

Assets

Max. Runtime ⓘ

No Resource Control ⓘ

Scanner

IOC Rulesets (optional)

MISP Rulesets (optional)

Scan Template ⓘ (optional)

Flags

2f44f3091ddae67b, 96066bd883e356c0, 2ca1746a6efd7460, c8a9b19f824c7372

4 days

☐

THOR 10.6 ⓘ

(no signatures selected)

(no signatures selected)

no scan template

--syslog %asgard-host%

Search Flags

Fig. 19: Scan Control - Multiple Single Scans

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.

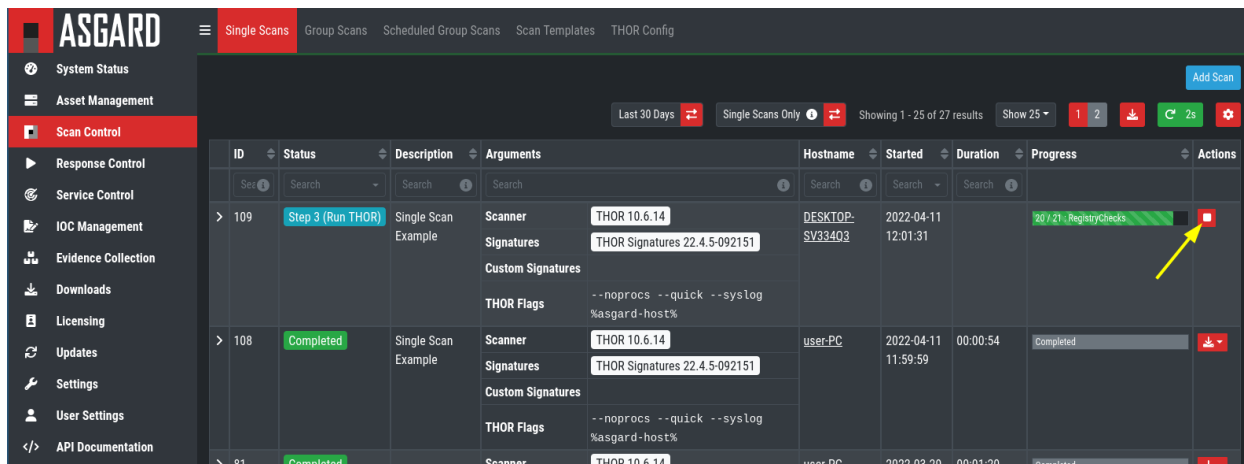


Fig. 20: Stopping a Single Scan

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)

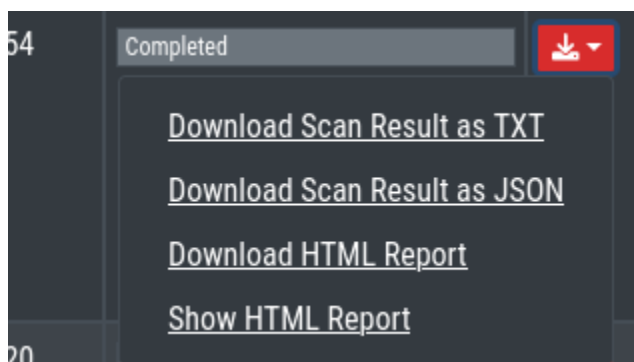


Fig. 21: Scan Control - Download Scan Results

4.5.3 Scan Groups of Systems

Create Grouped 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
Description	Freely selectable name for the group scan.
Scan Target	Here you can define which assets will be affected by 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 asset queries. Leaving this option empty will scan all assets.
Limit	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.
Rate	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.
Expires	After this time frame, no scan orders will be issued to the connected agents.
Scheduled Start	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.

List of all Group Scans

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

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
Paused	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).
Active	Scan is started, ASGARD will issue scans with the given parameters.
Inactive	No additional scan jobs are being issued. All single scans that are currently running will continue to do so.
Completed	The group scan is completed. No further scan jobs will be issued.

Add Group Scan
×

Description (optional)
Scan All Linux Workstations

Scan Target
Simple

Include Labels ⓘ (optional)
linux (25 assets) ×
OR ⓘ

Exclude Labels ⓘ (optional)
(no labels selected)
OR ⓘ

ASGARD Query ⓘ (optional)
labels = "linux"
Test Query

Expires ⓘ
2022-11-09 12:00:00

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 ⓘ

IOC Rulesets (optional)
(no signatures selected)

MISP Rulesets (optional)
(no signatures selected)

Scan Template ⓘ (optional)
no scan template

Flags
--quick

Search Flags

Fig. 22: Scan Control – Create Group Scan

The screenshot displays the ASGARD Management Center interface, specifically the 'Scan Control' section under 'Group Scans'. The sidebar on the left contains various navigation options, including 'System Status', 'Asset Management', 'Scan Control', 'Response Control', 'Service Control', 'IOC Management', 'Evidence Collection', 'Downloads', 'Licensing', 'Updates', 'Settings', 'User Settings', 'API Documentation', and 'Logout (admin)'. The main content area shows a table of group scans with columns for Status, Description, Arguments, Active Since, Issued, Completed, and Actions. A detailed view of a specific scan is shown below the main table, including a progress bar for 'Step 3 (Run THOR)'.

Status	Description	Arguments	Active Since	Issued	Completed	Actions
Active	Scan All Assets	Scanner: THOR 10.6 Signatures: THOR Signatures Custom Signatures: Testing THOR Flags: --noprocs --quick	2022-04-11 12:34:59	2	1	[Icons]

Status	Hostname	Started	Duration	Progress	Actions
Step 3 (Run THOR)	DESKTOP-SV334Q3	2022-04-11 12:38:39		20 / 21 : RegistryChecks	[Icon]
Completed	user-PC	2022-04-11 12:36:22	00:00:56	Completed	[Icon]

Status	Description	Arguments	Active Since	Issued	Completed	Actions
Active	Scan All Assets	Scanner: THOR 10.6 Signatures: THOR Signatures Custom Signatures: --noprocs --quick THOR Flags: --syslog %asgard-host%	2022-04-11 12:32:57	2	1	[Icons]
Completed	Scan All Assets	Scanner: THOR 10.6 Signatures: THOR Signatures	2022-03-28 12:00:15	2	2	[Icons]

Fig. 23: Scan Control – Group Scans – List

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".

Starting a 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.

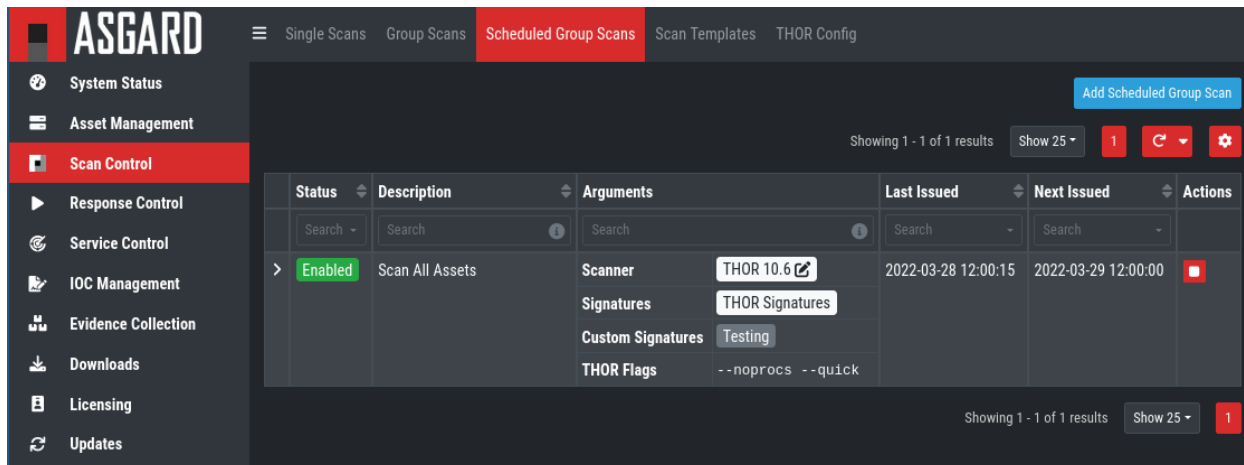


Fig. 24: Scan Control – Scheduled Group Scan

Details of a Group Scan

Further information about a group scan can be observed from the detail page of the group scan. Click the scan you are interested in and the details section will appear.

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.

4.5.4 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.

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

Add Scheduled Group Scan

Description (optional)

Scan all Assets in Subnet 172.28.30.0/24

First Run

2022-11-02 11:00:00

Repeat Interval

7 days

Scan Target

Simple

Include Labels ⓘ (optional)

(no labels selected)

OR ⓘ

Exclude Labels ⓘ (optional)

(no labels selected)

OR ⓘ

ASGARD Query ⓘ (optional)

interfaces = "172.28.30.1/24"

Test Query

ASGARD Query ⓘ (optional)

ASGARD Query

Test Query

Limit ⓘ

100

Rate

1 per minute

Expires ⓘ

in 7 days

Max. Runtime ⓘ

4 days

No Resource Control ⓘ

☐

Scanner

THOR 10.6 ⓘ

IOC Rulesets (optional)

(no signatures selected)

MISP Rulesets (optional)

(no signatures selected)

Scan Template ⓘ (optional)

no scan template

Flags

--quick

Fig. 25: Scan Control – New Scheduled Group Scan

Status	Description	Arguments	Last Issued	Next Issued	Actions
Search	Search	Search	Search	Search	
▼ Enabled	Scan All Assets	Scanner THOR 10.6	2022-04-11 12:34:59	2022-04-12 12:00:00	
		Signatures THOR Signatures			
		Custom Signatures Testing			
		THOR Flags --noprocs --quick			

Details

Group Tasks

ID

2

Module

THOR

Description

Scan All Assets

Scanner

THOR 10.6

Signatures

THOR Signatures

Custom Signatures

Testing

THOR Flags

--noprocs --quick

Asset Labels

all

Limit

max. 99999 assets

Rate

every 60 second(s)

Status

Enabled

Creator

admin

Last Issued

2022-04-11 12:34:59 (6 minutes ago)

Next Issued

2022-04-12 12:00:00 (in a day)

Repeat Interval

every 24h

Expires

after 3h

Max. Runtime

3h

Showing 1 - 1 of 1 results

Show 25

1

Fig. 26: Scan Control – Group Scans – Details

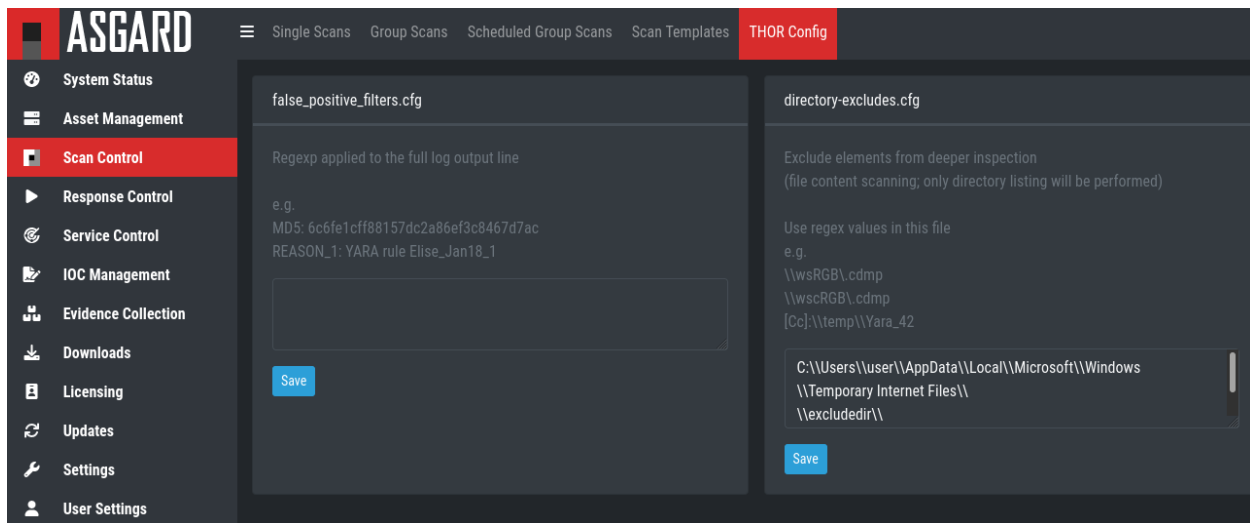
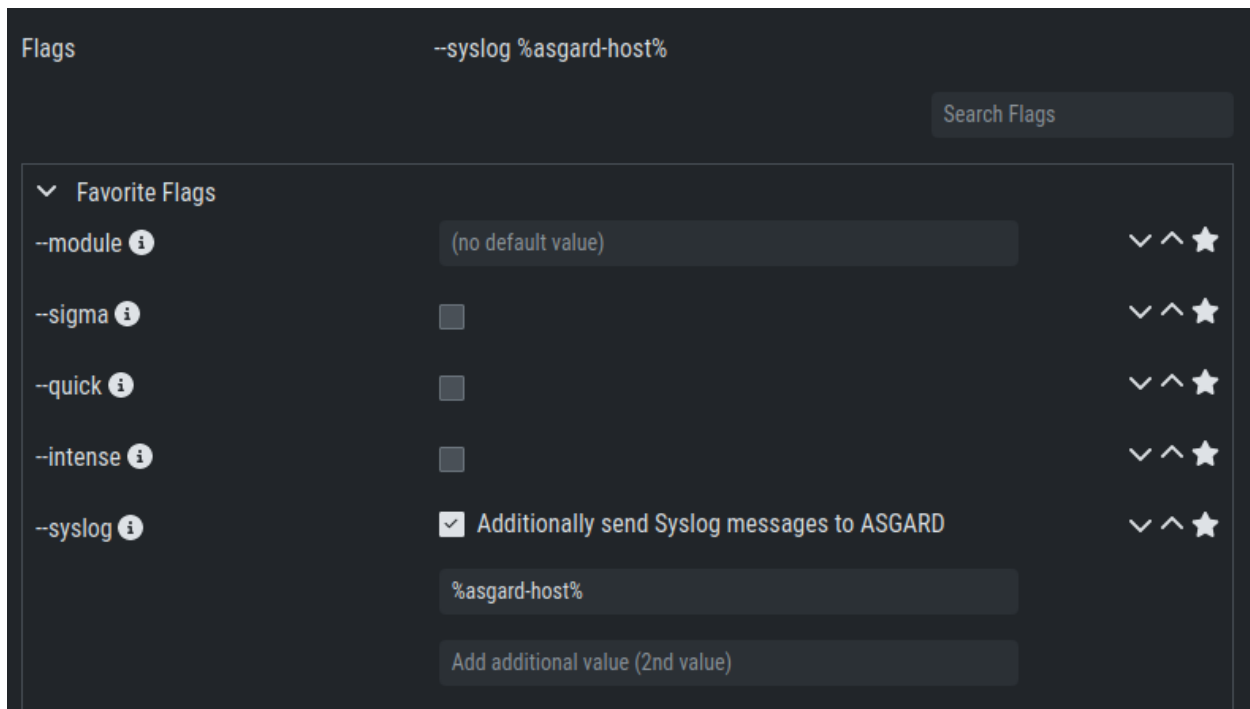


Fig. 27: Scan Control - Global Directory Exclude and FP Filtering

4.5.5 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 :

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	optional - the listening port on the remote system, default is 514	1 - 65535
3	Format	optional - the log format, default is DEFAULT	- DEFAULT ¹ - CEF - JSON - SYSLOGJSON - SYSLOGKV
4	Socket	optional - 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

4.6 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

¹ This is the default log format of THOR.

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

4.6.1 Opening a Remote Shell on an endpoint

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

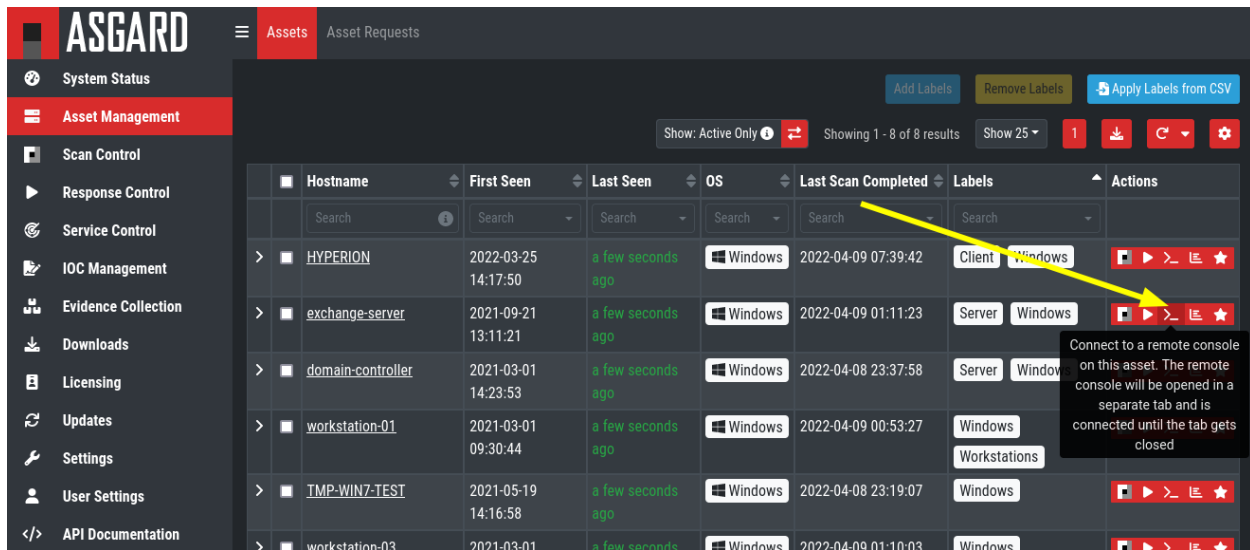


Fig. 28: Opening a Remote Shell from the Asset View

Depending on your configuration it may take between 10 seconds and 10 minutes for the remote shell to open. Please note that all actions within the remote shell are recorded and can be audited. All shells 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, select the Console Log tab and click the play button in the bottom row.

ASGARD users can only see their own remote shell session. Only users with the RemoteConsoleProtocol permission are able to replay all sessions from all users.

4.6.2 Response Control with Pre-Defined Playbooks

In addition to controlling THOR scans, ASGARD Management Center contains extensive response functions. Through ASGARD, 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 endpoint or groups of endpoints.

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

To execute a predefined response action on a single endpoint, navigate to the Asset Management view and click the "play" button in the Actions Column. This will lead you to a dialogue where you can select the desired action.

In this example, we collect a full triage package.

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

The screenshot displays the ASGARD Management Center interface. At the top, the ASGARD logo is visible. Below it, a terminal window shows a Windows command prompt session with the following text:

```
Microsoft Windows [Version 10.0.19043.1348]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
nt authority\system

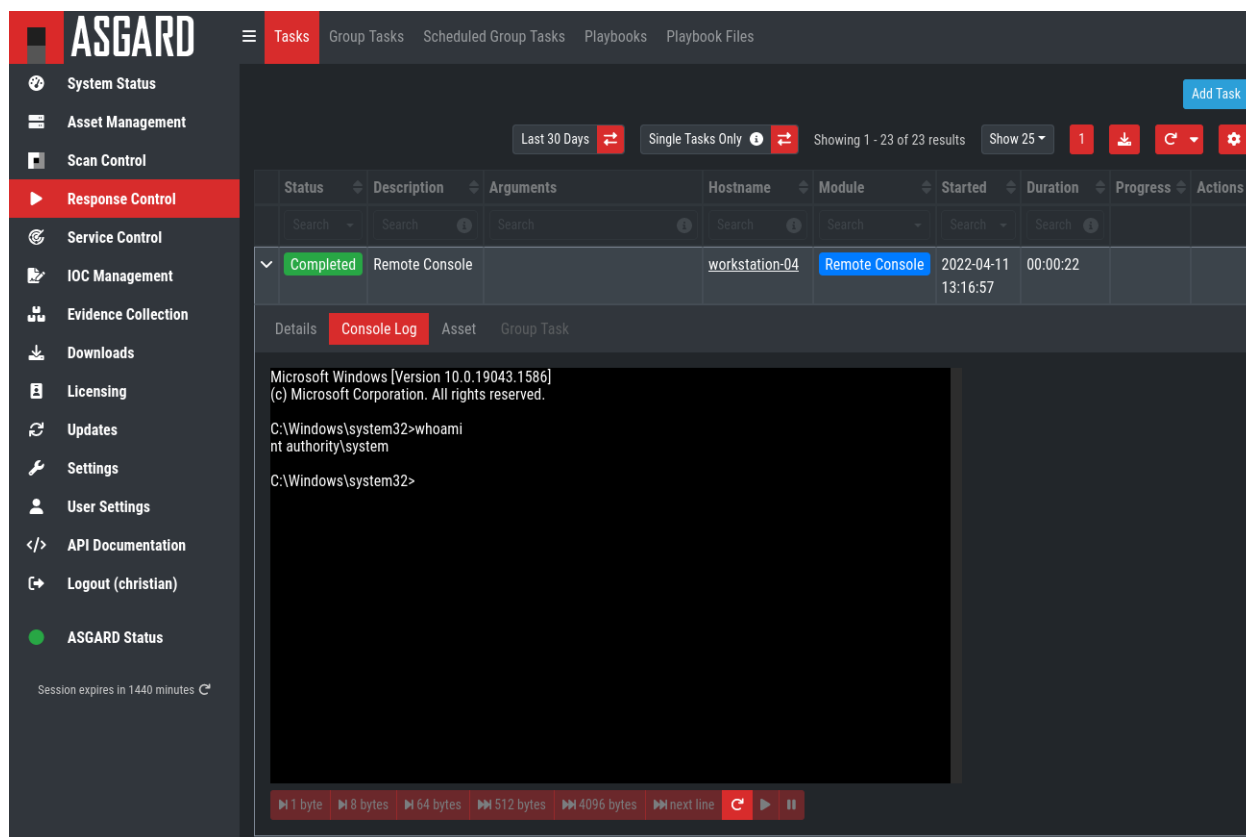
C:\Windows\system32>
```

Below the terminal window, there are four buttons: "Add Columns", "Remove Columns", "Add Rows", and "Remove Rows". Below these buttons, a message states: "In order to end the session gracefully, please [close this window](#)."

Below the message, there is a tabbed interface with the following tabs: "Details", "Tasks", "Services", "Timeline", "Software List", and "Local Users". The "Details" tab is currently selected, showing a list of system information:

ID	12
Hostname	workstation-04
FQDN	workstation-04.rt-testing.nextron
Netbios Domain	WORKSTATION-04
Interfaces	fe80::744c:f143:24fc:ff71 172.28.30.155 ::1 127.0.0.1
OS	windows (Windows 10 Enterprise)
Architecture	amd64
Is Domain Controller	No
First Seen	2021-11-03 15:19:38
Last Seen	a few seconds ago
Last Seen (Agent)	a few seconds ago
Last Seen (Service Controller)	a few seconds ago
Last Scan Completed	2022-01-24 15:32:13
Fast Poll	No
Agent	1.5.5
Service Controller	2.0.6
Total Memory	6 GB
CPU Count	2

Fig. 29: Remote Shell



The screenshot shows the ASGARD Management Center interface. The left sidebar contains navigation links: System Status, Asset Management, Scan Control, Response Control (highlighted), Service Control, IOC Management, Evidence Collection, Downloads, Licensing, Updates, Settings, User Settings, API Documentation, Logout (christian), and ASGARD Status. The main content area is titled 'Tasks' and includes sub-tabs: Group Tasks, Scheduled Group Tasks, Playbooks, and Playbook Files. A table of tasks is displayed, with columns for Status, Description, Arguments, Hostname, Module, Started, Duration, Progress, and Actions. The first task, 'Remote Console', is highlighted. Below the table, a console window shows the output of a 'whoami' command, indicating 'nt authority\system' privileges. The console window also includes a playback control bar at the bottom.

Status	Description	Arguments	Hostname	Module	Started	Duration	Progress	Actions
Completed	Remote Console		workstation-04	Remote Console	2022-04-11 13:16:57	00:00:22		

```

Microsoft Windows [Version 10.0.19043.1586]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>
  
```

Fig. 30: Replay Remote Shell Session

The screenshot shows the ASGARD Management Center interface. The sidebar on the left contains navigation links: System Status, Asset Management, Scan Control, Response Control (highlighted), Service Control, IOC Management, Evidence Collection, Downloads, Licensing, Updates, Settings, User Settings, API Documentation, and Logout (admin). Below the sidebar, it indicates 'ASGARD Status' and 'Session expires in 1440 minutes'. The main content area is titled 'Playbooks' and shows a list of built-in playbooks. The table has columns: Name, Steps, Creator, Modified, and Actions. The playbooks listed are:

Name	Steps	Creator	Modified	Actions
> Create and Collect Aurora Agent Diagnostics Pack (Windows)	<ul style="list-style-type: none"> aurora-agent-util.exe aurora-agent-util.exe diagnostics diagnostics.zip 	ASGARD	2022-03-29 16:03:54	[Icons]
> Install ASGARD Service Controller (Windows 32-bit)	<ul style="list-style-type: none"> asgard2-service-controller-windows-386.exe asgard2-service-controller-windows-386.exe 	ASGARD	2022-03-24 10:46:31	[Icons]
> Install ASGARD Service Controller (Windows 64-bit)	<ul style="list-style-type: none"> asgard2-service-controller-windows-amd64.exe asgard2-service-controller-windows-amd64.exe 	ASGARD	2022-03-24 10:46:31	[Icons]
> Uninstall ASGARD 1 Agent on Linux (RPM)	rpm -e grr	ASGARD	2022-03-24 10:46:31	[Icons]
> Uninstall ASGARD 1 Agent on Linux (DEB)	dpkg --purge grr	ASGARD	2022-03-24 10:46:31	[Icons]
> Uninstall ASGARD 1 Agent on Windows	<ul style="list-style-type: none"> sc.exe stop "grr monitor" sc.exe delete "grr monitor" reg.exe delete HKLM\Software\GRR /f rmdir /Q /S %SystemRoot%\System32\GRR 	ASGARD	2022-03-24 10:46:31	[Icons]
> De-Quarantine (Windows)	<ul style="list-style-type: none"> de-quarantine.bat de-quarantine.bat 	ASGARD	2022-04-11 09:48:59	[Icons]
> Quarantine (Windows)	<ul style="list-style-type: none"> quarantine.bat quarantine.bat 	ASGARD	2022-04-11 09:48:59	[Icons]
> Collect full triage package (Windows 32-bit)	<ul style="list-style-type: none"> CyLR_win-x86.zip CyLR.exe -od logs logs 	ASGARD	2022-03-24 10:46:31	[Icons]
> Collect full triage package (Windows 64-bit)	<ul style="list-style-type: none"> CyLR_win-x64.zip CyLR.exe -od logs logs 	ASGARD	2022-03-24 10:46:30	[Icons]

At the bottom right, it says 'Showing 1 - 10 of 19 results' and 'Show 10' with page numbers '1' and '2'.

Fig. 31: Built-in Playbooks

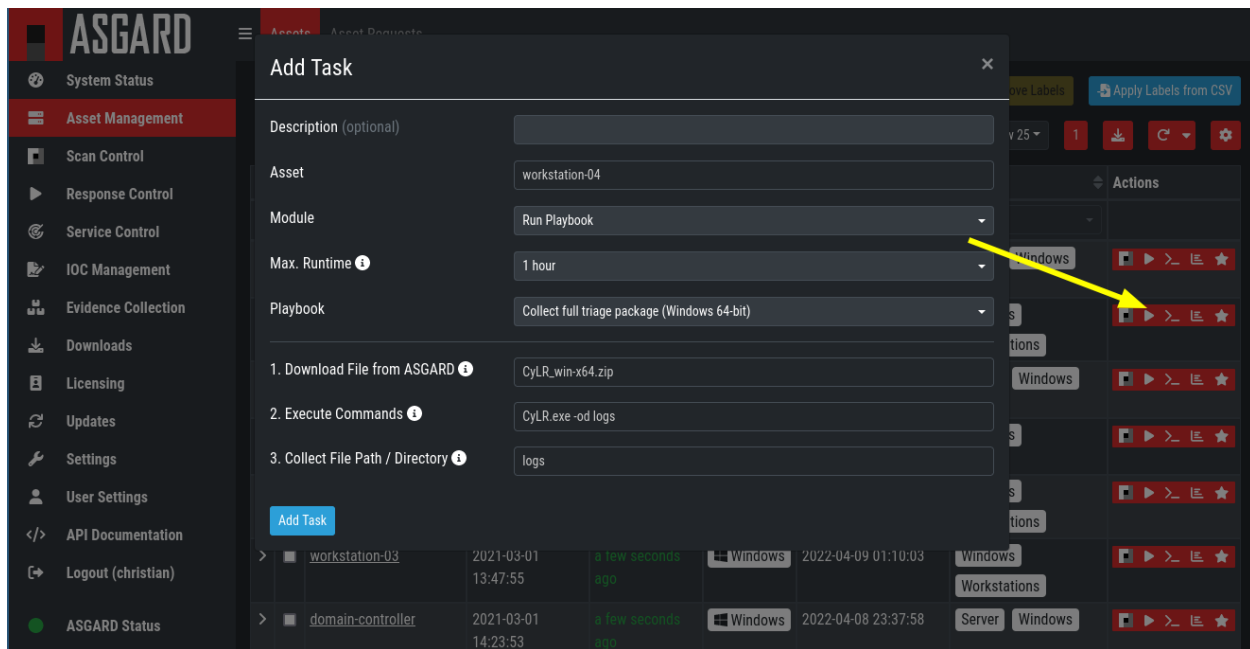


Fig. 32: Execute Playbook on Single Endpoint

- 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
- Execute command and collect stdout and stderr

Nextron provides additional playbooks via ASGARD updates.

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.

4.6.3 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.

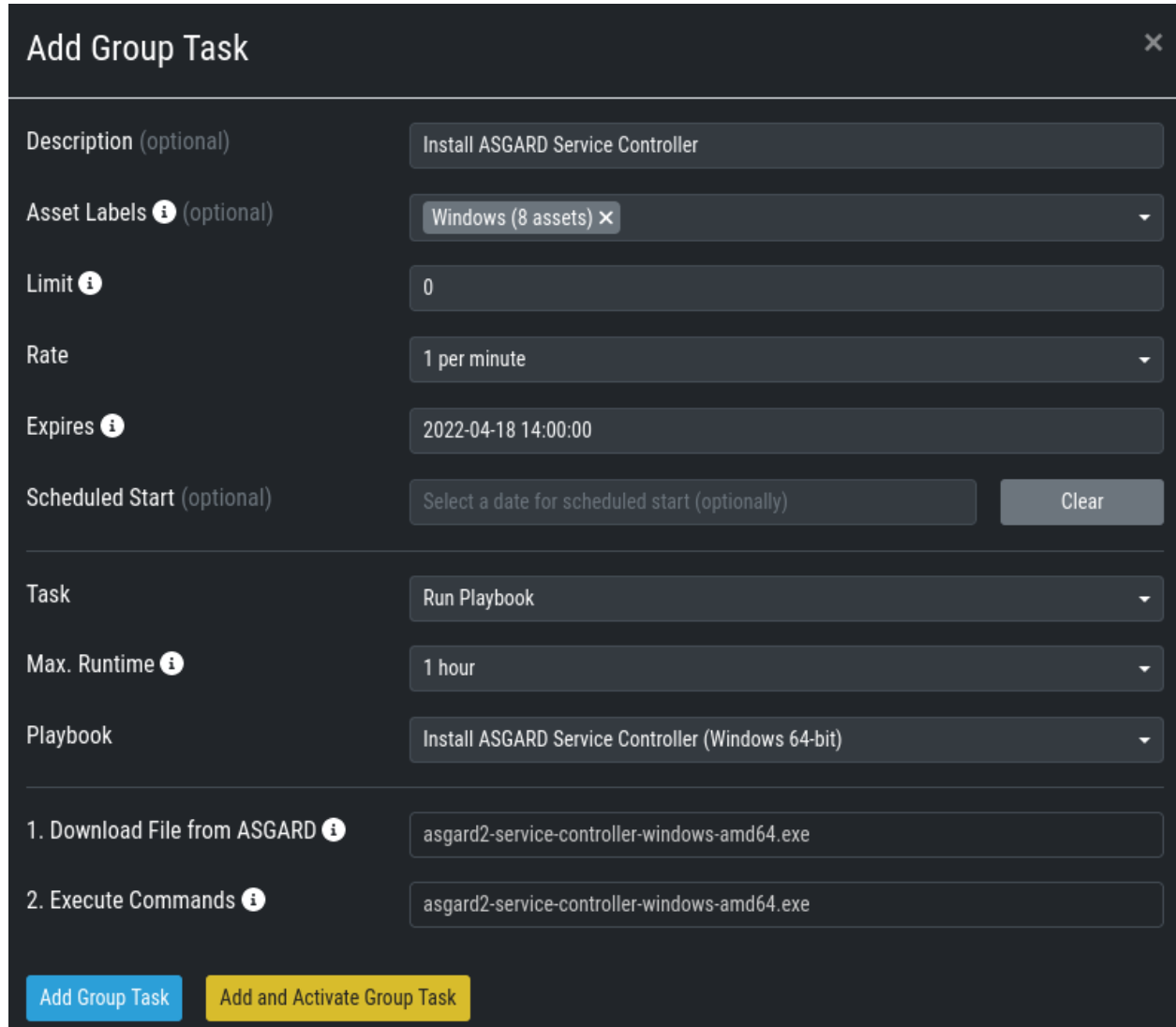


Fig. 33: Execute Playbook on Group of Endpoints

4.6.4 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.

If you need custom files for your playbook (scripts, configurations, binaries, etc.) you can select local files to be uploaded to ASGARD during the creation of the playbook step (by selecting "Upload New File" in the file drop-down).

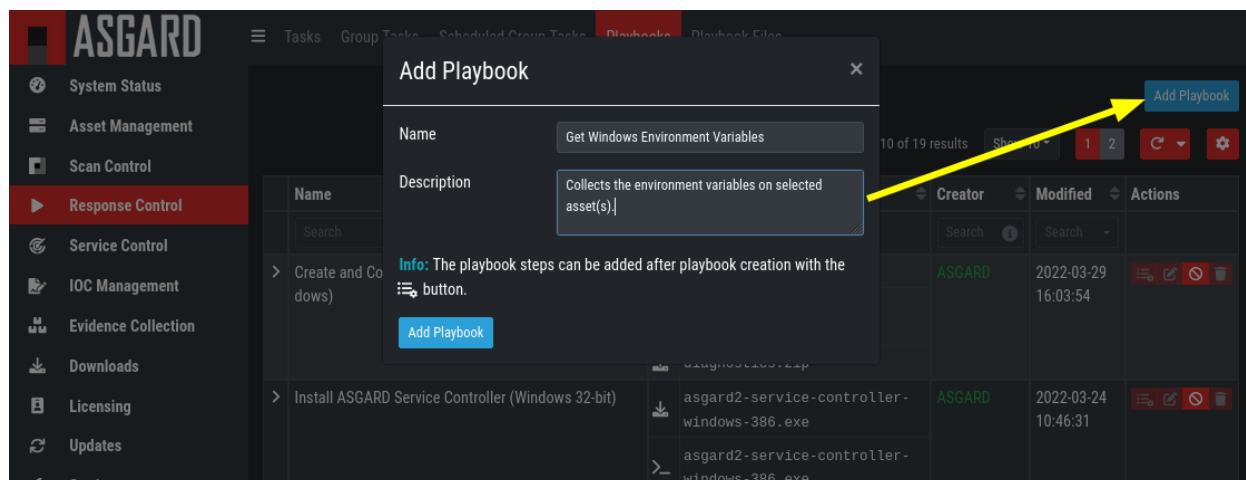


Fig. 34: Add Custom Playbook

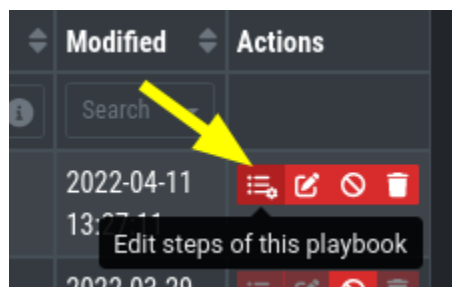


Fig. 35: Playbook Action Items

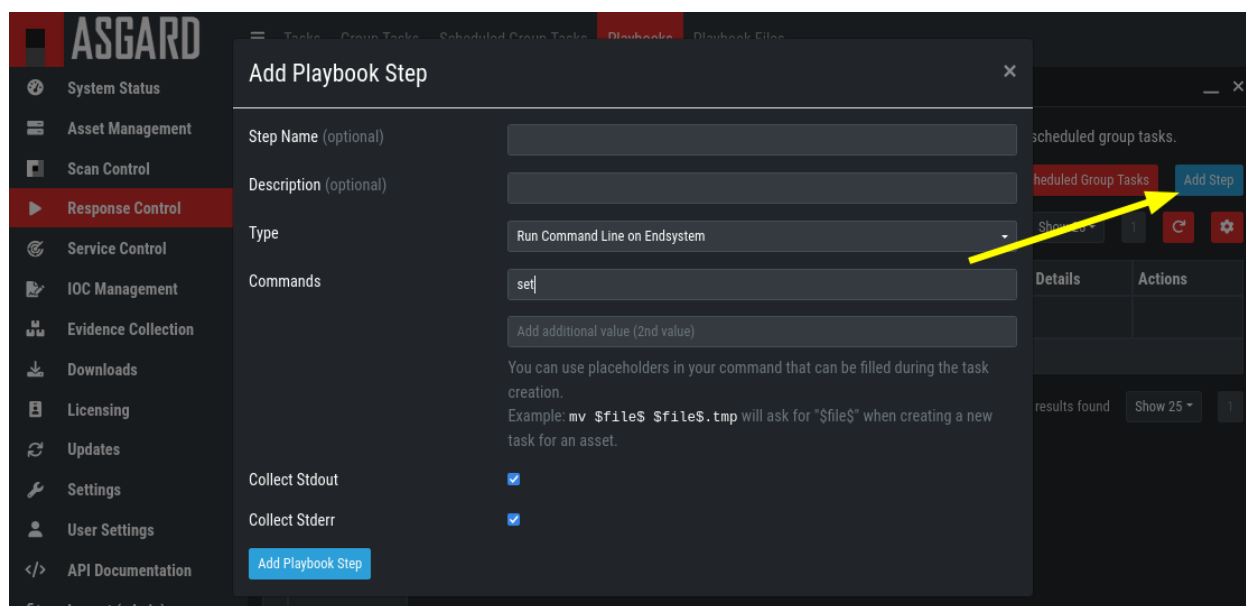


Fig. 36: Add Playbook Entry

You can manage these files at Response Control > Playbook Files and upload or update files using the Upload Playbook File button.

ASGARD

Tasks Group Tasks Scheduled Group Tasks Playbooks **Playbook Files**

System Status

Asset Management

Scan Control

Response Control

Service Control

IOC Management

Evidence Collection

Downloads

Licensing

Updates

Settings

User Settings

API Documentation

Logout (admin)

ASGARD Status

Session expires in 60 minutes

Upload Playbook File

Showing 1 - 11 of 11 results Show 25 1

Name	Size	Creator	Modified	Actions
Search	Search	Search	Search	
> aurora-agent-util.exe	69 B	ASGARD	2022-04-13 12:55:06	Download Delete
> filename-iocs.txt	207 B	admin	2022-04-13 12:55:06	Download Delete
> winpmem_x86.exe	217 KB	ASGARD	2022-04-13 12:55:06	Download Delete
> winpmem_x64.exe	528 KB	ASGARD	2022-04-13 12:55:06	Download Delete
> quarantine.bat	4 KB	ASGARD	2022-04-13 12:55:06	Download Delete
> linpmem.zip	994 KB	ASGARD	2022-04-13 12:55:06	Download Delete
> de-quarantine.bat	3 KB	ASGARD	2022-04-13 12:55:06	Download Delete
> asgard2-service-controller-windows-amd64.exe	57 B	ASGARD	2022-04-13 12:55:06	Download Delete
> asgard2-service-controller-windows-386.exe	55 B	ASGARD	2022-04-13 12:55:06	Download Delete
> CyLR_win-x86.zip	20 MB	ASGARD	2022-04-13 12:55:06	Download Delete
> CyLR_win-x64.zip	22 MB	ASGARD	2022-04-13 12:55:06	Download Delete

Showing 1 - 11 of 11 results Show 25 1

Fig. 37: Manage Playbook Files

You can have up to 16 steps in each playbook that are executed sequentially. Every step can be either "download something from ASGARD to the endpoint", "execute a command line" or "upload something from the endpoint to ASGARD". If you run a command line the stdout and stderr are reported back to ASGARD.

4.6.5 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. 38: Change/Set an assets Proxy

4.7 Service Control

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

4.7.1 Service Controller Installation

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

The screenshot shows the 'Add Task' dialog box. It has a title bar with a close button. The form contains the following fields and options:

- Description (optional):** A text input field.
- Asset:** A dropdown menu showing 'user-PC #1'.
- Module:** A dropdown menu showing 'Run Playbook'.
- Max. Runtime:** A dropdown menu showing '1 hour'.
- Playbook:** A dropdown menu showing 'Install ASGARD Service Controller (Windows 64-bit)'.
- 1. Download File from ASGARD:** A text input field containing 'asgard2-service-controller-windows-amd64.exe'.
- 2. Execute Commands:** A text input field containing 'asgard2-service-controller-windows-amd64.exe'.
- Add Task:** A blue button at the bottom left.

Fig. 39: Install Service Controller

4.7.2 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. For a single asset the task can be run in Asset Management > Assets > Run Task (play button action) or analogous as a (scheduled) group task under Response Control > (Scheduled) Group Tasks > Add (Scheduled) Group Task.

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

Add Task

Description (optional)

Asset

DESKTOP-SV334Q3

Module

Update Agent

Max. Runtime ⓘ

1 hour

Agent Type

ASGARD 2 Service Controller

Add Task

Fig. 40: Update Service Controller

4.7.3 Sigma

LogWatcher, as well as Aurora, are using Sigma in order to define their detections. The Sigma rule management is shared between the two services. But each service has its own configuration that defines which rules are actually used on the assets.

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 straight-forward 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.

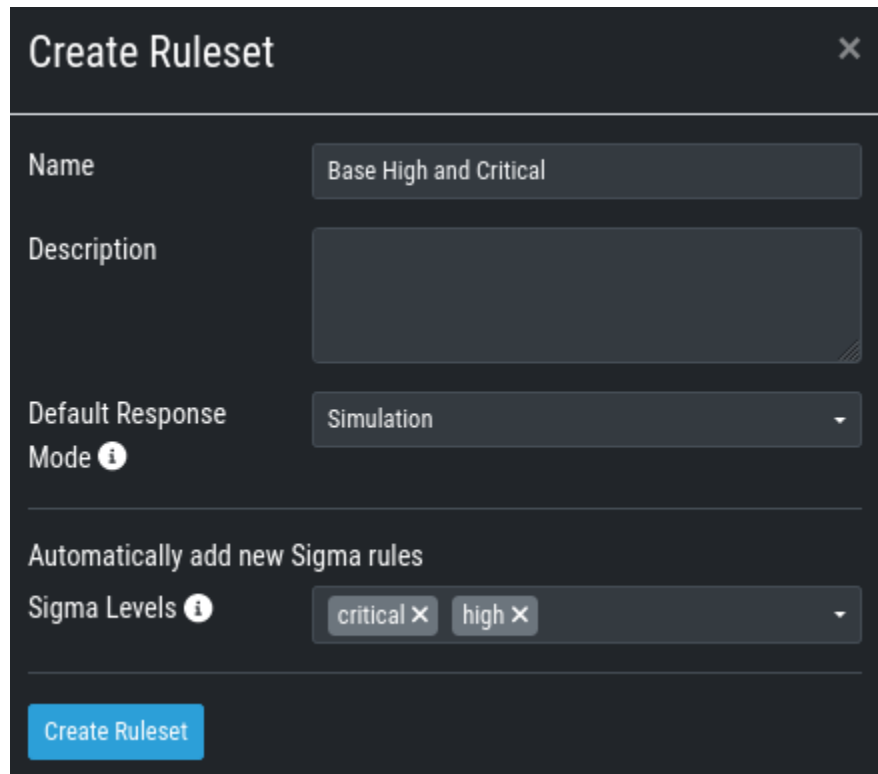
Sigma is for log files what [Snort](#) is for network traffic and [YARA](#) is for files.

