ASGARD Security Center v2 Manual

Nextron Systems

May 06, 2024

CONTENTS

The Nextron Security Center is intended to provide multi tenancy support to single ASGARD installations. It connects to the Analysis Cockpit and synchronizes data provided in cases within the Analysis Cockpit.

In the following chapters we will describe how the Security Center works, how to install the required components, and how to use it.

CHAPTER

ONE

BEFORE YOU BEGIN

This is an introductory chapter to the Security Center. Please read this chapter before you start installing or even configuring your new Security Center.

This chapter contains Hardware Requirements, Licensing and other topics.

1.1 Introduction

The Nextron Security Center is intended to provide multi tenancy support to single ASGARD installations. It connects to the Analysis Cockpit and synchronizes data provided in cases within the Analysis Cockpit.

All assets assigned to a specific tenant within the ASGARD Management Center will be synchronized to this tenant in the Analysis Cockpit and finally to the Security Center.

In a service provider setup, a team of analysts would be working on event analysis and would use the Analysis Cockpit for that. Event analysis is independent from specific tenants. A case created in the Analysis Cockpit can affect one or more tenants.

If a case meets pre-defined criteria its content gets synchronized to the Security Center and leads to the creation of one or more findings for one or more tenants within the Security Center.

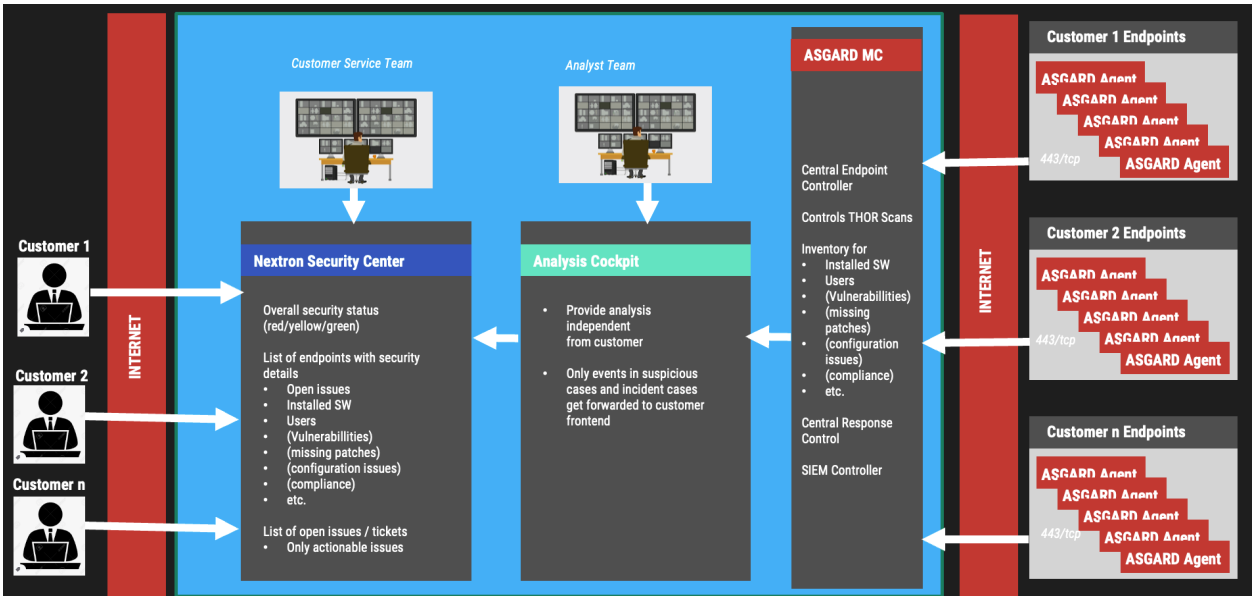
The Security Center provides the option for a second service provider team that is intended to assist the customers (tenants) with the findings. Communication between customers and the customer service team can be done through the "Comments" function within the Security Center.

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

In the figure above, the Security Center – which consists of the Security Center Frontend and the Security Center Backend – is shown as a single functional block. Security Center Frontend and Security Center Backend can be installed in separate DMZ networks if required. This is optional however.

1.2 Hardware Requirements

You can find the hardware requirements for the Security Center below



1.2.1 Security Center Hardware

The required hardware for your Security Center are as follows:

End-points	Frontend	Backend
up to 10.000	- CPU Cores: 4 - System memory: 8 GB - Hard Disk: 200 GB	- CPU Cores: 4 - System memory: 16 GB - Hard Disk: 500 GB SSD
up to 100.000	- CPU Cores: 4 - System memory: 8 GB - Hard Disk: 200 GB	- CPU Cores: 4 - System memory: 16 GB - Hard Disk: 2 TB SSD

Hint: For an infrastructure of up to 100.000 endpoints, consider a 2TB SSD for the backend.

1.3 Network Requirements

The ASGARD components use the ports in the following chapters. For a detailed and up to date list of our update and licensing servers, please visit https://www.nextron-systems.com/hosts/.

1.3.1 Management Workstation

Description	Port	Source	Destination
CLI administration	22/tcp	Workstation	Security Center Frontend
CLI administration	22/tcp	Workstation	Security Center Backend
Web administration	8443/tcp	Workstation	Security Center Backend

1.3.2 Customer Access

Description	Port	Source	Destination
Customer Web Interface	443/tcp	Workstation	Security Center Frontend

1.3.3 Analysis Cockpit

Description	Port	Source	Destination
Event and Asset synchronization	6443/tcp	ASGARD Analysis Cockpit	Security Center Backend

1.3.4 Security Center Frontend

Description	Port	Source	Destination
Event and Asset queries	7443/tcp	Security Center Frontend	Security Center Backend

1.3.5 Internet

The Security Center is configured to retrieve updates from the following URLs:

Description	Port	Source	Destination
Product Updates	443/tcp	Security Center Frontend & Backend	update3.nextron-systems.com
Product Updates	443/tcp	Security Center Frontend & Backend	update-301.nextron-systems.com
NTP	123/udp	Security Center Frontend & Backend	0.debian.pool.ntp.org[1]
NTP	123/udp	Security Center Frontend & Backend	1.debian.pool.ntp.org[1]
NTP	123/udp	Security Center Frontend & Backend	2.debian.pool.ntp.org[1]

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 Security Center. Only BASIC authentication is supported (no NTLM authentication support).

Hint: The Security Center installer requires Internet access during the setup. The installation process will fail if required packages cannot be loaded from our update servers (see table above).

1.3.6 DNS

All the components need to have a resolvable FQDN.

The Security Center needs to be able to resolve internal and external IP addresses. Connection to the Analysis Cockpit MUST be done with a resolvable FQDN. IP addresses will not work.

1.4 Verify the Downloaded ISO (Optional)

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

The hash and signature file are both part of the ZIP archive you download from our portal server.

[1] The NTP server configuration can be changed.

1.4.1 Via Hash

Extract the ZIP and check the sha256 hash:

On Linux

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

or in 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.
```

or in 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
```

1.4.2 Via Signature (Recommended)

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

On 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
```

or in 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`.

CHAPTER

TWO

SETUP GUIDE

This chapter contains the setup guide with an example on how to create a new ESXi virtual machine and installing the ASGARD Broker Network Components.

2.1 Create a new ESX VM and mount the ISO

In this manual we are working with one server for both the Security Center Frontend as well as the Backend. You can however install the two services on two separate servers. If this is the case please install a second server.

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 ISO to an accessible data store and mount the same to your newly created VM.

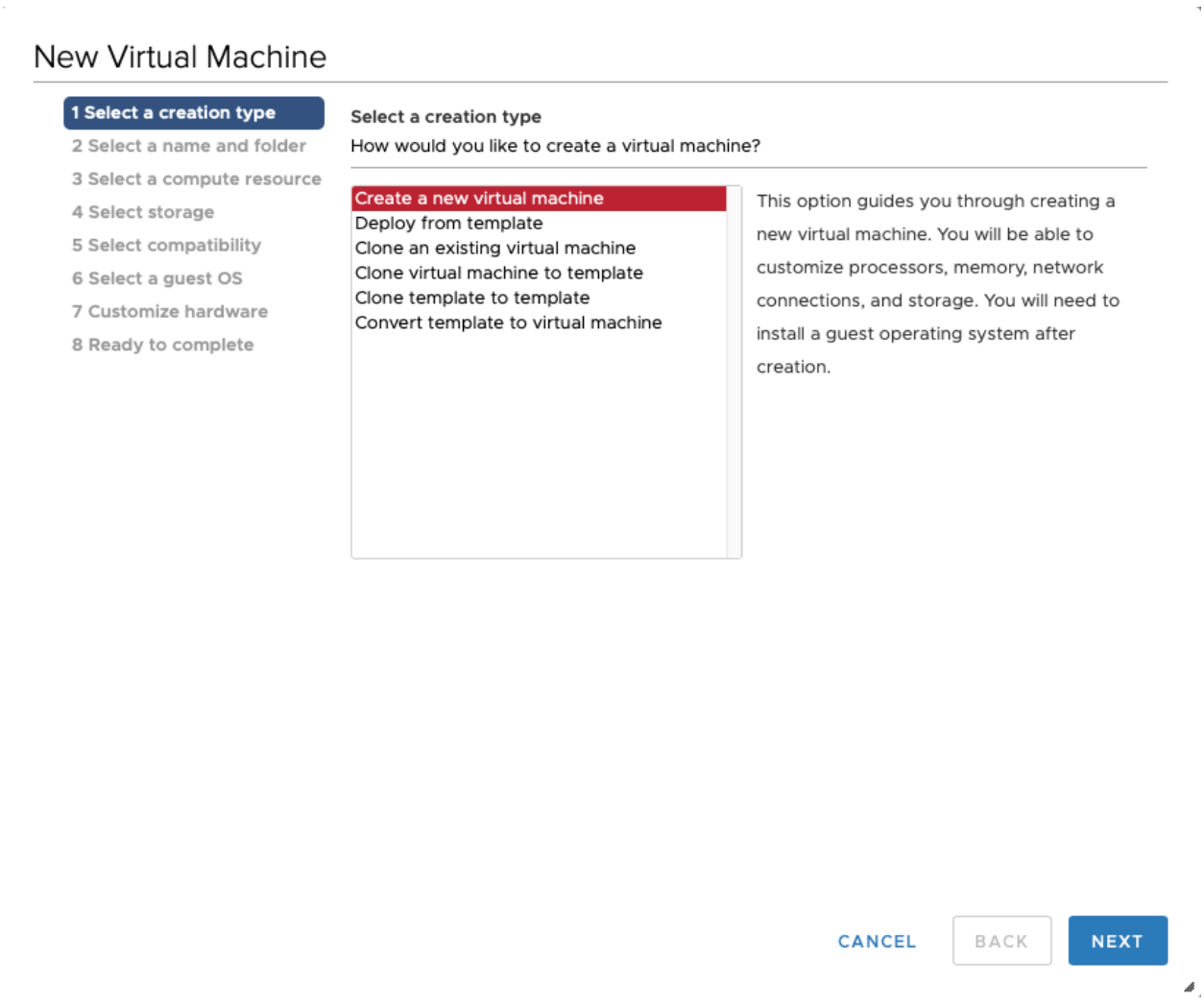
Please make sure to select a suitable v-switch or physical interface that reflects the IP address scheme you are planning to use for the new Security Center.

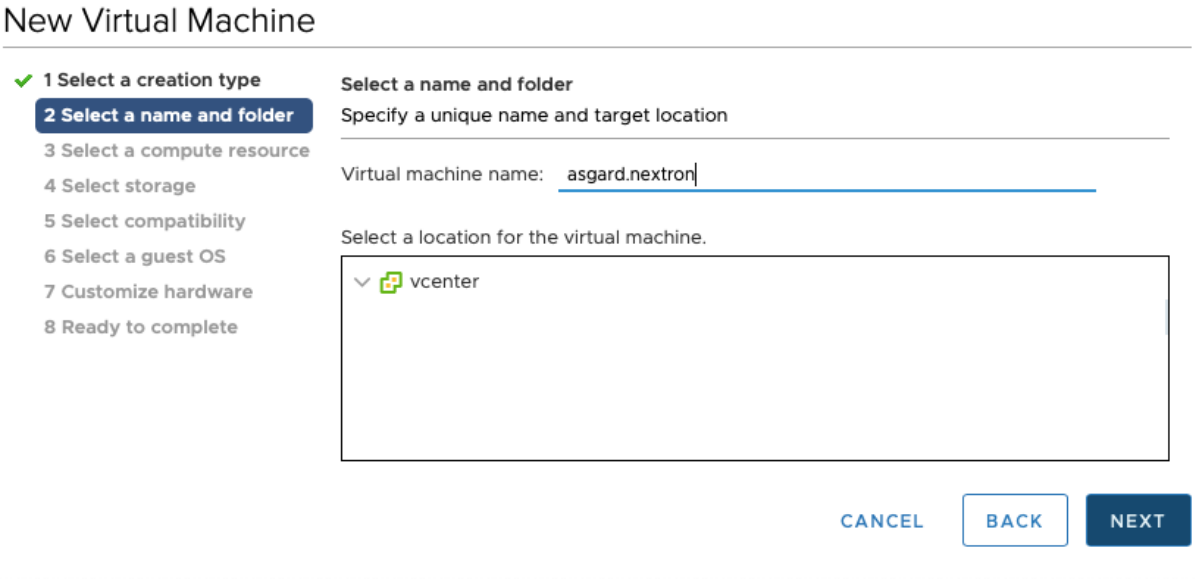
2.2 Navigate through the Installer

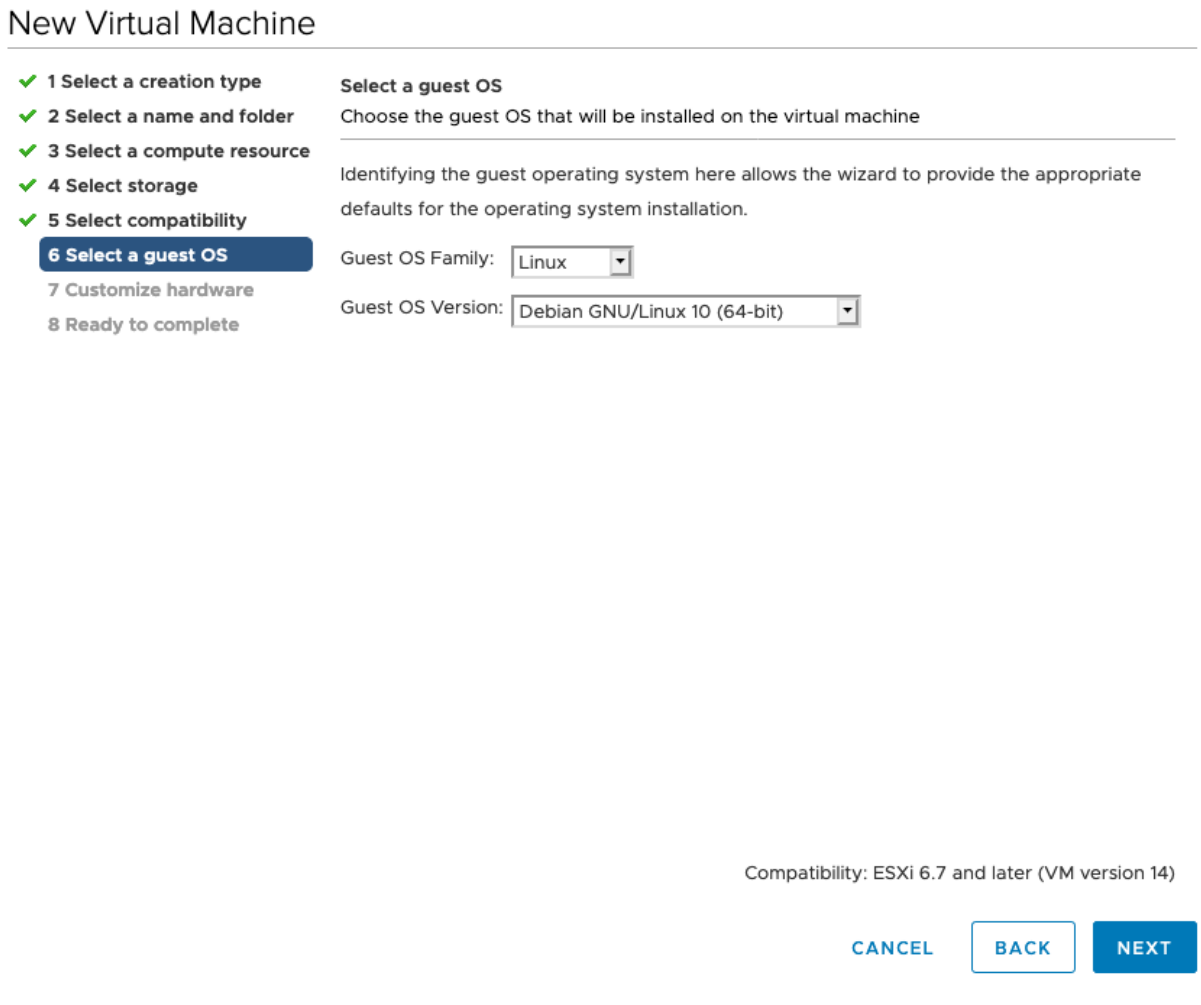
The installation Process is started by clicking on ASGARD Graphical install. The installer then loads the additional components from the ISO and lets you select location and language.

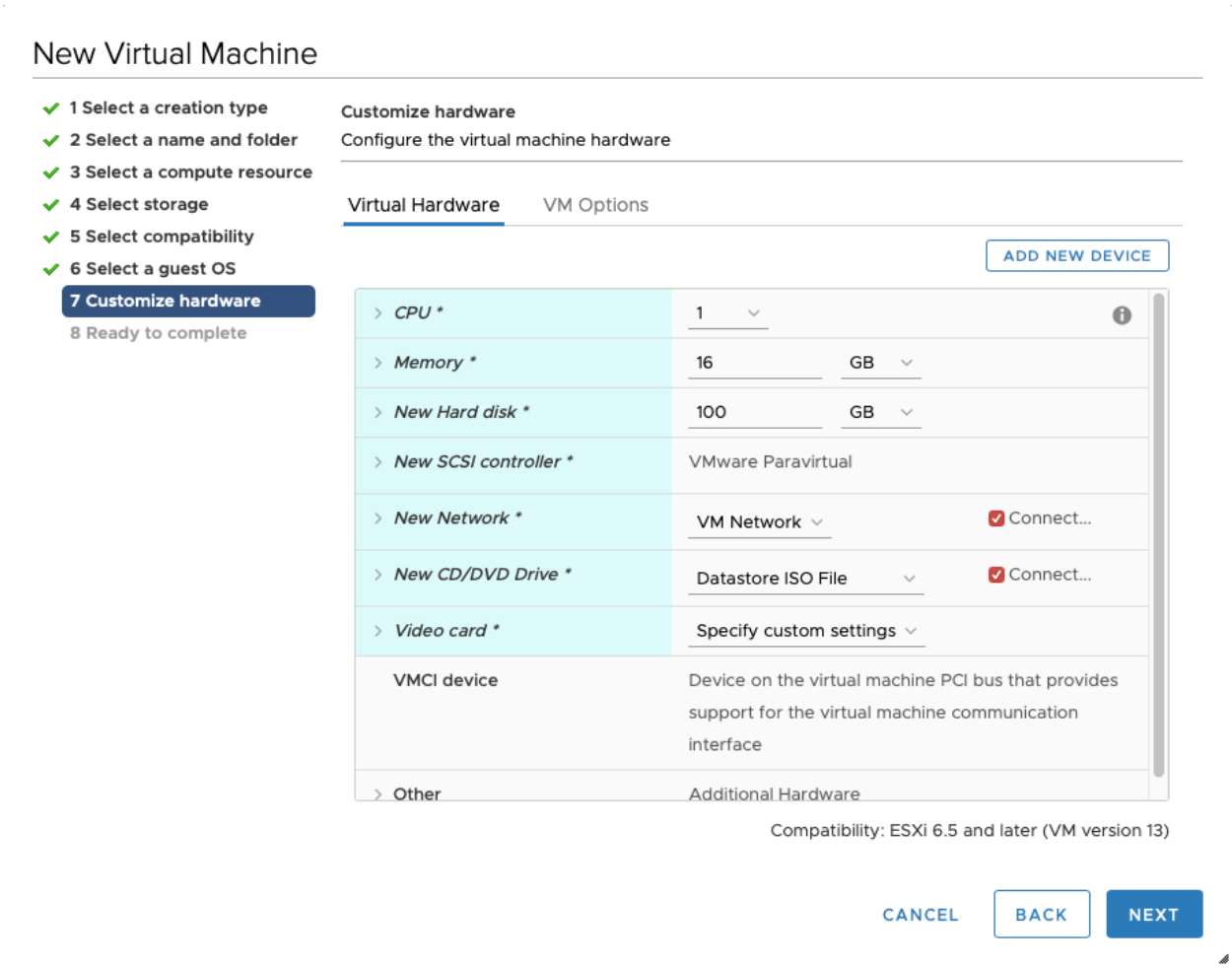
Warning: Please make sure to select the correct Country, as this will also set your local timezone!

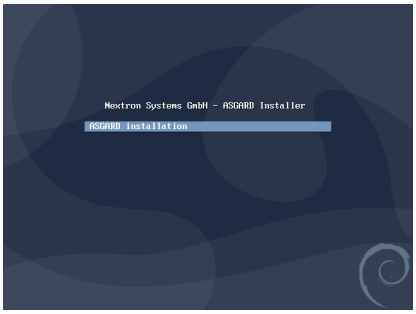
Note: If DHCP is available, network parameters will be configured automatically. Without DHCP, ASGARD drops into the manual network configuration dialogue. The IP address can be changed later, see *Changing the IP-Address*

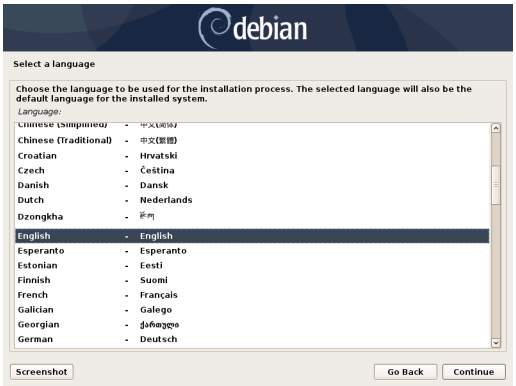

New Virtual Machine
1 Select a creation type
2 Select a name and folder
3 Select a compute resource
4 Select storage
5 Select compatibility
6 Select a guest OS
7 Customize hardware
8 Ready to complete
Select a creation type
How would you like to create a virtual machine?
Create a new virtual machine
Deploy from template
Clone an existing virtual machine
Clone virtual machine to template
Clone template to template
Convert template to virtual machine
This option guides you through creating a new virtual machine. You will be able to customize processors, memory, network connections, and storage. You will need to install a guest operating system after creation.
CANCEL
BACK
NEXT

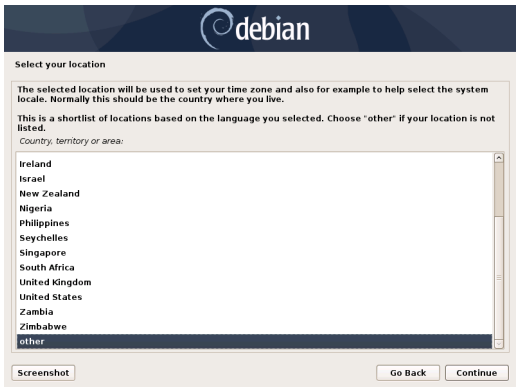

New Virtual Machine
1 Select a creation type
2 Select a name and folder
3 Select a compute resource
4 Select storage
5 Select compatibility
6 Select a guest OS
7 Customize hardware
8 Ready to complete
Select a name and folder