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 rule 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**.

If you have chosen that new Sigma rules should be added automatically they are added now. If you didn't 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 a user performing several configuration changes in succession, the user has to initiate the reloading of the new configuration by going to **Service Control >**



Create Ruleset [X]

Name: Base High and Critical

Description: [Empty text area]

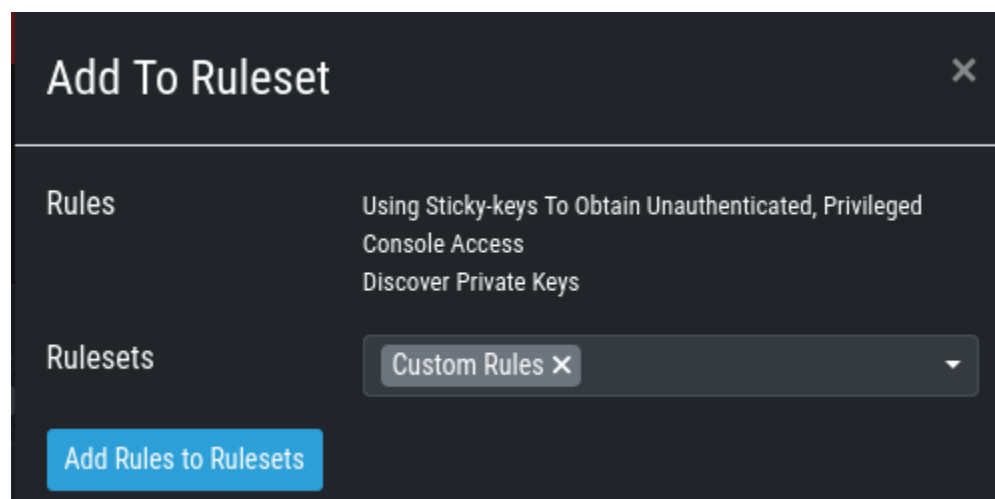
Default Response Mode: Simulation [i]

Automatically add new Sigma rules

Sigma Levels: critical X high X [i]

[Create Ruleset]

Fig. 41: Create a Ruleset



Add To Ruleset [X]

Rules: Using Sticky-keys To Obtain Unauthenticated, Privileged Console Access
Discover Private Keys

Rulesets: Custom Rules X [i]

[Add Rules to Rulesets]

Fig. 42: Add a Rule to Rulesets

Sigma > Rulesets and performing the **Compile ruleset** action (gear wheels). The need for compiling is indicated in the *Uncompiled Changes* column.

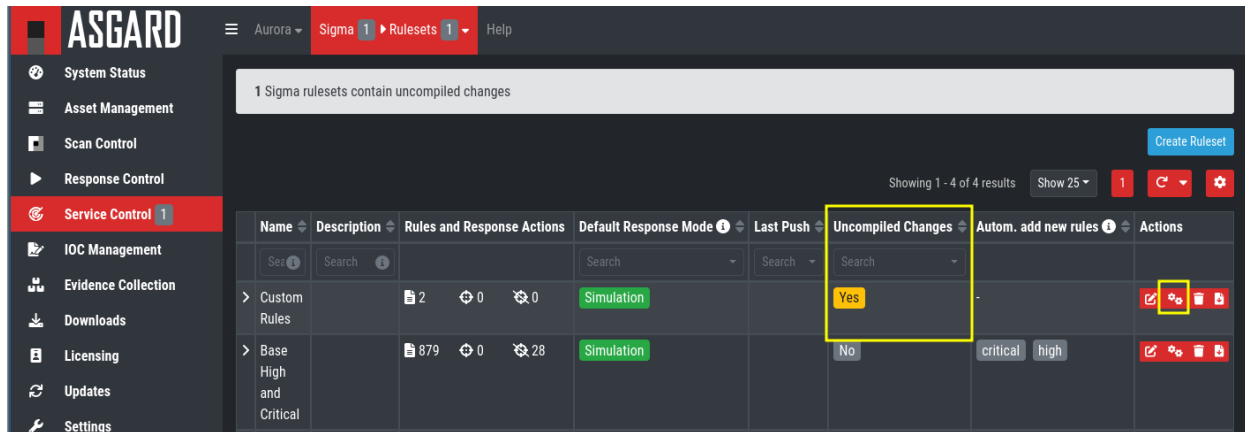


Fig. 43: Uncompiled Changes Indicator

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 or "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:

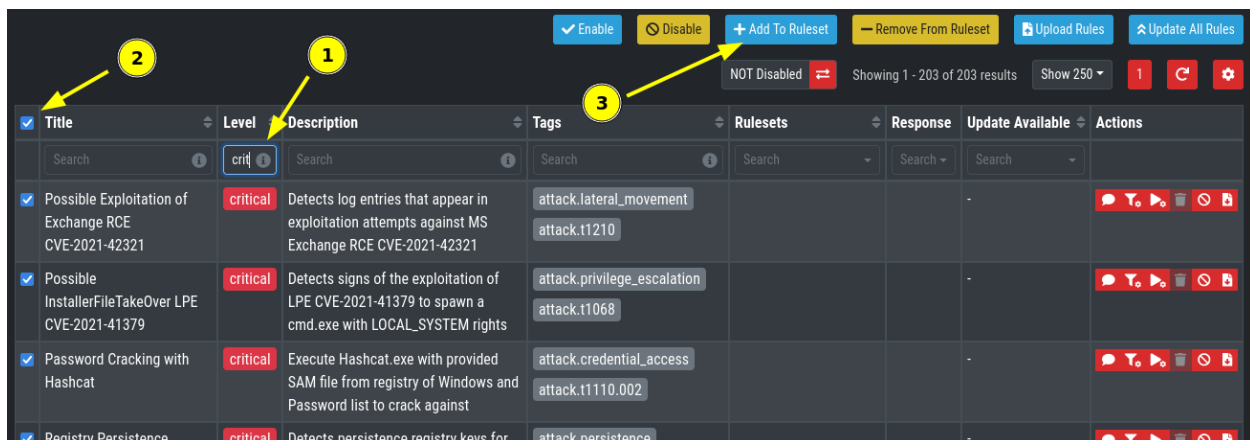


Fig. 44: Add All Critical Rules to a Ruleset

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

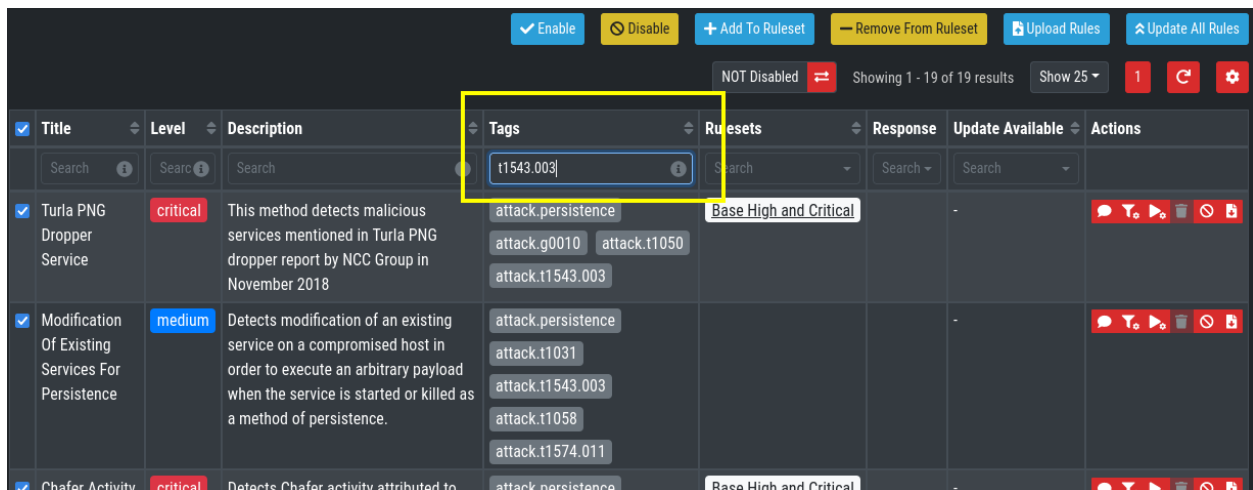


Fig. 45: Search by MITRE ATT&CK® ID

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).

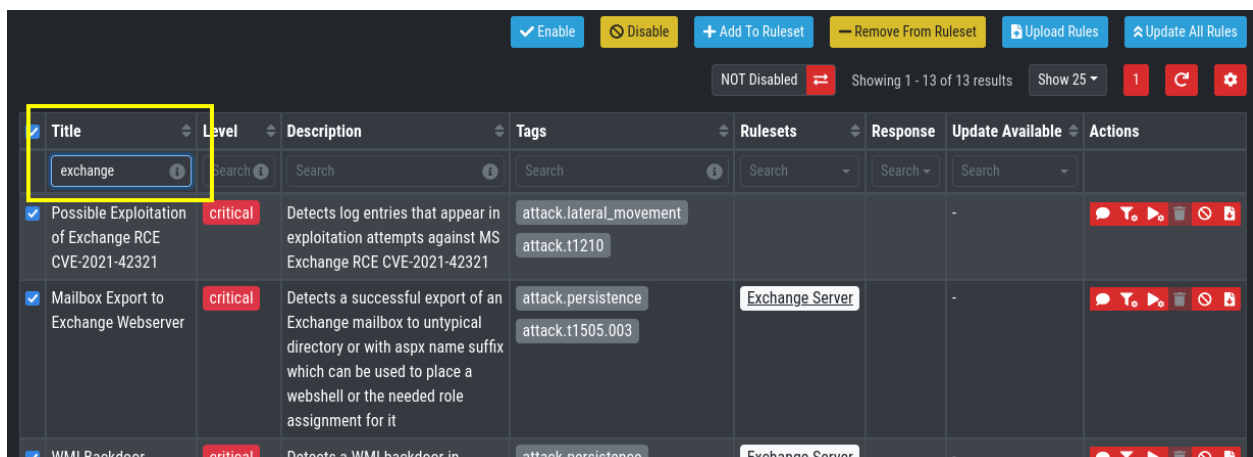


Fig. 46: Search by Rule Title or Description

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 \(rules@nexttron-systems.com\)](mailto:rules@nexttron-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.

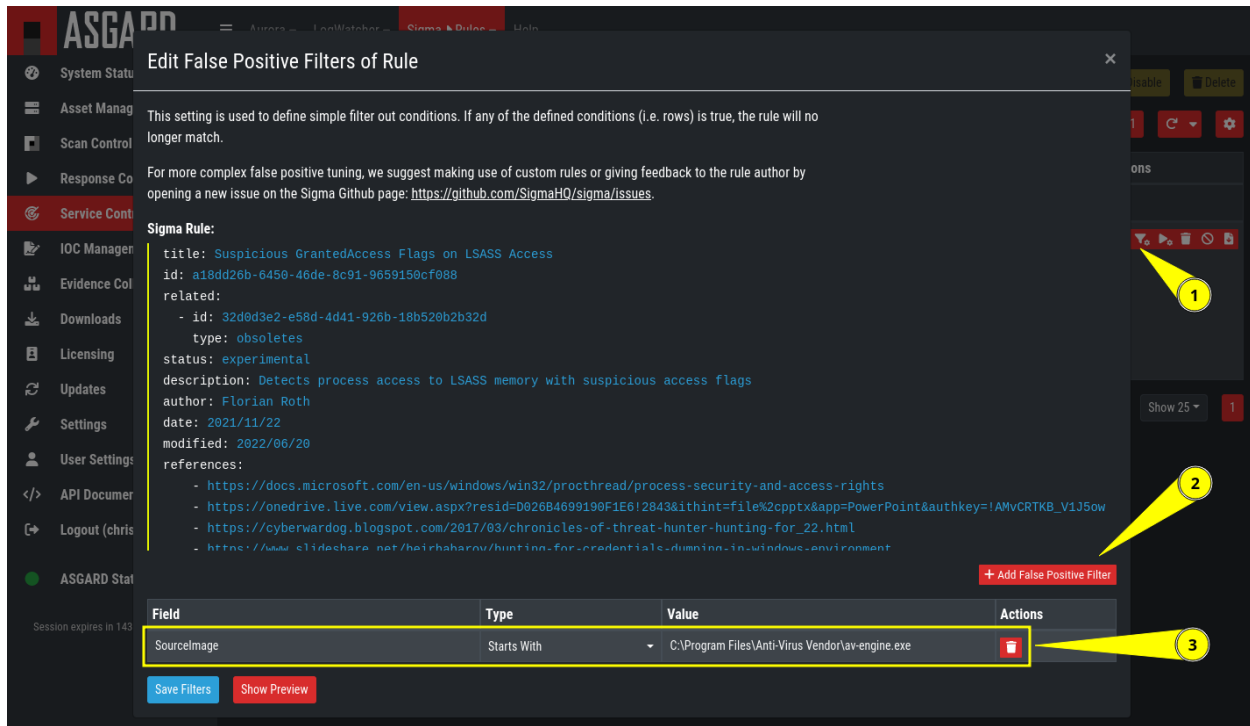


Fig. 47: Example of the false positive tuning of a Sigma rule

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.

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.

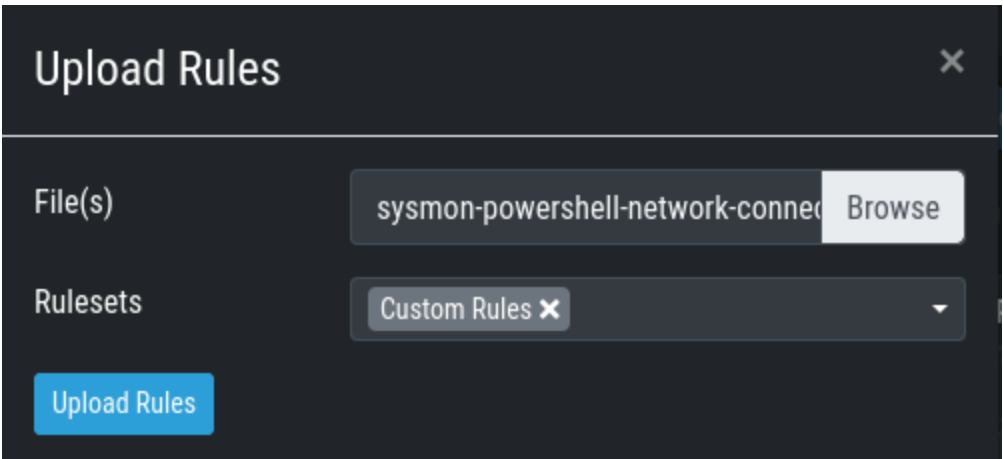


Fig. 48: Adding Custom Rules

Rule and Response Updates

If new rules or rule updates are provides 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.

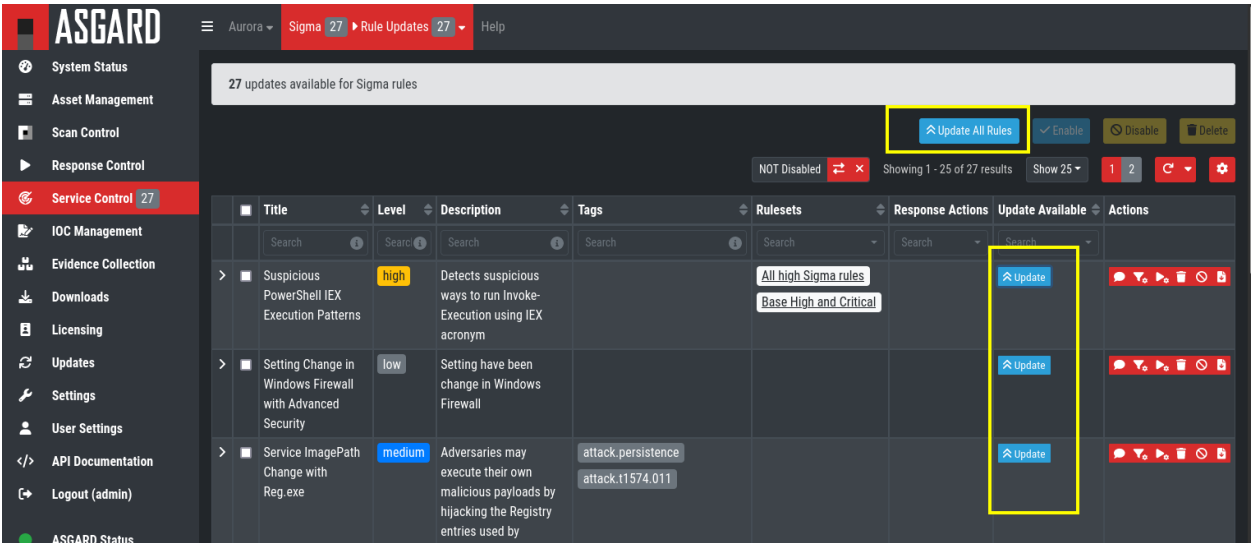


Fig. 49: Sigma Rule Updates for Aurora

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.

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.

Configuration	Configuration Settings	Number of Assets	Actions
Search			
> [Default] Standard configuration with critical and high Sigma rules	<div> <div>Agent</div> <div>Aurora Agent (Latest)</div> <div> <div>All critical Sigma rules</div> <div>All high Sigma rules</div> <div>Effective Rules and Response</div> </div> <div> <div>201</div> <div>678</div> <div>879</div> </div> <div> <div>5</div> <div>4</div> <div>9</div> </div> <div> <div>11</div> <div>8</div> <div>19</div> </div> </div>	2	
> [Default] Standard configuration with critical Sigma rules	<div> <div>Agent</div> <div>Aurora Agent (Latest)</div> <div> <div>All critical Sigma rules</div> <div>Effective Rules and Response</div> </div> <div> <div>201</div> <div>201</div> </div> <div> <div>5</div> <div>→</div> </div> <div> <div>11</div> <div>16</div> </div> </div>	0	

Fig. 50: 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.

In addition 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.

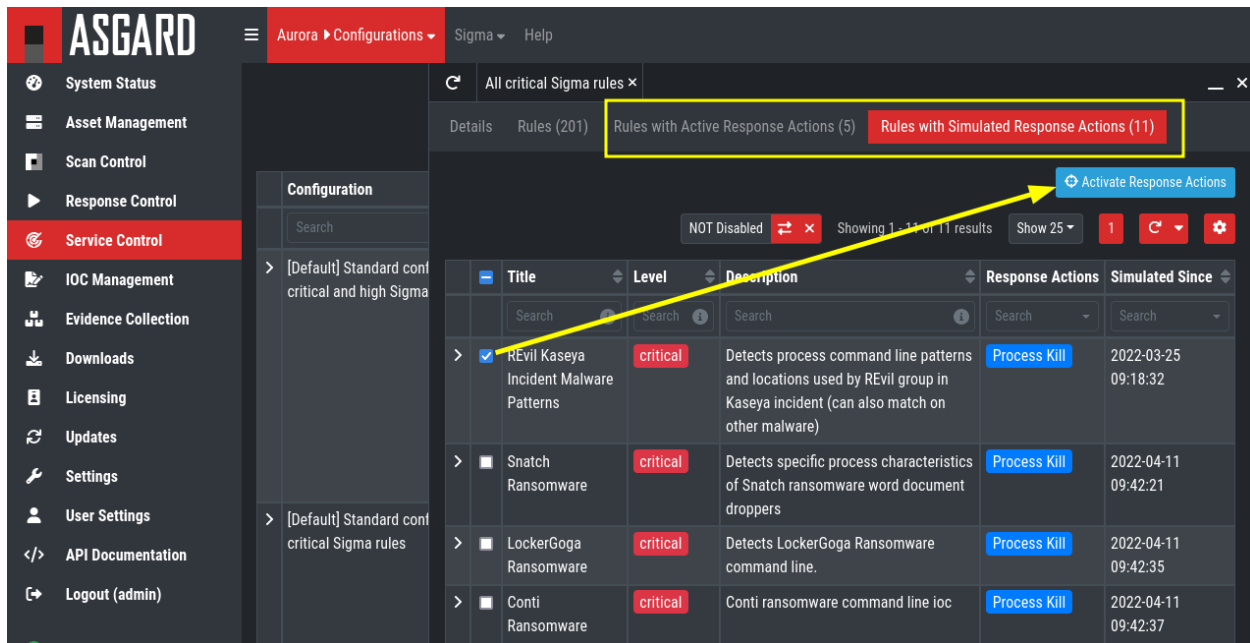


Fig. 51: Response Configuration in Rulesets

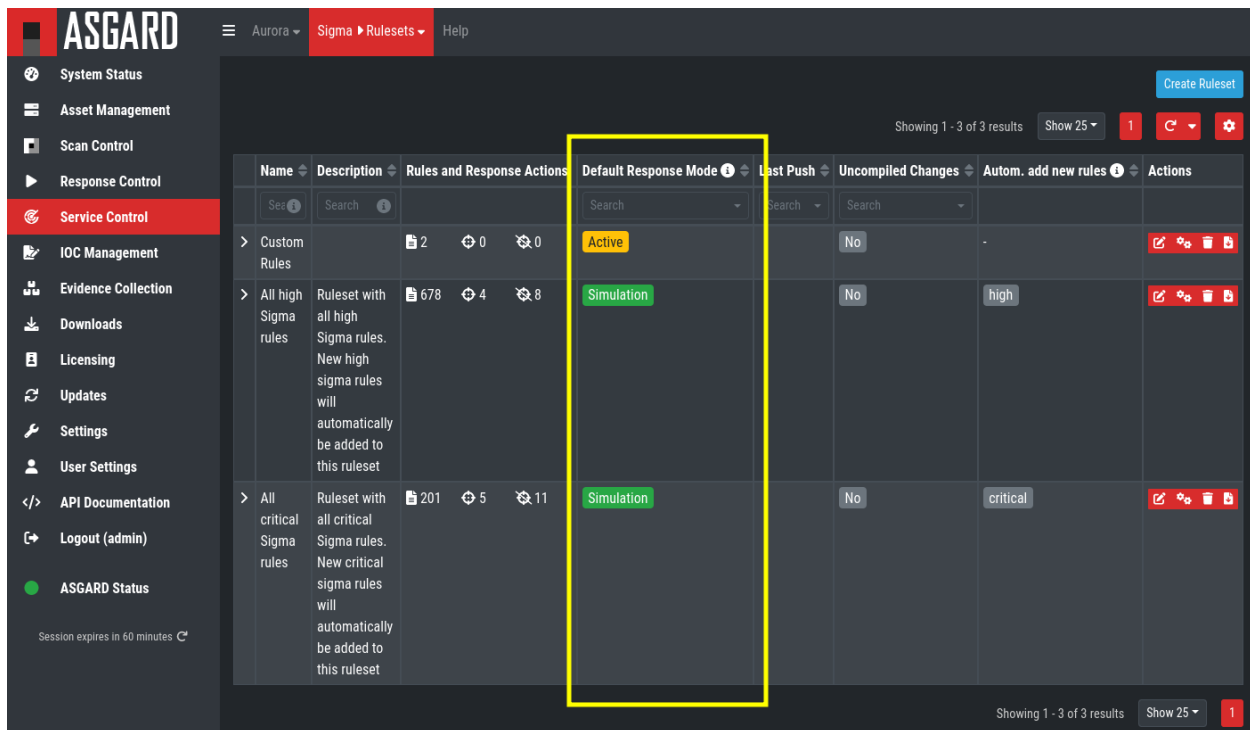


Fig. 52: Ruleset Default Response Mode

4.7.4 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 at aurora-agent-manual.nexttron-systems.com.

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.

Hostname	Last Seen	Labels	Deployed Configuration	Enabled	Active	Pending Changes	Actions
DESKTOP-SV334Q3	a few seconds ago	Client Germany R&D Windows x64	[Default] Standard configuration with critical and high Sigma rules	Yes	Yes	No	[Stop] [Refresh]
user-PC	a few seconds ago	Client Germany Windows x86	[Default] Standard configuration with critical and high Sigma rules	Yes	Yes	No	[Stop] [Refresh]

Fig. 53: Aurora Asset View

Deploy Aurora on Asset

Analogous you can 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.

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 asset, select it with the checkbox and use the **Enable** or **Disable** button or select the play or stop action icon on single assets.

Change Aurora Configuration

Showing 1 - 2 of 2 results Show 25 1

Assign	Configuration	Configuration Settings	Number of Assets
<div>></div> <div>Assign and Restart</div>	<div>Search</div> <div>[Default] Standard configuration with critical and high Sigma rules</div>	<div>Agent</div> <div>Aurora Agent (Latest)</div> <div>Sigma Rulesets</div> <div> <div>All critical Sigma rules</div> <div>All high Sigma rules</div> <div>Effective Rules and Response</div> </div> <div>IOC Rulesets</div> <div>MISP Rulesets</div> <div>Preset</div> <div>agent-config-standard.yml</div> <div>Options</div> <div>Activate Responses</div>	2
<div>></div> <div>Assign and Restart</div>	<div>[Default] Standard configuration with critical Sigma rules</div>	<div>Agent</div> <div>Aurora Agent (Latest)</div> <div>Sigma Rulesets</div> <div> <div>All critical Sigma rules</div> <div>Effective Rules and Response</div> </div> <div>IOC Rulesets</div> <div>MISP Rulesets</div> <div>Preset</div> <div>agent-config-standard.yml</div> <div>Options</div> <div>Simulate Responses</div>	0

Showing 1 - 2 of 2 results Show 25 1

Fig. 54: Change Aurora Service Configuration

Creating a Custom Aurora Service 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.

Add Configuration

Name: Aurora Workstations

Activate Responses ? ☐

Sigma Rulesets: All high Sigma rules × All critical Sigma rules × Custom Rules ×

IOC Rulesets (optional): (no signatures selected)

MISP Rulesets (optional): (no signatures selected)

Agent: Aurora Agent

Preset: agent-config-standard.yml ?

Options: (no options set)

Search Options

> Show Additional Options

Add Configuration

Fig. 55: Create a Custom Aurora Configuration

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 Excludes**

An overview over the top event producing processes is given on the bottom of the section. Another possibility is to *collect diagnostic packs of systems* in question and look in the `status.txt` at the event statistics by process.

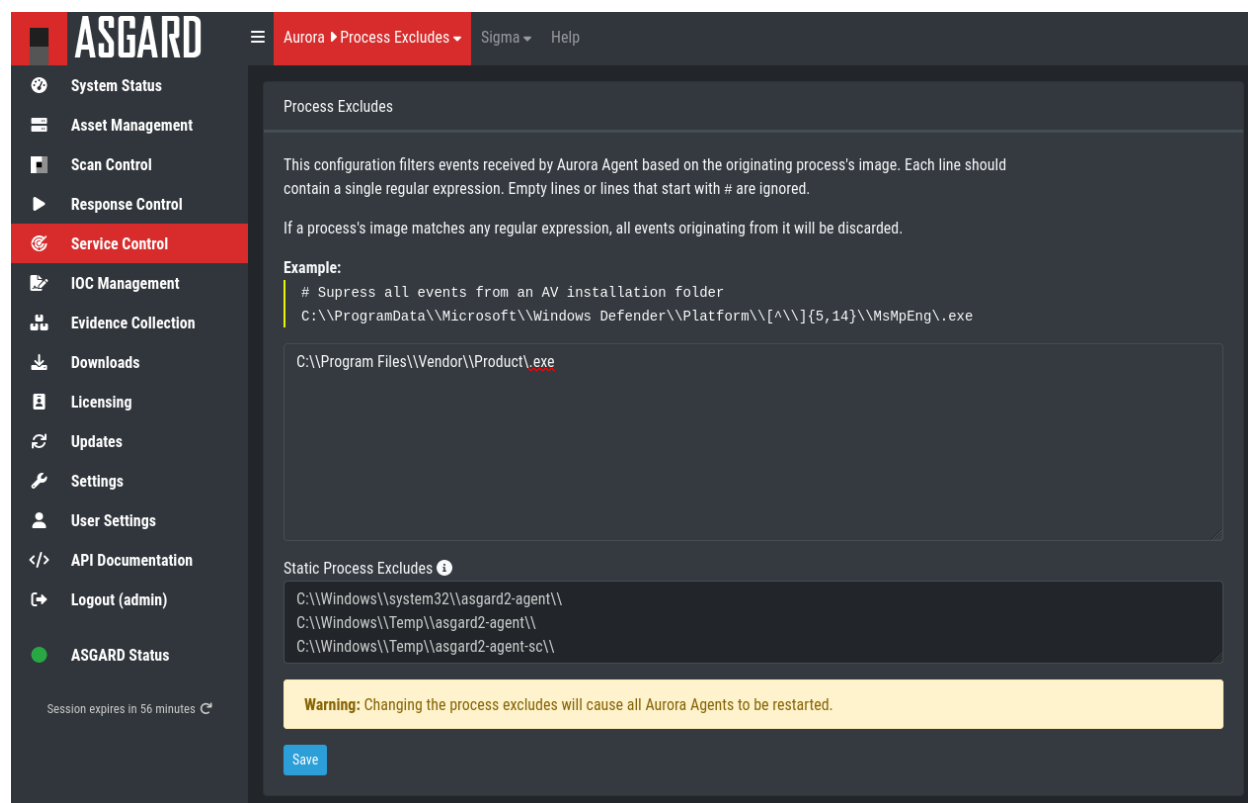


Fig. 56: Define Aurora Process Exclusion

False Positive Filters

If needed, false positives can be globally filtered 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.

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**.

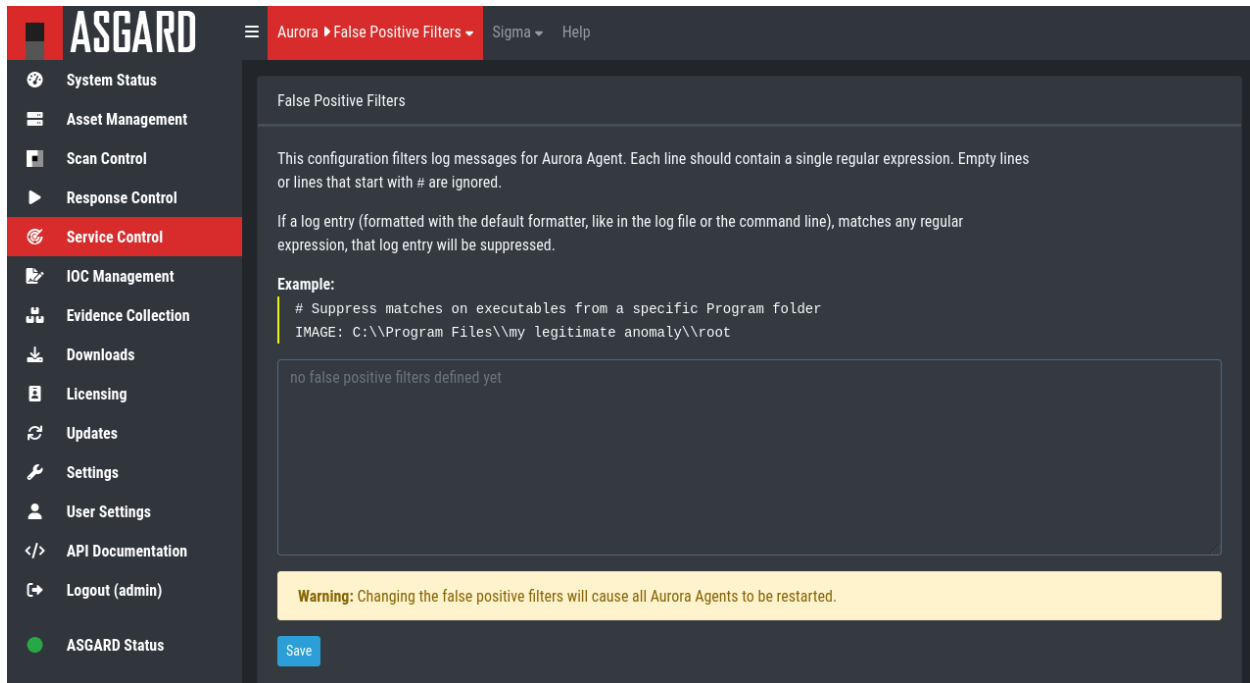


Fig. 57: Define Global Aurora False Positive Filters

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](#) on 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.
3. 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.

ASGARD

Aurora ▶ Response Action Logs ▼ Sigma ▼ Help

System Status
Asset Management
Scan Control
Response Control
Service Control
IOC Management
Evidence Collection
Downloads
Licensing
Updates
Settings
User Settings
API Documentation
Logout (admin)
ASGARD Status

Session expires in 58 minutes

Response Action Log Statistics

Events Today	0
Events Yesterday	0
Events Last 3 Days	0
Events Last 7 Days	0
Events This Week	0
Events Last Week	0
Events Last 4 Weeks	2
Events on desktop-sv334q3	1
Events on user-pc	1

Simulated Response Action Log Statistics

Events Today	0
Events Yesterday	0
Events Last 3 Days	0
Events Last 7 Days	0
Events This Week	0
Events Last Week	0
Events Last 4 Weeks	4
Events on desktop-sv334q3	2
Events on user-pc	2

Response Action Log

Mar 25 08:22:53 DESKTOP-SV334Q3 | AURORA: Info | MODULE: Sigma | MESSAGE: Executed response action | ACTION: kill | PROCESSES: 3272 / suspicious_shell.exe, 3904 / conhost.exe | RESPONSE_ORIGIN: inline | RULE: Renamed PowerShell | AURORA_EVENTID: 6000

Mar 25 08:22:30 user-PC | AURORA: Info | MODULE: Sigma | MESSAGE: Executed response action | ACTION: kill | PROCESSES: 3972 / suspicious_shell.exe | RESPONSE_ORIGIN: inline | RULE: Renamed PowerShell | AURORA_EVENTID: 6000

Simulated Response Action Log

Mar 25 08:27:58 user-PC | 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: 3496 / suspicious_shell.exe | RESPONSE_ORIGIN: inline | RULE: Renamed PowerShell | AURORA_EVENTID: 6001

Mar 25 08:27:44 DESKTOP-SV334Q3 | 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: 3420 / suspicious_shell.exe, 5204 / conhost.exe | RESPONSE_ORIGIN: inline | RULE: Renamed PowerShell | AURORA_EVENTID: 6001

Mar 25 08:27:56 user-PC | 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: 3496 / suspicious_shell.exe | RESPONSE_ORIGIN: inline | RULE: Renamed PowerShell | AURORA_EVENTID: 6001

Mar 25 08:27:43 DESKTOP-SV334Q3 | 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: 3420 / suspicious_shell.exe, 5204 / conhost.exe | RESPONSE_ORIGIN: inline | RULE: Renamed PowerShell | AURORA_EVENTID: 6001

Fig. 58: Aurora Response Action Logs

ASGARD

Aurora ▶ Asset View (Deployed) ▼ LogWatcher ▼ Sigma ▼ Help

Change Aurora Configuration Remove Aurora Enable Disable

Show: Active Only Showing 1 - 1 of 1 results Show 25 ▼ 1

Asset Details

Hostname	Last Seen	Labels	Deployed Configuration	Enabled	Active	Pending Changes	Actions
workstation-03	a few seconds ago	Windows Workstations tenant1	[Default] Standard configuration with critical and high Sigma rules	Yes	Yes	No	

Showing 1 - 1 of 1 results Show 25 ▼ 1

Fig. 59: Aurora Service Successfully Deployed

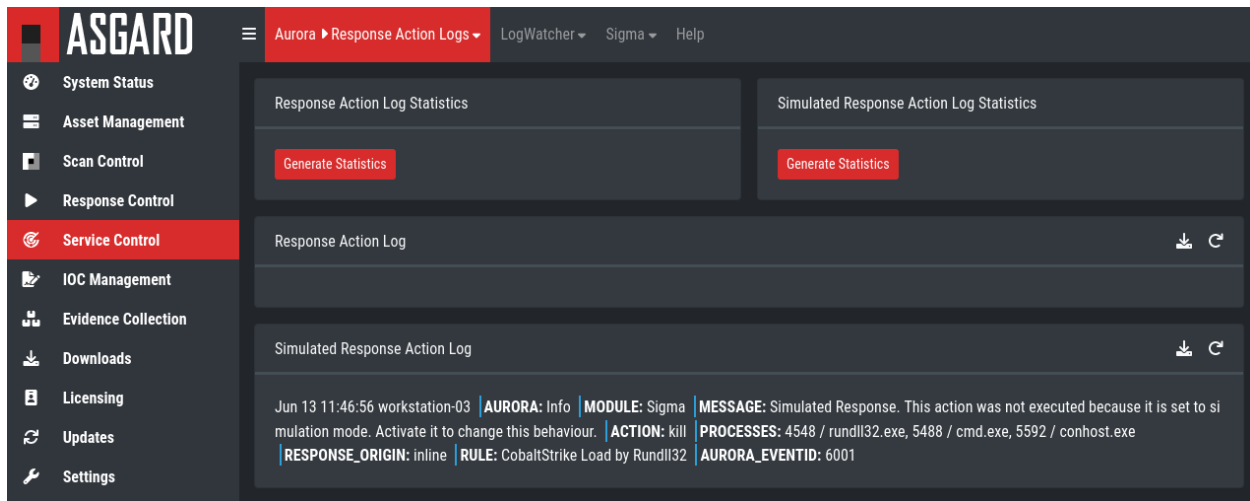


Fig. 60: Aurora Simulated Response Action

4.7.5 LogWatcher Service

The LogWatcher real-time service monitors the Windows Event Log using predefined rules in the Sigma format and creates an alert that is forwarded to ASGARD Analysis Cockpit if a match was found. The LogWatcher service is no longer shown by default on newly installed ASGARDs. To enable it go to **Settings > Advanced** and enable the **Show LogWatcher** checkbox.

Prerequisites

In order to make full use of ASGARD LogWatcher you need a Windows Audit Policy and Sysmon, both with a reasonable configuration, in place. We expect organizations to take care of providing a sane configuration by their own. This section helps in giving starting points, if needed.

Windows Audit Policy

The default audit policy of Windows is not suitable for security monitoring and needs to be configured. There are Microsoft recommendations available [online](#).

Also auditing the command line for process creation events should be enabled. Documentation for that task is available [here](#).

Sysmon Configuration Template

There are some best practice configurations available. See them as a good starting point to develop your own configuration. If you do not have a Sysmon configuration yet, there are several options we suggest:

1. The Nextron Systems fork of SwiftOnSecurity's [sysmon-config](#)
2. The [SwiftOnSecurity sysmon-config](#)
3. Olaf Hartong's [sysmon-modular](#)

In general we suggest our own configuration, as we test our rules with it and include changes from the upstream configuration. But depending on your preferences, either of those listed configurations is a good starting point for writing your own configuration.

Warning: Do not deploy those configurations to your production environment without prior testing.

It is expected that some tools you use will be the source of huge log volume and should be tuned in the configuration depending your environment.

Sysmon Installation

Sysmon is part of Microsoft Sysinternals and therefore has to be installed as a third party tool. The preferred way to distribute Sysmon and its configuration is using your organization's device management. If you do not have access to one, you can use ASGARD's playbook feature to distribute Sysmon and update its configuration. Documentation which describes the playbook creation and that offers maintenance scripts can be found in our [asgard-playbooks repository](#).

Operation

This chapter explains how to configure LogWatcher using Sigma rules.

LogWatcher Overview

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

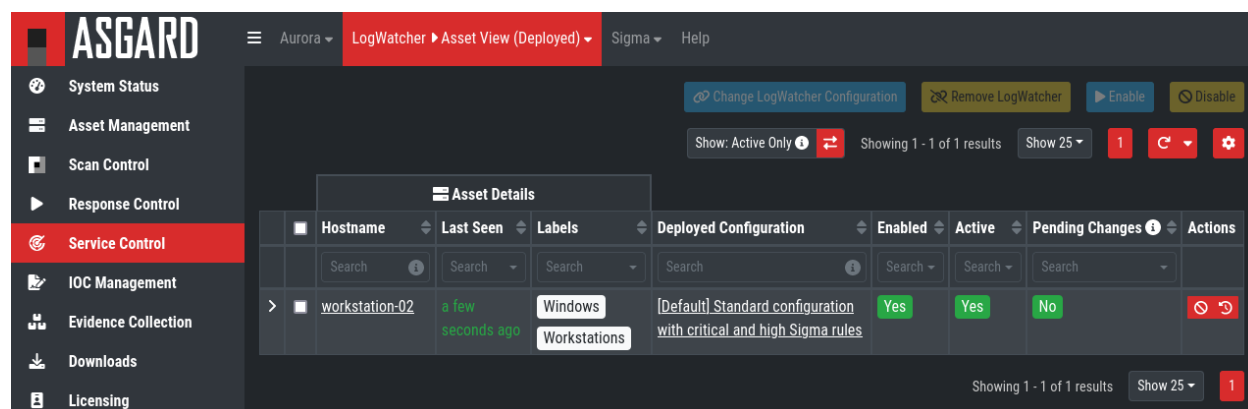


Fig. 61: LogWatcher Asset View

Analogous you can see an overview of all assets without an installed LogWatcher under Service Control > LogWatcher > Asset View (Not Deployed).

Enable Service for an Asset

To enable the LogWatcher service for an asset, navigate to Service Control > LogWatcher > Asset View, select the asset's checkbox and choose Assign Configuration. Then choose the desired service configuration by clicking Assign.

Assign Configuration

Showing 1 - 2 of 2 results
Show 25
1
Refresh
Settings

Assign	Name	Settings
<div> Assign </div>	Exchange Server	<div> Sigma Rulesets Custom Rules Exchange Server Base High and Critical </div> <div> Channels MSEExchange Management Microsoft-Windows-Sysmon/Operational Security Application Microsoft-Windows-PowerShell/Operational System </div> <div> Throttle 5 per minute </div>
<div> Assign </div>	Base Windows	<div> Sigma Rulesets Base High and Critical Custom Rules </div> <div> Channels Application Microsoft-Windows-PowerShell/Operational Microsoft-Windows-Sysmon/Operational Security System </div> <div> Throttle 5 per minute </div>

Showing 1 - 2 of 2 results
Show 25
1

Fig. 62: Enable a Service Configuration

Creating a Custom Logwatcher Service Configuration

A service configuration is used to group assets of similar type and assign them a set of rules (in form of rulesets).

Go to **Service Control > LogWatcher > Configurations > Add Configuration**, enter a name and add the rulesets that should apply for this service configuration (i.e. group of assets).

Fig. 63: Create a Service Configuration

If you have not configured a ruleset yet, you need to do so beforehand.

4.8 IOC Management

4.8.1 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.

Fig. 64: Add 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.

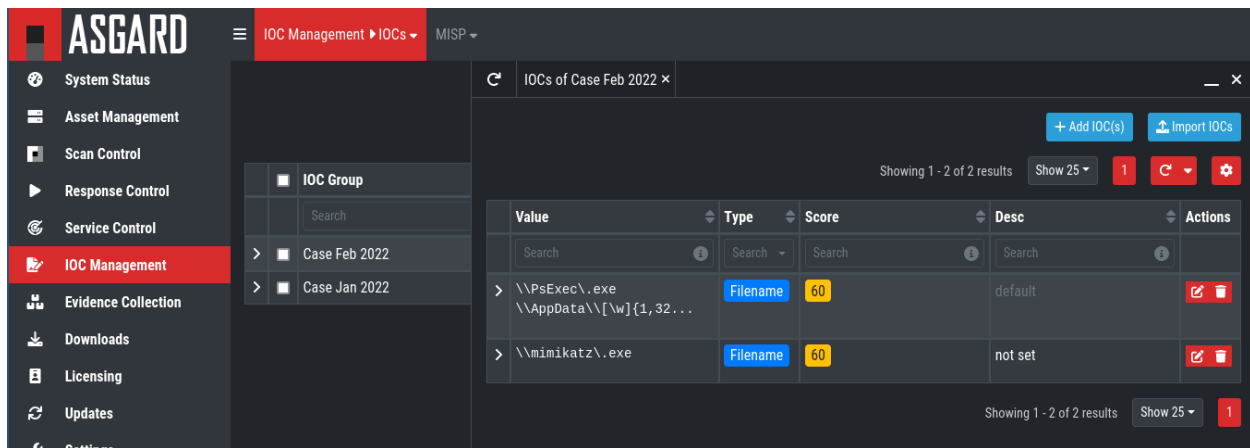


Fig. 65: Imported IOCs Overview

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.