Specify a unique name and target location
Virtual machine name:
asgard.nextron
Select a location for the virtual machine.
vcenter
CANCEL
BACK
NEXT


New Virtual Machine
1 Select a creation type
2 Select a name and folder
3 Select a compute resource
4 Select storage
5 Select compatibility
6 Select a guest OS
7 Customize hardware
8 Ready to complete
Select a guest OS
Choose the guest OS that will be installed on the virtual machine
Identifying the guest operating system here allows the wizard to provide the appropriate defaults for the operating system installation.
Guest OS Family:
Linux
Guest OS Version:
Debian GNU/Linux 10 (64-bit)
Compatibility: ESXi 6.7 and later (VM version 14)
CANCEL
BACK
NEXT

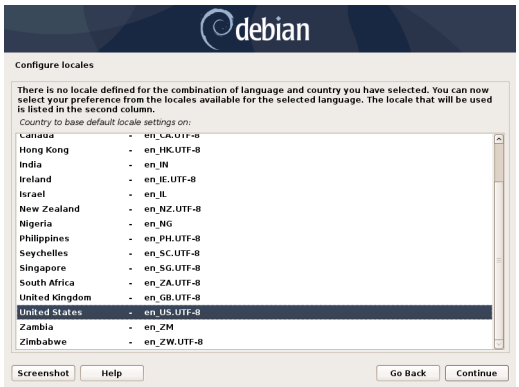

New Virtual Machine
1 Select a creation type
2 Select a name and folder
3 Select a compute resource
4 Select storage
5 Select compatibility
6 Select a guest OS
7 Customize hardware
8 Ready to complete
Customize hardware
Configure the virtual machine hardware
Virtual Hardware
VM Options
ADD NEW DEVICE
CPU *
1
Memory *
16
GB
New Hard disk *
100
GB
New SCSI controller *
VMware Paravirtual
New Network *
VM Network
Connect...
New CD/DVD Drive *
Datastore ISO File
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


Nextron Systems GmbH - ASGARD Installer
ASGARD installation

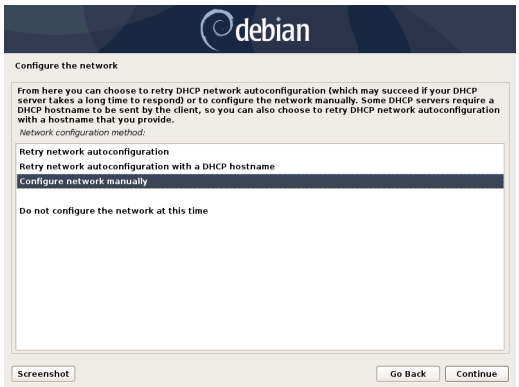

debian
Select a language
Choose the language to be used for the installation process. The selected language will also be the default language for the installed system.
Language:
Chinese (Traditional) - 中文(繁體)
Croatian - Hrvatski
Czech - Čeština
Danish - Dansk
Dutch - Nederlands
Dzongkha - རྫོང
English - English
Esperanto - Esperanto
Estonian - Eesti
Finnish - Suomi
French - Français
Galician - Galego
Georgian - ქართული
German - Deutsch
Screenshot
Go Back
Continue


debian
Select your location
The selected location will be used to set your time zone and also for example to help select the system locale. Normally this should be the country where you live.
This is a shortlist of locations based on the language you selected. Choose "other" if your location is not listed.
Country, territory or area:
Ireland
Israel
New Zealand
Nigeria
Philippines
Seychelles
Singapore
South Africa
United Kingdom
United States
Zambia
Zimbabwe
other
Screenshot
Go Back
Continue


debian
Select your location
The selected location will be used to set your time zone and also for example to help select the system locale. Normally this should be the country where you live.
Listed are locations for: Europe. Use the <Go Back> option to select a different continent or region if your location is not listed.
Country, territory or area:
Denmark
Estonia
Faroe Islands
Finland
France
Georgia
Germany
Gibraltar
Greece
Greenland
Guernsey
Holy See (Vatican City State)
Hungary
Screenshot
Go Back
Continue


debian
Configure locales
There is no locale defined for the combination of language and country you have selected. You can now select your preference from the locales available for the selected language. The locale that will be used is listed in the second column.
Country to base default locale settings on:
Hong Kong - en_HK.UTF-8
India - en_IN
Ireland - en_IE.UTF-8
Israel - en_IL
New Zealand - en_NZ.UTF-8
Nigeria - en_NG
Philippines - en_PH.UTF-8
Seychelles - en_SC.UTF-8
Singapore - en_SG.UTF-8
South Africa - en_ZA.UTF-8
United Kingdom - en_GB.UTF-8
United States - en_US.UTF-8
Zambia - en_ZM
Zimbabwe - en_ZW.UTF-8
Screenshot
Help
Go Back
Continue

2.3 Network Configuration

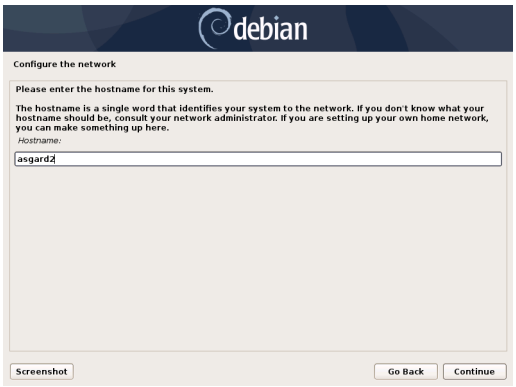


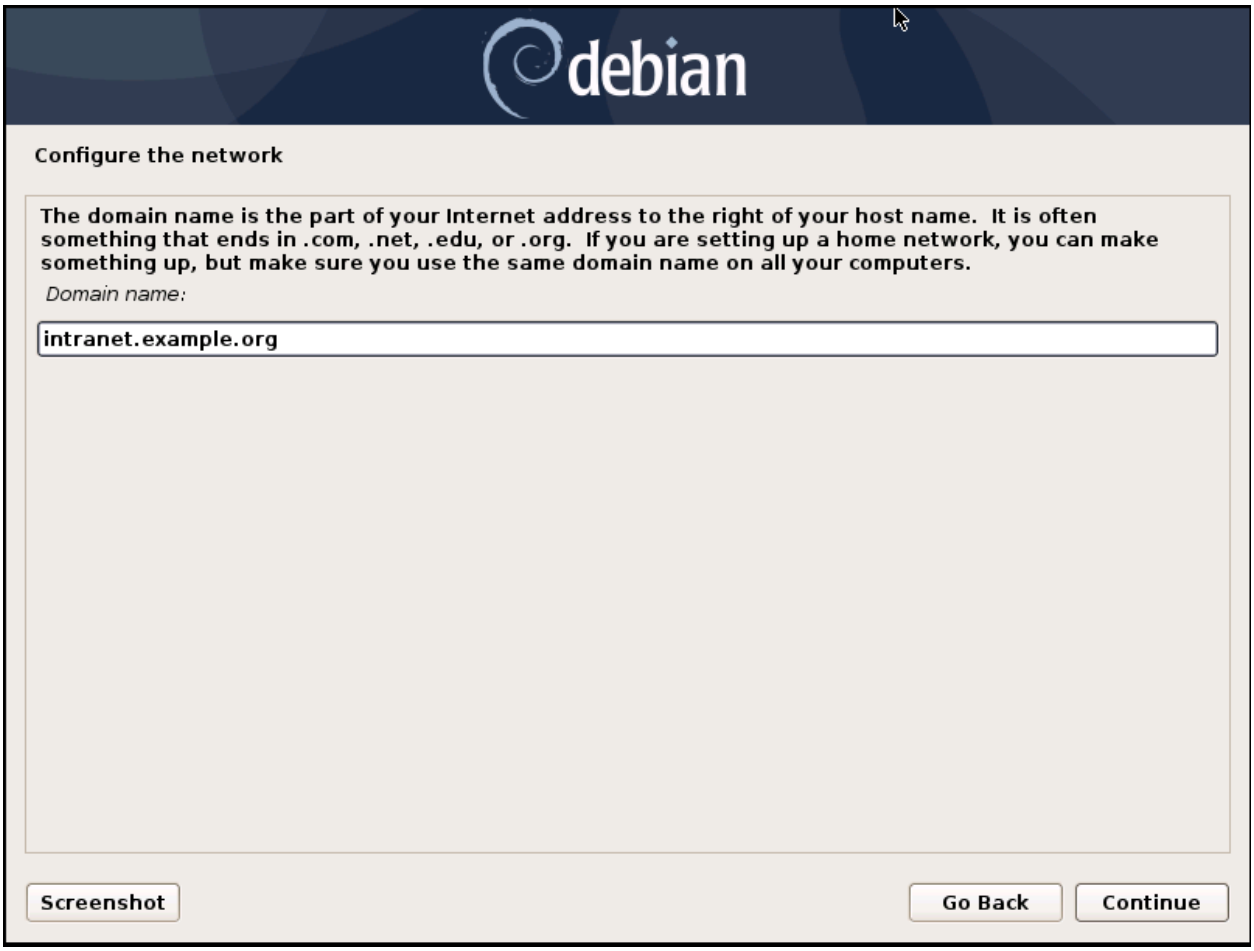
Warning: The Security Cockpit needs to be able to resolve internal and external IP addresses.

Danger: **Important:** Make sure that the combination of hostname and domain creates an FQDN that can be resolved from your Analysis Cockpit. Connection to ASGARD Analysis Cockpit will rely on the FQDN.


debian
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:
10.255.252.1
Screenshot
Go Back
Continue


debian
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:
10.255.252.1
Screenshot
Go Back
Continue


debian
Configure the network
Please enter the hostname for this system.
The hostname is a single word that identifies your system to the network. If you don't know what your hostname should be, consult your network administrator. If you are setting up your own home network, you can make something up here.
Hostname:
asgard2
Screenshot
Go Back
Continue


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

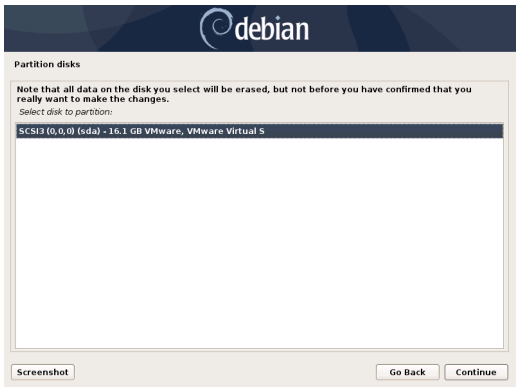
2.4 Choosing a Password

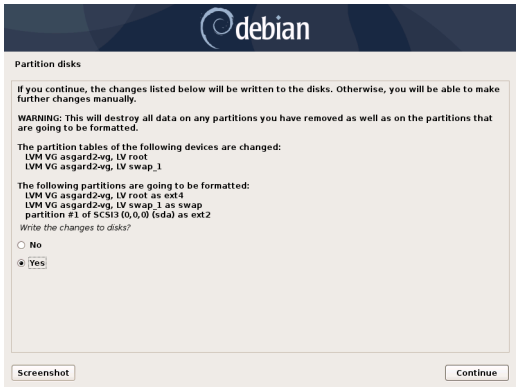
Fig. 1: Choosing a password for the `nextron` user

2.5 Partitioning of the Hard Disk

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

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.





2.6 Proxy Configuration

The base installation is now complete. In the next step we will install the Frontend and Backend Components. For this step **Internet connectivity is required**.

Use SSH to connect to the appliance using the user `nextron` and the password you specified during the installation. If SSH is not available, you can perform the next steps via the Console of your Virtualization Host, though SSH has better capabilities.

2.7 Changing the IP-Address

You servers IP Addresses can be changed in **/etc/network/interfaces**. The IP is configured with the address variable.