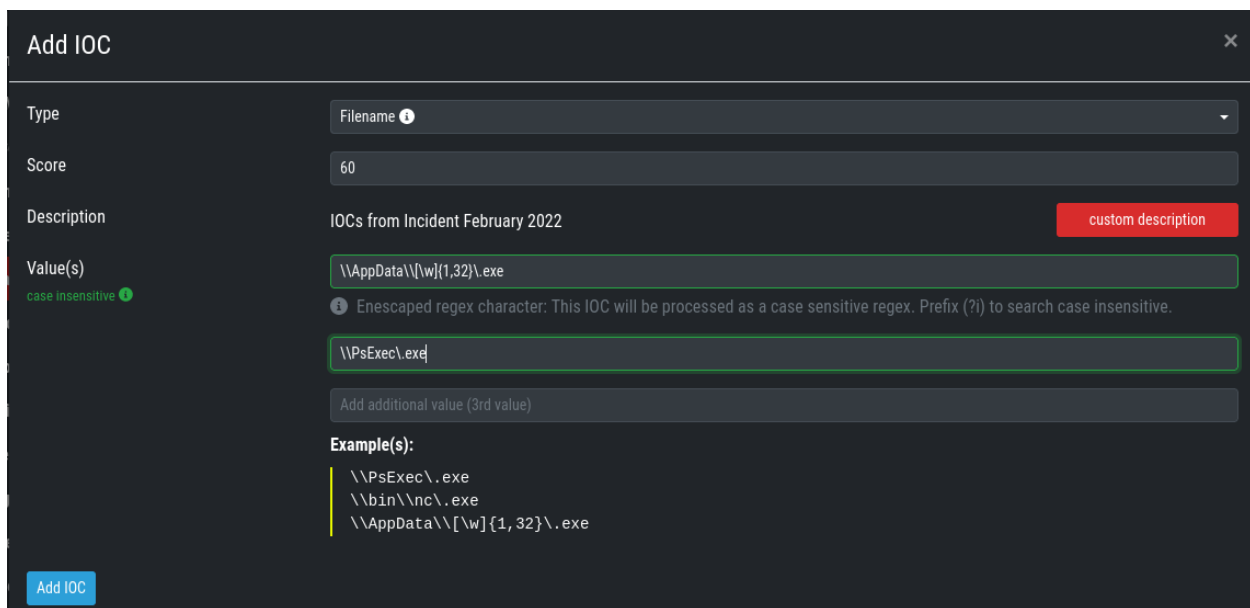


Fig. 66: Add IOCs

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.

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.

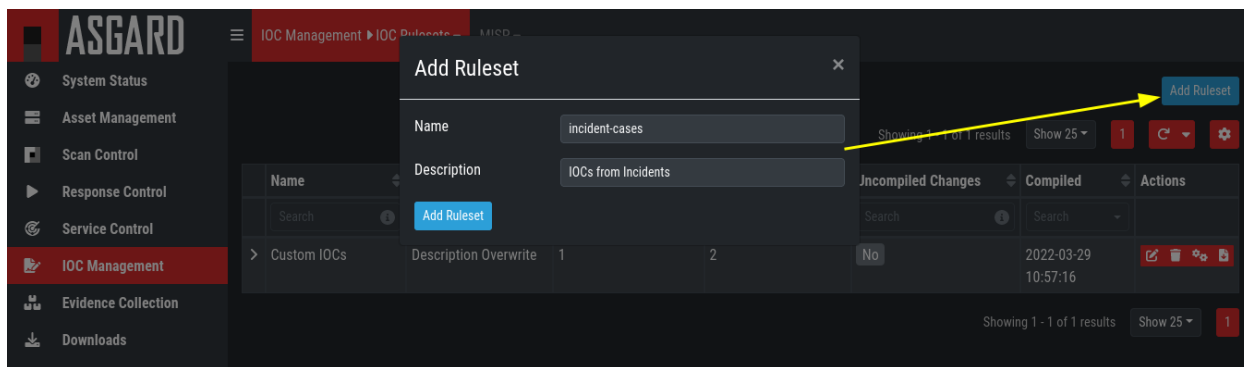


Fig. 67: Add Ruleset

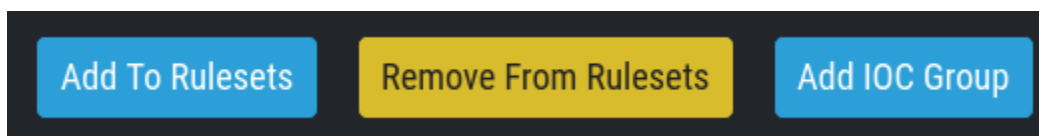


Fig. 68: Buttons to Add/Remove IOC Groups

4.8.2 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.

4.8.3 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.

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.

×

Add Group Scan

Description (optional)

Scan with Custom IOSs

Scan Target ⓘ (optional)

(no labels selected) ▾

Advanced

Expires ⓘ

2022-12-01 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 ⓘ ▾

IOC Rulesets (optional)

IOC Ruleset Cases ×

IOC Ruleset nmap ×

▾

MISP Rulesets (optional)

(no signatures selected) ▾

Scan Template ⓘ (optional)

no scan template ▾

Flags

–customonly –syslog %asgard-host%

cus

–customonly ⓘ

☒

☆

Add Group Scan

Add and Activate Group Scan

Fig. 69: Select Ruleset while creating a scan job

Info	Date	Published	Threat Level	Org	Tags	Rulesets
Testing Filename Prefix	2022-03-28 02:00:00	Yes	High	ORNAME		
Test Event	2022-03-28 02:00:00	No	Low	ORNAME		
Suspicious Shell (just a test)	2022-03-28 02:00:00	Yes	High	ORNAME	Just-A-Test	Testing MISP (manual) Testing MISP (auto compile)
Marcel Test 1	2022-03-07 01:00:00	No	High	ORNAME		
[ESET] IsaacWiper and Hermeti cWizard: New wiper and worm t argeting Ukraine	2022-03-02 01:00:00	Yes	Undefined	CERT-FR_1510	tlp:white fr-classif:non-classifieds="NON-CLASSIFIEDS" cossi:TLP="white" cossi:RechercheSourceOuverte="Autorisee"	
[NCS-CUK] Cyclops blink	2022-02-23 01:00:00	Yes	Undefined	CERT-FR_1510	tlp:white misp-galaxy:threat-actor="TeleBots" fr-classif:non-classifieds="NON-CLASSIFIEDS" cossi:TLP="white" cossi:RechercheSourceOuverte="Autorisee" misp-galaxy:threat-actor="IRIDIUM" misp-galaxy:threat-actor="Sandworm" misp-galaxy:threat-actor="ELECTRUM"	
[CERT-FR] Campagnes d'hameç onnage du mode opératoire d'at taquants Nobelium	2021-11-02 01:00:00	Yes	Undefined	CERT-FR_1510	tlp:white fr-classif:non-classifieds="NON-CLASSIFIEDS" cossi:TLP="white" cossi:RechercheSourceOuverte="Autorisee" cossi:fiabilite="Bonne"	
gsocket.io - Global Socket Rela y Network (GSRN) - infrastru ctu re	2022-03-01 01:00:00	Yes	Undefined	CIRCL	type:OSINT tlp:white adversary:infrastructure-state="active" osint:lifetime="perpetual" osint:certainty="50"	
CISA - Malware Analysis Report (AR22-055A) - MAR-10369127 -1.v1 - MuddyWater	2022-02-22 01:00:00	Yes	Medium	CIRCL	type:OSINT tlp:white osint:lifetime="perpetual" misp-galaxy:threat-actor="MuddyWater" misp-galaxy:mitre-enterprise-attack-intrusion-sets="MuddyWater - G0069" misp-galaxy:country="iran"	
HermeticWiper	2022-02-25 01:00:00	Yes	High	SCITF	tlp:white	

Fig. 70: MISP events

Add MISP Ruleset

Name: All MISP Events

Types: filename, filepath, ip-dst, domain, hostname, yara, sigma, md5, sha1, sha256

Auto Compile: ☒

Add

Showing 1 - 1 of 1 results

Types	Actions
domain, hostname, ip-dst, sha256	

Showing 1 - 1 of 1 results

Fig. 71: 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.

Add Group Scan [X]

Description: Example: Scan with MISP Events

Asset Labels ⓘ: Windows (7 assets) X

Limit ⓘ: 0

Rate: 2 per minute

Expires ⓘ: 2022-01-31 16:00:00

Scheduled Start: Select a date for scheduled start (optionally) [Clear]

Max. Runtime ⓘ: 4 days

Scanner: THOR ⓘ 10.6

IOC Rulesets: (no signatures selected)

MISP Rulesets: ALL MISP Events X

Scan Template ⓘ: Default Scan Template

Flags: --quick --syslog %asgard-host%

Fig. 72: Adding a MISP Ruleset to a 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
- 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.

4.9 Evidence Collection

4.9.1 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.

4.9.2 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.

4.10 Generate 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.

- System Status
- Asset Management
- Scan Control
- Response Control
- Service Control
- IOC Management
- Evidence Collection**
- Downloads
- Licensing
- Updates
- Settings
- User Settings
- API Documentation
- Logout (christian)
- ASGARD Status

Session expires in 1440 minutes

Collected Evidences

Bifrost Quarantine

Showing 1 - 10 of 14 results

Show 10

1 2

⌵

⚙️

Path	Size	Hostname	Type	SHA256	Actions
> C:\Windows\System32\winevt\Logs\Windows PowerShell.evtx	5 MB	workstation-01	Bifrost	ac5ff533d7b499ea817c1939da5d4cb9c53f6596d9d33681f3c62d2b1ce87b62	
> C:\Windows\System32\winevt\Logs\Microsoft-Windows-PowerShell%4Operational.evtx	16 MB	workstation-01	Bifrost	a8ae3ba8f4ba68066c11e42db371b14b8d6ddbf5756859361dafc4865acce177	
> C:\Users\user-workstation\Tools\mimikatz_trunk\x64\mimilib.dll	58 KB	workstation-01	Bifrost	fc77b7dc19250416baf67ae9f87e8Sebad700032b0d437c0bc2176b2585fca95	
> C:\Users\user-workstation\Tools\mimikatz_trunk\x64\mimidrv.sys	37 KB	workstation-01	Bifrost	2ff4c6949bab3ffb8c95b21f9c5eb597b93af66e3bf635ba2bf92fd534e995b	
> C:\Users\user-workstation\Tools\mimikatz_trunk\Win32\mimispool.dll	30 KB	workstation-01	Bifrost	9e49c482faf12eae6c2f5724c083e35de138b15d2c593db2398577ebd6dfd33	
> C:\Users\user-workstation\Tools\mimikatz_trunk\Win32\mimilove.exe	45 KB	workstation-01	Bifrost	2a74704d6eb53e9a97c063f182021c51b5f687882227902e020ac82f45ab1e4c	
> C:\Users\user-workstation\Tools\mimikatz_trunk\Win32\mimilib.dll	52 KB	workstation-01	Bifrost	77cfad99621ef6951ec4809a6641e2d7623238b66afa3f6e993703eeff161da6	
> C:\Users\user-workstation\Tools\mimikatz_trunk\Win32\mimikatz.exe	1 MB	workstation-01	Bifrost	a0010bd12872028ba8a53276313527fa332a23d4cdd0caed1060a45916e8cb4	
> C:\Users\user-workstation\Tools\mimikatz_trunk\Win32\mimidrv.sys	31 KB	workstation-01	Bifrost	9f7bb583f87b8cfc56d4319cdcf865c0db77a0f2110f87d5c694c7f7a0e514	
> C:\Users\user-workstation\Desktop\evillog	21 B	workstation-01	Bifrost	7b18427410e6c01b0db57fa47b58f7a877f689486c4393c14b5bb8e9c30ef7e2	

Showing 1 - 10 of 14 results

Show 10

1 2

⌵

⚙️

Fig. 73: Collected Evidence List

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.

4.10.1 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.

4.10.2 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...
```

4.10.3 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"
$Download_Url = "https://asgard2.nextron:8443/api/v1/downloads/thor?os=windows&type=$((
    ↪$Type)&scanner=thor10%4010.6&signatures=signatures&hostname=$(( $Hostname )&token=$((
    ↪$Token )"
```

4.11 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 or LogWatcher 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.

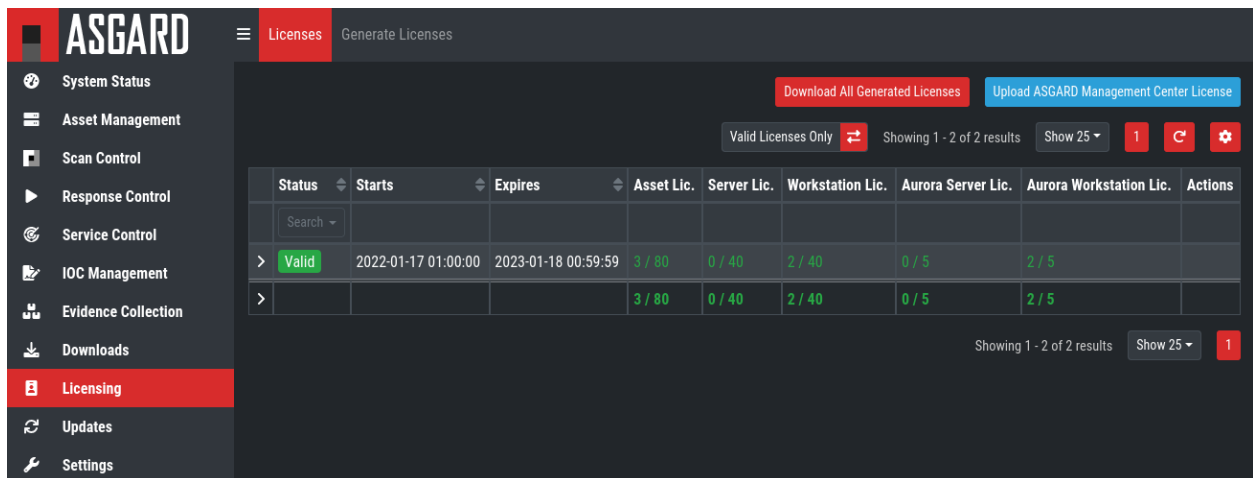


Fig. 76: ASGARD licensing

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

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).

4.12 Updates

4.12.1 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.

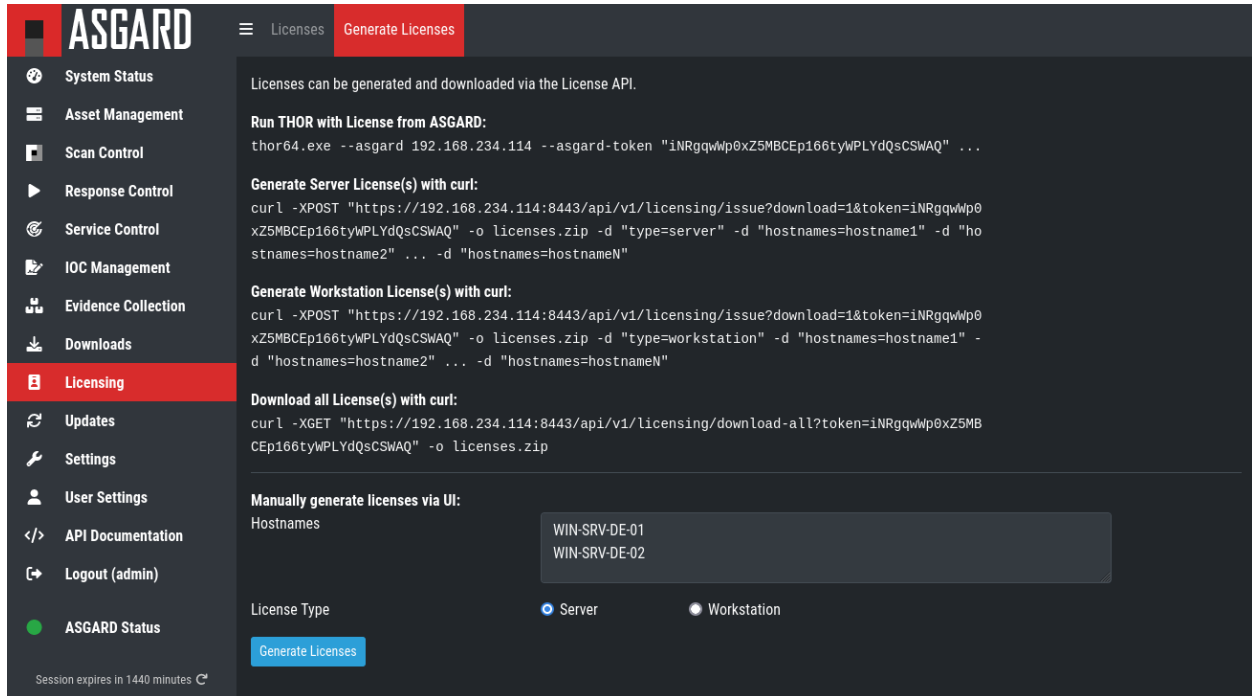


Fig. 77: Generate licenses

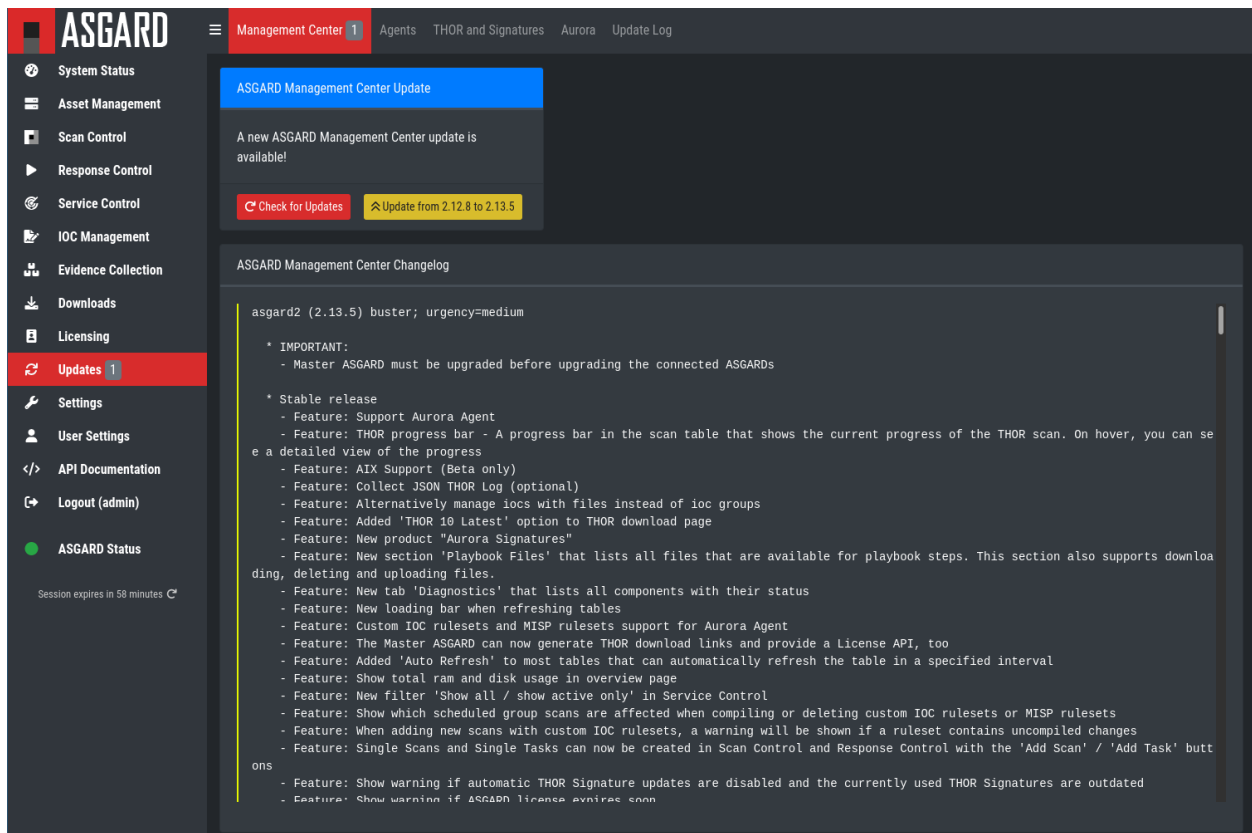


Fig. 78: Updating ASGARD

4.12.2 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	10.6.14	2022-03-24 11:29:05	10.6.14	2022-03-24 11:29:05	2022-04-12 02:00 [repeat daily]	[Pencil] [Delete]
THOR 10.6 for Linux	10.6.14	2022-03-24 11:26:42	10.6.14	2022-03-24 11:26:42	2022-04-12 02:00 [repeat daily]	[Pencil] [Delete]
THOR 10.6 for MacOS	10.6.14	2022-03-24 11:25:42	10.6.14	2022-03-24 11:25:42	2022-04-12 02:00 [repeat daily]	[Pencil] [Delete]
THOR 10.5 for Windows	10.5.18	2022-03-24 11:28:38	10.5.18	2022-03-24 11:28:38	2022-04-12 02:00 [repeat daily]	[Pencil] [Delete]
THOR 10.5 for Linux	10.5.18	2022-03-24 11:26:13	10.5.18	2022-03-24 11:26:13	2022-04-12 02:00 [repeat daily]	[Pencil] [Delete]
THOR 10.5 for MacOS	10.5.18	2022-03-24 11:25:28	10.5.18	2022-03-24 11:25:28	2022-04-12 02:00 [repeat daily]	[Pencil] [Delete]
THOR Lite 10.7 for Windows	10.7.1	2022-03-24 11:28:12	10.7.1	2022-03-24 11:28:12	2022-04-12 02:00 [repeat daily]	[Pencil] [Delete]
THOR Lite 10.7 for Linux	10.7.1	2022-03-24 11:27:18	10.7.1	2022-03-24 11:27:18	2022-04-12 02:00 [repeat daily]	[Pencil] [Delete]
THOR Lite 10.7 for MacOS	10.7.1	2022-03-24 11:24:37	10.7.1	2022-03-24 11:24:37	2022-04-12 02:00 [repeat daily]	[Pencil] [Delete]
THOR TechPreview 10.7 for Windows	10.7.1	2022-03-24 11:27:55	10.7.1	2022-03-24 11:27:55	2022-04-12 02:00 [repeat daily]	[Pencil] [Delete]

Fig. 79: 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.

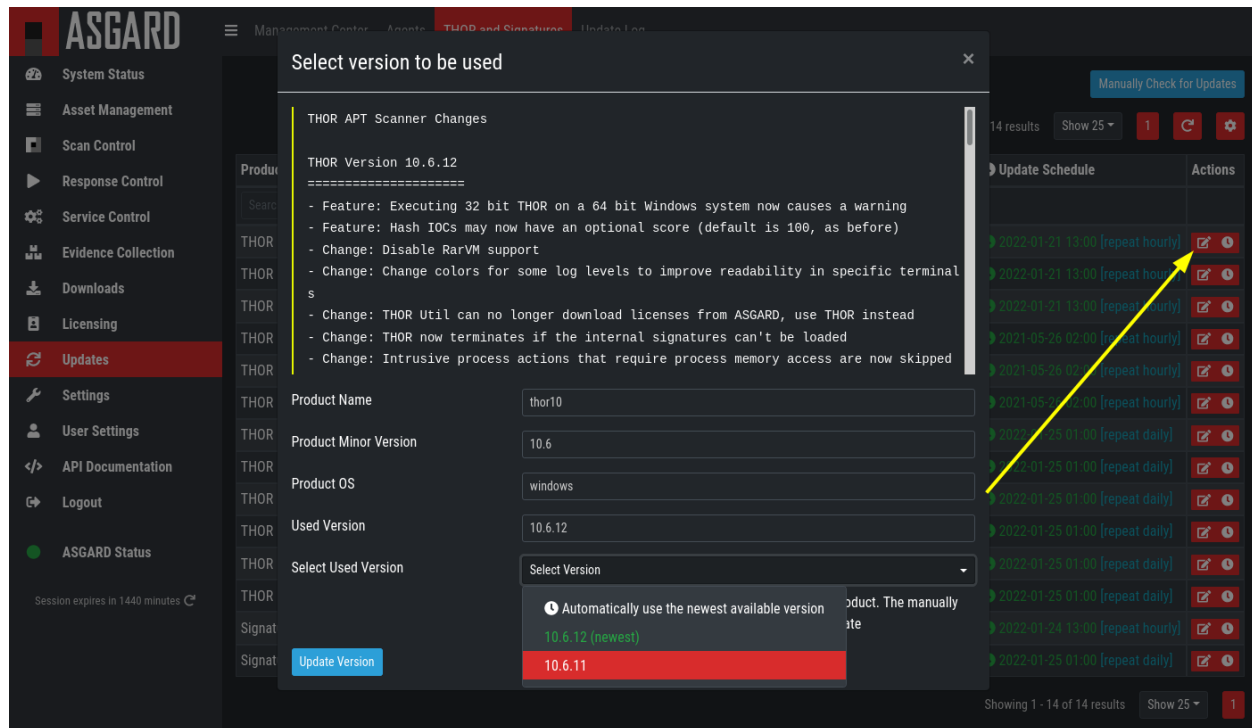


Fig. 80: Selecting a Scanner Version manually

4.12.3 Agent Updates

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

4.13 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.

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.

4.13.1 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.

ASGARD

Management Center **Agents** 1 THOR and Signatures Update Log

- Feature: Support for ARM64 MacOS
- Fix: Improved stability of task executions on clients with an EDR installed
- Fix: Gracefully shutdown running tasks on os signals
- Fix: Improved stability of config file on system crash

-- Nextron Systems GmbH <support@nextron-systems.com> Mon, 8 Nov 2021 06:59:00 +0100

asgard2-agent (1.4.3) stable; urgency=medium

- * Stable release
- Change: Rebuilt agent with newest Golang Version
- Change: Removed code fragments used for service controller

-- Nextron Systems GmbH <support@nextron-systems.com> Mon, 6 Sep 2021 12:19:00 +0200

asgard2-agent (1.4.2) stable; urgency=medium

- * Stable release
- Change: Signed MacOS binaries with a new certificate
- Fix: In some cases the ASGARD Agents sent many DNS requests for a few seconds
- Fix: Fixed non-starting task after module version upgrade in some cases

Service Controller Changelog:

asgard2-service-controller (2.0.6) stable; urgency=medium

- * Stable release
- Change: Increased max. offline mode time from 4 to 14 days
- Bugfix: Improved stability in offline mode
- Bugfix: Fixed sporadically service restarts due to connectivity issues

-- Nextron Systems GmbH <support@nextron-systems.com> Thu, 9 Dec 2021 09:42:00 +0100

asgard2-service-controller (2.0.5) stable; urgency=medium

- * Initial release

-- Nextron Systems GmbH <support@nextron-systems.com> Thu, 11 Nov 2021 16:38:00 +0100

Asset Update (ASGARD Agent)	Asset Update (ASGARD Service Controller)	Agent Installer Update
All active assets are up-to-date.	All active assets are up-to-date.	<p>Note: There is an agent update available for at least one Agent installer. The Agent Installers should be rebuilt with the asgard2-repacker. See asgard2-repacker --help or ASGARD Manual for more information.</p> <p>Repack Agent Installers Ignore this update</p>

Fig. 81: Update Agent

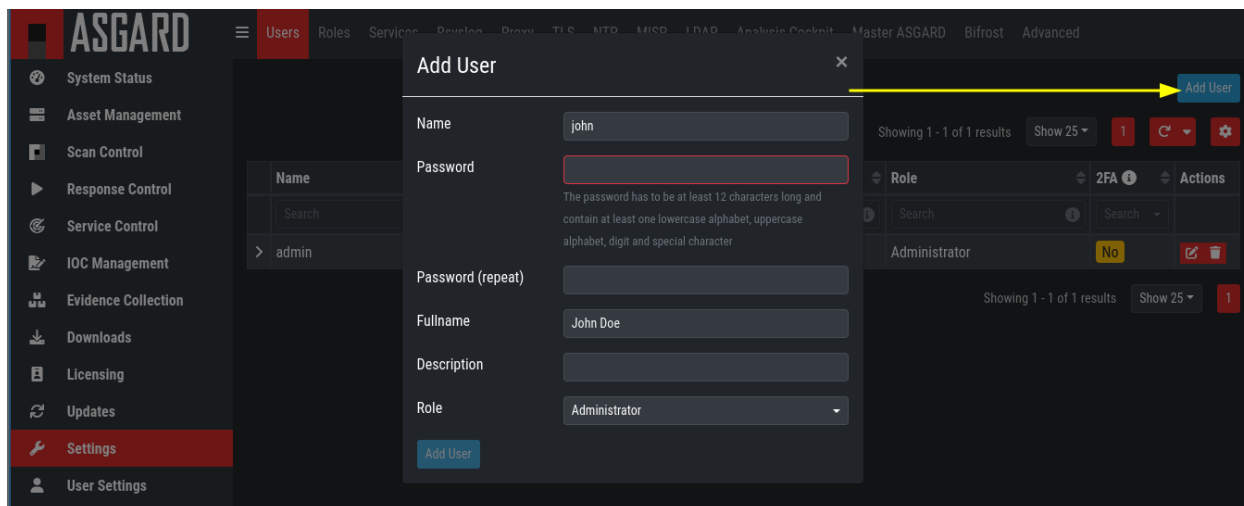


Fig. 82: Add User Account

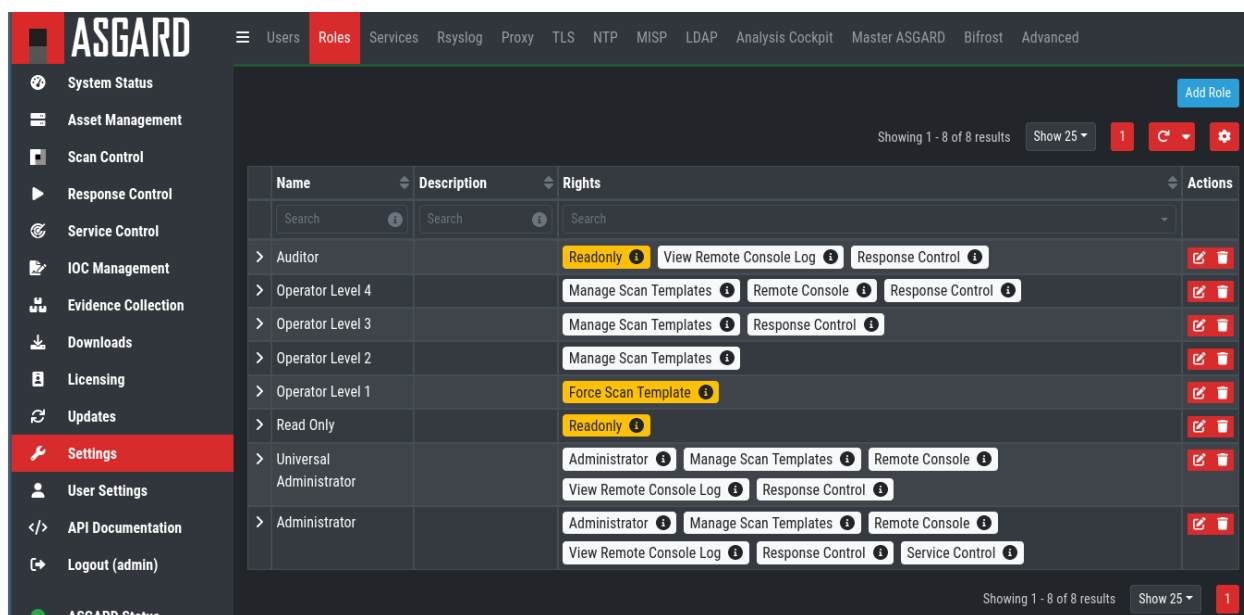


Fig. 83: User Roles – Factory Defaults

4.13.2 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 or LogWatcher

4.13.3 Restrictions

Role	Restrictions
Force Scan Template ²	Force user to use predefined scan templates that are not restricted
No Inactive Assets ^{Page 98, 2}	Cannot view inactive assets in asset management.
No Task Start ²	Cannot start scans or task (playbooks)
Readonly ²	Can't change anything, can't run scans or response tasks. Used to generate read-only API keys

4.13.4 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 the following fields and controls:

- Host:** Text input field containing 'dc.adt.local'.
- Port:** Text input field containing '389'.
- Use SSL:** A checkbox that is currently unchecked.
- Skip TLS:** A checkbox that is currently checked.
- Server Name:** Text input field containing 'dc.adt.local'.
- Test Connection:** A red button labeled 'Test Connection'.

Fig. 84: Configure the LDAP Server

² Restricted Roles have a yellow font in the UI

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 ASGARD configuration interface. It includes a 'Bind User' field with the value 'CN=adapi adapi,CN=Users,DC=adt,DC=local', a 'Bind Password' field with masked characters, and a red 'Test Bindings' button.

Fig. 85: 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.

The screenshot shows the 'Base' and 'Users and Groups' configuration sections. The 'Base' section has a 'Base' field with 'DC=adt,DC=local'. The 'Users and Groups' section includes a 'Use recommended filters' dropdown set to 'Microsoft Active Directory', 'User Filter' with '(&(objectClass=user)(objectCategory=user)(sAMAccountName=%s))', 'Group Filter' with '(&(objectCategory=group)(objectClass=group)(member=%s))', 'User UID' with 'dn', and 'Group GID' with 'cn'. There is a 'Test Login' button and a success message: 'The login was successful and the following groups for this user have been found: Administrators, ASGARD-Admins'. An 'Update LDAP Config' button is at the bottom left.

Fig. 86: Configure the LDAP User and Group Filters

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 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.

The screenshot shows the 'LDAP Roles' configuration page. At the top right is a blue 'Add LDAP Role' button. Below it, a status bar indicates 'Showing 1 - 2 of 2 results' with a 'Show 25' dropdown and a red button with the number '1'. The main table has four columns: 'Group', 'Role', 'Rights', and 'Actions'. Each of the first three columns has a search bar with an information icon. The table contains two rows:

Group	Role	Rights	Actions
ASGARD-Admins	Administrator	Admin, ManageScanTemplates, RemoteConsole, RemoteConsoleProtocol, ResponseControl, ServiceControl	[Trash Icon]
RDAdmin	Administrator	Admin, ManageScanTemplates, RemoteConsole, RemoteConsoleProtocol, ResponseControl, ServiceControl	[Trash Icon]

At the bottom right, another status bar shows 'Showing 1 - 2 of 2 results' with a 'Show 25' dropdown and a red button with the number '1'.

Fig. 87: LDAP Group to ASGARD Role Mapping

4.14 Additional Settings

4.14.1 Rsyslog Forwarding

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

The following log sources can be forwarded individually:

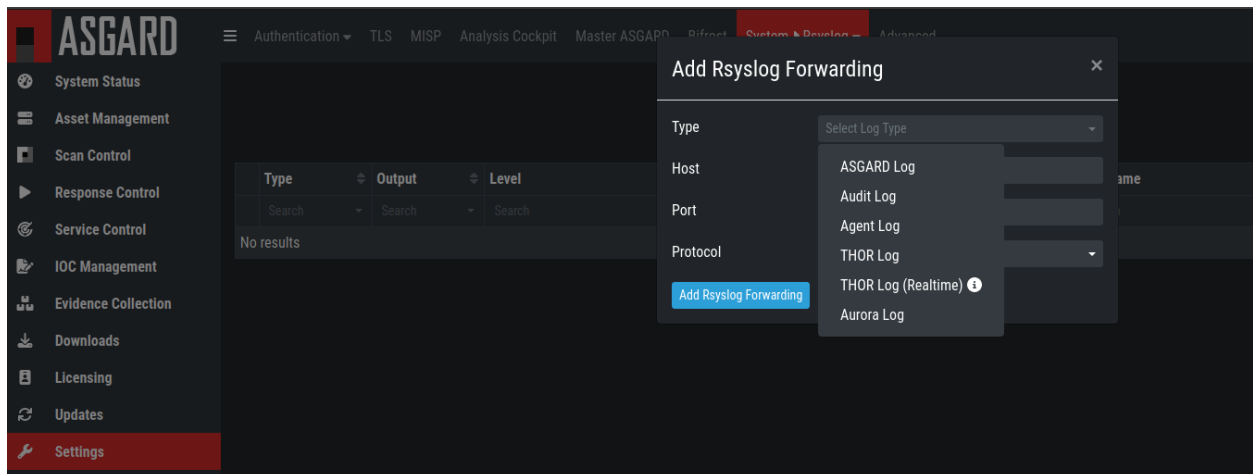


Table 1: Available Log Sources

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 Syslog Forwarding). Make sure the necessary firewall rules are in place to allow the asset to communicate with the ASGARD.
Aurora Log	Aurora Logs

4.14.2 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.

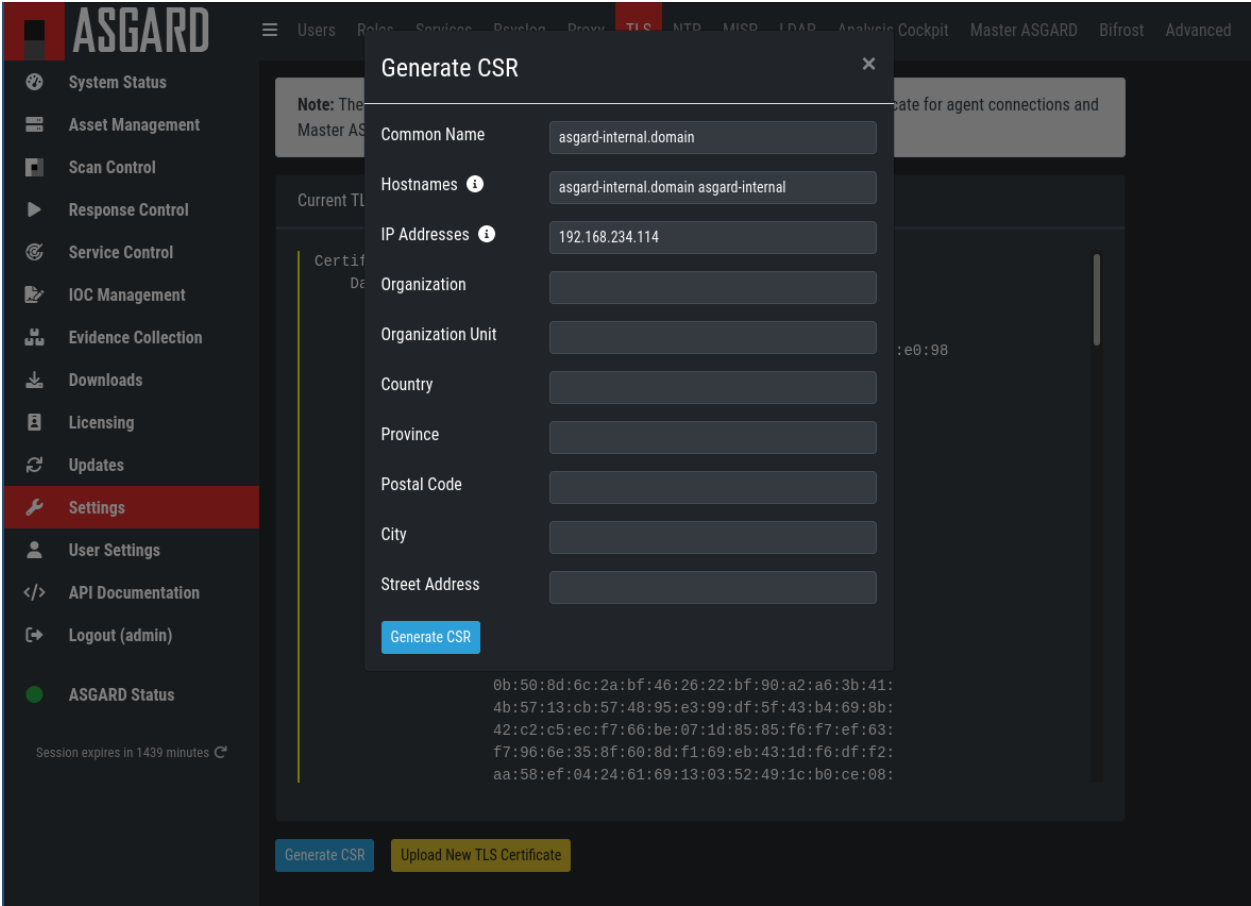


Fig. 88: Generate a Certificate Signing Request (CSR)

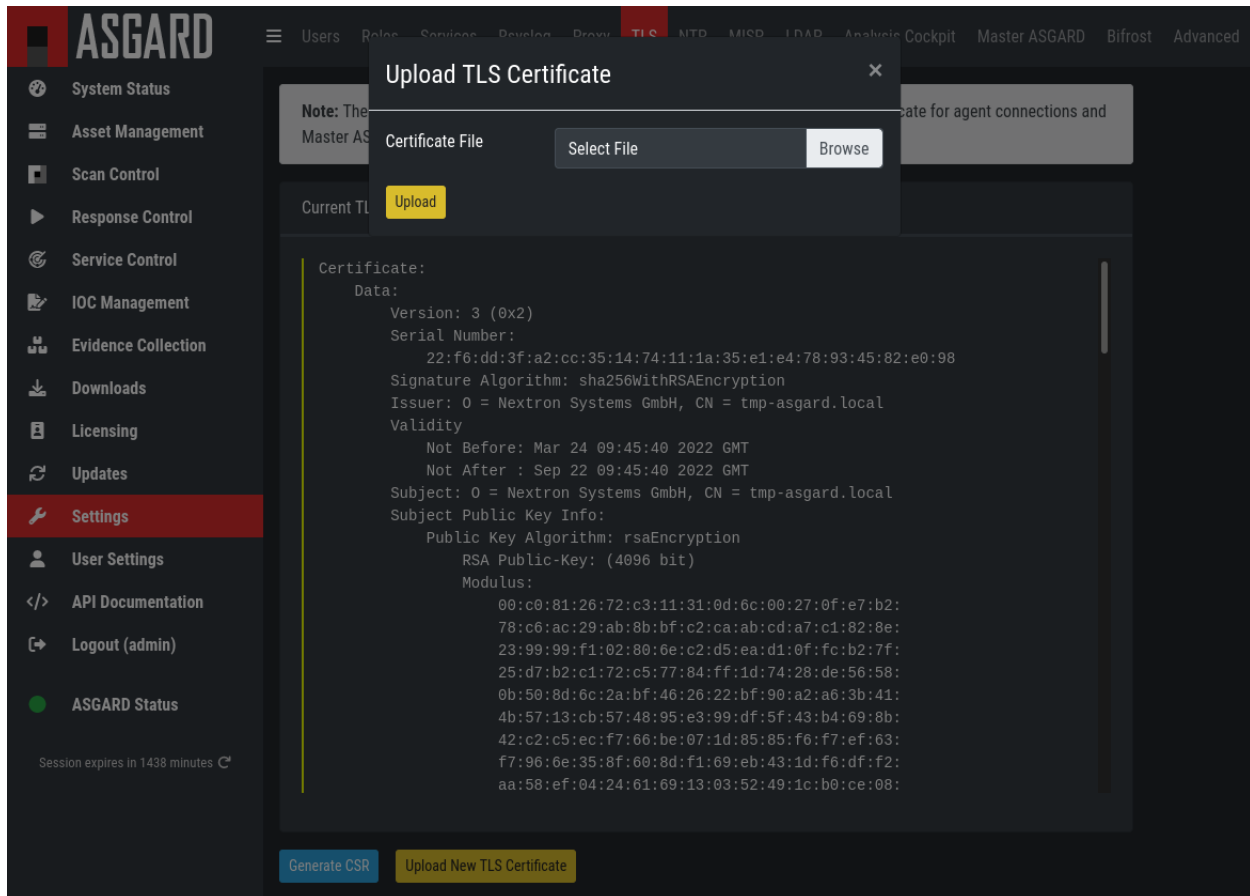
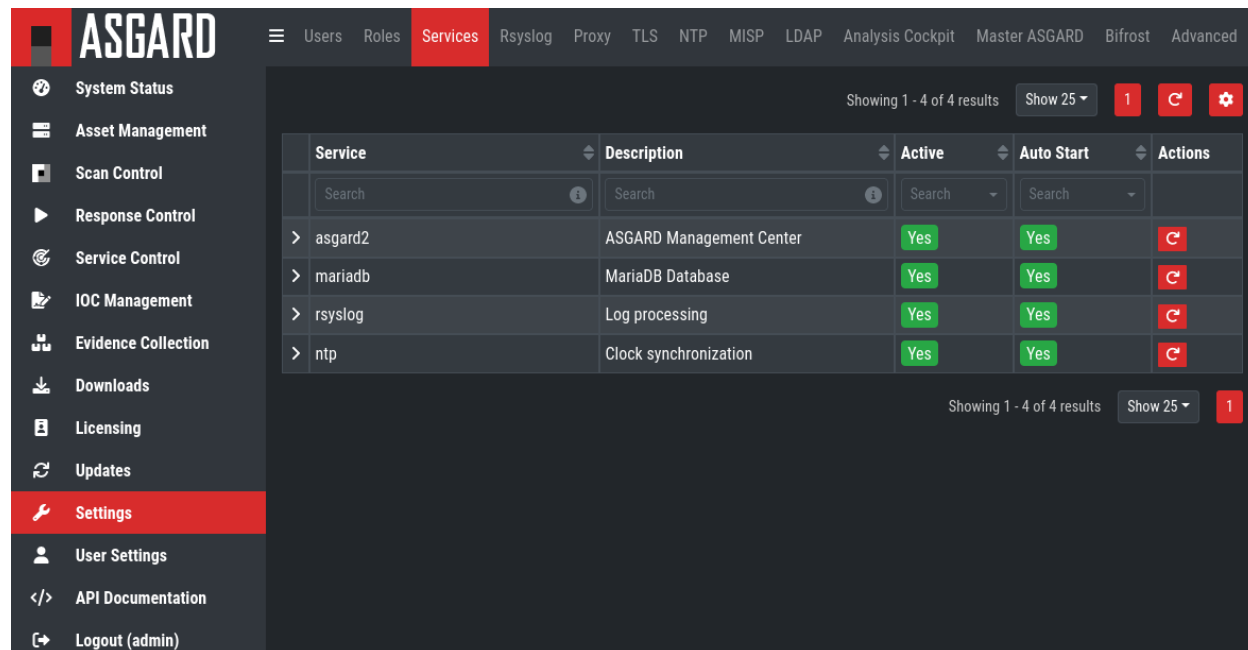


Fig. 89: Upload a TLS Certificate

4.14.3 Manage Services

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



Service	Description	Active	Auto Start	Actions
Search	Search	Search	Search	
> asgard2	ASGARD Management Center	Yes	Yes	
> mariadb	MariaDB Database	Yes	Yes	
> rsyslog	Log processing	Yes	Yes	
> ntp	Clock synchronization	Yes	Yes	

Fig. 90: Manage Services

4.14.4 NTP Configuration

The current NTP configuration can be found in the NTP sub-section.