```
nextron@sc-front:~$ 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
```

Note: There might be a case where the name of the network interface (in this example: `ens32`) is different. To verify this you can run `ip a` and see the name of the network interface.

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

Make sure to update the A-Records in your local DNS Server to reflect the IP changes.

2.7.1 Verifying DNS Settings

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

```
nextron@sc-front:~$ 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:

```
nextron@sc-front:~$ sudoedit /etc/resolv.conf
```

2.8 Installing the Components

This chapter will explain how to install the Security Center components on your server(s). We recommend to start with the Backend, since the Frontend installation requires the configuration of the Backend.

Please keep in mind that you can install the Frontend and Backend on two separate servers. For simplicity, we chose to install both services on the same server. If you wish to install the Frontend and Backend on two separate servers, please see *Installing two seperate servers*.

2.8.1 Install the ASGARD Security Center (All-in-one)

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

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

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

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

If you encounter problems during your installation, please see *Diagnostic Pack* for further instructions.

Requirements

The installation of the ASGARD Management Center requires the following:

- A valid license file for the ASGARD Security Center
- A configured FQDN (with some exceptions, see *Valid FQDN*)
- Internet access during installation (see *Connectivity Check*)
- Every Server must have a valid and resolvable FQDN (see *Network Configuration*)

Installation

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

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

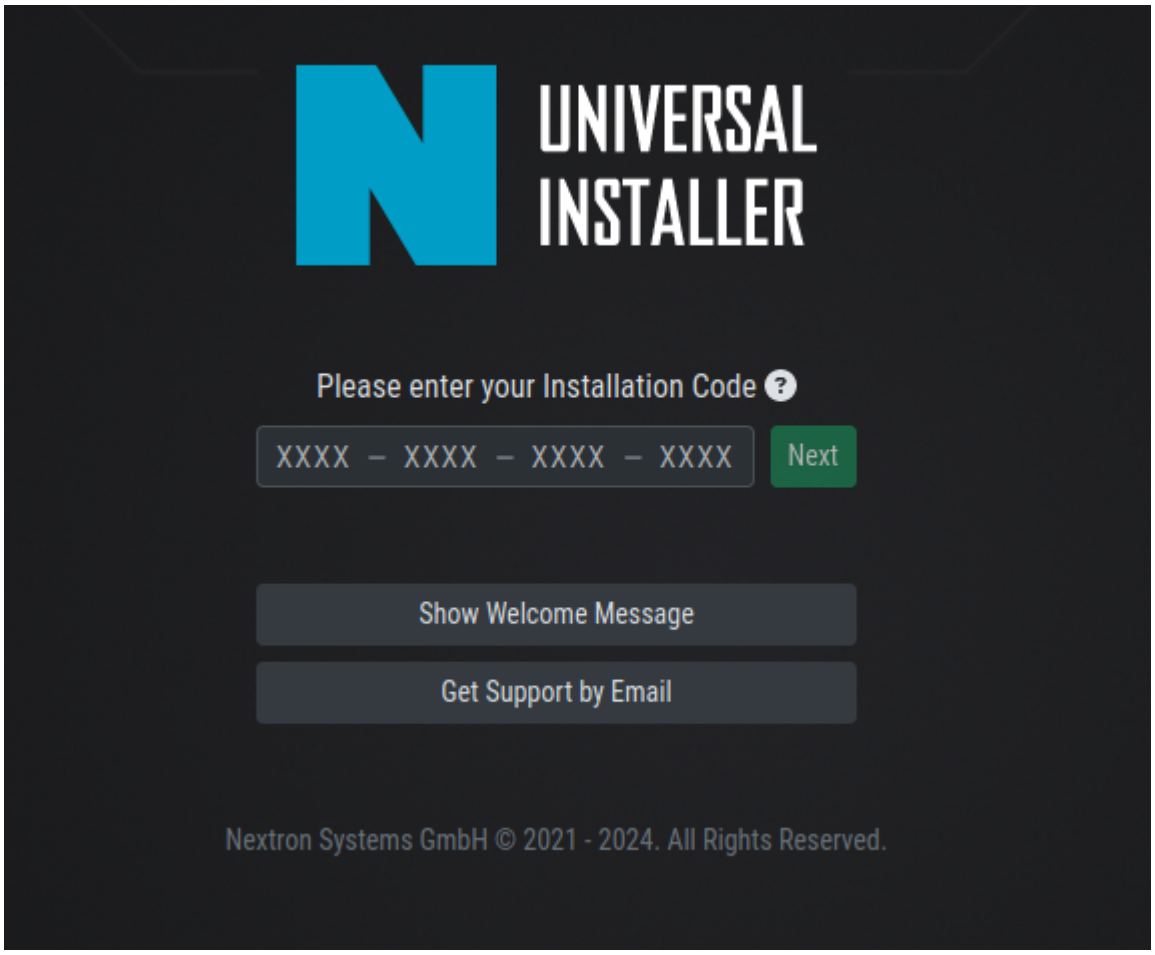
You will be greeted with a small introduction as to what the Nextron Universal Installer is and what it does. After you click `Next`, you will be presented with the landing page of the Nextron Universal Installer.