A Source Pool or Source Server can be removed by clicking the delete action. To create a new Source Pool or Source Server, click **Add NTP Source** in the upper right corner.

4.14.5 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).

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](#).

Add NTP Source

Type: Source Server

Address: 10.1.1.1

> Additional Options

Add NTP Source

Type	Address	Max Poll	Actions
Source Pool	1.debian.pool.ntp.org	No	Yes
Source Pool	2.debian.pool.ntp.org	No	Yes
Source Pool	3.debian.pool.ntp.org	No	Yes

Showing 1 - 4 of 4 results Show 25 1

NTP Service Status

- ntp.service - Network Time Service
 - Loaded: loaded (/lib/systemd/system/ntp.service; enabled; vendor preset: enabled)
 - Active: active (running) since Tue 2022-04-12 08:43:14 CEST; 6h ago
 - Docs: man:ntpd(8)
 - Process: 515 ExecStart=/usr/lib/ntp/ntp-systemd-wrapper (code=exited, status=0/SUCCESS)
 - Main PID: 524 (ntpd)
 - Tasks: 2 (limit: 3551)
 - Memory: 3.1M
 - CGroup: /system.slice/ntp.service
 - └─524 /usr/sbin/ntpd -p /var/run/ntpd.pid -g -u 107:113

Fig. 91: NTP configuration

Retention Time (Days)

0

Update

Fig. 92: Settings for Bifrost

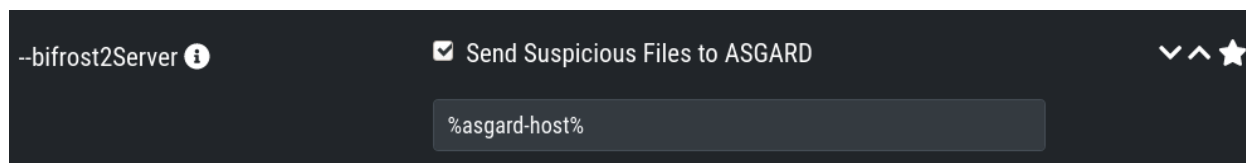


Fig. 93: Scan option for Bifrost

4.14.6 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.

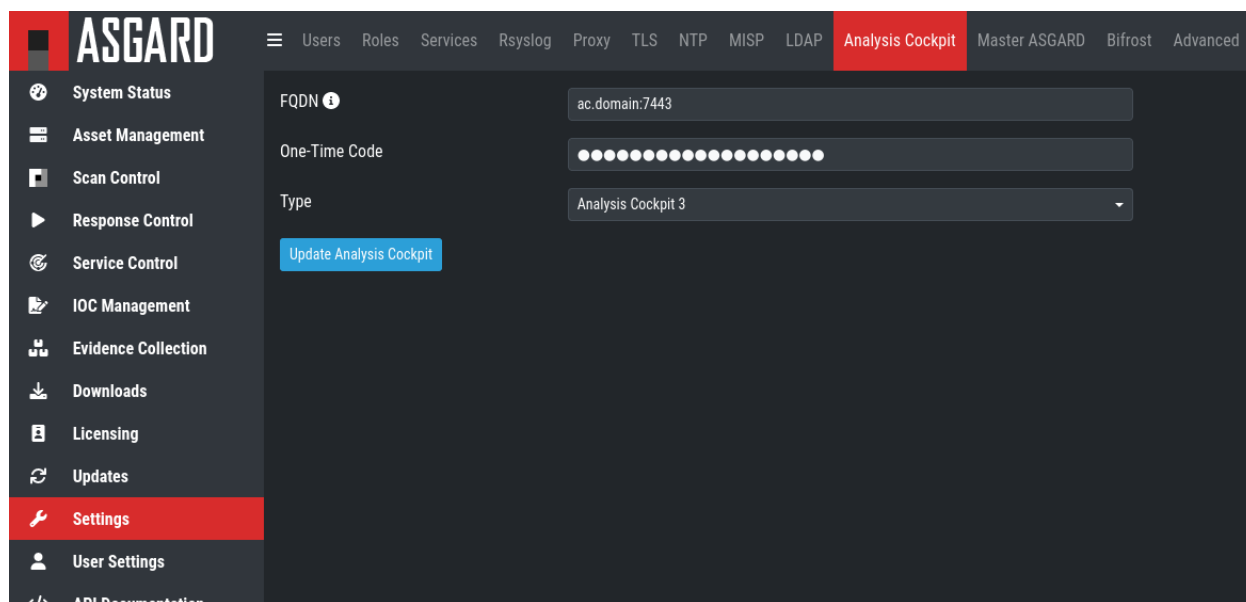


Fig. 94: Linking the Analysis Cockpit

The Cockpit's API key can be found at Settings > ASGARDs > Connect ASGARD.

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 ASGARDs 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.

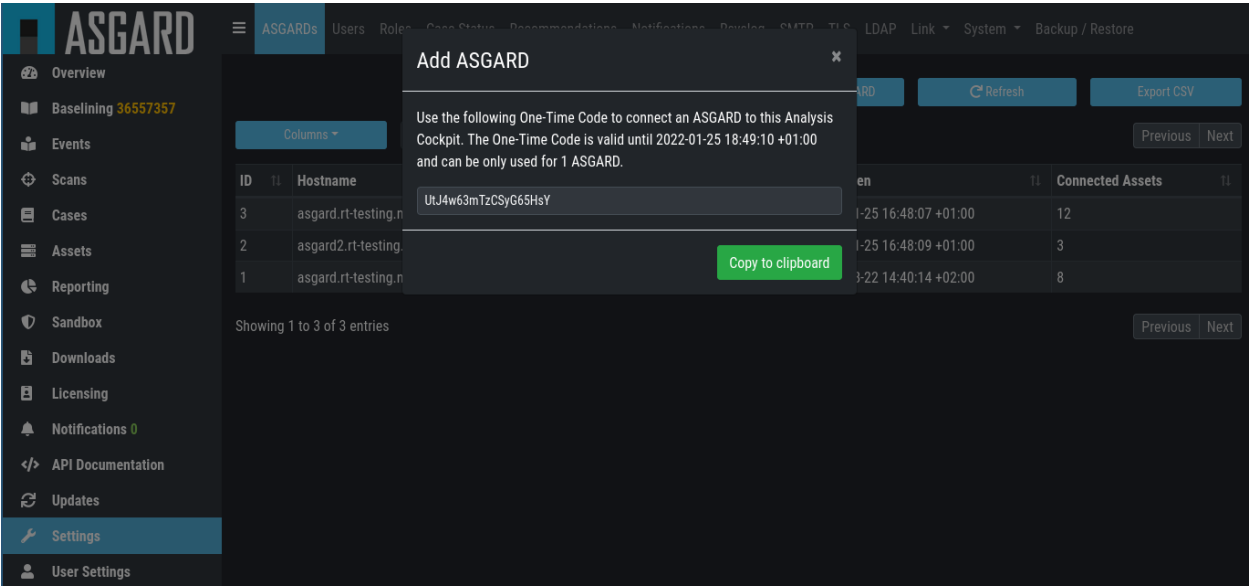


Fig. 95: Analysis Cockpit API Key

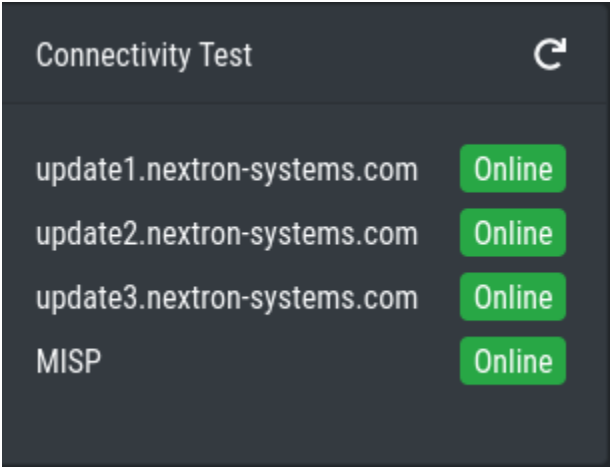


Fig. 96: Cockpit connectivity status

4.14.7 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**.

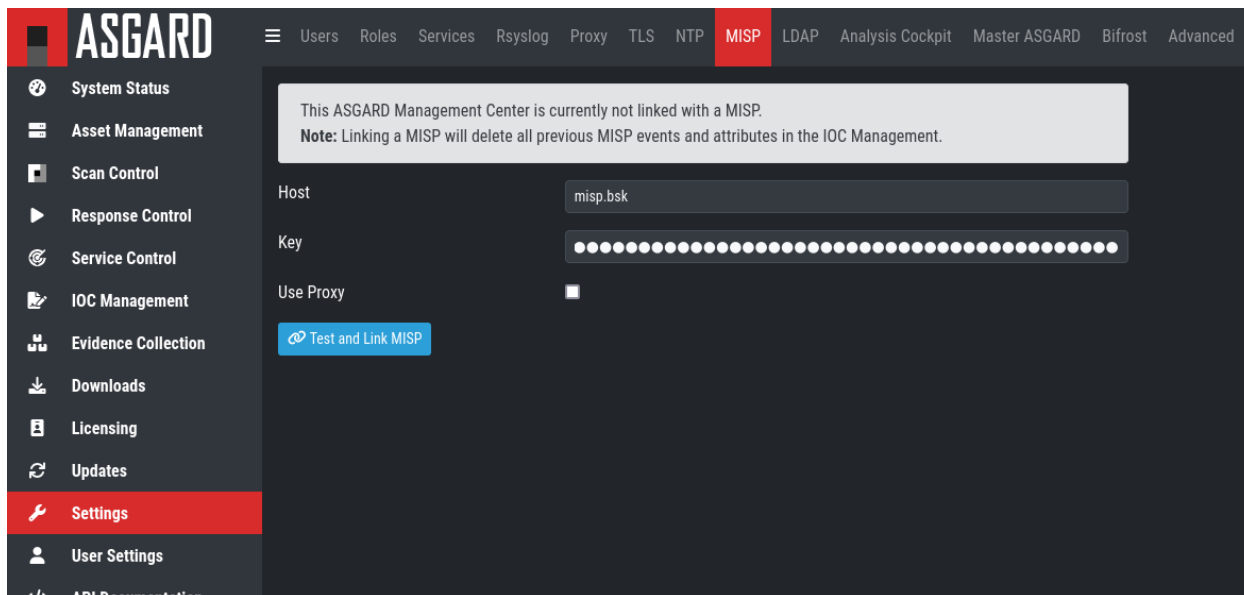


Fig. 97: Linking a MISP to ASGARD

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**.

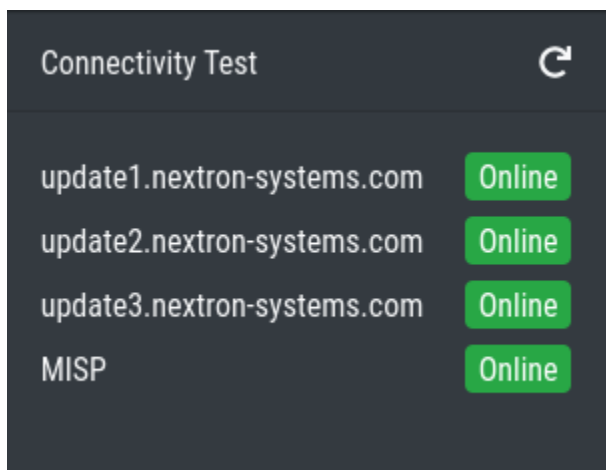


Fig. 98: MISP connectivity status

4.14.8 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.

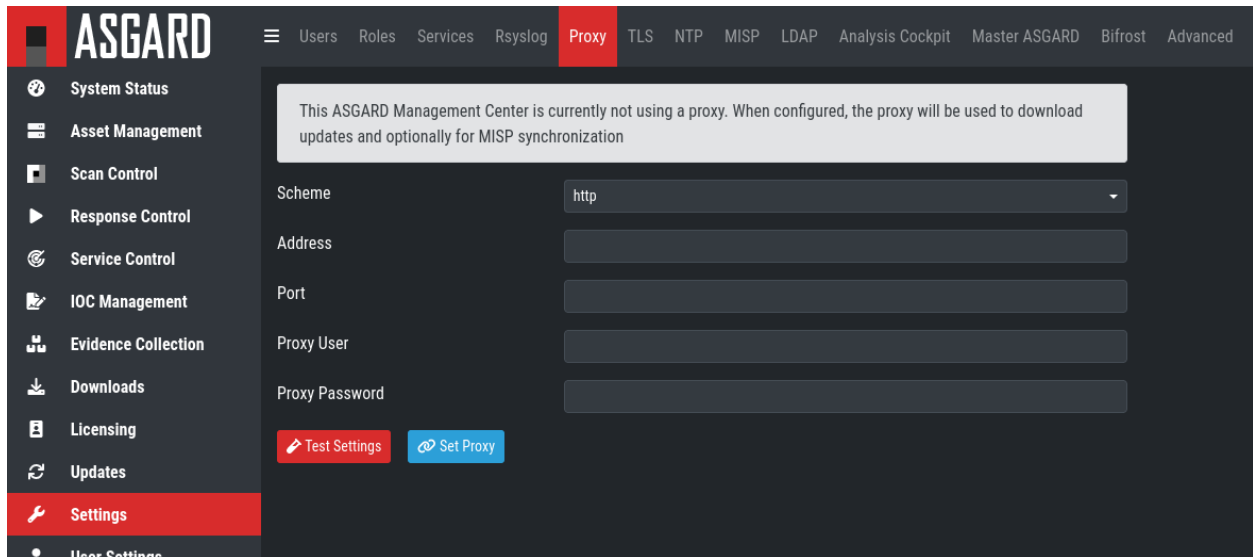


Fig. 99: Change Proxy Settings

Warning: This will also overwrite any changes made to the file `/etc/apt/apt.conf.d/proxy` on your system. If you changed the file before installation of your ASGARD services ([Changing Proxy Configuration](#)), you can safely go ahead and change your proxy settings.

4.14.9 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.

4.14.10 Advanced

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**.

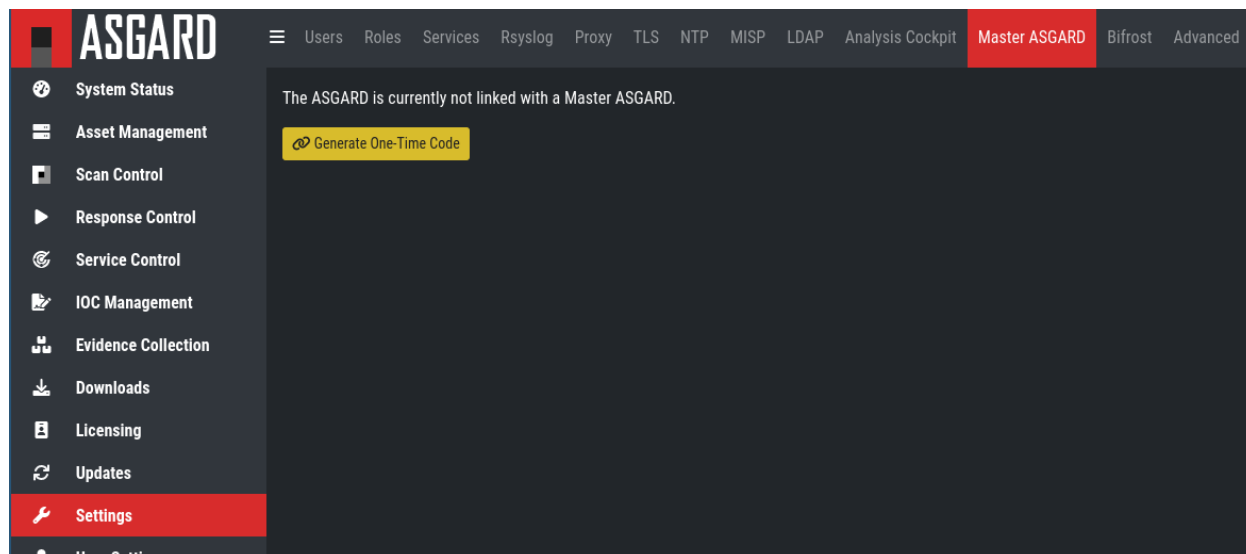


Fig. 100: Link MASTER ASGARD

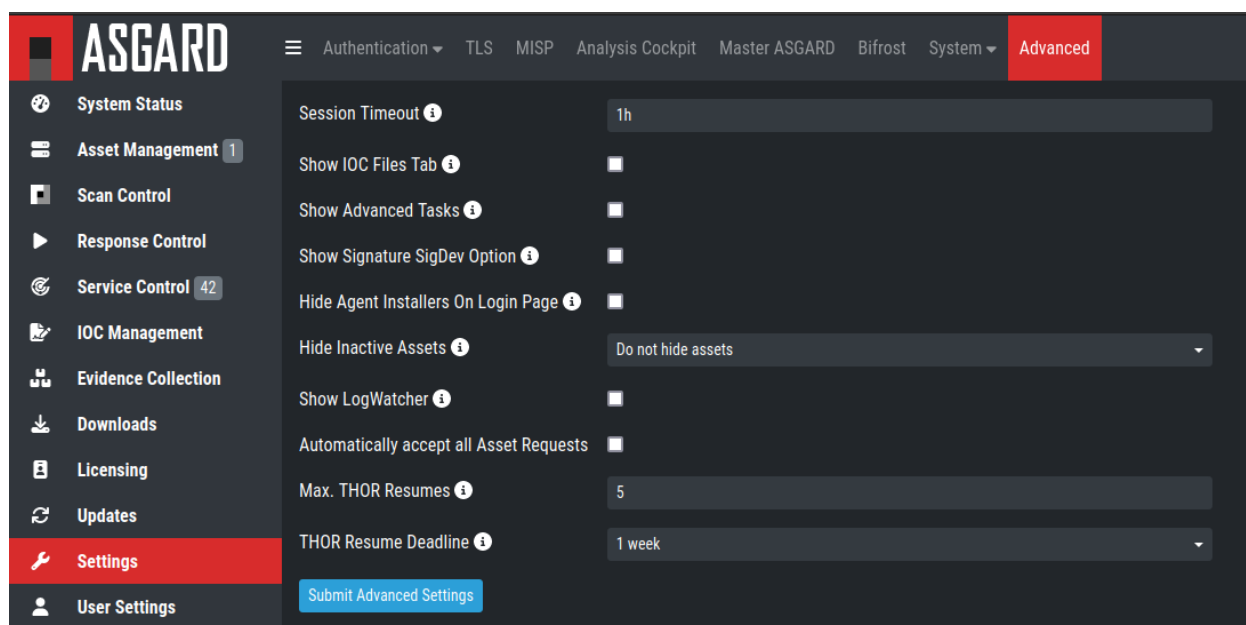


Fig. 101: Advanced Settings

4.15 User Settings

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

4.15.1 Changing your password

To change your password, navigate to the **User Settings** section.

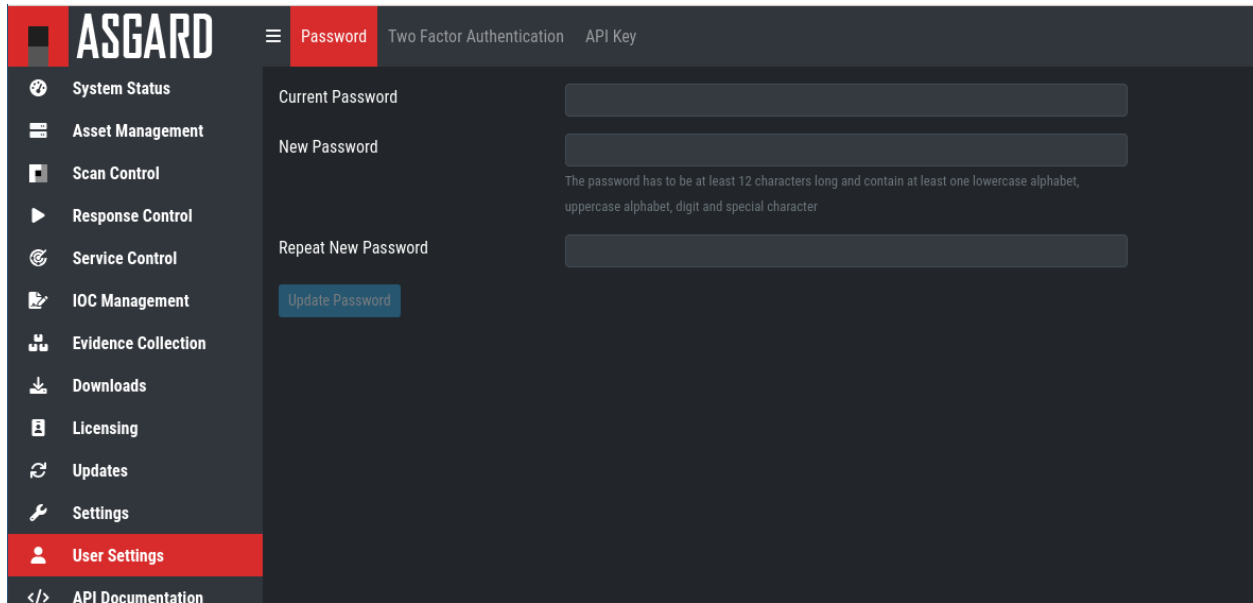


Fig. 102: Changing your password

4.15.2 Two Factor Authentication

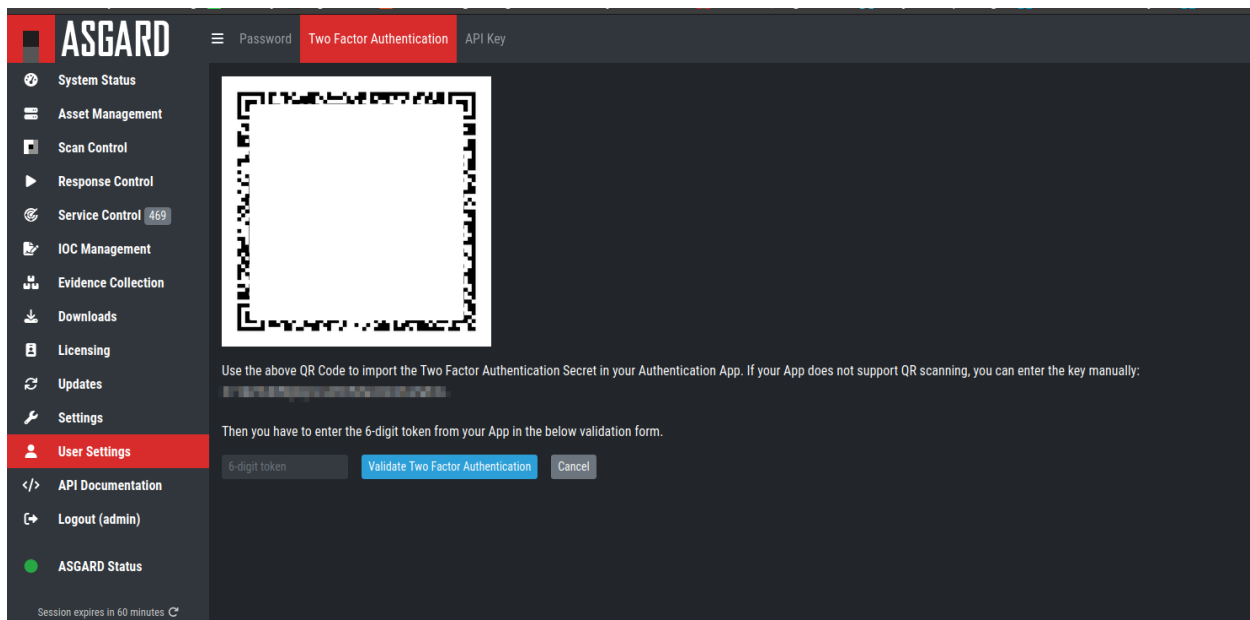
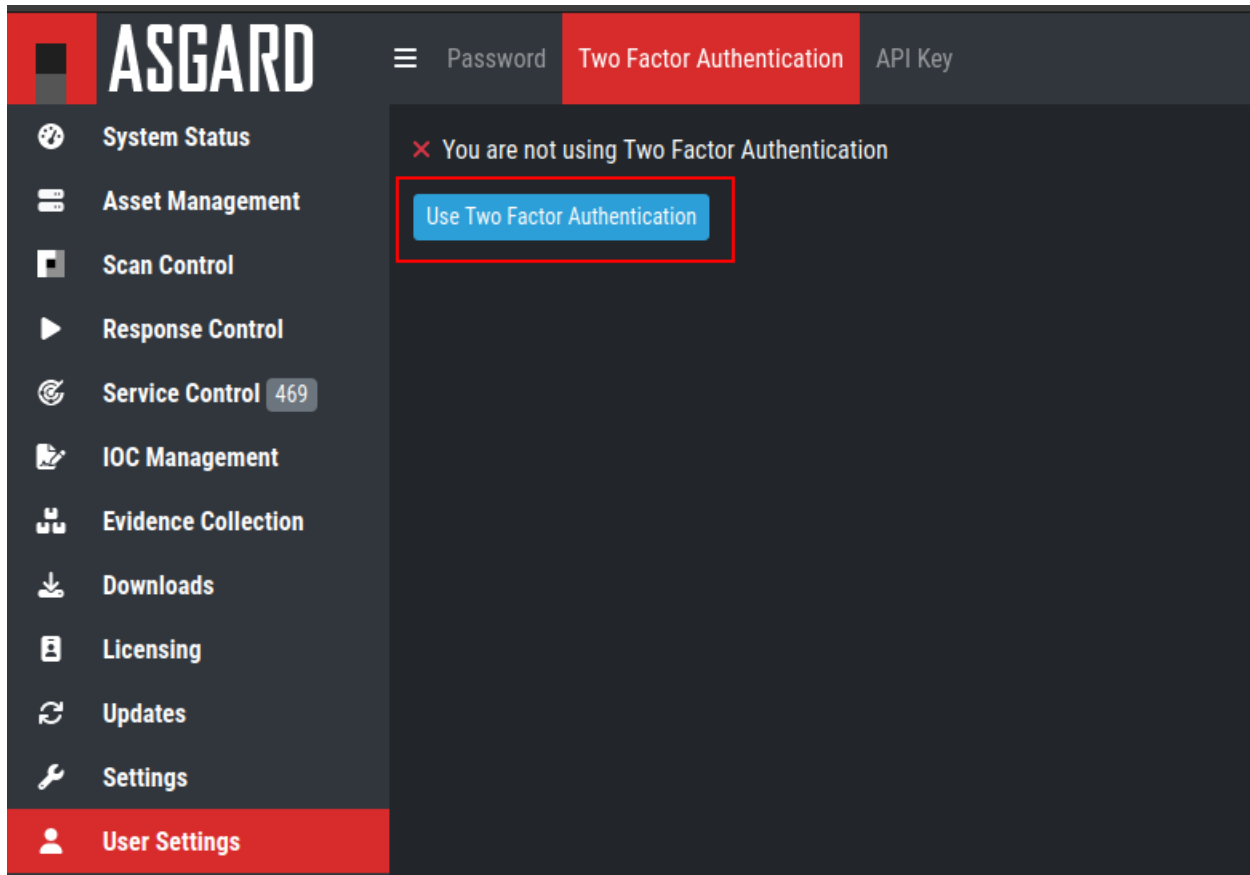
We are currently using the Time-based One-time Password (TOTP) algorithm for two factor authentication. We recommend one of the following mobile apps for 2FA:

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

Enable Two Factor Authentication

To enable Two Factor Authentication, navigate to **User Settings > Two Factor Authentication**. If 2FA is not enabled, you will see the option to **Use Two Factor Authentication**.

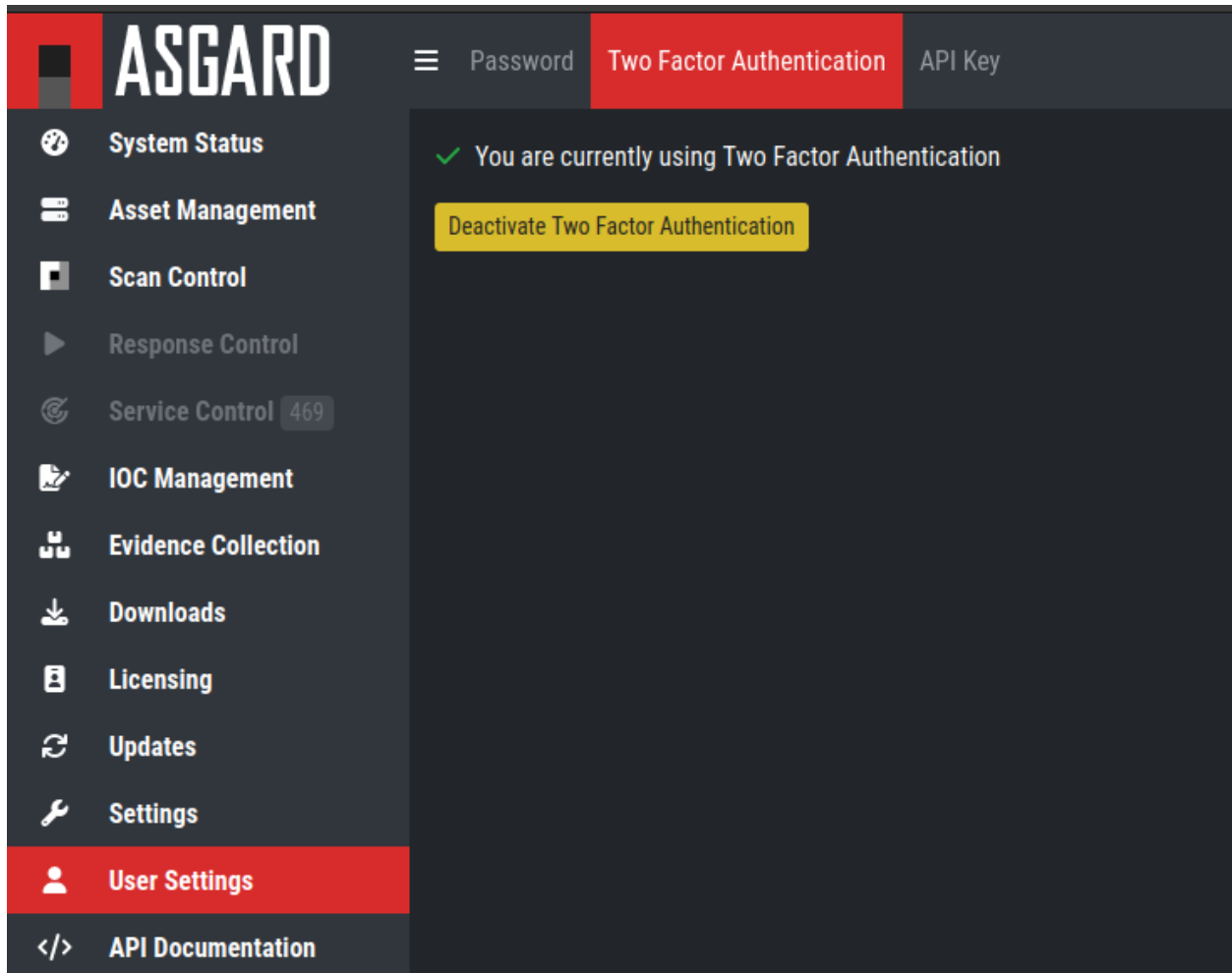
After clicking the button, you will be presented with a QR code for your authenticator app of your choice. Alternatively, you can use the secret key. You will need to verify the 6-digit token and click **Validate Two Factor Authentication** to enable 2FA.



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 [Reset Two Factor Authentication for a specific User](#)

4.15.3 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 ([Generate Download Links](#)).

4.16 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. In cases in which you've generated custom installer packages with a custom service and binary name, adjust the commands accordingly.

4.16.1 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.

4.16.2 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
```

4.16.3 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
```

4.17 Uninstall ASGARD Service Controller

Note: The command contains names used by the default installer packages. In cases in which you've generated custom installer packages with a custom service and binary name, adjust the commands accordingly.

If you want to uninstall the ASGARD Service Controller and Agent, see section *Uninstall ASGARD Agents*.

If you only want to uninstall the ASGARD Service Controller execute:

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


MASTER ASGARD

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 ASGAR, you have to choose the command line argument `-masterasgard` after the installation from our ISO. This has to be a new system, you cannot install a MASTER ASGAR on an existing ASGAR Management Center.

[illegible]

Fig. 1: Installation of Master ASGARD

After the MASTER ASGARD and later its license have been installed, many functions offer additional options. From that moment onwards, your MASTER ASGARD can use all endpoints connected to your linked ASGARD systems.

just like a normal ASGARD.

5.1 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

5.2 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.

5.3 Setting up MASTER ASGARD

The setup procedure for MASTER ASGARD is identical to the setup procedure for ASGARD Management Center, see [Setup Guide](#).

5.3.1 Default Credentials

Interface	Username	Password
Web UI	admin	admin
CLI/SSH	nexttron	<i>manually set during system installation</i>

5.4 Link ASGARD Systems with MASTER ASGARD

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

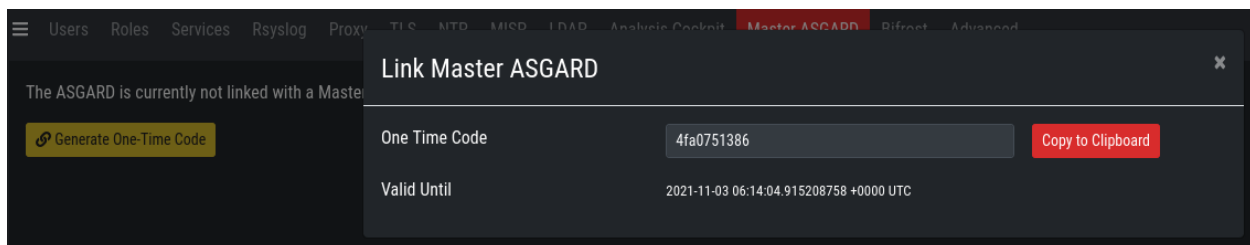


Fig. 2: Generate One Time Token on ASGARD

In MASTER ASGARD go to Connected ASGARs, 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.

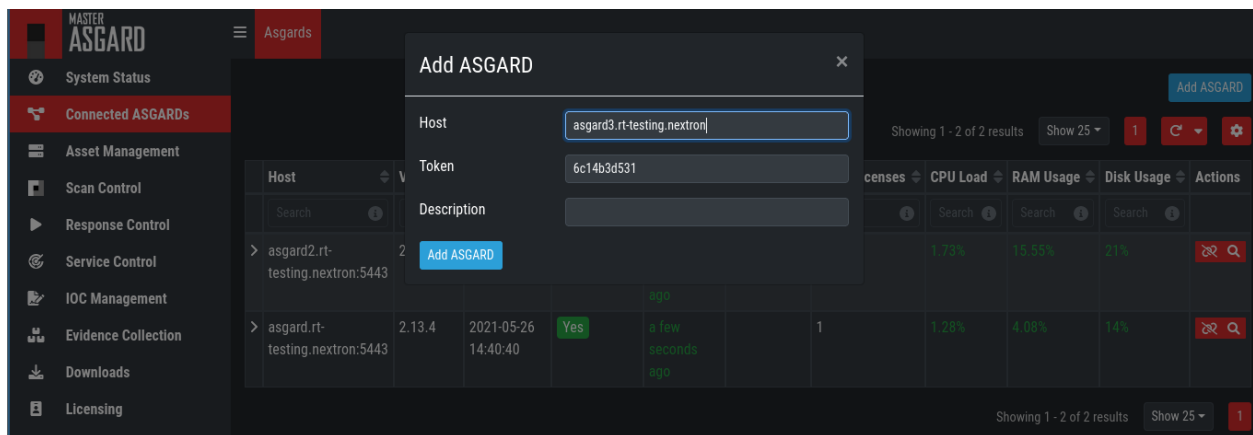


Fig. 3: Link ASGARD in MASTER ASGARD

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

5.5 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 ASGARs" to run the scans on.

5.6 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)

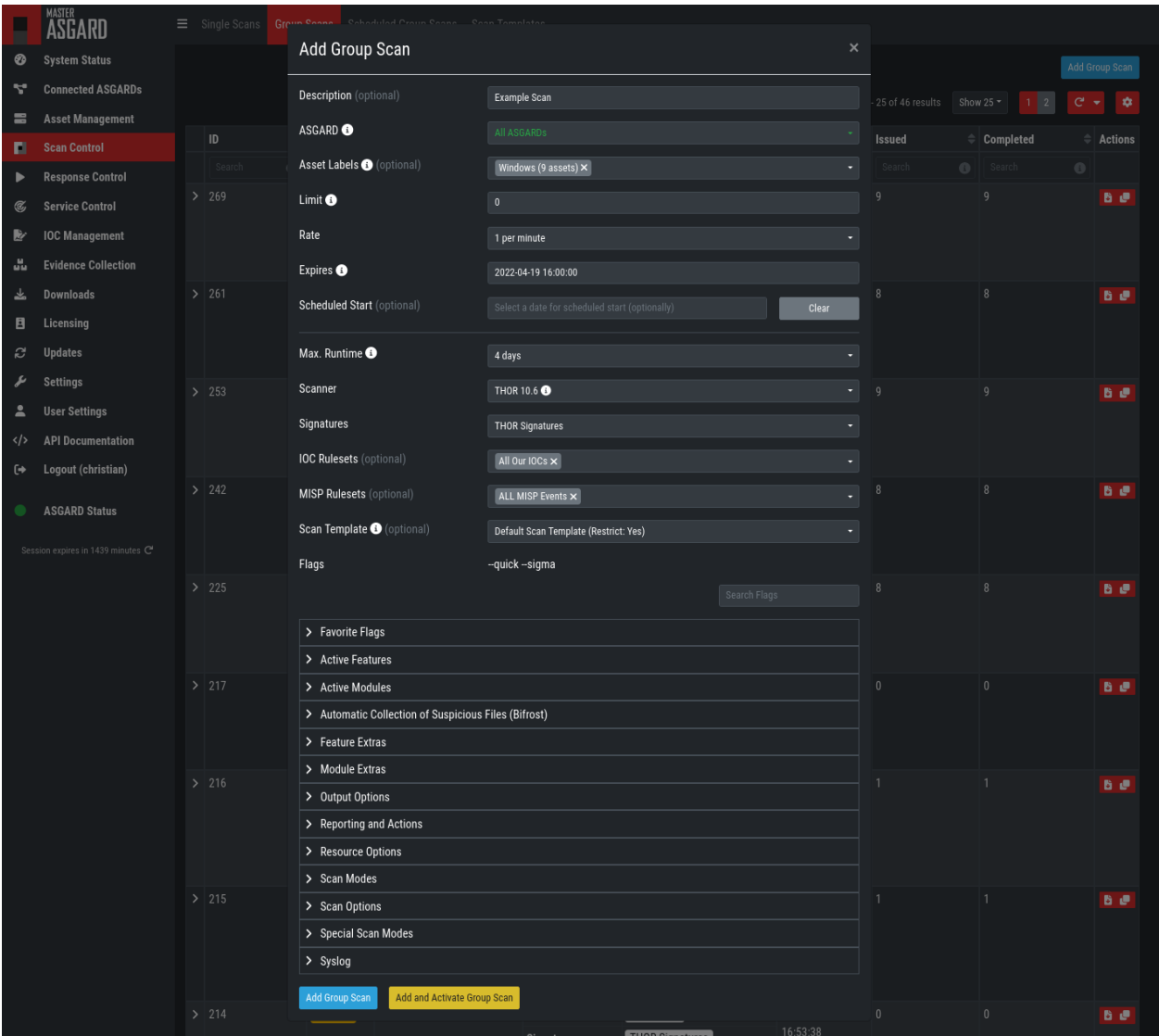


Fig. 4: Scan Control in MASTER ASGARD - Add Group Task

5.7 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.

5.8 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.

The screenshot shows the ASGARD Management Center interface. The left sidebar contains navigation links: System Status, Asset Management, Scan Control, Response Control, Service Control (highlighted), IOC Management, Evidence Collection, Downloads, Licensing, Updates, Settings, User Settings, API Documentation, and Logout (christian). The main content area is titled 'Aurora Asset View (Deployed)' and shows a table of assets. A yellow box highlights the 'Deployed Configuration' column, which contains the text '(Managed by Master ASGARD)' for all assets. The assets listed are workstation-04, exchange-server, TMP-WIN7-TEST, workstation-02, workstation-03, domain-controller, and workstation-01. Each asset row includes columns for Hostname, Last Seen, Labels, Deployed Configuration, Enabled, Active, Pending Changes, and Actions.

Hostname	Last Seen	Labels	Deployed Configuration	Enabled	Active	Pending Changes	Actions
workstation-04	a few seconds ago	Windows Workstations tenant1	(Managed by Master ASGARD)	Yes	Yes	No	[Stop] [Refresh]
exchange-server	a few seconds ago	Server Windows tenant2	(Managed by Master ASGARD)	Yes	Yes	No	[Stop] [Refresh]
TMP-WIN7-TEST	a few seconds ago	Windows tenant2	(Managed by Master ASGARD)	Yes	Yes	No	[Stop] [Refresh]
workstation-02	a few seconds ago	Windows Workstations retry_a19 tenant1	(Managed by Master ASGARD)	Yes	Yes	No	[Stop] [Refresh]
workstation-03	a few seconds ago	Windows Workstations tenant1	(Managed by Master ASGARD)	Yes	Yes	No	[Stop] [Refresh]
domain-controller	a few seconds ago	Server Windows retry_a19 tenant2	(Managed by Master ASGARD)	Yes	Yes	No	[Stop] [Refresh]
workstation-01	a few seconds ago	Windows Workstations tenant1	(Managed by Master ASGARD)	Yes	Yes	No	[Stop] [Refresh]

Fig. 5: Example: Service Controller listed in ASGARD but managed by MASTER ASGARD

5.9 Evidence Collection

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

5.10 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.

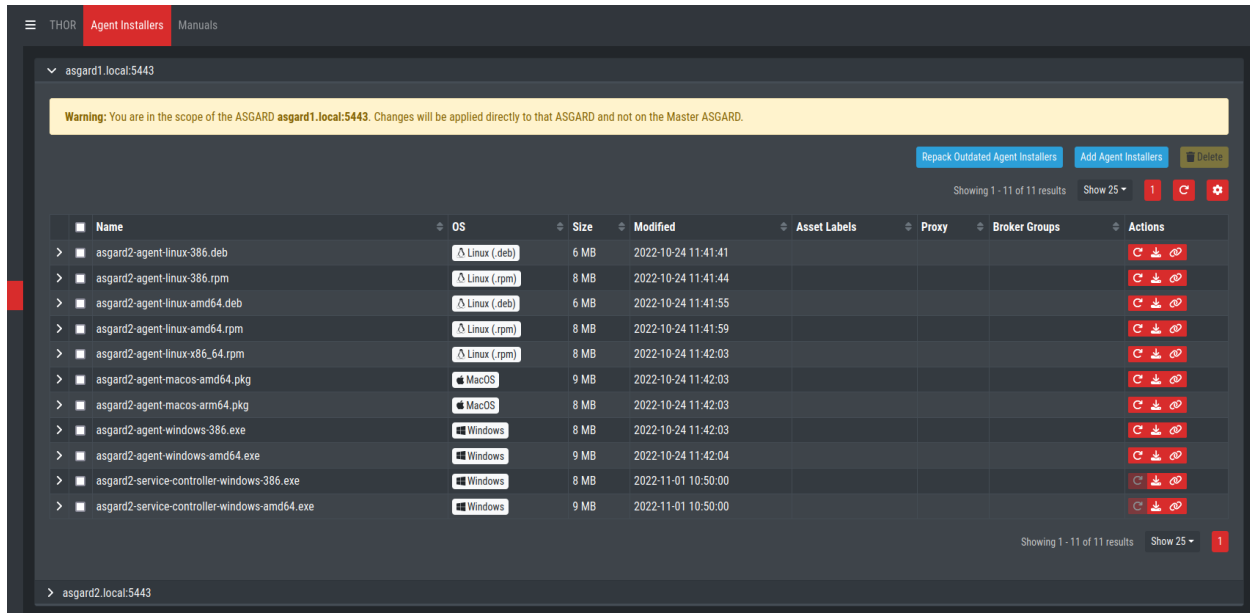


Fig. 6: Example: Download Section in ASGARD but managed by MASTER ASGARD

5.11 Updates

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

A third tab named THOR and Signatures gives you an overview of the used scanner and signature versions on all connected ASGARs.

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.

5.12 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.

MASTER

ASGARD

Management Center

Agents

THOR and Signatures

Aurora

Update Log

System Status

Connected ASGARs

Asset Management

Scan Control

Response Control

Service Control

IOC Management

Evidence Collection

Downloads

Licensing

Updates

Settings

User Settings

API Documentation

Logout (christian)

ASGARD Status

Session expires in 1440 minutes

Manually Check for Updates

Showing 1 - 15 of 15 results

Show 25

1

Product	Used Version	Used Since	Available Version	Available Since	Update Schedule of Used Version	Actions
THOR 10.6 for Windows	10.6.14	2022-02-04 17:48:24	10.6.14	2022-02-04 17:48:10	2022-04-13 01:00 [repeat daily]	
THOR 10.6 for Linux	10.6.14	2022-02-04 17:48:24	10.6.14	2022-02-04 17:47:49	2022-04-13 01:30 [repeat daily]	
THOR 10.6 for MacOS	10.6.14	2022-02-04 17:48:24	10.6.14	2022-02-04 17:48:21	2022-04-13 01:30 [repeat daily]	
THOR 10.5 for Windows	10.5.18	2021-11-15 13:50:06	10.5.18	2021-11-15 13:50:06	2022-04-13 01:30 [repeat daily]	
THOR 10.5 for Linux	10.5.18	2021-11-15 13:49:23	10.5.18	2021-11-15 13:49:23	2022-04-13 01:30 [repeat daily]	
THOR 10.5 for MacOS	10.5.18	2021-11-15 13:46:53	10.5.18	2021-11-15 13:46:53	2022-04-13 01:30 [repeat daily]	
THOR Lite 10.7 for Windows	10.7.1	2022-03-19 00:30:28	10.7.1	2022-03-18 16:30:49	2022-04-13 01:30 [repeat daily]	
THOR Lite 10.7 for Linux	10.7.1	2022-03-19 00:30:28	10.7.1	2022-03-18 16:30:34	2022-04-13 01:30 [repeat daily]	
THOR Lite 10.7 for MacOS	10.7.1	2022-03-19 00:30:28	10.7.1	2022-03-18 16:31:10	2022-04-13 01:30 [repeat daily]	
THOR TechPreview 10.7 for Windows	10.7.1	2022-03-19 00:30:28	10.7.1	2022-03-18 16:30:57	2022-04-13 01:30 [repeat daily]	
THOR TechPreview 10.7 for Linux	10.7.1	2022-03-19 00:30:28	10.7.1	2022-03-18 16:30:42	2022-04-13 01:30 [repeat daily]	
THOR TechPreview 10.7 for MacOS	10.7.1	2022-03-19 00:30:28	10.7.1	2022-03-18 16:31:04	2022-04-13 01:30 [repeat daily]	
THOR Signatures	22.4.11-151628	2022-04-12 11:30:09	22.4.11-151628	2022-04-12 11:18:11	2022-04-13 11:30 [repeat daily]	
THOR Signatures Lite	22.4.11-114355	2022-04-12 01:30:09	22.4.12-062559	2022-04-12 08:48:21	2022-04-13 01:30 [repeat daily]	
THOR Signatures SigDev	22.4.11-114326	2022-04-12 02:00:10	22.4.12-062529	2022-04-12 08:48:19	2022-04-13 02:00 [repeat daily]	

Showing 1 - 15 of 15 results

Show 25

1

Fig. 7: MASTER ASGARD Scanner Updates

5.13 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.

5.14 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)

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

Fig. 8: MASTER ASGARD API Peculiarity

MAINTENANCE

6.1 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`.

6.1.1 Syslog Logs

ASGARD will store all logs under `/var/lib/nextron/asgard2/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
Agent Agent and Service Controller	agent.log
THOR via Syslog	scan.log
THOR via Syslog (Scan Start, Licensing, Completion only)	subscan.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.

6.2 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

6.2.1 Safe-to-Delete Files

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

- `/var/lib/nextron/asgard2/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/nextron/asgard2/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.

6.2.2 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/nextron/asgard2/scan-results/*.gz`
- `/var/lib/nextron/asgard2/generic-results/*`
- `/var/lib/nextron/asgard2/remote-console/protocol/*`

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/nextron/asgard2/<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

7.1 Performance Tuning

7.1.1 Overview

The ASGARD agent polls the ASGARD 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/nextron/asgard2/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.

7.1.2 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.

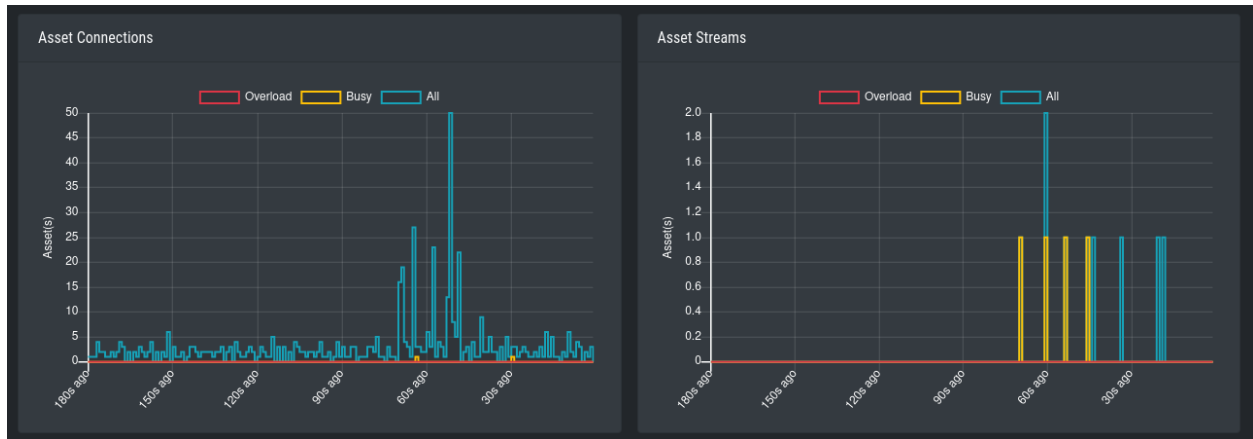


Fig. 1: Asset Connections and Asset Streams

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.

7.2 Managing Logs

ASGARD will store all logs under `/var/lib/nexttron/asgard2/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!

Log	Name	Rsyslog
Audit	asgard-audit.log	Audit Log ¹
ASGARD Management Center	asgard.log	ASGARD Log ^{Page 130, 1}
Agent Agent and Service Controller	agent.log	Agent Log ^{Page 130, 1}
THOR via Syslog	scan.log	THOR Log ^{Page 130, 1}
THOR via Syslog (Scan Start, Licensing, Completion only)	subscan.log	THOR Log ^{Page 130, 1}

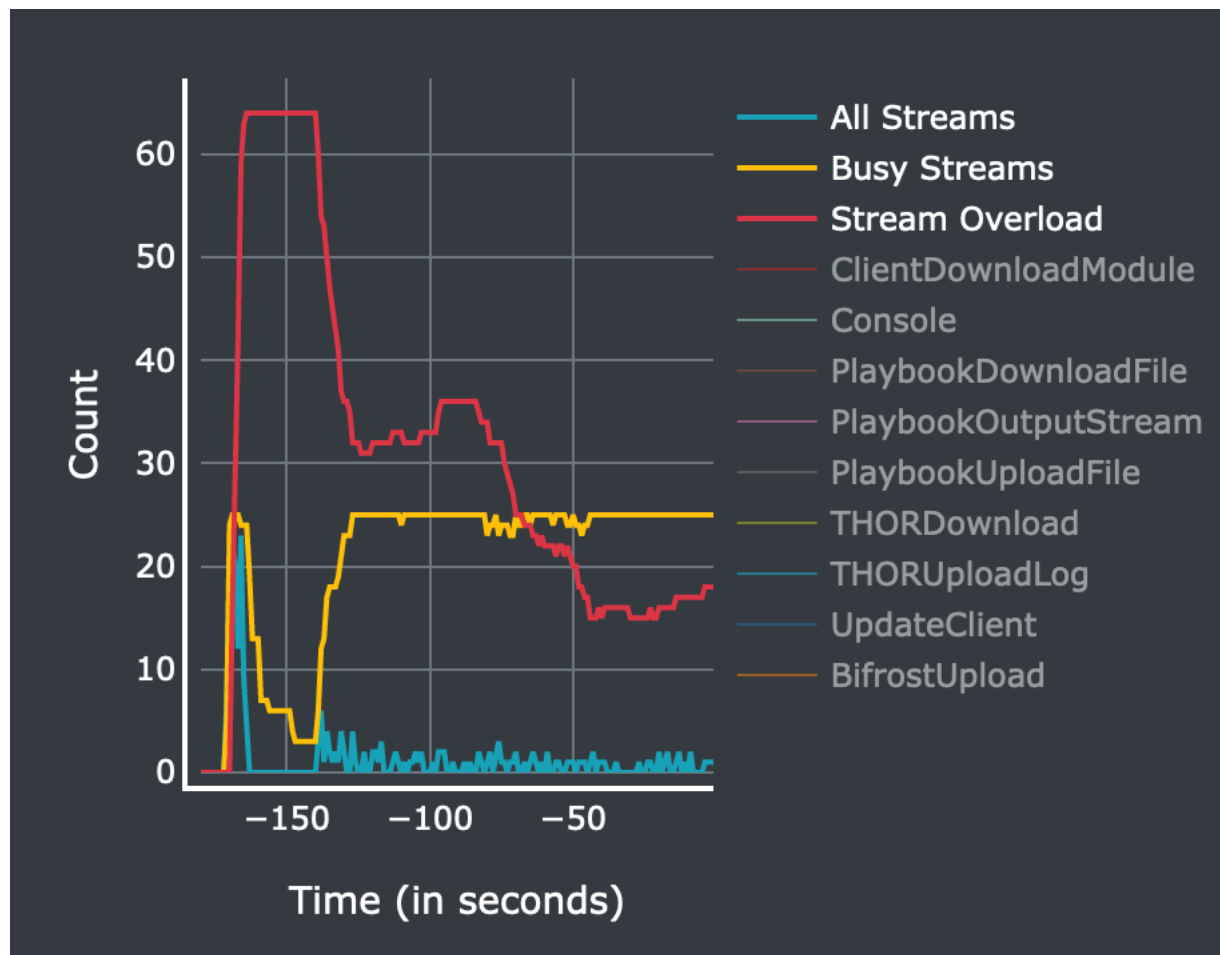


Fig. 2: Asset Streams in an overload situation

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

7.2.1 Scan Logs

ASGARD will store all scan logs under `/var/lib/nextron/asgard2/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.

7.3 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.

7.3.1 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.

7.3.2 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 as you might have customized your installers. If this is the case you have to repack the agent installers as explained in *section Creating Custom Agent Installer*.

If you use the default installer without any modifications you can run the following command to update the agent installers:

```
nextron@asgard:~$ sudo asgard2-repacker
```

Or you can execute the agent installer update from within the WebUI at **Updates > Agents > Repack Agent Installers** at the bottom.

¹ This is the **Type** you can select in *Rsyslog Forwarding*.

Add Group Task

Description

RunTask

Asset Labels

(no labels selected)

Limit

100

Rate

1 per minute

Expires

2021-11-15 17:00:00

Scheduled Start

Select a date for scheduled start (optionally)

Clear

Max. Runtime

4 days

Task

Update Agent

Agent Type

ASGARD 2 Agent

Add Group Task

Add and Run Group Task

Fig. 3: Example Group Task for Agent Update

Agent Installer Update

Note: There is an agent update available for at least one Agent installer. The Agent Installers should be rebuilt with the asgard2-repacker. See asgard2-repacker --help or ASGARD Manual for more information.

Repack Agent Installers

Ignore this update

Fig. 4: Execute asgard2-repacker from the WebUI

7.4 Creating Custom Agent Installer

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

7.4.1 Creating Custom Agent Installer From GUI

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.

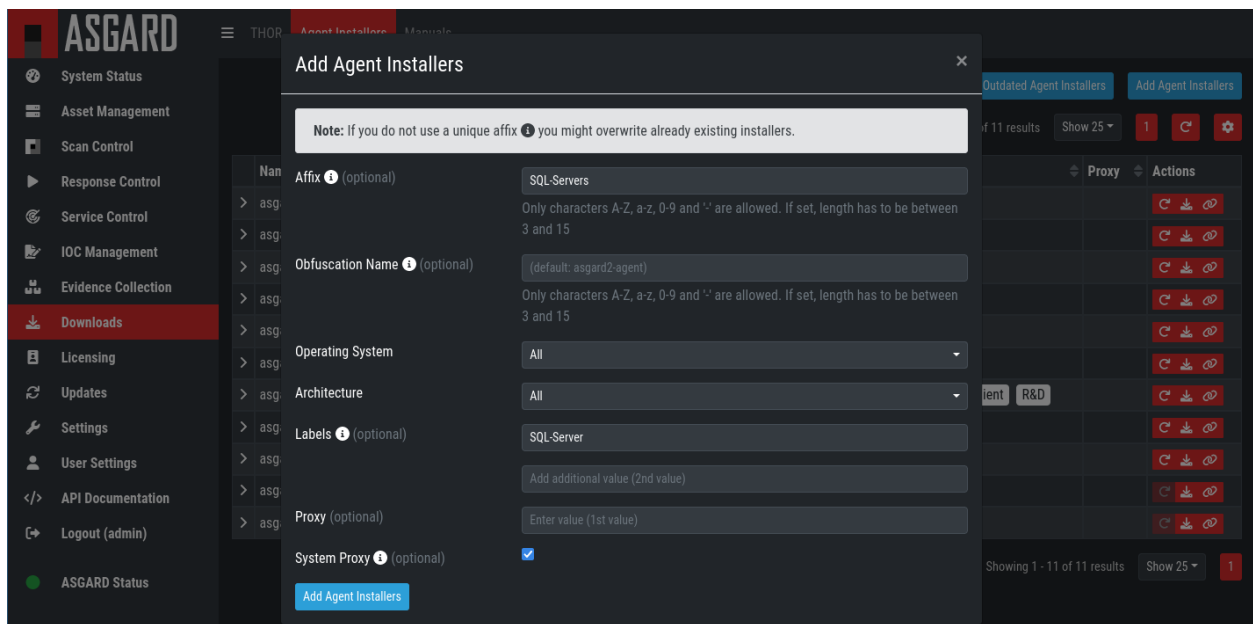


Fig. 5: Custom Agent Installer from the WebUI

You can also delete old Agent Installers which are not needed anymore. Just select the Installer(s) and Click the Delete button in the top right corner.

7.4.2 Creating Custom Agent Installer From CLI (deprecated)

In order to create your custom ASGARD agent, save the current agents stored in `/var/lib/nextron/asgard2/installer/` to a directory of your choosing and run `sudo asgard2-repacker` with one or more of the following flags:

`-labels string`

Add initial labels to clients comma separated list, e.g. `[label1,label2,label3]`

`-proxies string`

Proxies to be used by agents comma separated list, e.g. `[proxy1.nextron:3128,proxy2.nextron:3128]`

Example: In order to create an installer for servers that initially show up in ASGARD with the label SQL-Servers use:

```
nexttron@asgard:~$ sudo asgard2-repacker -label SQL-Servers
```

Your newly generated agents will show up in `/var/lib/nextron/asgard2/installer` and will immediately be available for download from the login page. You can store multiple custom agents under `/var/lib/nextron/asgard2/installer/`. In this case all agents will be available for download from ASGARDe login page.

You can obfuscate the default asgard2-agent name with a custom one. The chosen name will generate new agents which can be deployed to the endpoints. These agents will create a service with the chosen name and will have no reference to ASGARD.

`-name string`

```
nexttron@asgard:~$ sudo asgard2-repacker -name javax
```

This command will create a new agent for all operating systems. This is specially designed for cases where an agent obfuscation is required.

An installed agent with the name "javax" would look like this:

```
nexttron@asgard:~$ systemctl status javax
javax.service
Loaded: loaded (/etc/systemd/system/javax.service; enabled; vendor preset: enabled)
Active: active (running) since Thu 2020-xx-xx 16:47:22 CET; 5s ago
Main PID: 20048 (javax-service)
    Tasks: 7 (limit: 4915)
Memory: 4.7M
CGroup: /system.slice/javax.service
        20048 /usr/sbin/javax-serviceMar 26 16:47:22 asgard2-dev systemd[1]: Started.
↪javax.service.
```

7.5 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.

7.5.1 Backup

The command `asgard2-backup` 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 asgard2-backup
Writing backup to '/var/lib/nextron/asgard2/backups/20200427-1553.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 nextron user and change the permissions:

```
nexttron@asgard:~$ sudo cp /var/lib/nextron/asgard2/backups/20200427-1553.tar /home/
↪nexttron
nexttron@asgard:~$ sudo chown nextron:nextron /home/nextron/20200427-1553.tar
nexttron@asgard:~$ ls -l
total 596496
-rw-r--r-- 1 nextron nextron 309217280 Nov  1 12:01 20200427-1553.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/nextron/asgard2/backups"
3 NEWDIR="/home/nextron/backups"
4 date
5
6 echo "checking for destination folder"
7 if ! [ -d "$NEWDIR" ]; then
8     mkdir $NEWDIR
9     chown -R nextron: $NEWDIR
10 fi
11
12 echo "stopping asgard2.service"
13 if ! systemctl stop asgard2.service; then
14     echo "could not stop asgard2.service, exiting script"
15     exit 1
16 fi
17
18 sleep 3
19 echo "running backup script"
20 /usr/sbin/asgard2-backup
21
22 sleep 3
23 echo "starting asgard2.service"
24 if ! systemctl start asgard2.service; then
25     echo "could not start asgard2.service, needs manual debugging"
```

(continues on next page)

(continued from previous page)

```

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 asgard2-backup 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/sbin/asgard2-backup to a different value.

7.5.2 Restore

You can use the asgard2-restore command to restore a backup.

```

nextron@asgard:~$ sudo asgard2-restore
Usage: /usr/sbin/asgard2-restore <BACKUP FILE>
nextron@asgard:~$ sudo asgard2-restore /var/lib/nextron/asgard2/backups/20200427-1553.tar
Stopping services... Removed /etc/systemd/system/multi-user.target.wants/asgard2.service.
done.
etc/nextron/asgard2/
etc/nextron/asgard2/upgrade2.sh
etc/nextron/asgard2/run_asgard2.sh
etc/nextron/asgard2/server.pem
etc/nextron/asgard2/ca2.key
etc/nextron/asgard2/pre_asgard2.sh
etc/nextron/asgard2/rsyslog-asgard-audit.conf
etc/nextron/asgard2/client.yaml
...
1+0 records in
1+0 records out
24 bytes copied, 3.2337e-05 s, 742 kB/s
Starting services... Created symlink /etc/systemd/system/multi-user.target.wants/asgard2.
↪service → lib/systemd/system/asgard2.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.

7.6 Disable Remote Console Globally

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

```
nexttron@asgard:~$ sudo touch /etc/nextron/asgard2/disable_console
```

To re-enable Remote Console simply remove the created file

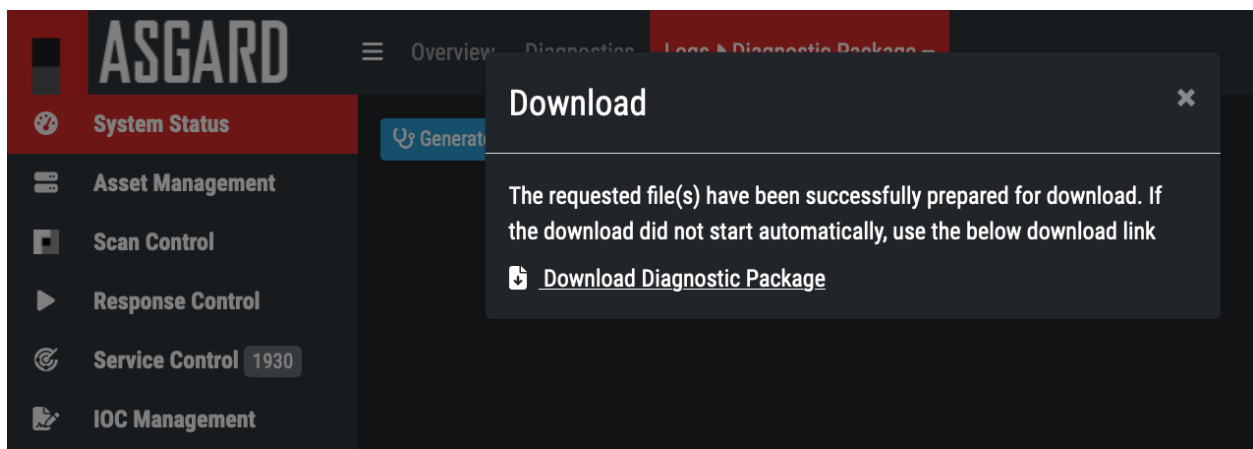
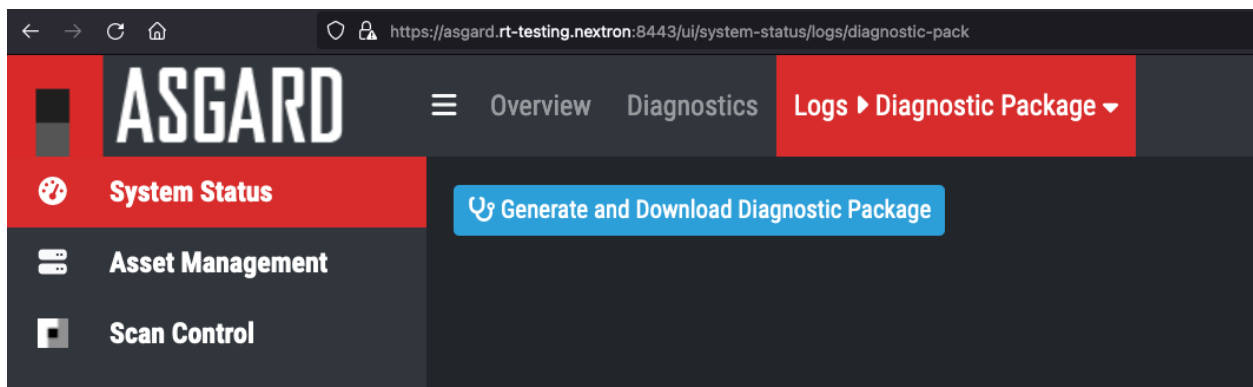
```
nexttron@asgard:~$ sudo rm /etc/nextron/asgard2/disable_console
```

TROUBLESHOOTING

8.1 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 > Tab: 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/nextron/asgard2/log/agent-access.log` is often responsible for 97% of the package size)

8.2 Agent Debugging

8.2.1 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.

8.2.2 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
```

8.2.3 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.

8.2.4 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.

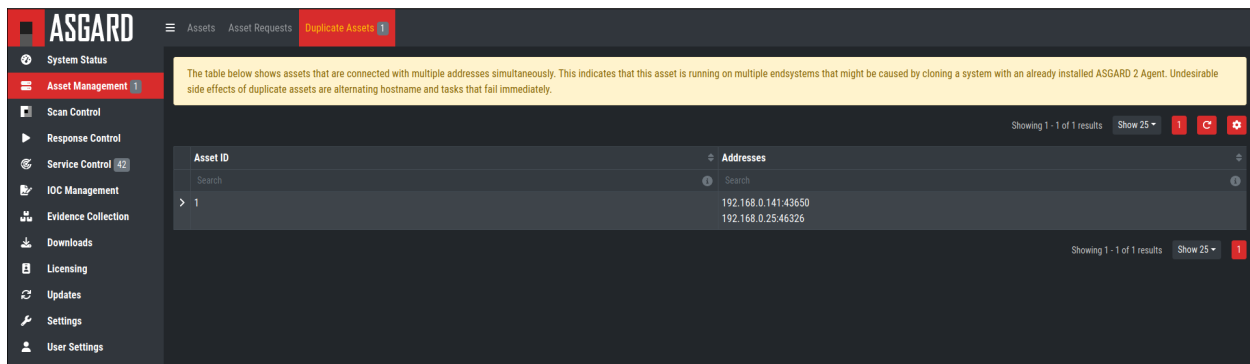


Fig. 1: Troubleshooting Duplicate Assets

- 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.

8.3 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.

- update3.nexttron-systems.com

Used for THOR updates:

- update1.nexttron-systems.com
- update2.nexttron-systems.com

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

8.4 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.

8.4.1 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.nexttron.internal"
```

8.4.2 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.

```
nexttron@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/nextron/asgard2/server_cert_ext.cnf.in > /etc/nextron/
   ↪ asgard2/server_cert_ext.cnf
5 openssl req -new -nodes -subj "/O=Nextron Systems GmbH/CN=${FQDN}" -key /etc/nextron/
   ↪ asgard2/client-service.key -out /etc/nextron/asgard2/client-service.csr
6 openssl x509 -req -in /etc/nextron/asgard2/client-service.csr -CA /etc/nextron/asgard2/
   ↪ ca.pem -CAkey /etc/nextron/asgard2/ca.key -CAcreateserial -days 36500 -out /etc/
   ↪ nextron/asgard2/client-service.pem -extfile /etc/nextron/asgard2/server_cert_ext.cnf
7 systemctl restart asgard2
8 asgard2-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:

```
nexttron@asgard-mc:~$ chmod +x fix-fqdn.sh
nexttron@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](#)

8.5 ASGARD Errors

8.5.1 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 or EDR Exclusions](#) for more details.

8.6 Resetting TLS/SSL Certificates

8.6.1 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=Nextron Systems GmbH/CN=$(hostname --fqdn)" -keyout /etc/nextron/asgard2/server.key -
↳ out /etc/nextron/asgard2/server.pem
```

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

```
nexttron@asgard:~$ sudo systemctl restart asgard2.service
```

8.6.2 Regenerate ASGARD Server Certificate Agent Communication

Please see chapter [Using Hostname instead of FQDN](#).

8.7 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 -e "UPDATE users SET password = 'YmIc6P_
↳ 6jdbEEL0HY4xIcpYstmM' WHERE name = 'admin';"
```

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

8.8 Reset Two Factor Authentication for a specific User

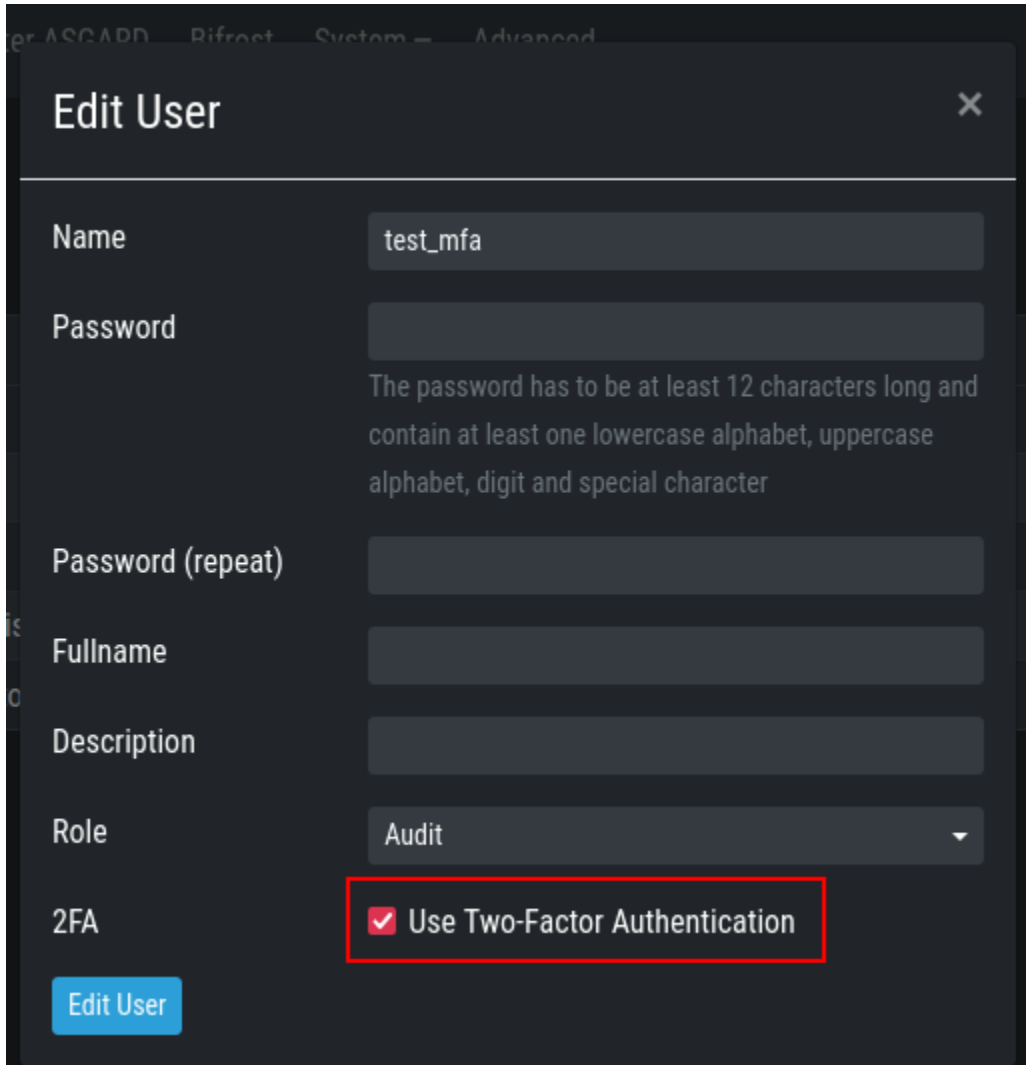
If you or another user lost their second factor (2FA) to log into the ASGARD Web UI, you have to reset the users MFA Settings. If you cannot access the Web UI, use the Command Line method.

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

8.8.1 Using the Web UI

Log into ASGARDe 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 popup 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).



The screenshot shows the 'Edit User' dialog box with the following fields and values:

- Name: test_mfa
- Password: (empty)
- Password (repeat): (empty)
- Fullname: (empty)
- Description: (empty)
- Role: Audit
- 2FA: ☒ Use Two-Factor Authentication

A red box highlights the 'Use Two-Factor Authentication' checkbox. At the bottom left, there is a blue button labeled 'Edit User'.

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

8.8.2 Using the Command Line Interface

Note: This method needs SSH access to ASGARD.

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 --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 --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).

8.9 Scheduled Scans do not run at the correct 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!

8.10 Aurora is generating 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

9.1 AMC#015: 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

9.1.1 AMC#015: 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.

9.2 AMC#014: 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:

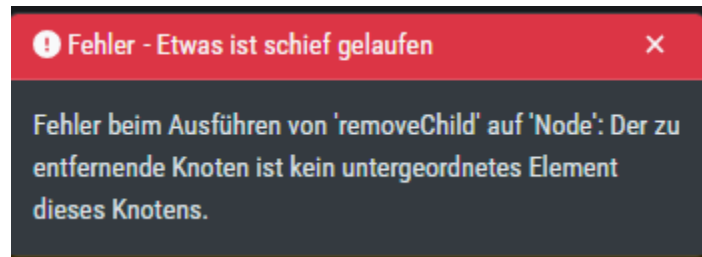


Fig. 1: removeChild Error with Edge translation

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.

9.3 AMC#013: Master ASGARD custom IOCs in Scheduled Group Scan

Introduced Version	Fixed Version
<= 2.15.3	2.15.5

Due to a bug in the handling of scheduled group scans in your Master ASGARD, you will face an issue, were custom IOCs are not updated. This means that you would use an old version of your custom IOCs for this specific scheduled group scan, even if they have changed since the scheduled group scan was created. This scenario happens if the following conditions are given:

- Scheduled Group Scan on your Master ASGARD for **one specific ASGARD**
- Your Custom IOCs changed **after** the scheduled group scan was created (compiled)

This led to the Master ASGARD not pushing the Custom IOC changes to the specific ASGARD (which you created the scheduled group scan for), after your IOCs have changed and your IOC Ruleset was compiled.

From version 2.15.5, you will receive the following warning, if you have a scheduled group scan active with this bug:

Warning: Warning: Due to a bug in the Master ASGARD, some scheduled group scans might not be affected by custom signature updates. We highly recommend to stop and recreate the group scans with the following ids: 59

9.3.1 AMC#013: Fix

After you installed the version 2.15.5 or newer in your Master ASGARD and all connected ASGARDs, make sure to fix any scheduled group scan which are being reported by the above warning.

To do this, go to Scan Control > Scheduled Group Scans and activate the ID column. Search for the specific scan with the reported ID.

The screenshot shows the ASGARD Management Center interface. At the top, there is a navigation bar with tabs: Single Scans, Group Scans, Scheduled Group Scans (selected), Scan Templates, and THOR Config. Below the navigation bar, a yellow warning banner states: "Warning: Due to a bug in the Master ASGARD, some scheduled group scans might not be affected by custom signature updates. We highly recommend to stop and recreate the group scans with the following IDs: 59".

Below the warning, there is a table of Scheduled Group Scans. The table has columns: ID, Status, Description, Arguments, Last Issued, Next Issued, and Actions. The first row shows a scan with ID 59, Status Enabled, and a description. The Arguments column shows the following flags: Scanner: THOR 10.6, Signatures: THOR Signatures, Custom Signatures: [redacted], No Resource Control: No, THOR Flags: --customonly --module Filescan --path /:NOWALK --syslog %asgard-host%.

Below the table, there is a "Details" section for the selected scan (ID 59). It shows the following information: ID: 59, ASGARD: [redacted], Module: THOR, Description: [redacted], Scanner: THOR 10.6, Signatures: THOR Signatures, Custom Signatures: [redacted], No Resource Control: No, THOR Flags: --customonly --module Filescan --path /:NOWALK --syslog %asgard-host%, Asset Labels: [redacted], and Query: [redacted].

Copy your THOR Flags and disable the scheduled group scan. You can now recreate the scheduled group scan with the exact settings and your target ASGARD. Afterwards, you can activate the scheduled group scan again, this time no warnings will appear. From this point onwards, any changes to your IOCs and IOC Rulesets within your Master ASGARD will also be reflected on the ASGARD from your new scheduled group scan.

Repeat this step for any scheduled group scans which show in the warning message of your Master ASGARD. Newly created scheduled group scans do not have this bug.

9.4 AMC#012: 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.
```

9.4.1 AMC#012: 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
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
```

(continues on next page)

(continued from previous page)

```

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.

9.5 AMC#011: 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 }

```

9.5.1 AMC#011: 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.

9.6 AMC#010: 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.

9.6.1 AMC#010: 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 in the meantime, to avoid cleaning up after the changes to the endpoints have been made.

9.7 AMC#009: agent-access.log is not being rotated

Introduced Version	Fixed Version
<= 2.14.6	>2.14.6

The file `/var/lib/nextron/asgard2/log/agent-access.log` is not included in the logrotate configuration. This could cause a full disk after a certain period of time, due to the file growing bigger and not being rotated.

9.7.1 AMC#009: Workaround

To fix that problem you have to connect via ssh to your ASGARD Management Center and edit the following file (as root user):

```
user@unix:~$ ssh nextron@asgard
```

```
nextron@asgard:~$ sudoedit /etc/logrotate.d/asgard
[sudo] password for nextron:
```

You will see the contents of the asgard logrotate file. The entry on the bottom of the file will be the one you need to change. Please make sure to only change the following highlighted line:

Listing 3: old agent-access.log location

```
51 /etc/nextron/asgard2/log/agent-access.log {
52     rotate 14
53     missingok
54     notifempty
55     compress
56     delaycompress
57     maxsize 10G
58     daily
59     postrotate
60         pkill -SIGHUP rsyslogd >/dev/null 2>&1 || true
61     endscript
62 }
```

Listing 4: new agent-access.log location

```
51 /var/lib/nextron/asgard2/logs/agent-access.log {
52     rotate 14
53     missingok
54     notifempty
55     compress
56     delaycompress
57     maxsize 10G
58     daily
59     postrotate
60         pkill -SIGHUP rsyslogd >/dev/null 2>&1 || true
61     endscript
62 }
```

You can save the file by pressing CTRL + O (you will be asked what File Name to write to, you can just press Enter here). Exit the file by pressing CTRL + X.

Since the logrotate job will run every day at a certain time, the changes will take affect with the next run. If you need to rotate the file immediately, run the following command:

```
nextron@asgard:~$ sudo logrotate -v /etc/logrotate.d/asgard
```

You should see in your output something along the lines of the following:

```
rotating pattern: /var/lib/nextron/asgard2/log/agent-access.log after 1 days (14
↳ rotations)
empty log files are not rotated, log files >= 10737418240 are rotated earlier, old logs
↳ are removed
considering log /var/lib/nextron/asgard2/log/agent-access.log
Now: 2023-02-13 10:10
Last rotated at 2023-02-13 10:00
log does not need rotating (log has been already rotated)
```

9.8 AMC#008: Show Asset Timeline Fails

Introduced Version	Fixed Version
<= 2.14.6	>2.14.6

After clicking on the asset timeline, the following error appears:

```
could not get client stats ID:7 ERROR: no agentlog could be opened
```

9.8.1 AMC#008: Workaround

To fix that problem you have to connect via ssh to your ASGARD Management Center and run the following commands.

```
user@unix:~$ ssh nextron@asgard
```

```
nextron@asgard:~$ sudo touch /var/lib/nextron/asgard2/log/agent.log
[sudo] password for nextron:
nextron@asgard:~$ sudo chown asgard2: /var/lib/nextron/asgard2/log/agent.log
```

9.9 AMC#007: Sigma Rule Update Fails

Introduced Signature Set	Fixed Signature Set
23.1.5-122954	23.1.9-153938 or newer

The signature set released on the 06.01.2023 contains a rule with an author field which is too long for the database field we use in AMC.

Updating the ruleset results in an error message:

could not use new blob ERROR: Error 1406: Data too long for column 'author' at row 1

9.9.1 AMC#007: Workaround

Search for rule title `Malicious PowerShell Commandlets`, click on `Update`, and deny the problematic update for this single rule by selecting `Keep current version`. You can now update the rest of the ruleset using the `Update All Rules` button.

This will disable/skip the current update of the rule. As soon as a new update is available, the rule will be shown again in the `Rule Updates` view.

Note: Denying an update for a rule will only deny the current rule update. Any future updates to this rule will be available again.

9.10 AMC#006: 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.

9.10.1 AMC#006: Workaround

Change your LDAP GroupFilter to the following:

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

9.11 AMC#005: Basename Missing Operand after SSH Login

Introduced Version	Fixed Version
2.0.0	>=2.14.5

After logging into ASGARD Management Center via SSH right after installing the base system, the following message can appear:

```
basename: missing operand
Try 'basename --help' for more information
```

It is caused by a unhandled condition in the MOTD (message of the day) script that evaluates the version of the scanners and signatures. After installing ASGARD it takes some minutes to retrieve and install all scanners from the update servers.

The issue is known and can be ignored.

9.11.1 AMC#005: Workaround

No workaround required. The issue solves itself after the download of the scanner and signature packages.

9.12 AMC#004: RPM Packages do not have a compatible architecture

Introduced Version	Fixed Version
	Under investigation

Some Linux systems return this error message when installing the RPM packages of the ASGARD agents.

```
Depsolve Error occurred: \n Problem: conflicting requests\n - package asgard2-agent-1-1.0.0.amd64 does not have a compatible architecture.
```

The issue is known and can be ignored. The installation completes successfully regardless of this error message.

9.12.1 AMC#004: Workaround 1

No workaround required. Regardless of the message the package installation completes successfully.

You can avoid the error messages using this command:

```
user@host:~$ sudo yum install --forcearch amd64 ./asgard2-agent-linux-amd64.rpm
```

For an unattended installation (no user interaction) use:

```
user@host:~$ sudo yum install -y --forcearch amd64 ./asgard2-agent-linux-amd64.rpm
```

9.12.2 AMC#004: Workaround 2

You can build a new RPM package and use it for automated installations.