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

```
Nextron Universal Installer

Ready to complete your setup? Get started by visiting https://asgard.local.
To proceed, you'll need to enter the installation code Z9CU-6Q3H-VKZ4-X7YS in the Web UI.

asgard login: _
```



Connectivity Check

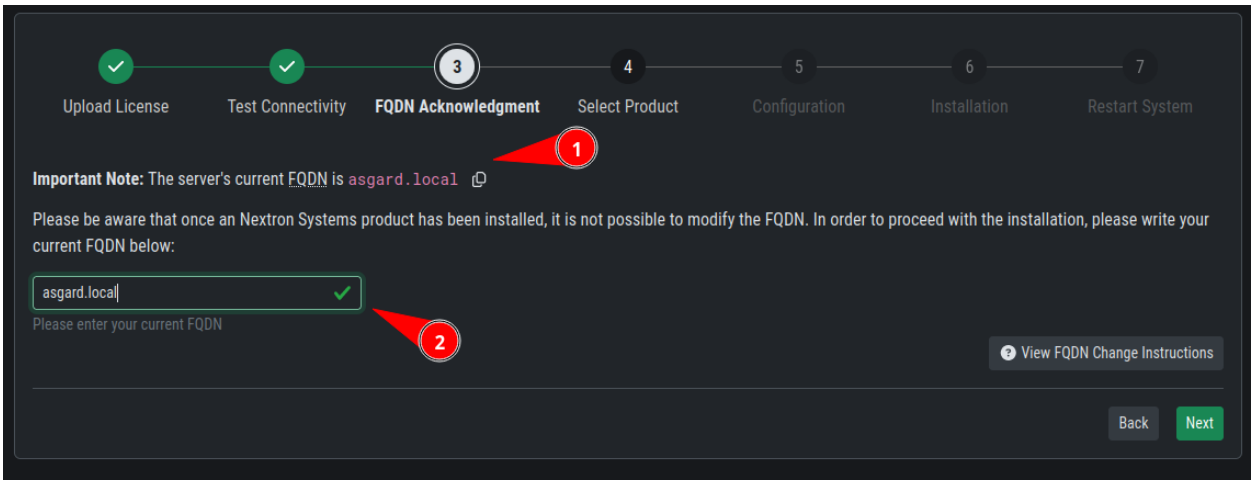
The Nextron Universal Installer will try to connect to our update server in order to download all the necessary packages once the installation starts. Make sure you can reach the update servers (see *Internet*).

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

Valid FQDN

The Nextron Universal Installer will prompt you to verify the FQDN which you configured during the installation of the base system (see *Network Configuration*). This is needed in order for your ASGARD Components to communicate via a HTTPs connection with each other. If there is a mismatch of FQDNs your components will not be able to communicate with each other.

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



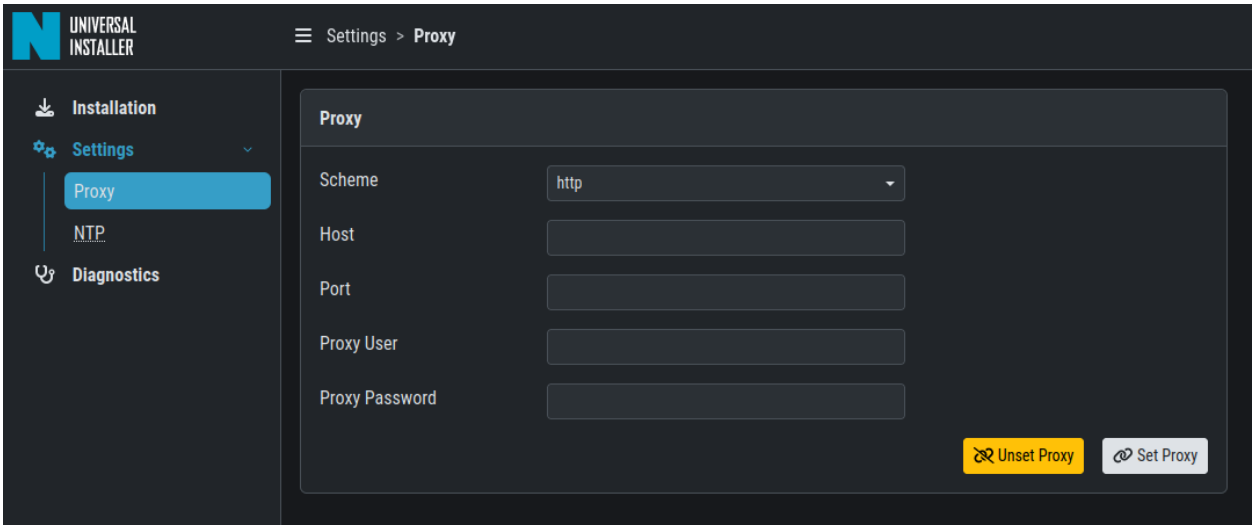
Proxy and NTP Settings

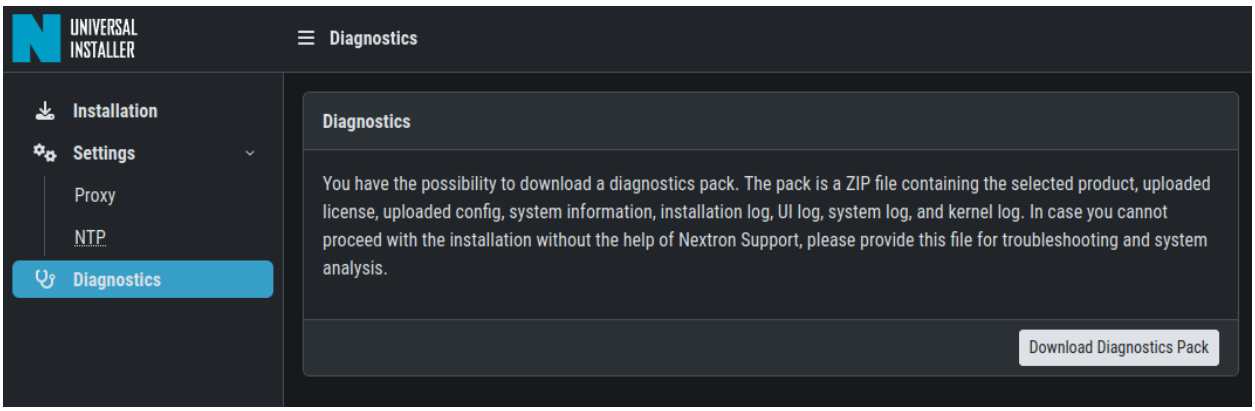
If you need to configure a proxy or change the NTP settings of your system, you can do so by clicking on the `Settings` button in the left menu of the Nextron Universal Installer.

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

Diagnostic Pack

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


UNIVERSAL INSTALLER
Settings > Proxy
Installation
Settings
Proxy
NTP
Diagnostics
Proxy
Scheme
http
Host
Port
Proxy User
Proxy Password
Unset Proxy
Set Proxy


UNIVERSAL INSTALLER
Diagnostics
Installation
Settings
Proxy
NTP
Diagnostics
Diagnostics
You have the possibility to download a diagnostics pack. The pack is a ZIP file containing the selected product, uploaded license, uploaded config, system information, installation log, UI log, system log, and kernel log. In case you cannot proceed with the installation without the help of Nextron Support, please provide this file for troubleshooting and system analysis.
Download Diagnostics Pack

2.8.2 Installing two seperate servers

If you wish to separate the Frontend and Backend of the ASGARD Security Center, you can do so by installing the Backend on one server and the Frontend on another server. Simply choose one of the options during the `Select Product` stage of the Nextron Universal Installer.

Hint: You have to start with the installation of the Backend, since the Frontend needs the configuration of the Backend to work properly.

ASGARD Security Center (Backend Only)

After the Nextron Universal Installer finished the installation of the ASGARD Security Center Backend, you have to download the configuration file from it (`model.config`). You can do this by connecting to the server via SSH. The file can be found in the following directory:

`/etc/asgard-security-center-backend/model.config`

You can now start with the installation of the Frontend.

You can also check if the service of the Backend was installed successfully.

```
nextron@gatekeeper:~$ systemctl status asgard-security-center-backend.service
```

The status of the service should be `active (running)`.