Log into the Asgard server which should be used by the clients to connect to and execute the following steps:

```
nexttron@asgard:~$ sudo -u asgard2 -s # Open a shell with the access rights of the_
↪ asgard2 user
asgard2@asgard:~$ rpmbuild --target x86_64 --buildroot /var/lib/nexttron/asgard2/
↪ templates/rpm/BUILDROOT/x86_64 -bb /var/lib/nexttron/asgard2/templates/rpm/SPECS/
↪ asgard2-agent-amd64.spec
```

Use the following file instead of the RPM from the Agent Download section in the Asgard UI:

```
/var/lib/nexttron/asgard2/templates/rpm/x86_64/asgard2-agent-1-1.0.0.x86_64.rpm
```

When using `scp` to transfer the file from the server, you will need to copy the file to a directory that is accessible by the `nexttron` user. You also need to change the file permissions. One possibility to achieve this is to use the following commands:

```

asgard2@asgard:~$ exit # close the session of the asgard2 user if still open
nexttron@asgard:~$ sudo cp /var/lib/nextron/asgard2/templates/rpm/x86_64/asgard2-agent-1-
↳ 1.0.0.x86_64.rpm /home/nextron/
nexttron@asgard:~$ sudo chown nextron:nextron /home/nextron/asgard2-agent-1-1.0.0.x86_64.
↳ rpm
    
```

The resulting RPM should no longer cause the described "unsupported architecture" error message when it is used with yum or dnf.

9.12.3 AMC#004: Workaround 3

There are rare cases where the package installation should be automated and the command line flags are not an option. In this cases it is possible to perform the ASGARD agent installation manually. This requires to collect some files from ASGARD and move them to the asset that should be connected.

```

# For 64-bit systems
/var/lib/nextron/asgard2/templates/linux/asgard2-agent-amd64
/var/lib/nextron/asgard2/templates/linux/client-amd64

# For 32-bit systems
/var/lib/nextron/asgard2/templates/linux/asgard2-agent-386
/var/lib/nextron/asgard2/templates/linux/client-386

# For all systems
/etc/nextron/asgard2/ca.pem
/etc/nextron/asgard2/client.yaml
    
```

These files have to be located on the target asset as follows

```

# Preparation if it is a first time installation
mkdir -p /var/lib/asgard2-agent/

# For 64-bit systems
mv asgard2-agent-amd64 /usr/sbin/asgard2-agent-service
mv client-amd64 /var/lib/asgard2-agent/asgard2-agent

# For 32-bit systems
mv asgard2-agent-386 /usr/sbin/asgard2-agent-service
mv client-386 /var/lib/asgard2-agent/asgard2-agent

# For all systems
mv ca.pem /var/lib/asgard2-agent/ca.pem
mv client.yaml /var/lib/asgard2-agent/asgard2-agent.yaml

# Make sure access rights in the file system are secure
chown -R root:root /var/lib/asgard2-agent
chmod -R g-rwx /var/lib/asgard2-agent
chmod -R o-rwx /var/lib/asgard2-agent
    
```

Afterwards the installation is done by running:

```

user@host:~$ sudo /var/lib/asgard2-agent/asgard2-agent -install
    
```

To uninstall the ASGARD agent without using the RPM package the following steps can be used:

```
user@host:~# sudo /var/lib/asgard2-agent/asgard2-agent -uninstall
user@host:~# sudo rm /usr/sbin/asgard2-agent-service
user@host:~# sudo rm -Rf /var/lib/asgard2-agent/
```

9.13 AMC#003: Error on newly installed Management Center

Introduced Version	Fixed Version
2.11.11	Open

You just installed an ASGARD Management Center and get error messages such as

```
Error: Something went wrong
c is null
```

or

```
Error: Something went wrong
Cannot read properties of null (reading 'forEach')
```

This happens if you want to initiate THOR scans or access THOR scan settings before ASGARD was able to download the THOR packages from our update servers.

9.13.1 AMC#003: Workaround

Make sure ASGARD is able to access our update servers (see [System Status: Connectivity Test](#) or [System Status > Diagnostics](#) and that you have imported a valid license (see [Licensing](#)).

You can either wait for ASGARD to download the THOR packages automatically (check at [Updates > THOR and Signatures](#)) or initiate a download of THOR packages and signatures manually by clicking the "Manually Check for Updates" button at [Updates > THOR and Signatures](#).

9.14 AMC#002: Aurora False Positive Filters Cleared After Saving

Introduced Version	Fixed Version
<2.14.5	>=2.14.5

If the global Aurora false positive filter at [Service Control > Aurora > False Positive Filters](#) is used, the text box is empty/cleared after saving and refreshing the page.

9.14.1 AMC#002: Workaround

If the false positive tuning you want to achieve is only affecting one rule, the best place to tune it is a single rule false positive tuning at Service Control > Sigma > Rules and choosing the "Edit false positives filters of this rule" action.

If you need global false positive filter, you can edit the file `/var/lib/nextron/asgard2/products/aurora-config/false-positives.cfg` directly via the ASGARD command line. In order for the changes to take effect it is important **NOT** to click the Service Control > Aurora > False Positive Filters > Save button.

Instead go to Service Control > Aurora > Configurations and edit the configuration of the assets that need the false positive filter. To do so just open the configuration using the edit action and saving without any modifications using the "Save Configuration and Restart Aurora Agents" button. This will use the false positive filter defined in the file via CLI and restarts the assets to use the new configuration.

9.15 AMC#001: API Documentation Curl Examples Not Working

Introduced Version	Fixed Version
2.12.8	>=2.13.5

The API documentation is not showing the API key in example queries as it should and did.

9.15.1 AMC#001: Workaround

You need to manually add `-H 'Authorization: <your-API-key>'` to your queries.

Example with API endpoint `/playbooks/search`:

Non-working curl example:

```
user@host:~$ curl -X 'GET' \
'https://asgard.local:8443/api/v1/playbooks/search?limit=1' \
-H 'accept: application/json'
```

Working curl example:

```
user@host:~$ curl -X 'GET' \
'https://asgard.local:8443/api/v1/playbooks/search?limit=1' \
-H 'accept: application/json' \
-H 'Authorization: <your-API-key>'
```

You also need the `--insecure` curl flag, if you are using the self-signed certificate that ASGARD shipped with.

APPENDIX

10.1 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 }
```

10.2 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  }

```

10.3 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.

10.4 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.

10.4.1 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!

10.4.2 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.

10.5 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.

10.5.1 Use Case 1 - CSR Signing with a Microsoft Based CA

Open the Certificate Authority snap-in within Windows Server

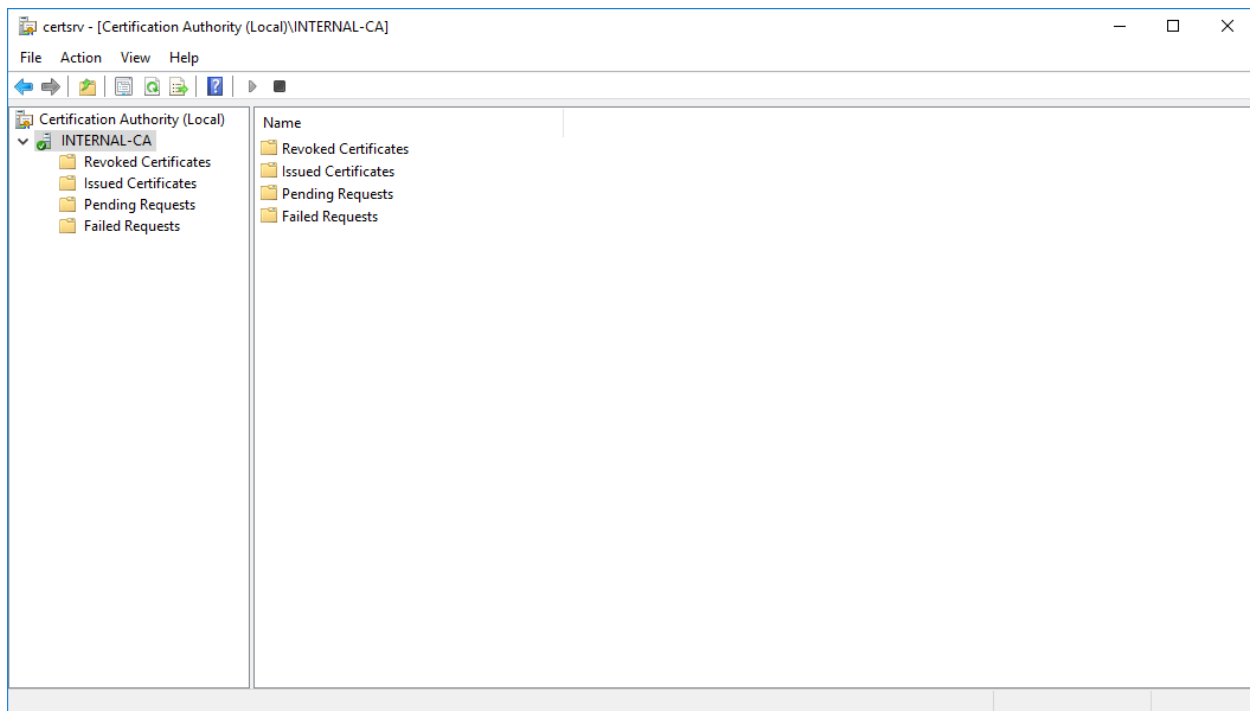


Fig. 1: certsrv – Microsoft Certification Authority Main Page

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.

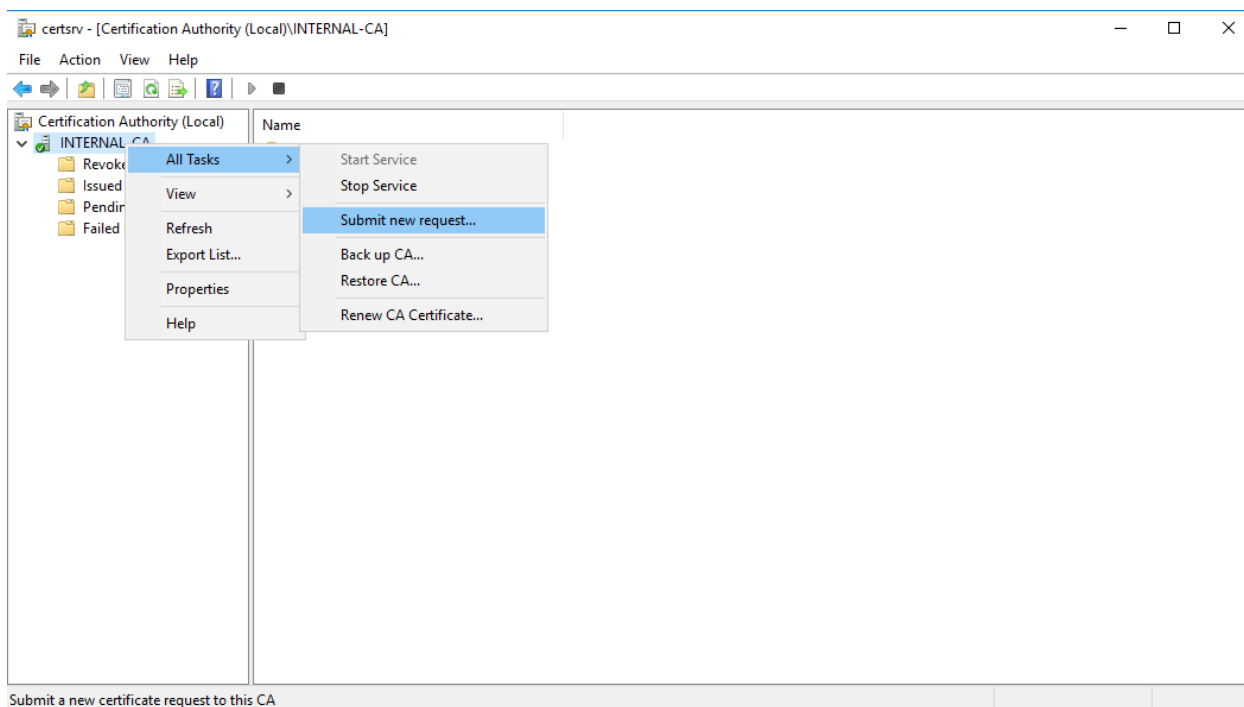


Fig. 2: certsrv – Submit new request

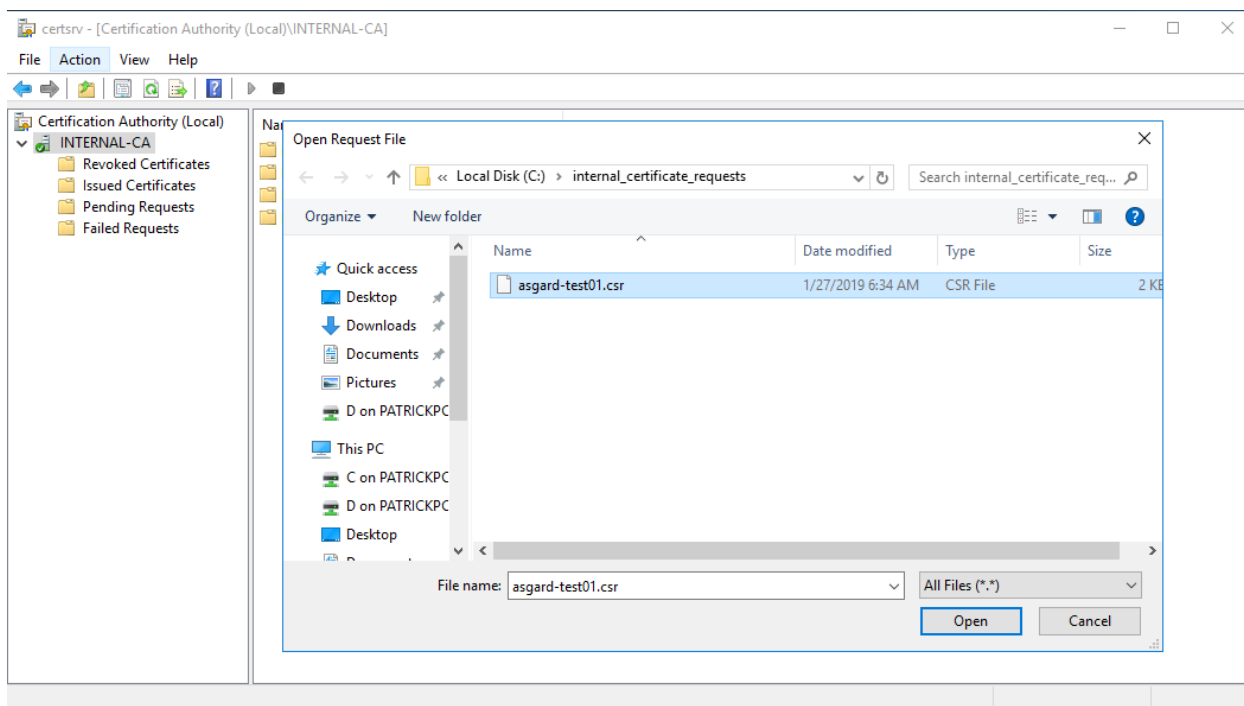


Fig. 3: certsrv – Locate the CSR to be signed

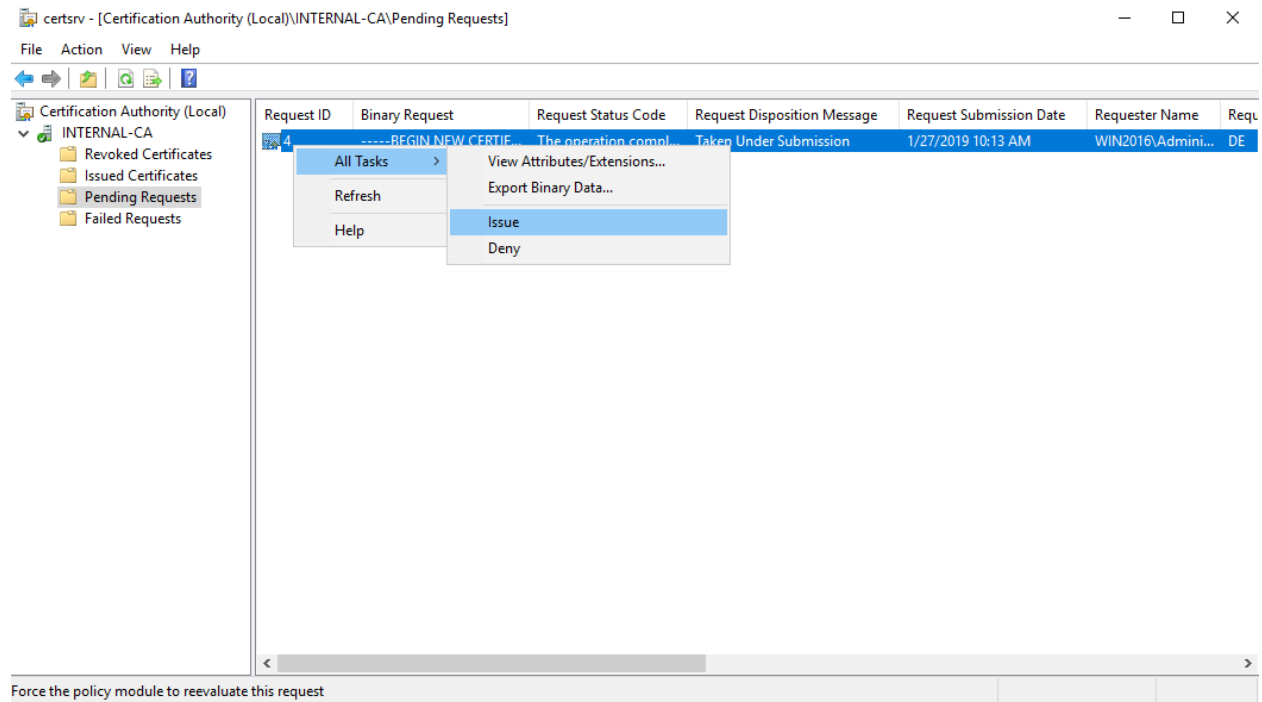


Fig. 4: certsrv – Issue the certificate

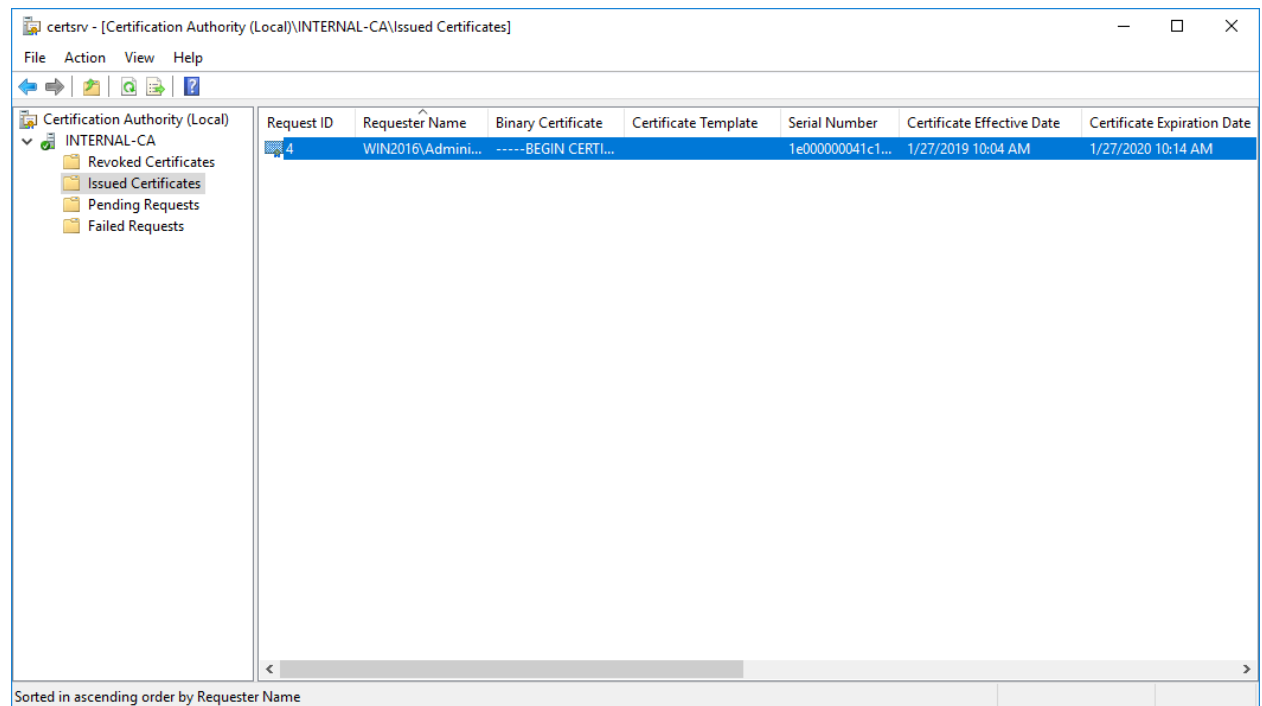


Fig. 5: certsrv – Locate issued certificate

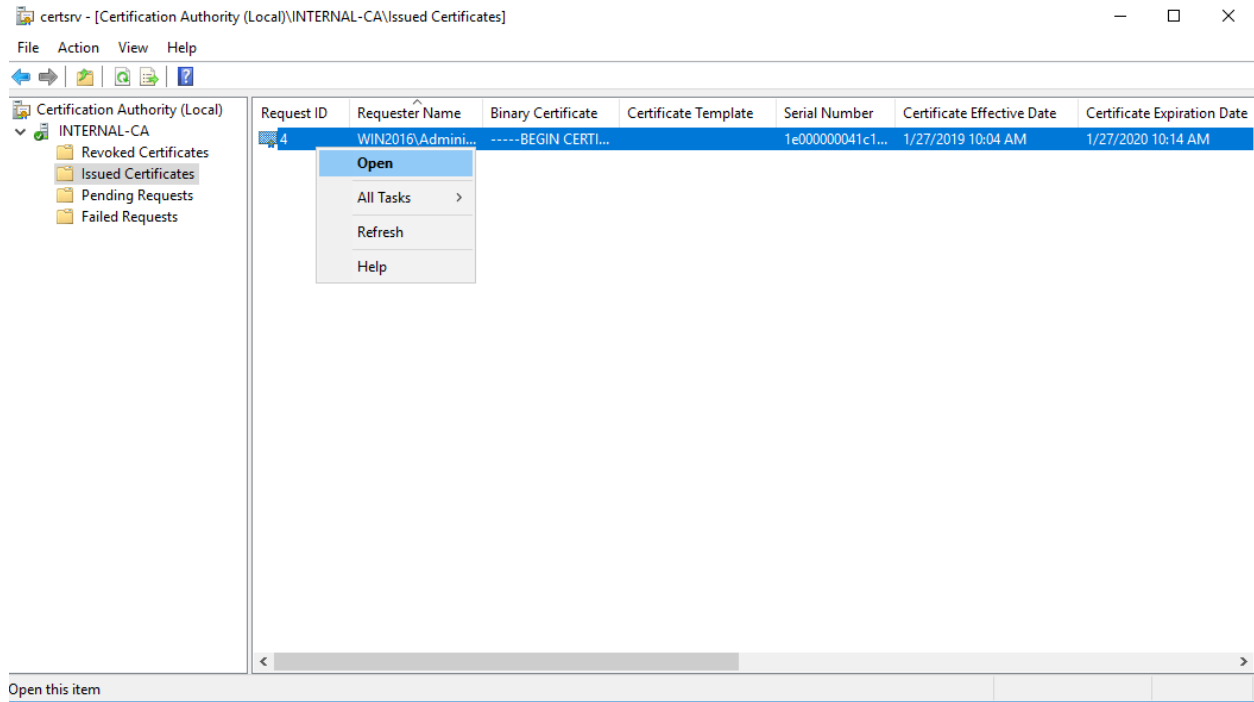


Fig. 6: certsrv – Export certificate

After the service has been successfully restarted, the installed certificate is shown in the browser.

10.5.2 Use Case 2 - CSR Signing with an OpenSSL Based CA

Warning: In order to avoid security warnings¹ 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)

¹ 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).