The Backend is running on TCP port 8443. You can now log into the Backend via `https://<FQDN>:8443`.

ASGARD Security Center (Frontend Only)

During the installation of the ASGARD Security Center Frontend, you will be prompted to upload the configuration file of the Backend. Use the file (`model.config`) you downloaded earlier from the Backend. Once the installation is finished, you can check if the service was installed successfully.

```
nextron@security-center:~$ systemctl status asgard-security-center-frontend.service
```

If the status of the service is `active (running)`, the installation is finished.

You can now log into the frontend via `https://<FQDN>`.

CHAPTER

THREE

FIRST STEPS

This chapter contains the first steps after installing the Security Center. Please follow along those steps to avoid issues at further stages. Here we will change the default credentials, and connect your Security Center with your existing Analysis Cockpit. Additionally, we will create your first tenant.

3.1 Credentials

You can log into the Backend with the following default credentials. The admin user will work for both Frontend and Backend, but for the initial configuration, we recommend to perform the next steps on your backend.

- User: `admin`
- Password: `admin`

After you logged in for the first time, you have to change the default password before you can continue.

The password has to be at least 12 characters long and contain at least one lowercase alphabet, uppercase alphabet, digit and special character.

After you have changed the default password, we advise to set up the second factor. You can do this by clicking your username in the top right corner and navigating to `User Settings`.

> **Warning:** The `admin` user has access to all tenants. Use this user only for administrative tasks, as you will have access to all the sensitive data within the Security Center.

3.2 Connect your Analysis Cockpit

In order to get data from your Analysis Cockpit into the Security Center, we need to connect both systems first. This can be done via the Web UI of both systems.

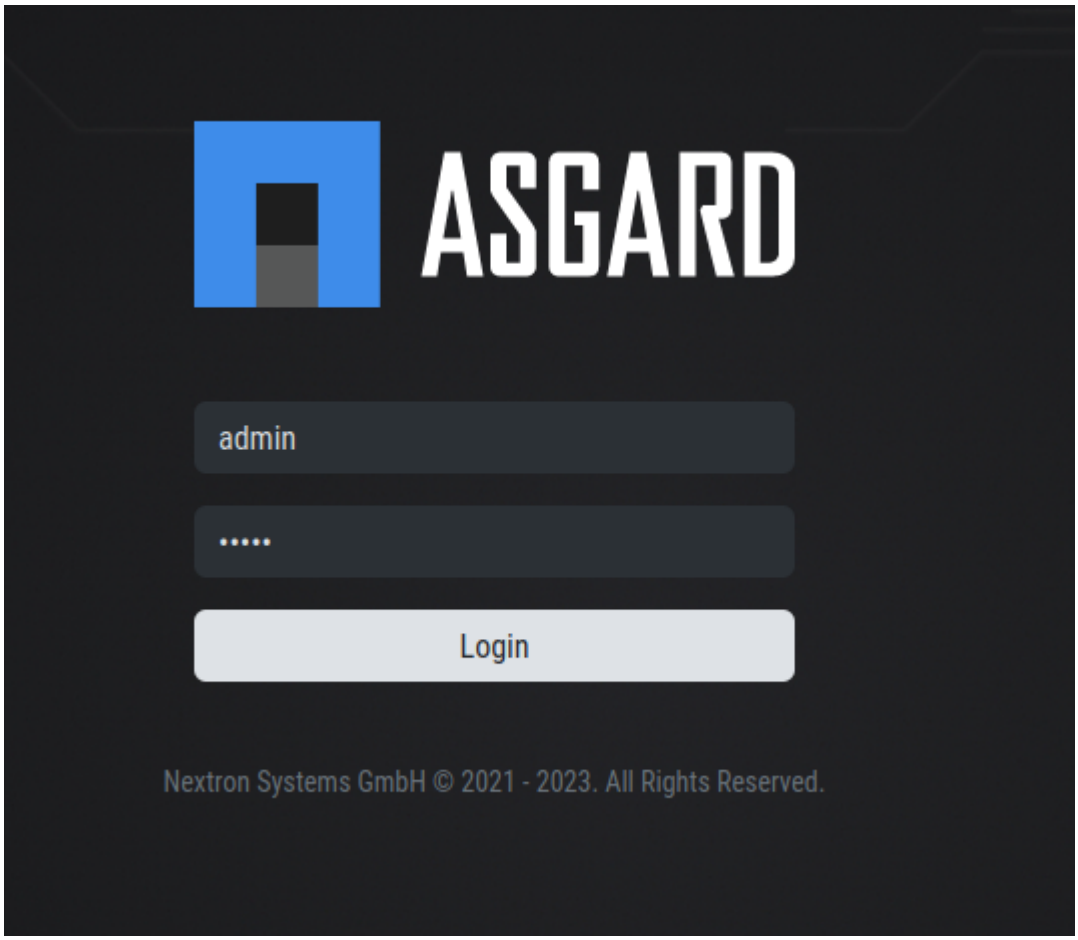


Fig. 1: Security Center Login Page

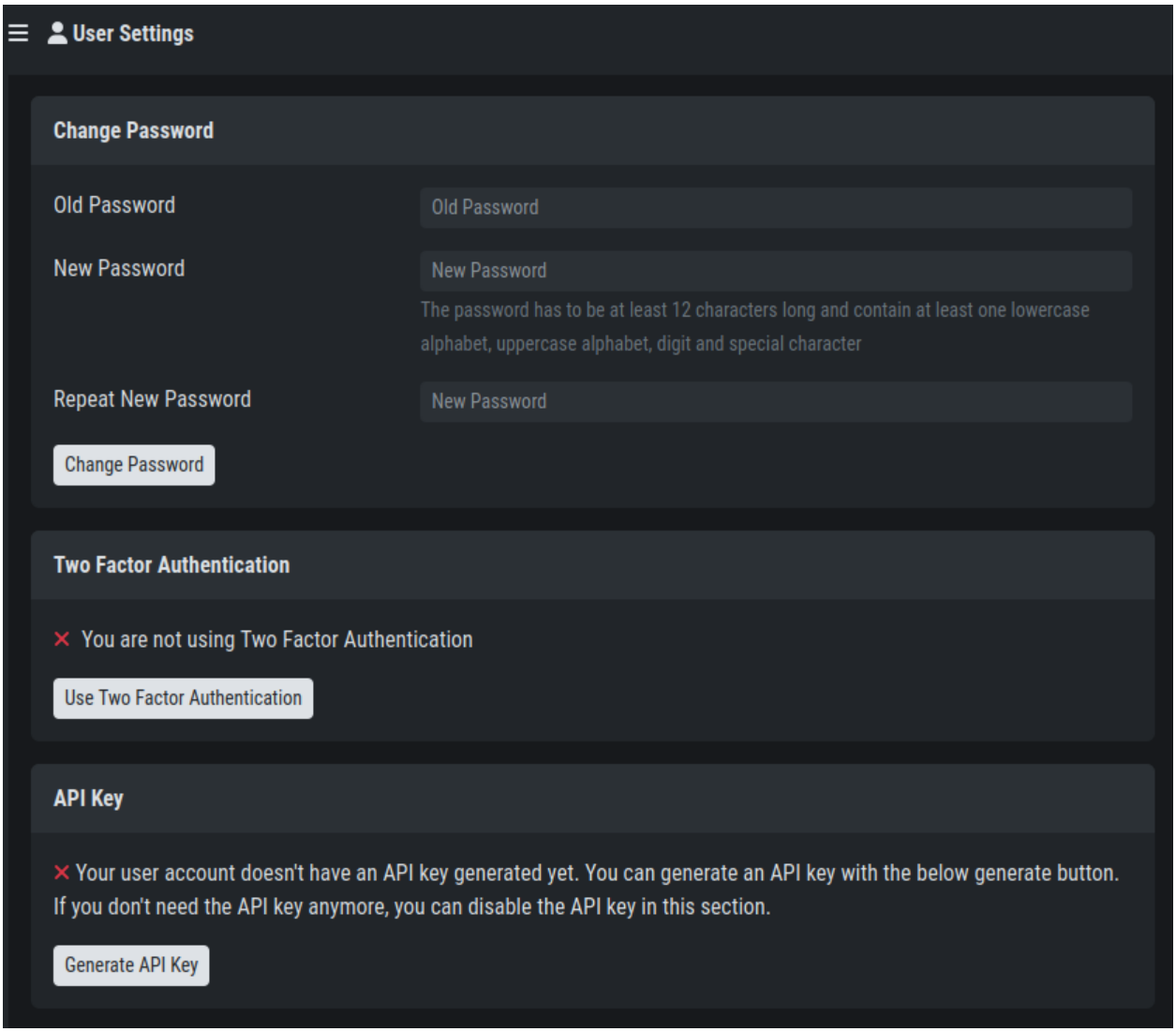


Fig. 2: Security Center User Settings

3.2.1 Prepare your Security Center

To connect your Analysis Cockpit with your Security Center, you have to navigate to `Settings` > `Analysis Cockpit`.