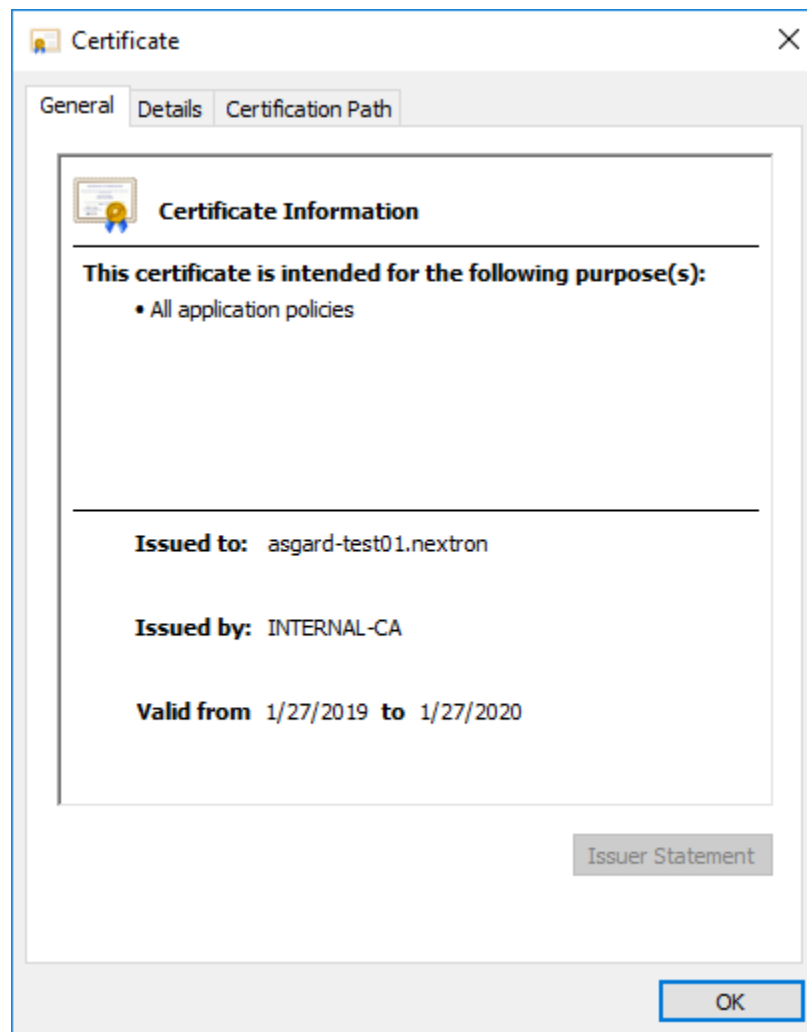


Fig. 7: certsrv – Export certificate

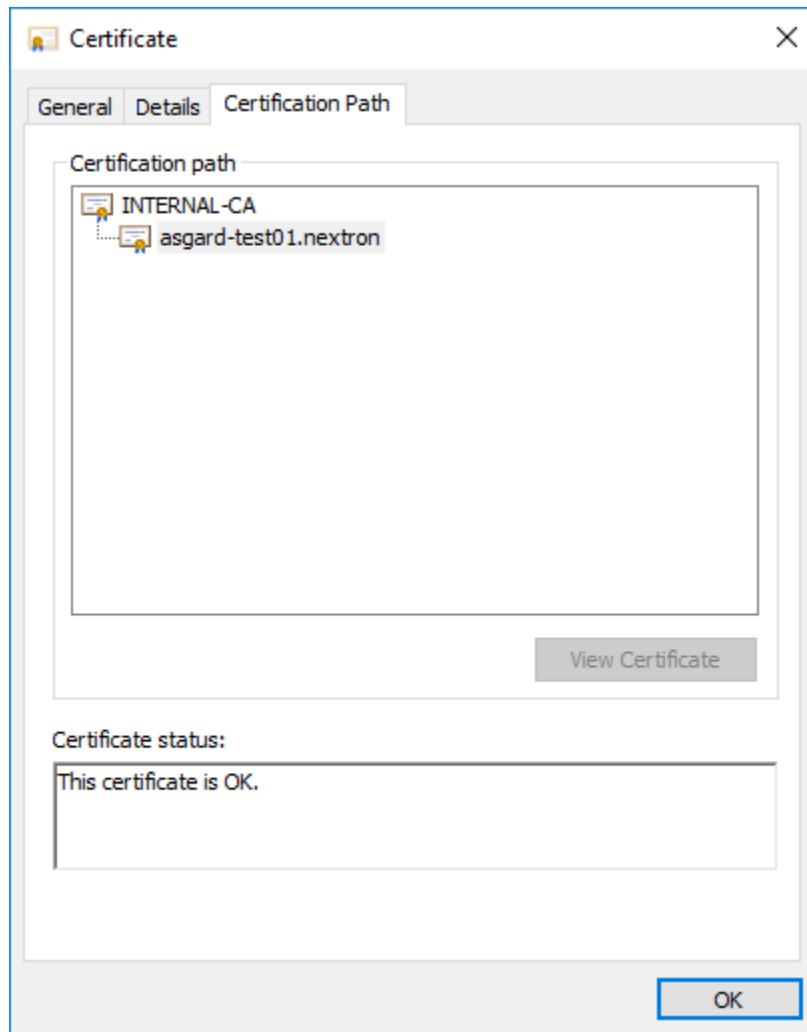


Fig. 8: certsrv – Export certificate

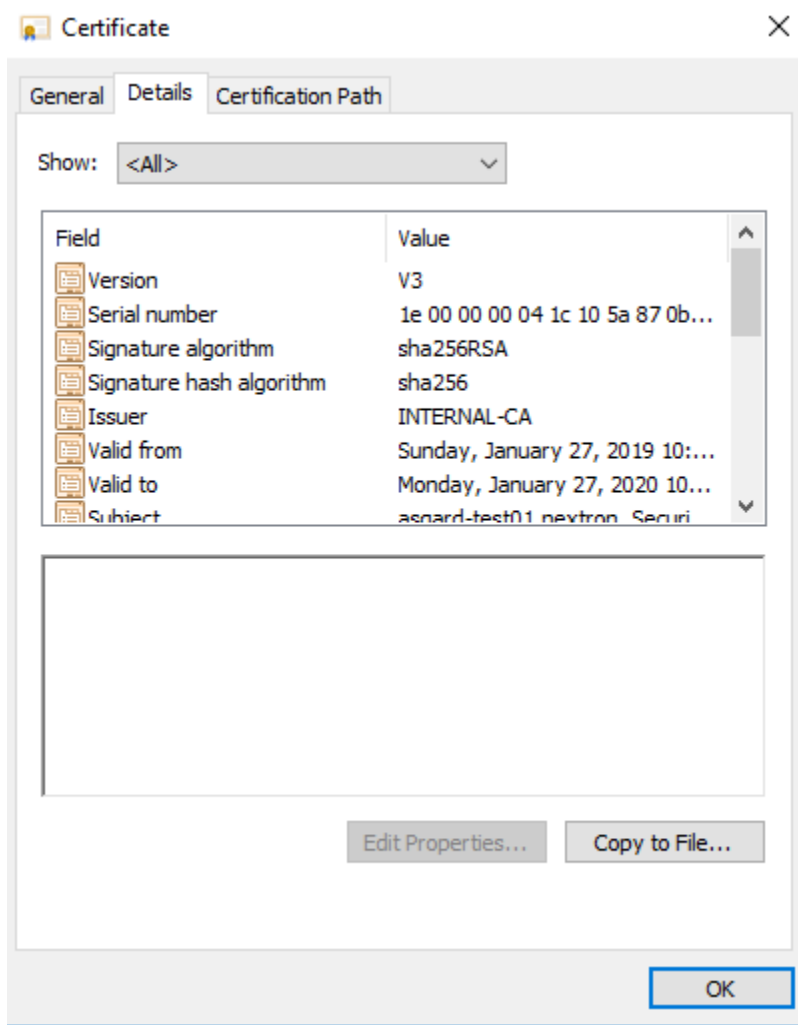


Fig. 9: certsrv – Export certificate

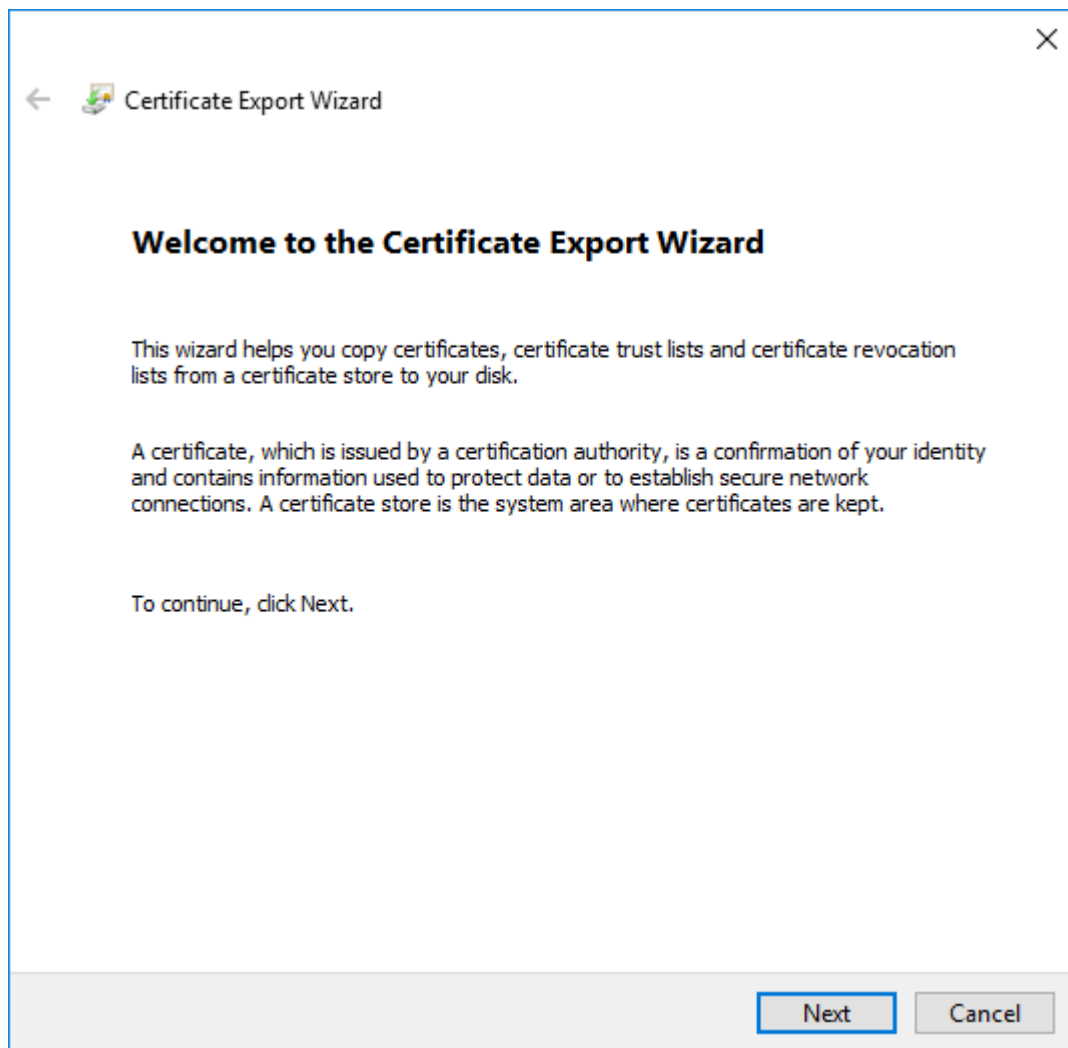


Fig. 10: certsrv – Export certificate

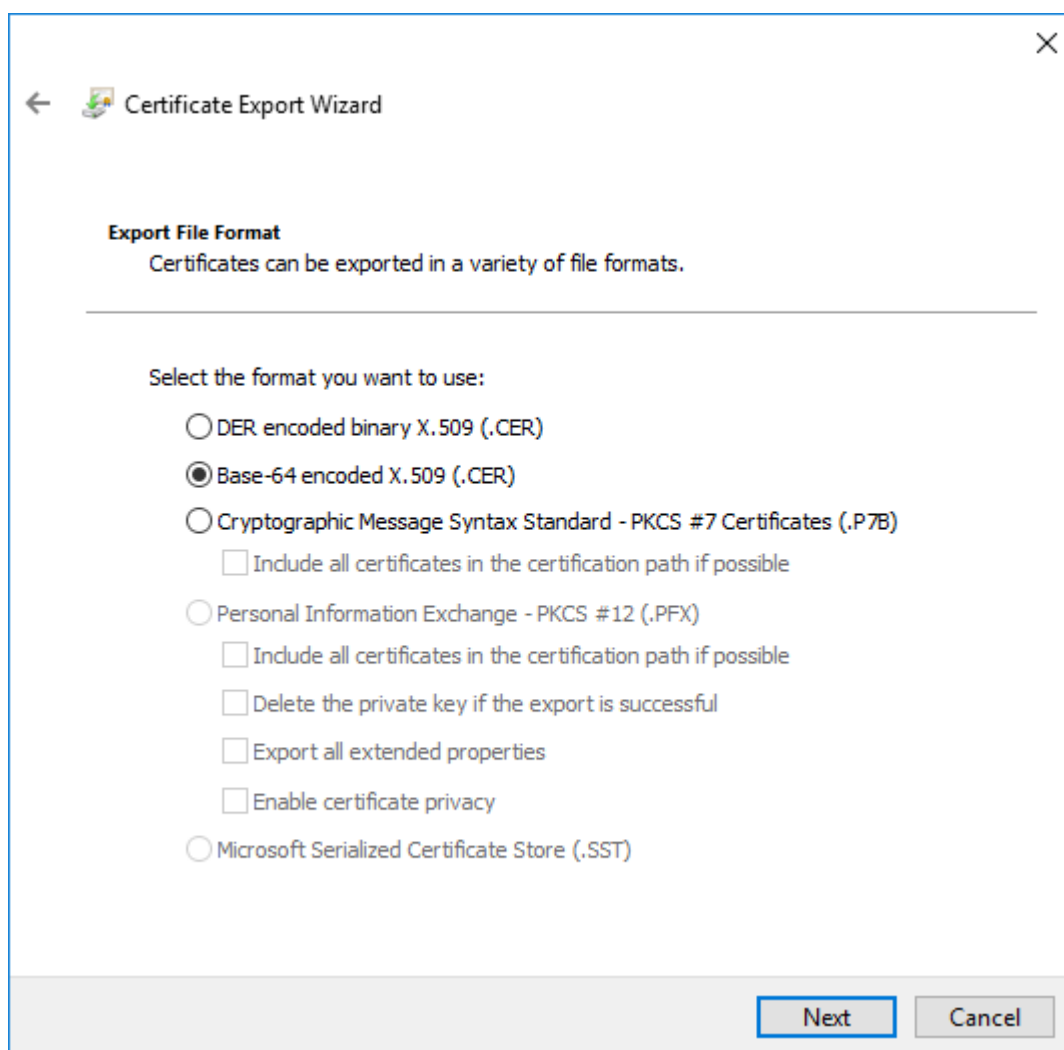


Fig. 11: certsrv – Export certificate

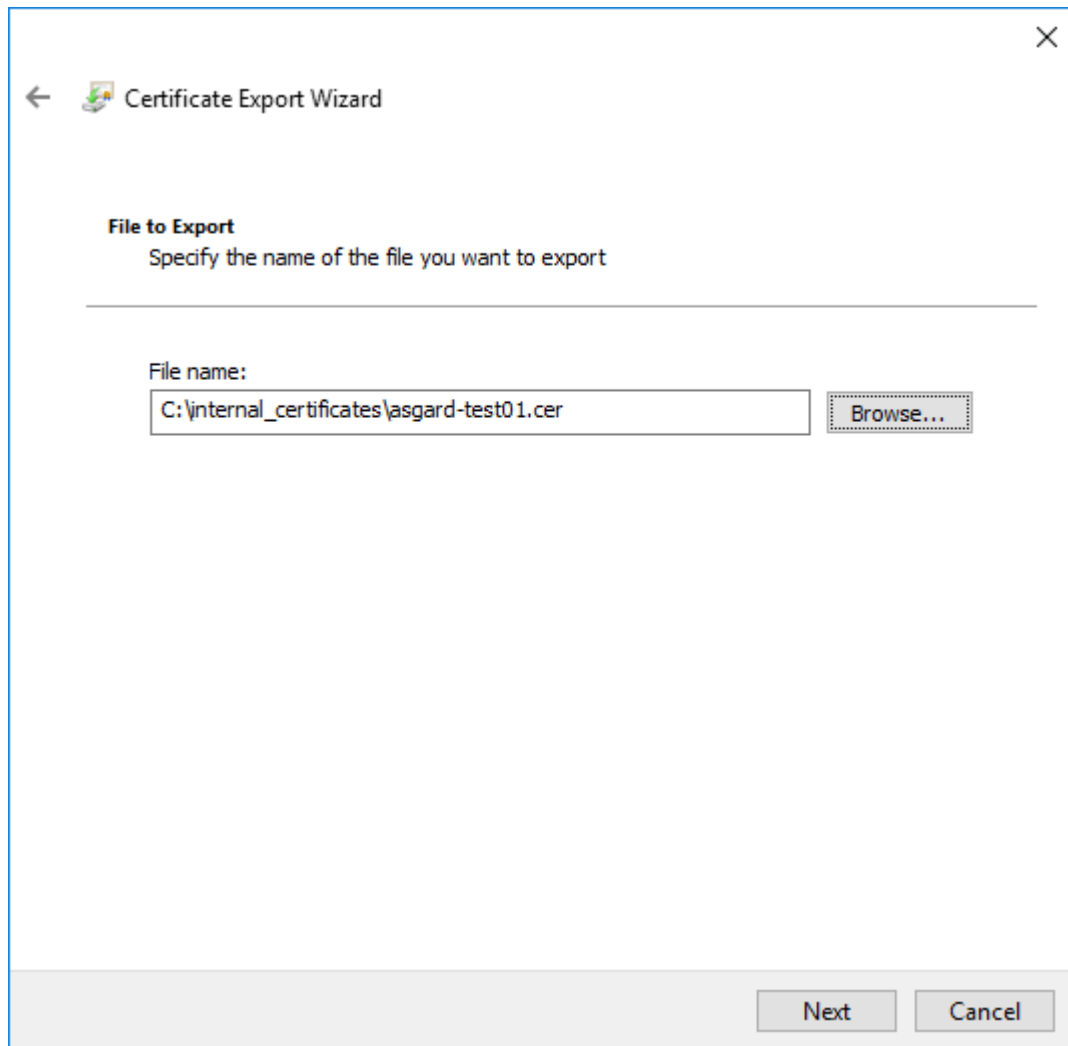


Fig. 12: certsrv – Export certificate

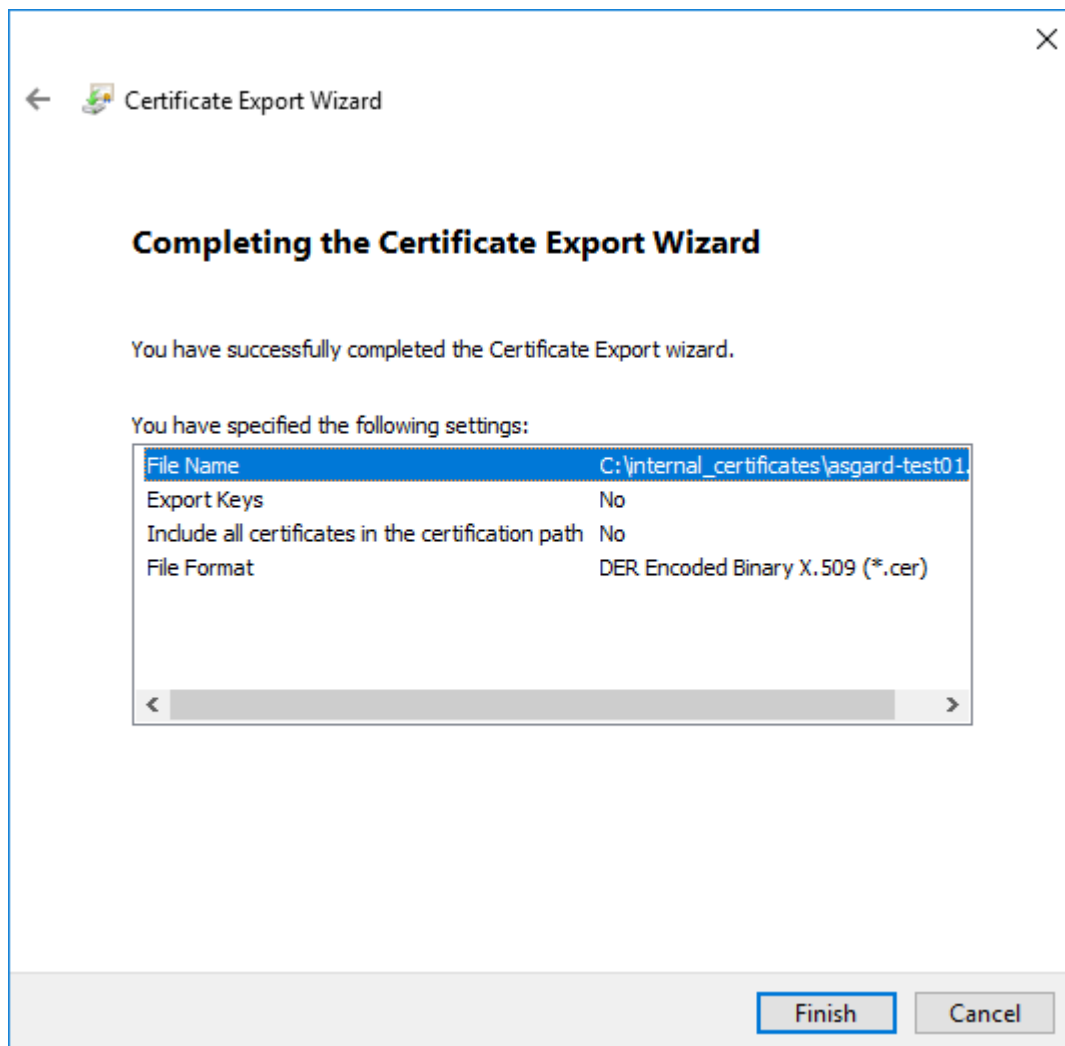


Fig. 13: certsrv – Export certificate

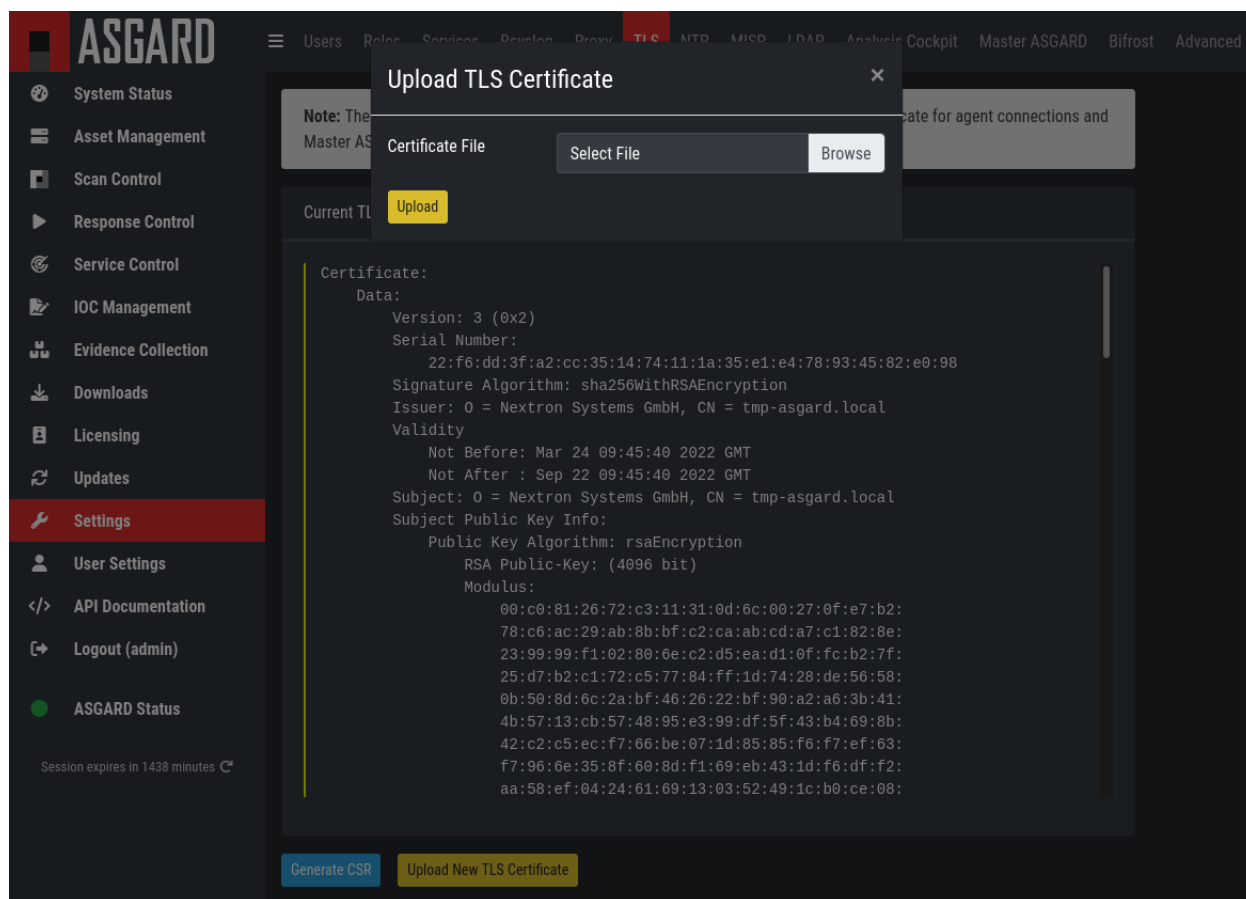


Fig. 14: ASGARD Certificate Import

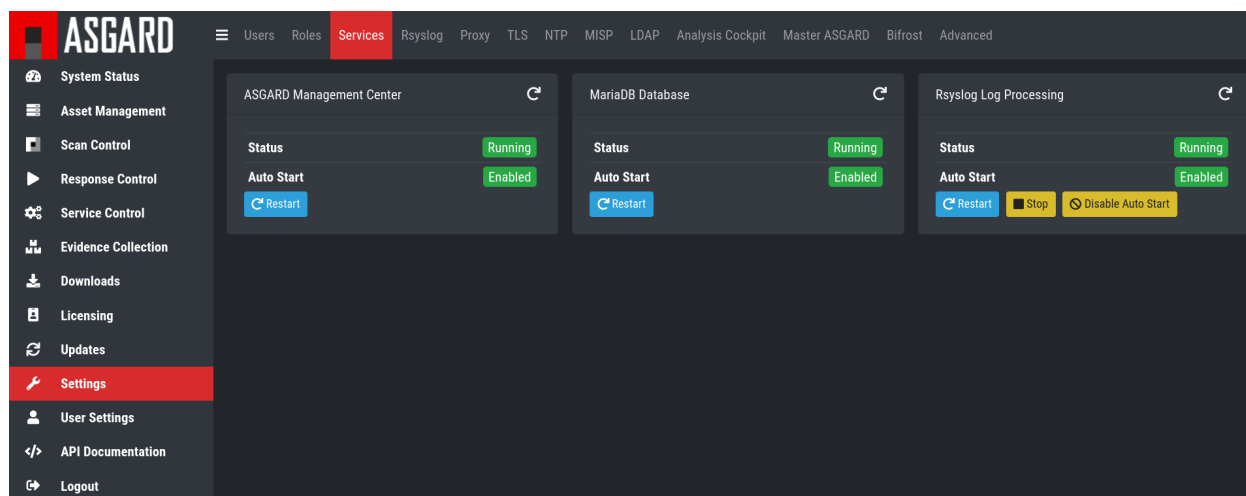


Fig. 15: ASGARD service restart

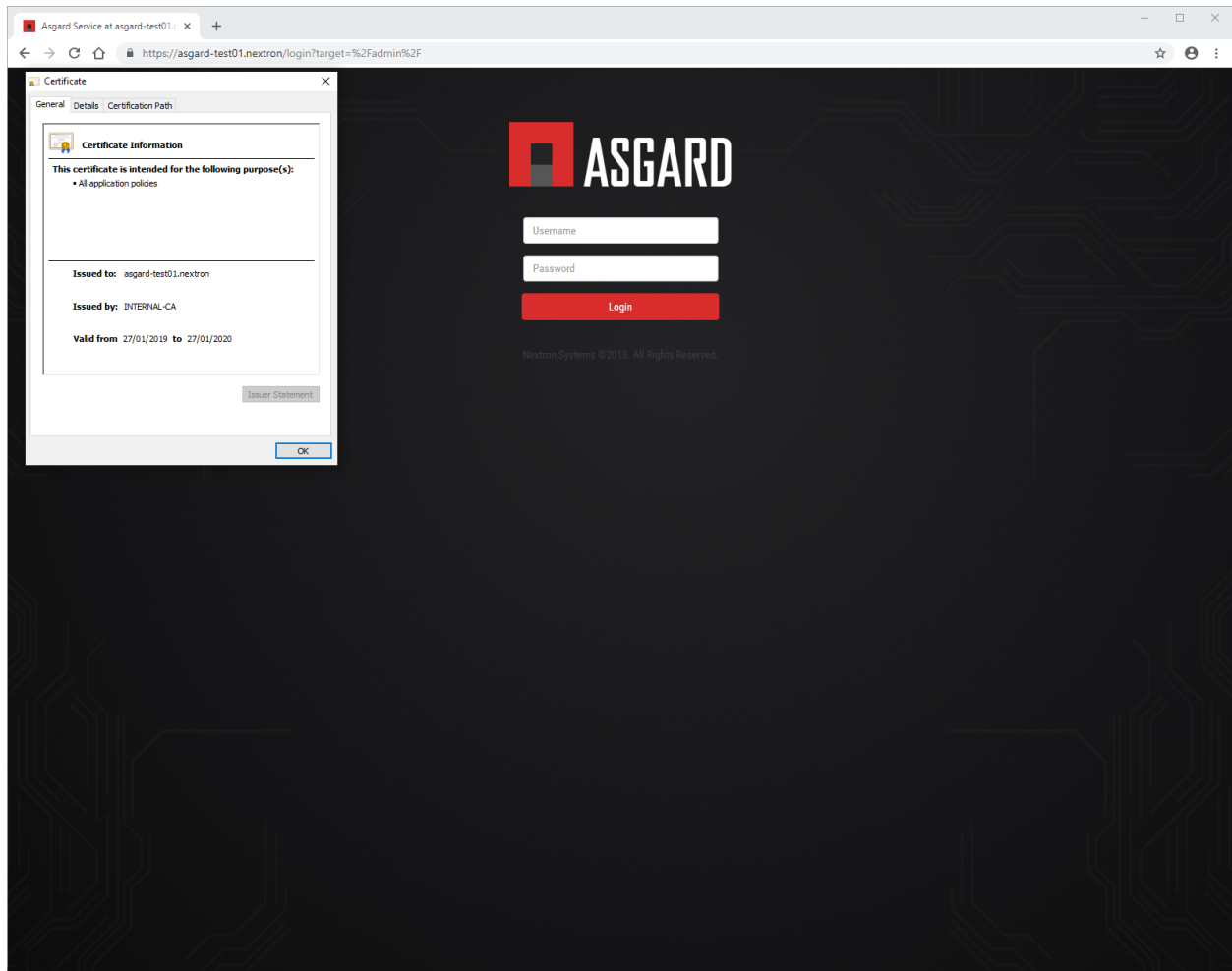


Fig. 16: ASGARD certificate installation check

(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)

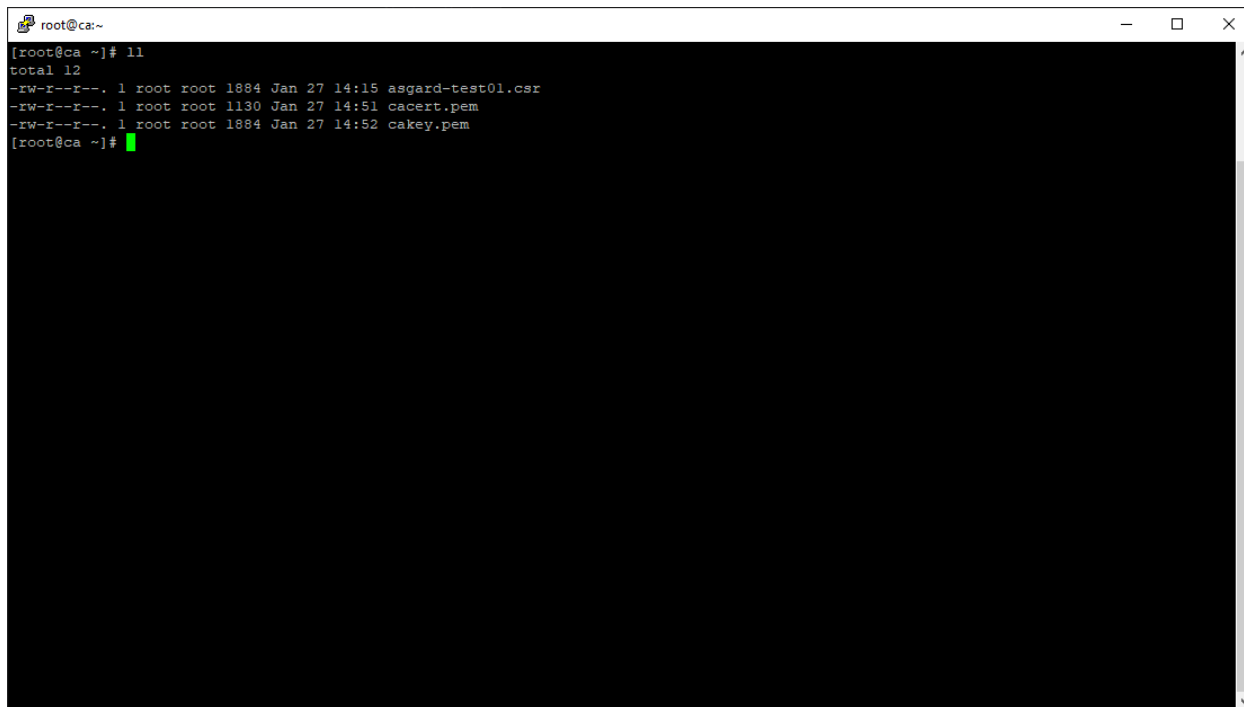
(continued from previous page)

```

c2:9f:69
Exponent: 65537 (0x10001)
Attributes:
Requested Extensions:
X509v3 Subject Alternative Name:
DNS:asgard-test01.nextron, 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. 17: 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. 18: 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:~# 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. 19: Signing procedure

```

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. 20: 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. 21: 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. 22: Signing procedure – Locating the generated certificate

10.6 Agent Migration from ASGARD v1 to v2

This document will guide customers with an existing ASGARD version 1.x to perform an agent migration to ASGARD version 2.x.

The new release of ASGARD Management Center brings not only a redesigned interface, but also major changes in the architecture and usability, making it faster, more robust and easier to use.

10.6.1 Prerequisites

You need to prepare some data prior to starting the migration.

Account Data and Network Access

Ensure you have access and credentials to the following systems, as well as connectivity as follows:

- **ASGARD Management Center version 1**
 - Administrative Web User
 - Credentials for the ssh user: bsk
- **ASGARD Management Center version 2**
 - Administrative Web User
 - Credentials for the ssh user: nextron
- **Connectivity between ASGARD 1 and ASGARD 2**
 - Required only if new agents are transferred via SCP
- **Client/Server System(s) connected to ASGARD v1 needs connectivity to ASGARD v2**
- **Access to a new update server**
 - update1.nextron-systems.com
 - update2.nextron-systems.com
 - update3.nextron-systems.com

For a detailed and up to date list of our update and licensing servers, please visit <https://www.nextron-systems.com/hosts/>.

10.6.2 Migration

Identify the agents you want to migrate and perform the following actions on each of the them.

Identify the system to be migrated

Connect to your ASGARD Management Center version 1.x and identify the system you plan to migrate.

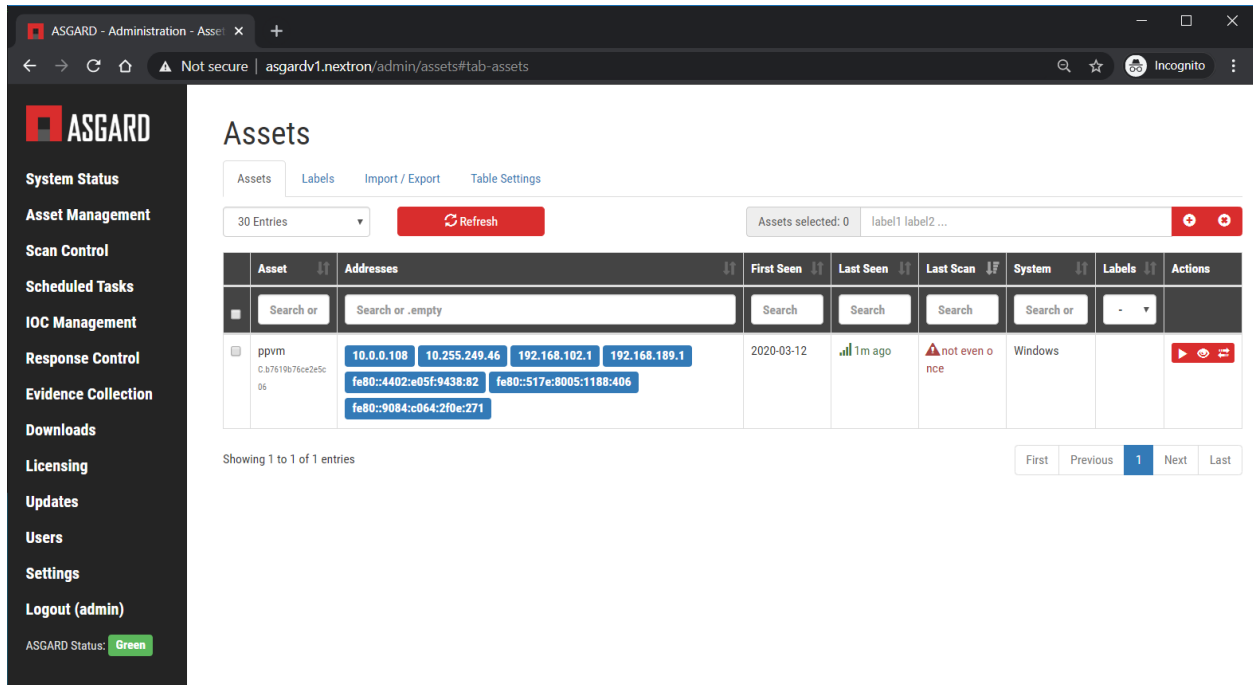


Fig. 23: Overview of Assets

Transfer the new ASGARD Windows agent to the ASGARD version 1.x Server

Connect to your new ASGARD version 2.x server over SSH and transfer the new windows agent to the old ASGARD version 1.x server.

This step will allow the old ASGARD version 1.x server to distribute the new agent.

Note: In this step you require the password of your ASGARD version 1.x and your ASGARD version 2.x

Connect to ASGARD version 2 over SSH

```
user@unix:~$ ssh nextron@asgard-v2.domain
nextron@asgard-v2.domain's password:
nextron@asgard-v2:~$
```

Copy the new agent(s) to ASGARD version 1.x

You will find all new agents under `/var/lib/nextron/asgard2/installer`, this example will cover a migration of a windows x64 system. Please see the following chapters for Linux/macOS hosts.

```
nextron@asgard-v2:~$ sudo su -
[sudo] password for nextron:
root@asgard-v2:~# cd /var/lib/nextron/asgard2/installer/
root@asgard-v2:~# scp asgard2-agent-windows-amd64.exe bsk@asgard-v1.domain:
bsk@asgard-v1.domain's password:
asgard2-agent-windows-amd64.exe                                100% 8380KB 116.9MB/s
↪ 00:00
root@asgard-v2:~#
```

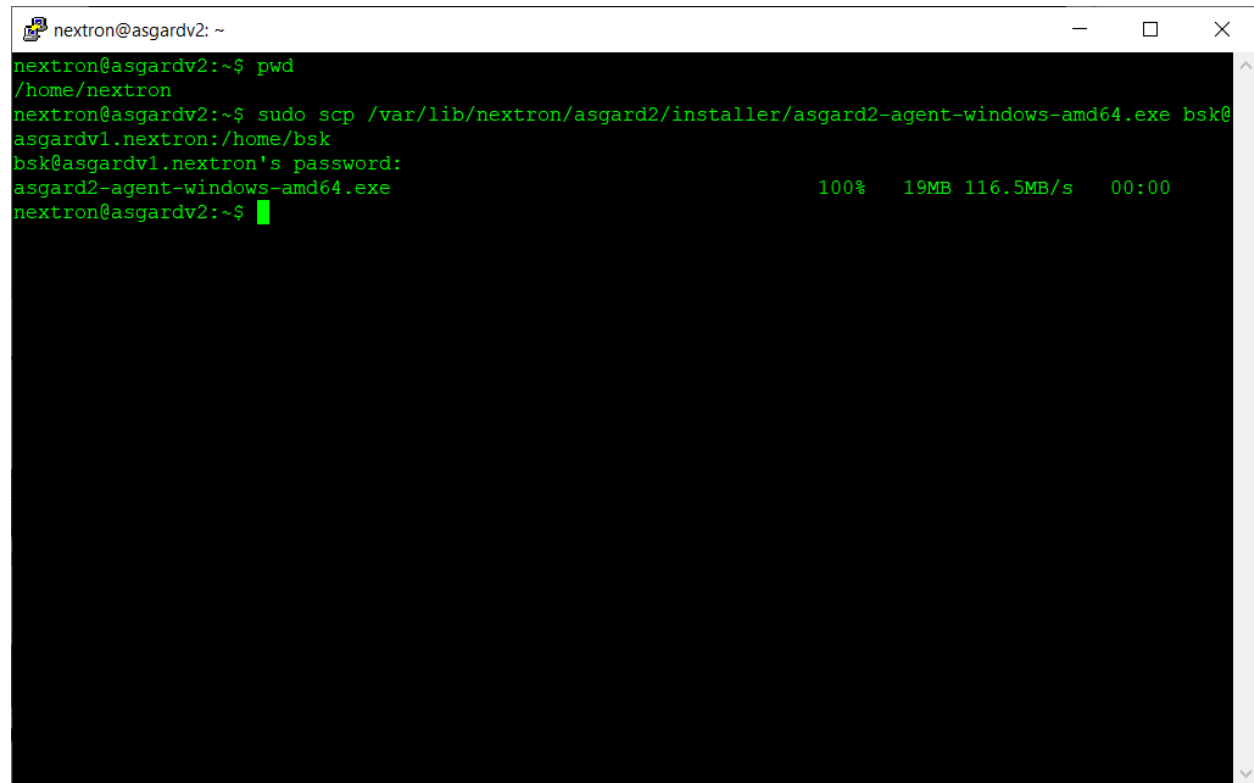


Fig. 24: New agent distribution to old ASGARD v1.x Server

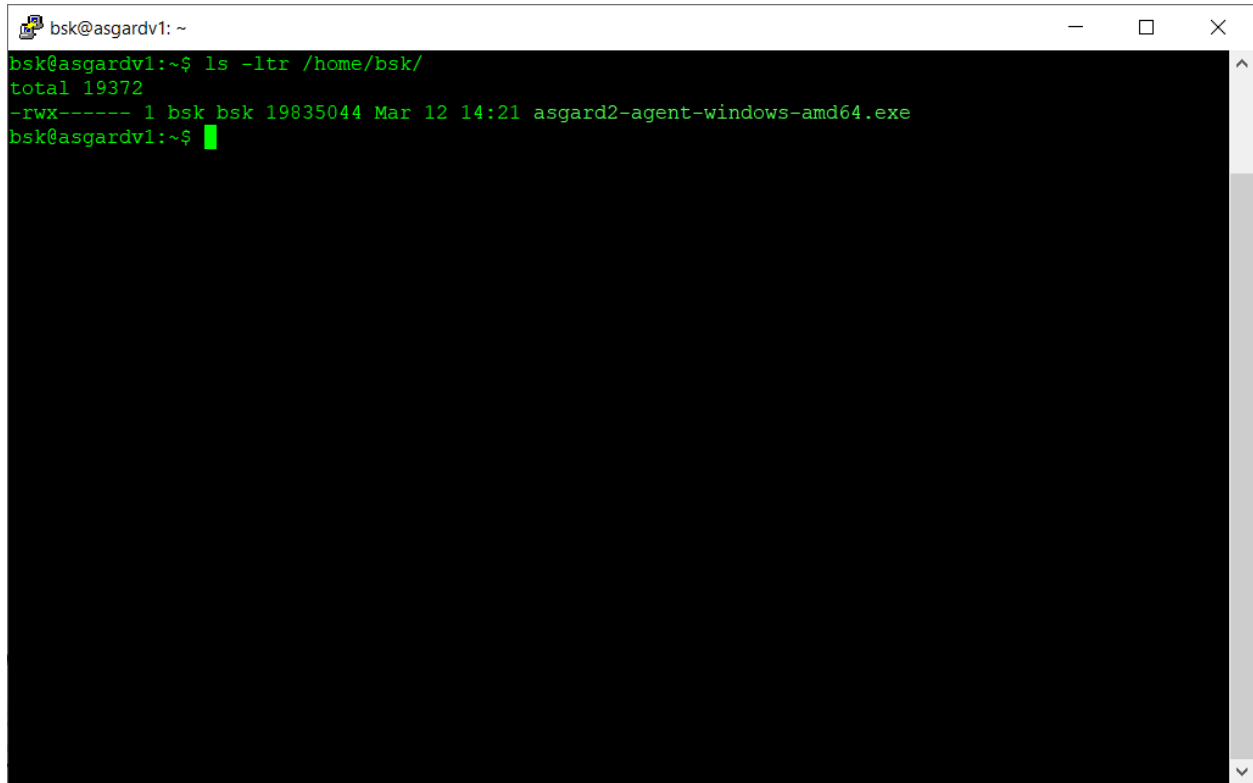
Check that the new agent has been transferred to the old ASGARD version 1.x Server

```
user@unix:~$ ssh bsk@asgard-v1.domain
bsk@asgard-v1.domain's password:
bsk@asgard-v1:~$ ls -l
total 8380
-r--r--r-- 1 bsk bsk 8580773 Feb 23 09:14 asgard2-agent-windows-amd64.exe
bsk@asgard-v1:~$ chmod 744 asgard2-agent-windows-amd64.exe
bsk@asgard-v1:~$ ls -l
```

(continues on next page)

(continued from previous page)

```
total 8380
-rwxr--r-- 1 bsk bsk 8580773 Feb 23 09:14 asgard2-agent-windows-amd64.exe
```



```
bsk@asgardv1: ~
bsk@asgardv1:~$ ls -ltr /home/bsk/
total 19372
-rwx----- 1 bsk bsk 19835044 Mar 12 14:21 asgard2-agent-windows-amd64.exe
bsk@asgardv1:~$
```

Fig. 25: Listing of agents on ASGARD version 1.x

Sign the new agents

```
bsk@asgard-v1:~$ sudo grr_config_updater upload_exe --file asgard2-agent-windows-amd64.
↪exe --dest_path aff4:/asgard-v1.domain/asgard2-agent-windows-amd64.exe --platform_
↪windows --arch amd64
```

Please modify the `aff4:/` part of the command above to reflect your hostname.

`aff4:/<your-host-fqdn>/asgard2-agent-windows-amd64.exe`

Note: Remember to save the `--dest_path`. In our case it is `aff4:/asgardv1.nexttron/asgard2-agent-windows-amd64.exe`

```

bsk@asgardv1: ~$ sudo grr_config_updater upload_exe --file asgard2-agent-windows-amd64.exe --dest_path aff4:/asgardv1.nexttron/asgard2-agent-windows-amd64.exe --platform windows --arch amd64
[sudo] password for bsk:
Using configuration <GrrConfigManager file="/usr/share/grr-server/install_data/etc/grr-server.yaml"
file="/etc/grr/server.local.yaml" >
Uploaded to aff4:/asgardv1.nexttron/asgard2-agent-windows-amd64.exe
bsk@asgardv1:~$

```

Fig. 26: Signing of executable(s)

Switch to Advanced Mode within GRR

Open your ASGARD version 1.x web interface and navigate to the **Response Control** view. You will be prompted for a username and password, use the same login information as you use to log into ASGARD.

Once you reach the Response Control Section (GRR) please navigate to the top right corner (settings gear) and switch to the Advanced Mode. Apply the settings.

Asset Selection

Navigate to the **Asset List** section on the left menu and select the asset you want to migrate. A click on the asset will select it.

Once the asset has been selected (clicking on it), navigate to the **Start new flows** section, located on the left menu.

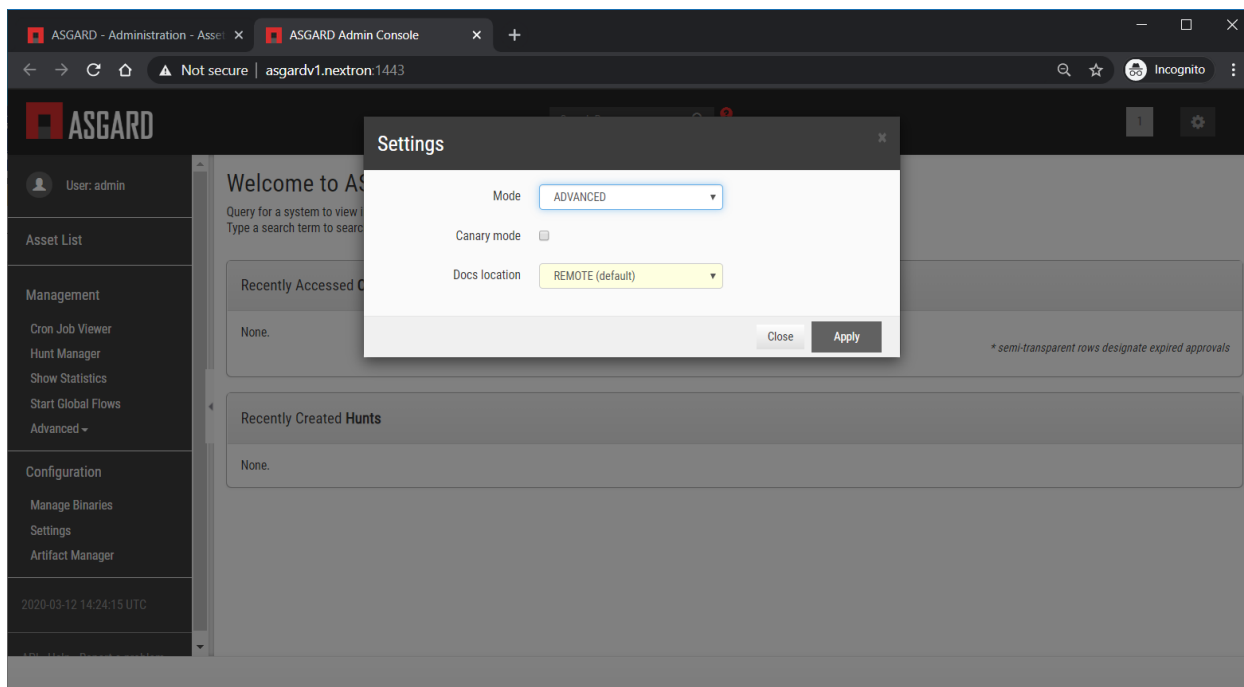


Fig. 27: GRR Advanced Mode

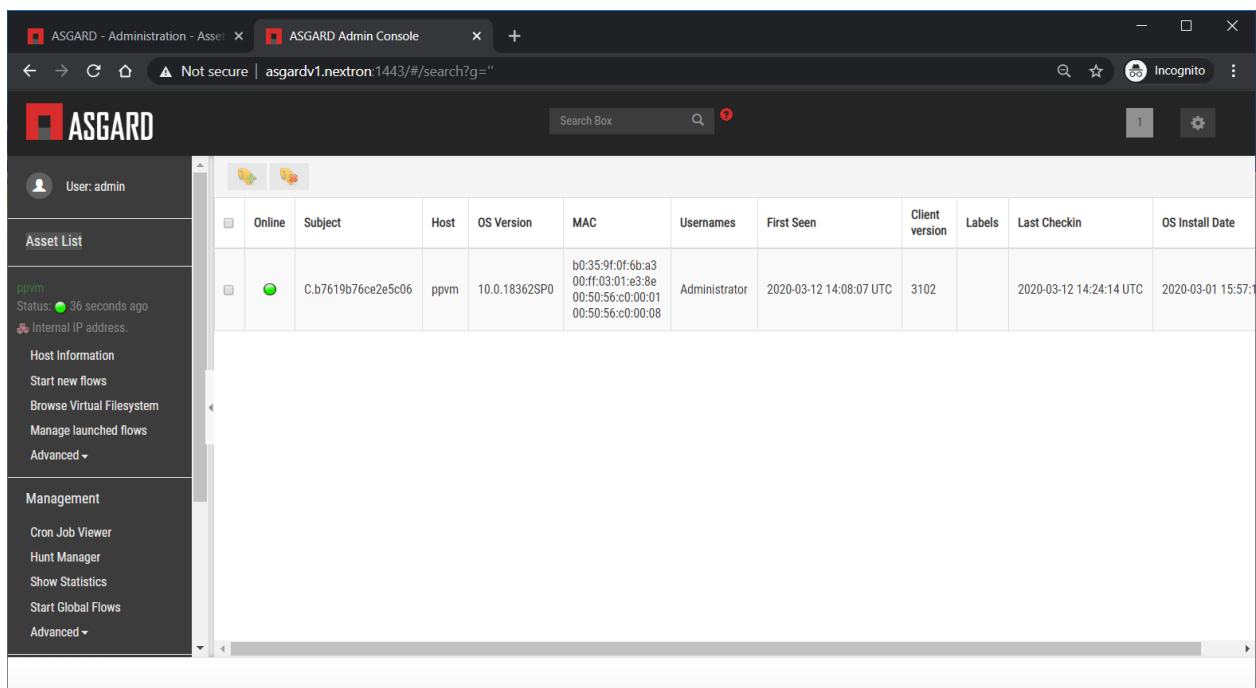


Fig. 28: Asset List view

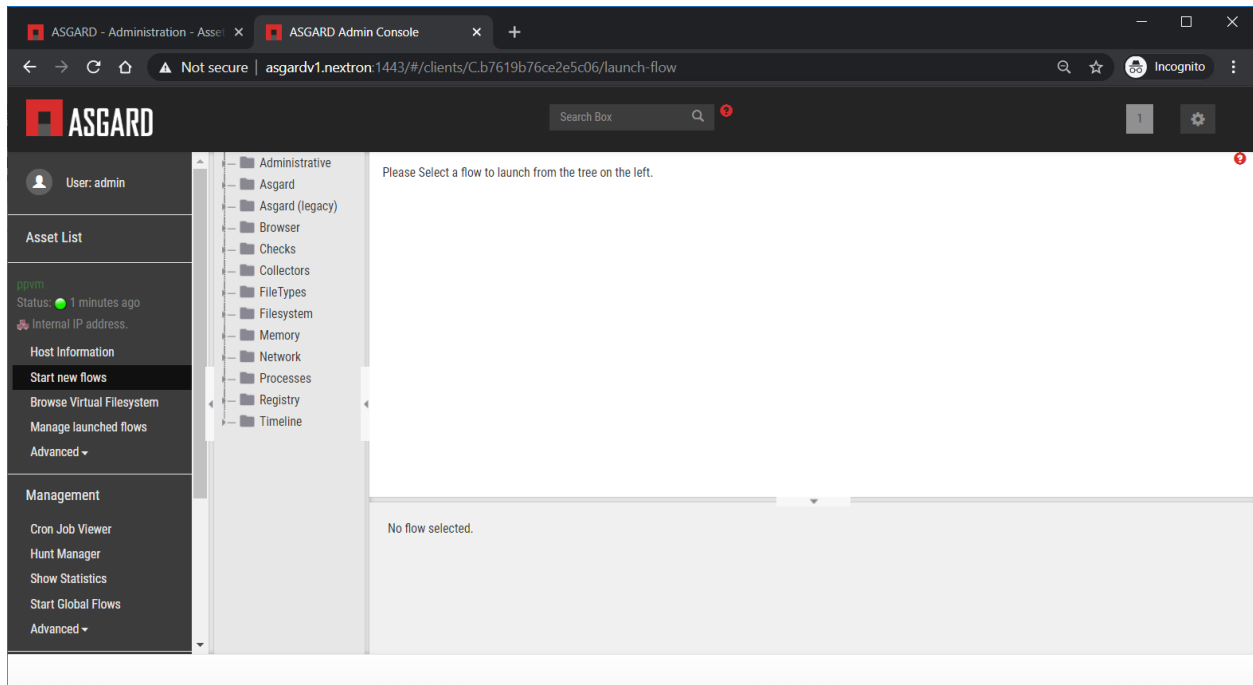


Fig. 29: Start new flow

Install the new ASGARD2 Agent

In order to install the new agent, we will need to expand the **Administrative** folder and select **Launch Binary**.

We will be requested to put in a binary, please use the binary name we gathered/created in step [Sign the new agents](#) and click **Launch**.

The used binary name was extracted from step [Sign the new agents](#). In this example `aff4:/asgardv1.nexttron/asgard2-agent-windows-amd64.exe`

After approximately 10 minutes, the binary will be executed and installed on the selected system. The status can be retrieved by navigating to the **Manage launched flows** section on the left menu.

Linux Hosts

For migrating Linux hosts please create a shell script and follow the above procedure to deploy it.

An example shell script for Debian based systems could look like this:

```
1 #!/bin/bash
2 cd /tmp
3 wget -O agent-linux.deb --no-check-certificate https://asgardv2:8443/agent-installers?
   ↳ asgard2-agent-linux-amd64.deb
4 dpkg -i /tmp/agent-linux.deb
5 rm -f /tmp/agent-linux.deb
```

Save this script in your ASGARD v1.x and sign/upload it to GRR as described in section [Sign the new agents](#), afterwards you will be able to launch a HUNT to your connected Linux Systems.

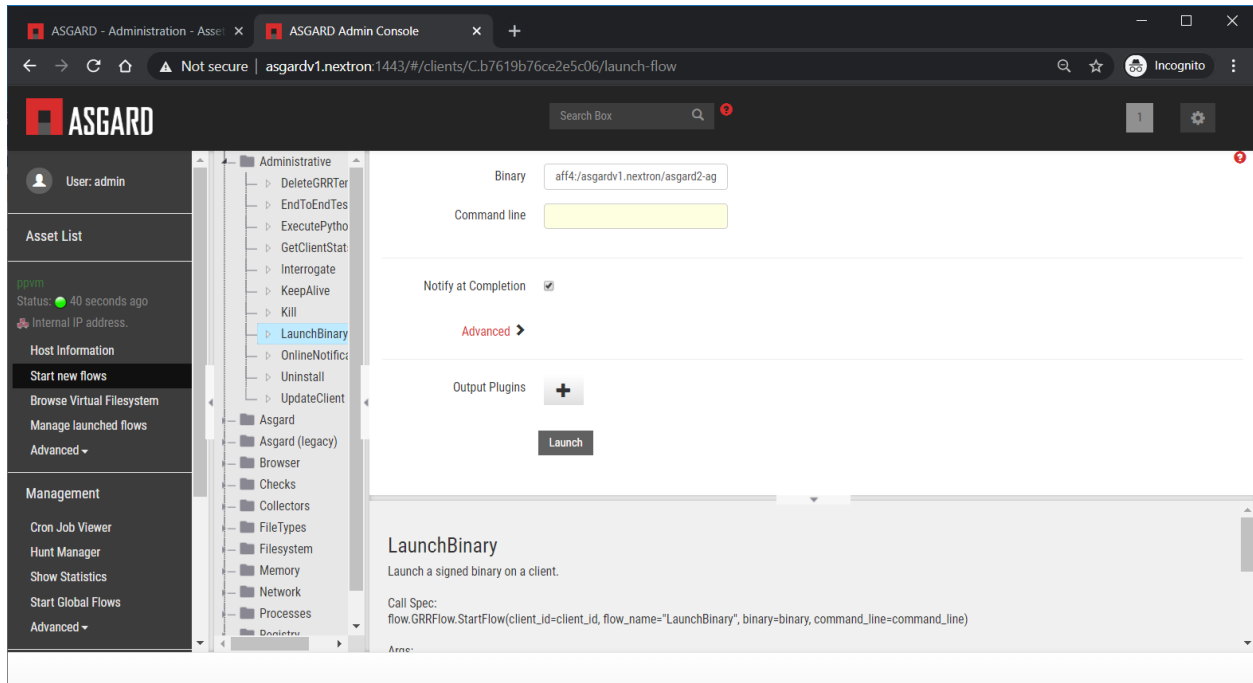


Fig. 30: Launch Binary

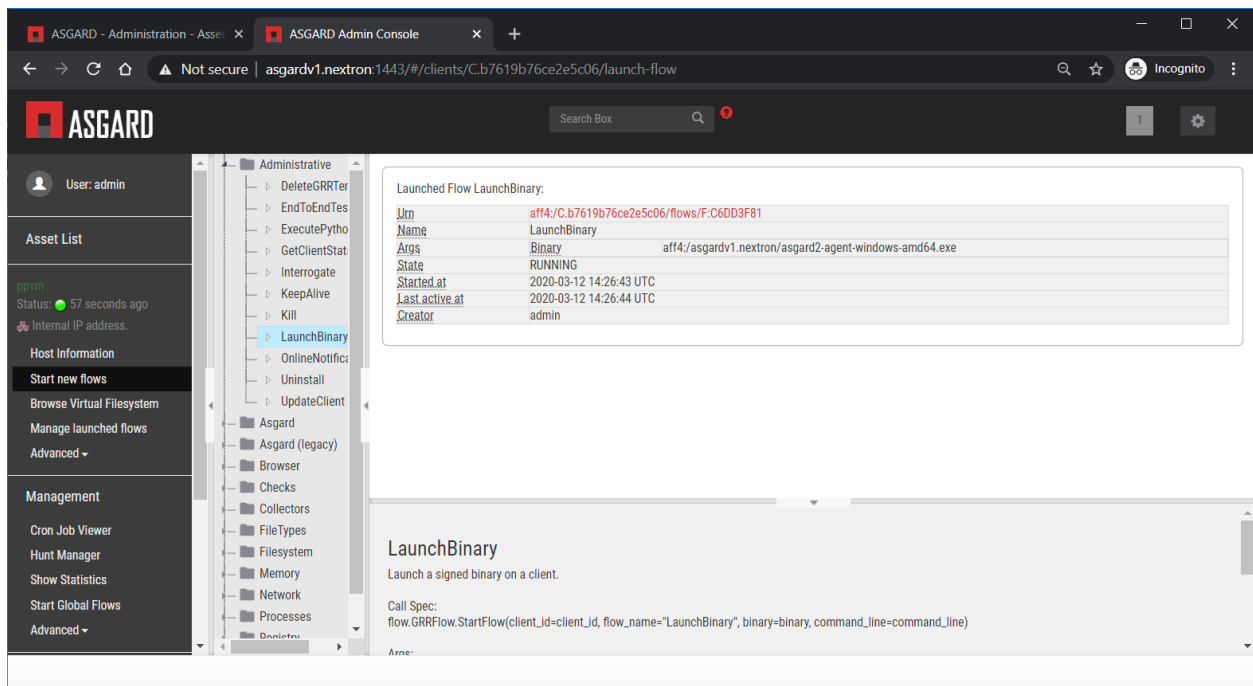


Fig. 31: Confirmation after launching the binary

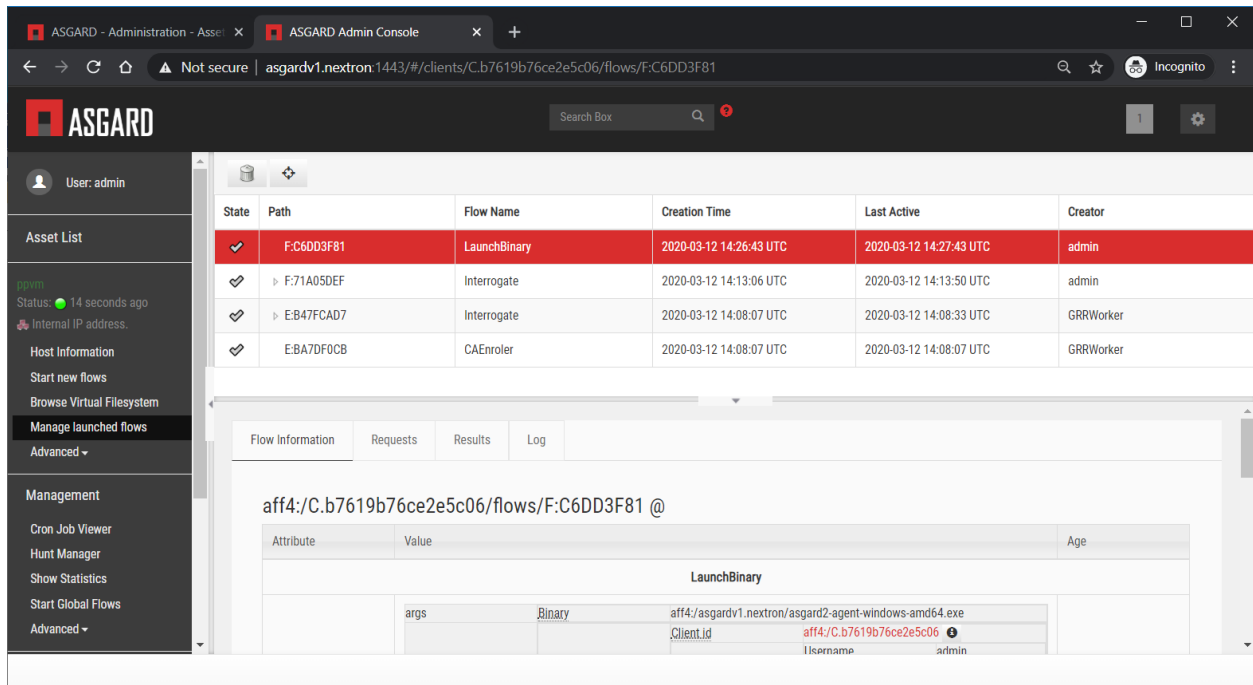


Fig. 32: Manage launched flows

Note: Please bear in mind that the above script will work only for Ubuntu/Debian systems and needs to be adapted for Redhat/CentOS systems.

MacOS Hosts

For migrating macOS hosts please create a shell script and follow the above procedure to deploy it.

An example shell script for macOS based systems could look like this:

```
1 #!/bin/bash
2 cd /tmp
3 curl -o agent-darwin.pkg -k "https://asgardv2.bsk:8443/agent-installers?asgard2-agent-
4   ↪macos-amd64.pkg"
5 sudo installer -pkg /tmp/agent-darwin.pkg -target /
rm -f /tmp/agent-darwin.pkg
```

Save this script in your ASGARDv1 and sign/upload it to GRR as described in section *Sign the new agents*, afterwards you will be able to launch a HUNT to your connected macOS Systems.

10.6.3 Migration check and completion

After the above steps have been executed, the agent should be reporting to the new ASGARD version 2.x server.

At this moment the system will have 2 agents installed, the agent reporting to ASGARD version 1.x and the agent reporting to ASGARD version 2.x

Accept the agent request

Once a new agent is reporting to ASGARD version 2.x it will automatically create a request to be part of the same. We need to accept that request.

Log into ASGARD version 2.x and navigate to the Asset Management – Requests.

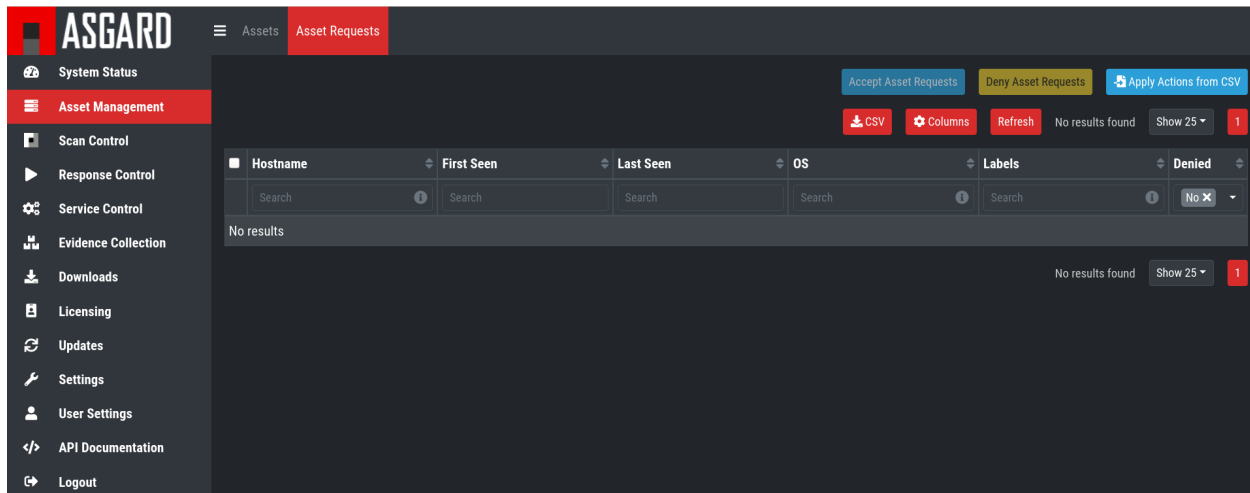


Fig. 33: Asset Management (Requests)

Select the migrated system and click on the top right on Accept. This should place the system in the Assets tab.

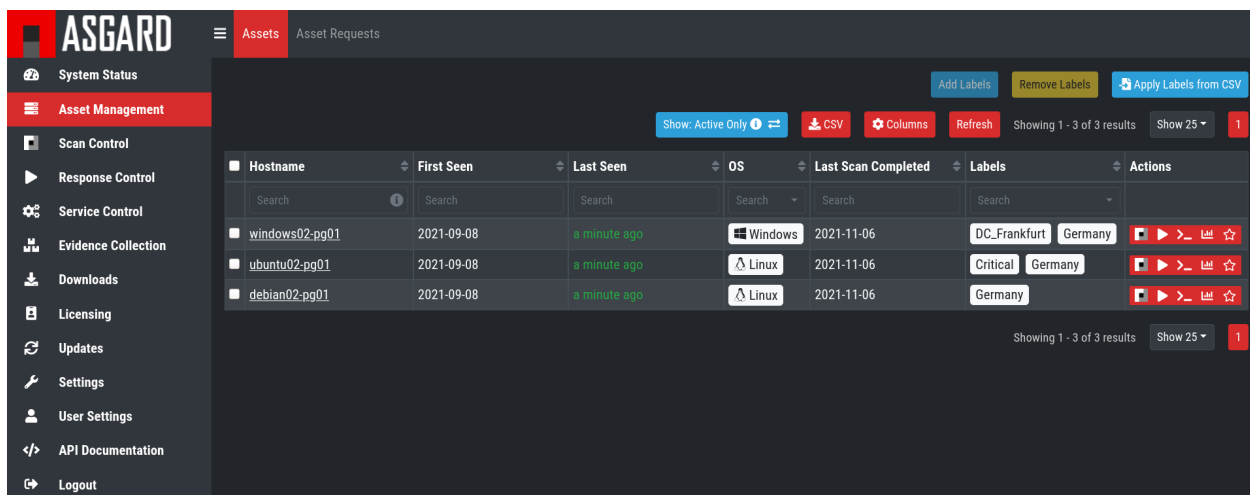


Fig. 34: Asset Management (Assets View)

10.6.4 Frequently Asked Questions

This section will cover frequent questions regarding the migration.

Will there be any problem running both agents (v1, v2) at the same time?

There are no known issues running both agents at the same time. The new ASGARD v2 agent is more lightweight and has better performance. The expected RAM utilization in idle mode demonstrated in our tests puts the new agent in a very good position, consuming only 1 MB.

Will I need more resources for my new ASGARD v2 server?

Please refer to *Hardware Requirements* for specific sizing. The overall tests performed highlight that both, server and agents, have better performance, which will allow more agents to be management per ASGARD (compared to version 1).

Can I import my memory dumps and file collections made on ASGARD v1?

Unfortunately, importing memory dumps and/or file collections made on ASGARD v1 is not possible.

CHANGELOG

This chapter contains all the changes of the ASGARD Management Center.

11.1 ASGARD Management Center

Changelog of ASGARD Management Center releases since version 2.0.0

11.1.1 ASGARD 2.17

ASGARD 2.17.2

Release Date
Thu, 1 Feb 2024 15:55:00 +0100

Type	Description
Major	Prepare for Debian 12 Upgrade (but still allow minor updates)
Bugfix	Fixed loading of sigma response rules, when corresponding sigma rules are missing

11.1.2 ASGARD 2.16

ASGARD 2.16.3

Release Date
Mon, 8 Oct 2023 13:12:00 +0200

Type	Description
Bugfix	Fixed wording in MacOS binary signatures

ASGARD 2.16.2

Release Date
Fri, 1 Sep 2023 15:49:00 +0200

Type	Description
Feature	Added uuids to tables like THOR scans, Aurora services, group tasks and many more
Change	Improved license generation for assets, THOR and Aurora. Licenses will no longer be max. valid for 90 days. Instead, they are valid as long as the ASGARD license. We also added a small tolerance that allows you to slightly exceed the license limit.
Security	OS Security Fix
Bugfix	Fixed issues with regenerating IOC rulesets for scheduled group scans (Master ASGARD only)
Bugfix	Fixed an ASGARD license issue in combination with Master ASGARD and Broker Network
Bugfix	Fixed an MacOS signing issue
Bugfix	Fixed small bug in agent installer for MacOS
Bugfix	Fixed freezing Broker Network configuration page (Master ASGARD only)
Bugfix	Fixed issues with delayed Full Disk Access on MacOS
Bugfix	Fixed inaccurate RAM usage measurement on MacOS and AIX in THOR launcher and Playbook launcher

11.1.3 ASGARD 2.15

ASGARD 2.15.3

Release Date
Tue, 16 May 2023 11:59:00 +0200

Type	Description
Change	Improved error message on wrong 2FA code
Change	Synchronize deleted assets with Analysis Cockpit
Change	Updated Sigma LogSources for LogWatcher
Bugfix	Fixed non-working gatekeeper to broker connection for two different host names
Bugfix	Removed some debug messages in asgard log
Bugfix	Fixed a typo in logrotate config that caused agent access log to not be rotated
Bugfix	Fixed non-working agent timeline if not agent log file exists
Bugfix	Truncate sigma rule title and creator to fit the database table requirements
Bugfix	Fixed typo in detection of deprecated and unsupported THOR versions
Bugfix	Removed raw code line in custom signature ioc table
Bugfix	Do not show 'labels: all' in group tasks that are based on ASGARD Query
Bugfix	Fixed non-working deletion of agent installers that are tagged as legacy
Bugfix	Fixed synchronization issues with Analysis Cockpit in very large environments
Bugfix	Fixed crashing LogWatcher caused by Sigma rulesets without custom rules

11.1.4 ASGARD 2.14

ASGARD 2.14.6

Release Date
Mon, 7 Nov 2022 15:39:00 +0100

Type	Description
Bugfix	Fixed non-working advanced labeling in group scan/task dialog

ASGARD 2.14.5

Release Date
Wed, 2 Nov 2022 10:49:00 +0100

Type	Description
Feature	Broker Network support
Feature	Search and select assets with queries, e.g. 'hostname ends with "-dev" OR labels = "dev"'
Feature	Optionally create group tasks with an asset query instead of labels
Feature	The agent config can now be maintained from ASGARD, e.g. change proxy settings
Feature	Move agent to a different ASGARD
Feature	Automatically resume THOR scans that have been terminated due to shutdown signals (e.g. on reboot)
Feature	Added a lot new ASGARD features to Master ASGARD, e.g. manage and download agent installers, manage Broker Network
Feature	Allows to delete assets
Feature	Delete agent installers
Feature	Added diagnostic checks to diagnostic download packs
Feature	Support unix filepath format in playbooks for Windows targets
Feature	Detect assets that run with same key material, e.g. cloned assets
Feature	Forward THOR and Aurora events via rsyslog
Feature	Migrate key material from old agent config on agent re-installation
Feature	Added more columns in some tables, e.g. 'creator' in service configurations or 'active since' in services
Feature	Download ASGARD users as CSV
Feature	Set description for remote consoles
Feature	New default playbook "Collect Agent Log" (requires an agent update)
Feature	Bulk task / scan creation
Change	Require min. TLS 1.3 for all agent connections. To disable min. TLS 1.3, set "LegacyTLS=1" in the ASGARD config file.
Change	Disable "Add and activate" button for "Add group task", if "Scheduled start" is set
Change	Allow "--nohtml" flag for THOR
Change	Set scan status to error if THOR scan result does not contain 'THOR scan finished' message
Change	Collect stdout/stderr at the end of each playbook step instead of streaming it directly to ASGARD

continues on next page

Table 1 – continued from previous page

Type	Description
Change	Automatically set THOR's max runtime to unlimited and removed THOR's max runtime argument from THOR flag list
Change	Ignore deprecated sigma rules
Change	Improved compression level of some generated zip files
Change	Allow stop of group tasks without starting it
Change	Improved diagnostics for synchronization with Analysis Cockpit
Change	Disabled syslog debug log on agents by default, added option to agent installer to enable syslog
Change	Added key usage and SAN to self-signed TLS certificate for UI on installation
Bugfix	Security fixes
Bugfix	Fixed missing 'Default response mode' in Sigma ruleset details
Bugfix	Fixed some missing Aurora flags
Bugfix	Fixed non-working save button for global Sigma false positive filter list
Bugfix	Fixed NaN when removing the score of an IOC
Bugfix	Fixed a bug in event caching in offline mode of Aurora Agent and LogWatcher
Bugfix	Fixed 'Windows 11' detected as 'Windows 10'
Bugfix	Fixed missing LastLogon date in local users table
Bugfix	Disable deletion of the own user
Bugfix	Added "x86_64" in addition to "amd64" for agent installer rpm packages to support older yum/rpm
Bugfix	Fixed wrong YARA rule count after uploading YARA rules
Bugfix	Fixed "in a few seconds" last seen timestamps that have been caused by either a wrong server or browser clock
Bugfix	Removed some Aurora and Sigma error messages in ASGARD log after fresh installation
Bugfix	Removed a race condition between automatic and manual update checks that may cause corrupt product version numbers
Bugfix	Fixed missing "enabled/disabled service" history entries on ASGARDs that are connected to a Master ASGARD
Bugfix	Fixed corrupt network interfaces search in asset table for new assets that had no interrogate job yet
Bugfix	Fixed a bug in motd config that causes some error messages after a fresh installation
Bugfix	Removed c2 file name prefix from some compiled custom signatures
Bugfix	Fixed non-working obfuscated agent for AIX

11.1.5 ASGARD 2.13

ASGARD 2.13.11

Release Date
Wed, 14 Sep 2022 10:44:00 +0200

Type	Description
Bugfix	Fixed possible deadlock in synchronization between Master ASGARD and ASGARD
Bugfix	Fixed EOF error in synchronization between Master ASGARD and ASGARD
Bugfix	Removed a hard-coded limit that caused some missing data in UI

ASGARD 2.13.8

Release Date
Fri, 8 Jul 2022 08:57:00 +0200

Type	Description
Security	TLS Hardening
Security	Trusted Proxies
Bugfix	Fixed missing description for ASGARs on Master ASGARD
Bugfix	Fixed bug in first sync between ASGARD and Master ASGARD

ASGARD 2.13.7

Release Date
Mon, 30 May 2022 11:46:00 +0200

Type	Description
Security	OS Security Fix

ASGARD 2.13.6

Release Date
Wed, 18 May 2022 12:49:00 +0200

Type	Description
Bugfix	fixed non-working creation of tasks with "unlimited" rate
Bugfix	added missing "No Resource Control" option in scan control
Bugfix	fixed wrong Aurora status in expanded asset view
Bugfix	short C2 IP addresses such as 1.1.1.1 are no longer getting a 'short' hint message

ASGARD 2.13.5

Important: Master ASGARD must be upgraded before upgrading the connected ASGARs

Release Date
Tue, 12 Apr 2022 15:18:00 +0200

Type	Description
Feature	Support Aurora Agent
Feature	THOR progress bar - A progress bar in the scan table that shows the current progress of the THOR scan. On hover, you can see a detailed view of the progress
Feature	AIX Support (Beta only)
Feature	Collect JSON THOR Log (optional)
Feature	Alternatively manage iocs with files instead of ioc groups
Feature	Added 'THOR 10 Latest' option to THOR download page
Feature	New product "Aurora Signatures"
Feature	New section 'Playbook Files' that lists all files that are available for playbook steps. This section also supports downloading, deleting and uploading files.
Feature	New tab 'Diagnostics' that lists all components with their status
Feature	New loading bar when refreshing tables
Feature	Custom IOC rulesets and MISP rulesets support for Aurora Agent
Feature	The Master ASGARD can now generate THOR download links and provide a License API, too
Feature	Added 'Auto Refresh' to most tables that can automatically refresh the table in a specified interval
Feature	Show total ram and disk usage in overview page
Feature	New filter 'Show all / show active only' in Service Control
Feature	Show which scheduled group scans are affected when compiling or deleting custom IOC rulesets or MISP rulesets
Feature	When adding new scans with custom IOC rulesets, a warning will be shown if a ruleset contains uncompiled changes
Feature	Single Scans and Single Tasks can now be created in Scan Control and Response Control with the 'Add Scan' / 'Add Task' buttons
Feature	Show warning if automatic THOR Signature updates are disabled and the currently used THOR Signatures are outdated
Feature	Show warning if ASGARD license expires soon
Feature	Show warning if a configured scheduled group scan is running with an outdated THOR version
Feature	Added ntp to services in settings section
Feature	Custom max. runtime for scans and tasks
Feature	Added API endpoints 'Add Playbook File' and 'Search Playbook Files' to API documentation
Feature	In the Downloads > THOR > Download Token section, the latest usage of the download token will be shown
Feature	New Sigma response flag "lowprivonly" that applies responses only on processes with low privileges
Feature	Logging time stats and network traffic of Master ASGARD synchronization
Feature	Show services that use ioc / misp / sigma ruleset when compiling / deleting ruleset
Feature	Show number of assets per service configuration
Feature	Show pending changes, available revision and running revision in service table
Feature	"Available since" and "Used since" in THOR / THOR Signatures and Aurora products table
Feature	Show warning if selecting all entries in a table but table has more than 1 page
Feature	Test proxy
Feature	Show TLS information
Feature	Show NTP information
Feature	Recommended response actions for Sigma
Feature	Added success notifications in UI
Feature	The version of the used Aurora Agent can now be pinned per service configuration
Feature	Completely refactored agent installer section. Added more information like asset labels and proxy and added repacker buttons per installer.
Change	Removed the 'is directory' property in playbook steps. There will be no difference anymore between files and directories when collecting a filepath or directory
Change	Completely refactored the API documentation, the API itself has not been changed

continues on next page

Table 2 – continued from previous page

Type	Description
Change	Cosmetics
Change	Wordings
Change	Added a lot more tooltips and information
Change	Other smaller UX stuff
Change	Improved performance between Master ASGARD and ASGARD
Change	Table columns are not clickable anymore, use the expand button in the first column instead
Change	Added hostname of ASGARD to CSR generator
Change	Playbook steps can now be managed in the right sidebar instead of the expanded table row in the playbook table
Change	Separated playbooks in 'new task' dialog into 'pre-installed' and 'custom'
Change	When adding new scans or creating THOR download links, the latest THOR version will automatically be selected in the dialog
Change	Changing a THOR or Signature version manually will now disable the auto update, auto update can now be activated in the 'set version' dialog, too
Change	Added fallback logic for missing THOR versions - e.g. scan with 10.5 if 10.6 was not found
Change	Creating a Sigma ruleset with "Auto Config" will now add all existing rules that match the config to the ruleset
Change	Security Fix - Updated TLS cipher suite
Change	Upgraded winpmem
Change	The asset view per service is now splitted into two tabs, one with already deployed services and one with non-deployed services
Change	Hiding LogWatcher per default if LogWatcher has not been used yet
Bugfix	Added info that filename iocs are not case insensitive if applied as regex
Bugfix	Fixed reset of MISP form data on error
Bugfix	Fixed adding users without role
Bugfix	Fixed missing ntp restrictions in ntp config
Bugfix	Fixed performance and stability of MISP event synchronization
Bugfix	Automatically refresh the UI if the UI version differs from server's UI version
Bugfix	Some collected Aurora or LogWatcher events were corrupt
Bugfix	Fixed synchronization issues between Master ASGARD and ASGARs caused by time sync issues
Bugfix	Fixed non-working 'Agent Update Available' and 'Service Controller Update Available' indicators on Master ASGARD
Bugfix	Added autoremove to upgrade routine to prevent issues with boot partition

11.1.6 ASGARD 2.12

ASGARD 2.12.10

Release Date
Mon, 7 Mar 2022 11:22:00 +0100

Type	Description
Bugfix	Fixed some missing MISP attributes in MISP events

ASGARD 2.12.9

Release Date
Wed, 26 Jan 2022 12:29:00 +0100

Type	Description
Bugfix	Fixed non-working tls certificate upload

ASGARD 2.12.8

Release Date
Mon, 24 Jan 2022 12:20:00 +0100

Type	Description
Feature	Support Aurora Agent (Beta Only)
Feature	Manage Sigma Responses and False Positives (Aurora Only)
Feature	Enable / Disable Sigma Rules
Feature	Manually check for THOR and Signature Updates
Feature	Show log of previous update process
Feature	Auto Config for Sigma Rulesets (Automatically add new Sigma Rules based on level)
Feature	The UI now has a lot more indicators for e.g. 'Asset Requests', 'Uncompiled Rulesets' and more
Feature	Added more graphs to overview page, e.g. incoming Aurora and Log Watcher events
Feature	Added bulk update for available Sigma rule updates
Feature	Added default Sigma Rulesets (if no ruleset has been created yet)
Feature	Added background routine that removes older and unused THOR / Signature versions
Feature	Edit Scan Templates
Feature	Search THOR Flags / Aurora Options
Feature	Download THOR Zip with target hostname as filename
Change	Improved Server Status indicators
Change	Improved licensing
Change	LDAP users require at least one LDAP role, otherwise they are not authenticated anymore
Change	Updated Sigma rules
Change	Cosmetics and UX improvements
Change	Updated default THOR and Signature auto-update config
Change	Added more links and password reset help to login page
Change	Improved usability and feedback in IOC Management section
Change	Require current password for password change
Bugfix	Re-added and improved "no labels" filter in assets table
Bugfix	Re-added resize buttons for Remote Console
Bugfix	Fixed an issue that causes some API keys to be corrupt
Bugfix	Fixed non-working 'Install Service Controller' playbook on Master ASGARD
Bugfix	Updated interrogate job to detect 'Windows 11' correctly
Bugfix	Fixed corrupt 'Is Domain Controller: No' filter
Bugfix	Fixed missing default value when editing Sigma or YARA rules in IOC Management
Bugfix	Fixed non-working "use newer Sigma rule" button

continues on next page

Table 3 – continued from previous page

Type	Description
Bugfix	Fixed CRLF issues in IOC Management for some IOC types
Bugfix	Fixed some missing MISP iocs in THOR download package
Bugfix	Fixed permissions on some files that caused backup process of ASGARD config files on Master ASGARD to not work properly
Bugfix	Fixed encryption issues with custom signatures for THOR Lite
Bugfix	Fixed missing import in ntp config that causes ntp to not work properly on some ASGARDs
Bugfix	Fixed tasks that are pending forever due to unknown task module
Bugfix	Fixed non-working rsyslog reload after monthly logrotation
Bugfix	Fixed wrong file extension of stdout and stderr file in group task result package

11.1.7 ASGARD 2.11

ASGARD 2.11.11

Release Date
Thu, 11 Nov 2021 16:38:00 +0100

IMPORTANT: Please read before you upgrade your ASGARD!

The upgrade can take up to one hour in large installations, do not reboot during installation
 The API has been revised. This will potentially break existing API integrations
 Master ASGARD must be upgraded before upgrading the connected ASGARDs
 To enable new Service Control section add Service Control right to respective roles (Settings > Roles)
 Existing group scans will be stopped and can not be restarted or resumed and must therefore be recreated
 Scheduled group scans will continue working unless custom IOCs are in use. If custom IOCs are in use, scheduled group scans must be stopped and recreated in order to function properly
 The IOC Management has been completely revised. Existing custom IOCs will be deactivated and can be found and downloaded at /var/lib/nextron/asgard2/iocs/. Re-upload your existing custom IOCs through our new UI at Scan Control > IOC Management

Type	Description
Feature	Refactored and improved UI
Feature	Improved performance of tables on the UI
Feature	Updating the search in a UI table will now cancel the previous query instead of detaching the previous query in the background
Feature	A Service Controller Agent is now available to be installed in addition to the existing agent. It can be used to run services instead of one-shot tasks.
Feature	Added new service 'Log Watcher' that scans the Windows EventLog in real-time, based on Sigma Rules that are managed on the Management Center
Feature	Multiple THOR minor version can now be managed and used for Scan tasks
Feature	THOR flags in UI are now based on the selected THOR version
Feature	CPU-, RAM- and DISK-usage are now automatically refreshing in UI every second
Feature	New ASGARD status light in UI (green = no overload, yellow = temporary overloaded, red = overloaded)
Feature	CSV exports now contain more information, added CSV export to many more tables
Feature	ASGARD can now handle multiple licenses
Feature	Licenses for archived assets are invalidated after 3 month and the license count is reduced accordingly
Feature	Scans in the scan table now contain the exact THOR version and signature version that has been used for scanning
Feature	THOR scans are now terminated more gracefully to improve error handling
Feature	Completely refactored IOC Management
Feature	Improved LDAP settings and testing options
Feature	The asset timeline is now available on Master ASGARD
Feature	Repack agent installers from UI
Feature	MacOS ARM64 Support
Change	Requirements for password complexity has been increased
Change	The group task engine has been refactored to issue tasks asynchronously in background instead of synchronously on agent pings
Change	The single task table now only shows tasks that haven't been issued by a group task
Change	Improved security by adding more strict http headers to UI
Change	The Master ASGARD now requires that all connected ASGARs are at least version 2.11.0
Change	Regenerated ASGARD's certificate for agent communication with SAN extension
Change	The agent stream API now terminates streams that are inactive for over 10 minutes
Change	Added more retries and pauses to the agent functions to handle issues with EDRs and AVs
Change	Improved performance by removing some mutexes and using more specific mutexes for critical data
Change	Master ASGARD now synchronizes scanners and signatures with the connected ASGARs

11.1.8 ASGARD 2.10

ASGARD 2.10.10

Release Date
Thu, 24 Jun 2021 07:47:00 +0200

Type	Description
Change	Added a maximum of users that will be collected with interrogate

ASGARD 2.10.9

Release Date

Fri, 18 Jun 2021 11:08:00 +0200

Type	Description
Change	Improved interrogate by adding more output and timeouts for specific operations
Change	Cosmetics
Change	Replaced pdf manuals with online versions
Change	Upgraded CyLR Tool
Change	Improved IOC type detection of custom IOCs
Bugfix	Fixed non-working playbook step "Download File" from Master ASGARD
Bugfix	Fixed empty task table of a group task in response control
Bugfix	Fixed creation of playbook tasks with more than one placeholder
Bugfix	Fixed missing pending tasks in task table if filter is set to 'last x days'
Bugfix	Fixed non-working 'last x days' filter in response control's task table

ASGARD 2.10.8

Release Date

Wed, 12 May 2021 14:50:00 +0200

Type	Description
Feature	Added a new archive script that manually archives scans and scan results that are older than X days
Change	Notarization and new code signing certificate of MacOS binaries
Change	Signed MacOS installer with an installer certificate
Change	Updated Sigma Rules
Bugfix	In some cases the ASGARD Agents and Master ASGARD sent many DNS requests for a few seconds
Bugfix	Fixed ldap configuration issues

ASGARD 2.10.3

Release Date

Fri, 23 Apr 2021 07:29:00 +0200

Type	Description
Feature	Configurable host for agent API, GUI and other APIs
Bugfix	Fixed corrupt agent download links on some browsers

ASGARD 2.10.2

Release Date
Mon, 12 Apr 2021 16:00:00 +0200

Type	Description
Feature [beta]	Service Controller
Feature [beta]	New service 'Log Watcher' that scans EventLog with Sigma in real-time
Feature	Get additional asset information on interrogate, e.g. installed software and local users
Feature	New columns 'Error' and 'Error Help' in scan table to improve troubleshooting with THOR scan issues
Feature	New button in asset- and scan table that shows the history of an asset, including online/offline stats and scan stats
Feature	Added an Agent Log Analysis Tool to command line
Security	Smaller security fixes, e.g. increased min. TLS version, added more CSP headers, added more Logout headers, ...
Change	Improved LDAP with timeouts, retries and added BindDN/BindPassword to support Active Directory
Change	Refactored synchronization with Master ASGARD 2 and Analysis Cockpit 3 to improve MySQL workload
Change	Apply hostname and other system information on asset request accept
Change	Wordings
Bugfix	Do not abort THOR scan if license type could not be determined, the system will be treated as server, instead
Bugfix	Fixed corrupt group scan duplication on Master ASGARD
Bugfix	Fixed corrupt Asset Request deny on non-Master ASGARD

11.1.9 ASGARD 2.6

ASGARD 2.6.2

Release Date
Mon, 11 Jan 2021 14:20:00 +0200

Type	Description
Feature	Rescan assets that failed in a grouped task by duplicating the grouped task
Feature	Cache THOR scan results, if they can not be uploaded due to connection issues and collect them in a subsequent task
Feature	Two factor authentication
Feature	Network traffic graph in overview section
Feature	Import / Export scan templates
Feature	Search for "never" in 'Last Scan Completed' column of asset table
Feature	Added new column 'Status Text' in scan table that contains more information about the status, e.g. error message
Feature	Added button to manually synchronize with MISP
Change	Wordings
Change	Cosmetics
Bugfix	Fixed usage of unpublished MISP events in generated rulesets
Bugfix	No proxy for initial Analysis Cockpit 3 connection

11.1.10 ASGARD 2.5

ASGARD 2.5.7

Release Date
Wed, 18 Nov 2020 09:12:00 +0200

Type	Description
Change	Use proxy for MISP synchronization (optionally)
Bugfix	Fixed duplicate files in THOR zip packages
Bugfix	Fixed removal of THOR config files if content is empty on update

ASGARD 2.5.6

Release Date
Fri, 6 Nov 2020 12:17:00 +0200

Type	Description
Feature	Encrypt custom IOCs and MISP IOCs in the download packages
Feature	Download THOR packages with IOCs from Master ASGARD 2 on ASGARD 2
Change	Master ASGARD 2 now synchronizes the custom IOCs to the connected ASGARDS per default
Bugfix	Fixed asset synchronization with Analysis Cockpit 2
Bugfix	Fixed proxy issues between Master ASGARD 2 and ASGARD 2 and between ASGARD 2 and Analysis Cockpit 3
Bugfix	Fixed rejection of custom ioc deletion when Master ASGARD 2 is connected
Bugfix	Fixed browser cache issues in THOR config management
Bugfix	Fixed issues with log file collection after THOR crashed
Bugfix	Fixed calculation of used RAM in the Overview section

ASGARD 2.5.4

Release Date
Thu, 1 Oct 2020 16:31:00 +0200

Type	Description
Bugfix	Added default false_positive_filters.cfg in THOR packages if not configured via GUI

ASGARD 2.5.3

Release Date
Wed, 30 Sep 2020 12:24:00 +0200

Type	Description
Bugfix	Fixed connectivity issues with Analysis Cockpit 2

ASGARD 2.5.2

Release Date
Mon, 28 Sep 2020 17:43:00 +0200

Type	Description
Feature	Support for Analysis Cockpit 3
Feature	Support for THOR 10 TechPreview
Feature	Added description field to single scans
Feature	Generate and download THOR licenses via GUI
Feature	Remote console can be disabled via command line
Feature	Improved download token management
Feature	Use download token for license API, support THOR's --asgard flag
Feature	Added watcher to THOR launcher that will terminate THOR if system resources run out
Feature	Download ASGARD's ca.pem via GUI that will be used for Agent- and THOR communication
Feature	Manage THOR config files via GUI (Direcotry Excludes, False Positive Filters)
Feature	New tab 'Agents' in update section that will show assets with legacy agents and legacy installers
Change	Exchanged code signing certificate and added time stamping
Change	Redesigned management of events in MISP rulesets
Change	Added unlink buttons for Analysis Cockpit and MISP
Change	Page content will now be vertically scrollable if large tables exceed the 100% width
Change	Wordings
Change	Cosmetics
Bugfix	Fixed corrupt THOR Manual download link in IOC Management

11.1.11 ASGARD 2.4

ASGARD 2.4.4

Release Date
Fri, 19 Jun 2020 16:58:00 +0200

Type	Description
Bugfix	Fixed disabled delete and edit buttons for playbook steps

ASGARD 2.4.3

Release Date
Mon, 15 Jun 2020 08:40:00 +0200

Type	Description
Change	Improved system stability during process memory collection by adding more watchers on the pmem process
Change	Cosmetics
Change	Improved audit logging for Bifrost settings
Bugfix	Fixed sporadically wrong task stats graph in grouped task details view (Master ASGARD only)
Bugfix	Added 'missingok' to logrotate config

ASGARD 2.4.2

Release Date
Mon, 8 Jun 2020 13:04:00 +0200

Type	Description
Change	Improved differentiation between ASGARD and Master ASGARD by adding separate logo and page title

ASGARD 2.4.1

Release Date
Mon, 8 Jun 2020 08:34:00 +0200

Type	Description
Bugfix	Added missing column in asset request's table when upgrading from ASGARD 2.3

ASGARD 2.4.0

Release Date
Thu, 28 May 2020 13:10:00 +0200

Type	Description
Feature	Master ASGARD v2
Feature	Added 'Collected Evidences' section that unites incoming evidences from multiple sources
Feature	Added notifications that can be dismissed for a whole session, e.g. that 'admin' password was not changed
Feature	When creating a scan, you can now decide between THOR and THOR Lite (a trimmed THOR that doesn't cost you a license)
Change	Refactored remote console to be much more stable
Change	Improved error messages when THOR exits with non-zero status code
Change	Using stacked graph for issued / completed tasks of grouped tasks
Change	Cosmetics
Change	Upgraded swagger UI
Change	Improved audit logging
Change	Added warning to product update popup, if product has automatic updates configured
Bugfix	Fixed bug in graph of issued / completed tasks of grouped task
Bugfix	Fixed process leak that may occur on too many page clicks that causes missing system info on overview page

11.1.12 ASGARD 2.3

ASGARD 2.3.3

Release Date
Fri, 8 May 2020 11:16:00 +0200

Type	Description
Bugfix	Removed legacy auto-update config that may cause unwanted THOR/Signatures updates in background

ASGARD 2.3.2

Release Date
Wed, 6 May 2020 15:50:00 +0200

Type	Description
Feature	THOR HTML reports will be generated after THOR scans and can be downloaded via GUI
Feature	Added MOTD to SSH sessions
Feature	New playbook - List processes
Feature	New playbook - Kill process
Feature	New playbook - Uninstall ASGARD 1 Agent
Feature	MISP Rulesets don't have to be generated manually anymore. Adding MISP Events to a ruleset that doesn't exist will automatically create a new one
Feature	Added port 80 listener that redirects to port 8443
Feature	Improved detailed view of playbook results. Stdout/Stderr and collected files are now shown in the GUI
Feature	New user restriction 'NoInactiveAssets' that restricts users from seeing inactive assets in the Asset Management
Change	Added hostname and task start date to filename of scan results
Change	Update filename of memory dumps from mem.raw to mem.aff4
Change	Default admin role will now have all rights (doesn't affect ASGARs that were upgraded to 2.3)
Change	Wordings
Change	Download tokens are not based on query parameters anymore
Change	Reduced default validity for self-signed ASGARD certificate
Change	License adjustments
Change	Removed memory collection playbook for MacOS
Bugfix	Removed loading circle when clicking on an attribute in a MISP event
Bugfix	Improved IE support
Bugfix	Hide proxy credentials in log
Bugfix	Fixed a field name in Swagger API documentation
Bugfix	Fixed THOR flag synchronization issues due to too large description

11.1.13 ASGARD 2.2

ASGARD 2.2.1

Release Date
Wed, 8 Apr 2020 14:46:00 +0200

Type	Description
Security	Always clear all temporary files and use random names for temp directories

ASGARD 2.2.0

Release Date
Mon, 6 Apr 2020 11:37:00 +0200

Type	Description
Feature	API documentation in GUI
Feature	Improved query APIs for assets, tasks and more
Feature	Dynamic ping rate based on number of connected assets
Feature	Added default roles
Feature	Quarantine playbook (and de-quarantine playbook)
Feature	Download file or directory playbook
Feature	Backup and restore scripts
Feature	Create diagnostic pack script + download via GUI
Feature	Added "NoTaskStart" right
Feature	Search for multiple values using pipe
Feature	Show head and tail of THOR logs in preview instead of head only
Feature	Check total memory and free disk space before running PMEM
Feature	Throttle uploads
Feature	Specify max. file size / dir size using 'KB', 'MB', ...
Feature	Show badge in sidebar if ASGARD update is available
Feature	Resizable remote console
Feature	Set max. runtime for a task (default is 1 week)
Feature	Added new flag '-systemproxy' to agent repacker. Agents will then use system-configured proxy.
Feature	Support agent obfuscation by passing '-name <name>' to agent repacker
Feature	Support more search types, e.g. '< 3 GB'. All types are now shown as tooltip in search fields
Feature	Improved uninstall of agents
Feature	Edit playbooks and playbook steps
Feature	License API
Feature	Automatically hide assets that haven't been seen for X days (can be configured)
Change	Wording Client > Agent
Change	Cosmetics
Change	Agents do not write local log anymore (except with <i>write_log: true</i> in config)
Change	Automatically download newest THOR and signatures every hour (per default, can be disabled)
Change	Improved error handling in remote console sessions

continues on next page

Table 4 – continued from previous page

Type	Description
Change	Improved usability in playbook section
Change	Restrict uploads of ioc files with unknown file type
Change	Differentiate between rights and restrictions in User Management
Change	Improved IOC generation from MISP (reduces false positives)
Change	Download API is now protected with unique tokens (validation can be disabled)
Security	Improved randomness of login tokens
Security	Added CSRF tokens for POST requests
Bugfix	Fixed escape problems in windows playbooks
Bugfix	Fixed typo in logrotate config
Bugfix	Fixed missing filenames in file upload forms
Bugfix	Fixed missing role descriptions
Bugfix	Fixed wrong permissions of agent installers
Bugfix	Fixed missing debian packages for changelog extraction
Bugfix	Do not hide other labels when searching for a label
Bugfix	Fixed wrong disk usage on ASGARs that were installed with an ISO
Bugfix	Generate a server license for an asset that already has a workstation license but now requires a server license

11.1.14 ASGARD 2.1

ASGARD 2.1.0

Release Date
Mon, 2 Mar 2020 16:12:00 +0200

Type	Description
Feature	Master ASGARD Support
Feature	LDAP Authorization
Feature	Remote Console
Feature	Remote Console Protocol
Feature	Cache THOR on assets (encrypted)
Feature	Show asset labels in task tables
Feature	Grouped navigation bar items
Feature	Role Management
Feature	Import / Export client requests as CSV
Feature	Download all group task results as tar.gz
Feature	Schedule start of group task
Feature	Added more lines to group task graphs, e.g. errored tasks
Feature	Dynamic playbooks (by using placeholders)
Change	Automatically check for updates after license installation
Change	Cosmetics
Bugfix	Fixed corrupt bifrost files download
Bugfix	Threadsafe config writings
Bugfix	Changed agent binary directory to /usr/sbin/ due to problems with SELinux
Bugfix	Security Fixes - Improved TLS cipher suites and http headers

11.1.15 ASGARD 2.0

ASGARD 2.0.3

Release Date
Wed, 19 Feb 2020 09:38:00 +0200

Type	Description
Bugfix	Added missing upgrade script to /etc/nextron/asgard2

ASGARD 2.0.2

Release Date
Wed, 19 Feb 2020 08:24:00 +0200

Type	Description
Bugfix	Fixed gz issues on log forwarding to Analysis Cockpit

ASGARD 2.0.1

Release Date
Tue, 18 Feb 2020 12:15:00 +0200

Type	Description
Feature	Import / Export assets as CSV
Bugfix	Support IE 11 (Protofills, JS syntax error fixes)
Bugfix	Fixed spec file for RPM 32bit installer
Bugfix	Fixed non-working table filters
Bugfix	Fixed upgrade procedure

ASGARD 2.0.0

Release Date
Wed, Mon, 17 Feb 2020 14:17:00 +0200

Type	Description
Major Release	Initial release

11.2 ASGARD Agent

Changelog of ASGARD Agent releases since version 1.2.0

11.2.1 Agent 1.6.5

Release Date
Mon, 24 Oct 2022 15:00:00 +0200

Type	Description
Feature	Support for ASGARD Broker
Change	Improved proxy support
Change	Improved logging. Logs are now written in log/ subdirectory and rotated based on file size
Change	Disabled syslog per default

11.2.2 Agent 1.5.5

Release Date
Mon, 8 Nov 2021 06:59:00 +0100

Type	Description
Feature	Support for ARM64 MacOS
Fix	Improved stability of task executions on clients with an EDR installed
Fix	Gracefully shutdown running tasks on os signals
Fix	Improved stability of config file on system crash

11.2.3 Agent 1.4.3

Release Date
Mon, 6 Sep 2021 12:19:00 +0200

Type	Description
Change	Rebuilt agent with newest Golang Version
Change	Removed code fragments used for service controller

11.2.4 Agent 1.4.2

Release Date
Tue, 11 May 2021 05:16:00 +0200

Type	Description
Change	Signed MacOS binaries with a new certificate
Fix	In some cases the ASGARD Agents sent many DNS requests for a few seconds
Fix	Fixed non-starting task after module version upgrade in some cases

11.2.5 Agent 1.3.5

Release Date
Mon, 28 Sep 2020 10:38:00 +0200

Type	Description
Change	Exchanged code signing certificate and added time stamping

11.2.6 Agent 1.2.0

Release Date
Wed, 19 Feb 2020 09:38:00 +0200

Type	Description
Major Release	Initial release

11.3 ASGARD Service Controller

Changelog of ASGARD Service Controller releases since version 2.0.5

11.3.1 Service Controller 2.1.2

Release Date
Tue, 13 Aug 2022 08:55:00 +0200

Type	Description
Feature	Support for ASGARD Broker
Change	Improved proxy support
Change	Improved logging. Logs are now written in log/ subdirectory and rotated based on file size

11.3.2 Service Controller 2.0.7

Release Date
Mon, 21 Feb 2022 15:05:00 +0100

Type	Description
Feature	Send more detailed status of currently running services

11.3.3 Service Controller 2.0.6

Release Date
Thu, 9 Dec 2021 09:42:00 +0100

Type	Description
Change	Increased max. offline mode time from 4 to 14 days
Bugfix	Improved stability in offline mode
Bugfix	Fixed sporadically service restarts due to connectivity issues

11.3.4 Service Controller 2.0.5

Release Date
Thu, 11 Nov 2021 16:38:00 +0100

Type	Description
Major Release	Initial release

INDICES AND TABLES

- search