Click `Connect Analysis Cockpit` in the top right corner. This will generate a **One-Time Code** which is valid for two hours. We need this code in our Analysis Cockpit now.

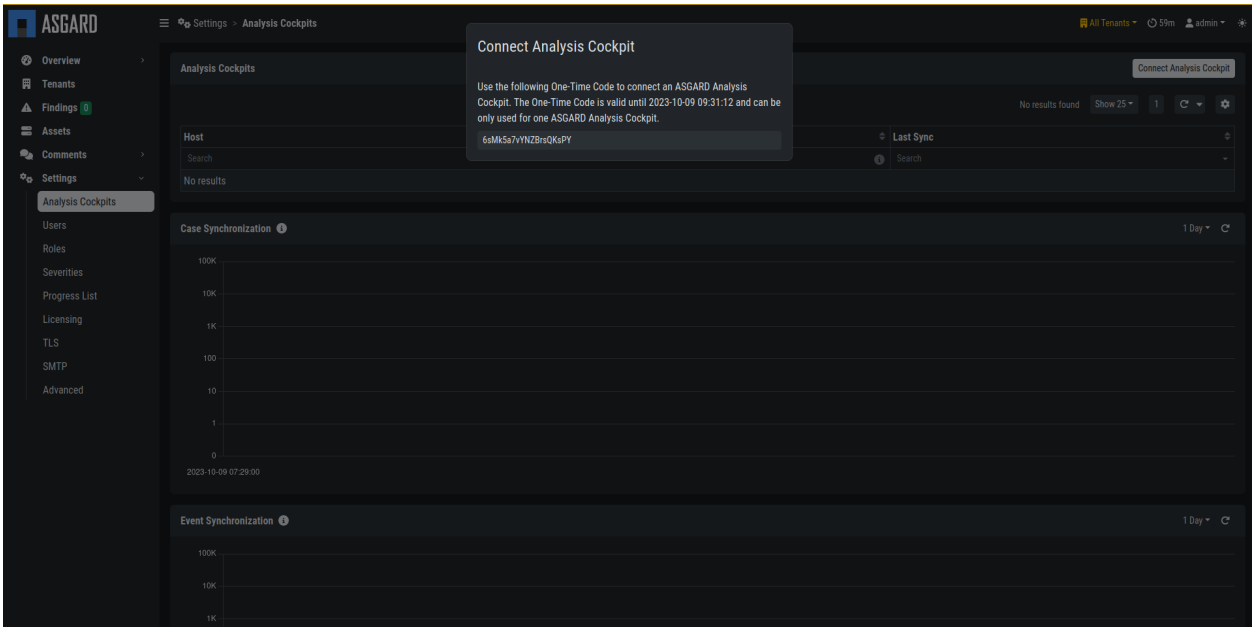


Fig. 3: Security Center Connect Analysis Cockpit

3.2.2 Before your connect

Before you connect your Analysis Cockpit to your Security Center, decide which cases should be synchronized to the Security Center. Keep in mind, that once synchronized, data will remain on the Security Center, even if synchronization criteria are modified.

We recommend to only synchronize cases that contain actionable information, which is fully analyzed and finally validated. For that reason, we recommend to only synchronize data with a case status of `Closed`. In this situation, `Closed` means that the analysis is finished.

It is important to understand that a case with status `Closed` will lead to one or more `Findings` being opened within the Security Center. The actual remediation is then tracked within the Security Center.

3.2.3 Configure your Analysis Cockpit

Log into your Analysis Cockpit and navigate to `Settings` > `Link` > `Security Center`.

The **Automatic Mode** will automatically flag all cases in your Security Center, which match the criteria from `Case Types` and `Case Status`.

Important: As with all our products, you have to use a FQDN to connect the Analysis Cockpit with your Security Center. Make sure that the Analysis Cockpit can resolve the FQDN of the Security Center and reach it via the necessary port.

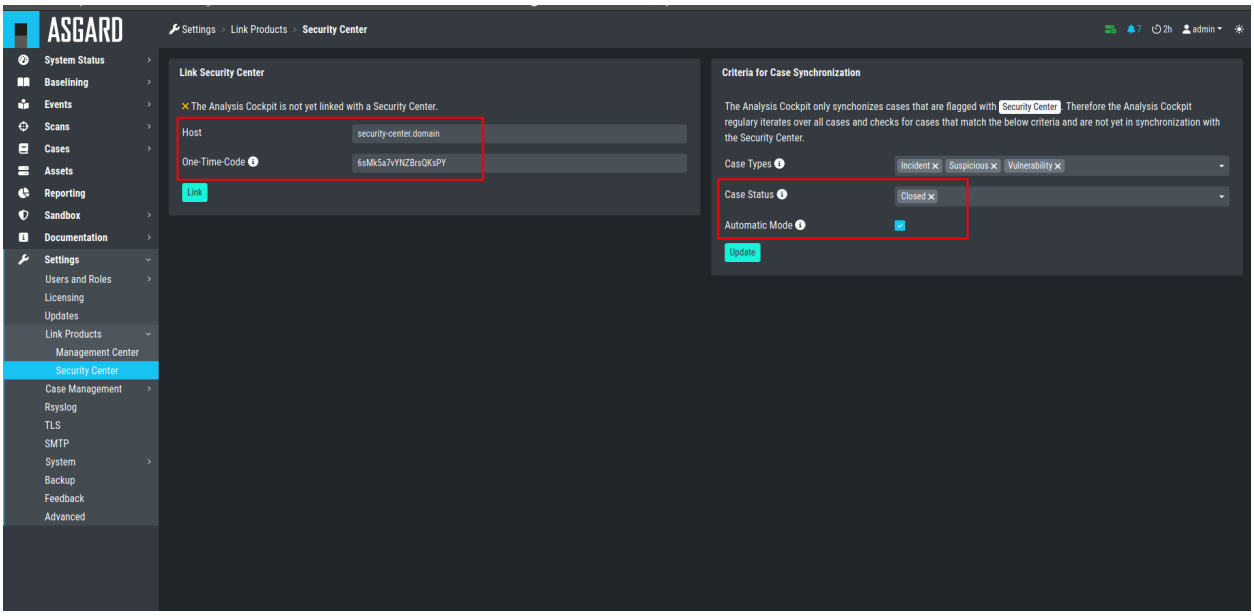


Fig. 4: Connect Analysis Cockpit

You can have find the needed network ports in the chapter *Analysis Cockpit*.

Once you connected your Analysis Cockpit to your Security Center, you can find the status and some statistics in your Security Center in `Settings` > `Analysis Cockpit`.

3.3 Tenants

In this chapter we will create our first tenant. All of the configuration will again be done in your Backend (port 8443 HTTPs).

3.3.1 Setting up your first Tenant

Open your browser and connect to the Security Center Backend. After logging in with your administrative credentials, navigate to `Tenants` and click `Add Tenant` in the top right corner.

Choose a `Name` for the tenant and the `Asset Labels` associated with this tenant. The labels are used to assign assets from the Analysis Cockpit to a tenant. An asset will be assigned to a tenant, if it has at least one of the labels selected.

You can always modify the labels for a tenant by clicking the `Edit` button in the `Actions` column.

> **Danger:** It is important to understand that an asset is assigned to a specific tenant the moment it first shows up with a label that fits to this specific tenant. Changing the label at a later point will **NOT** cause the asset to be assigned to another tenant.

Hint: To automatically assign assets to the correct tenant, service providers can create a tenant specific agent installer (on the ASGARD Management Center) with a preset and unique label for every tenant. This agent installer can be

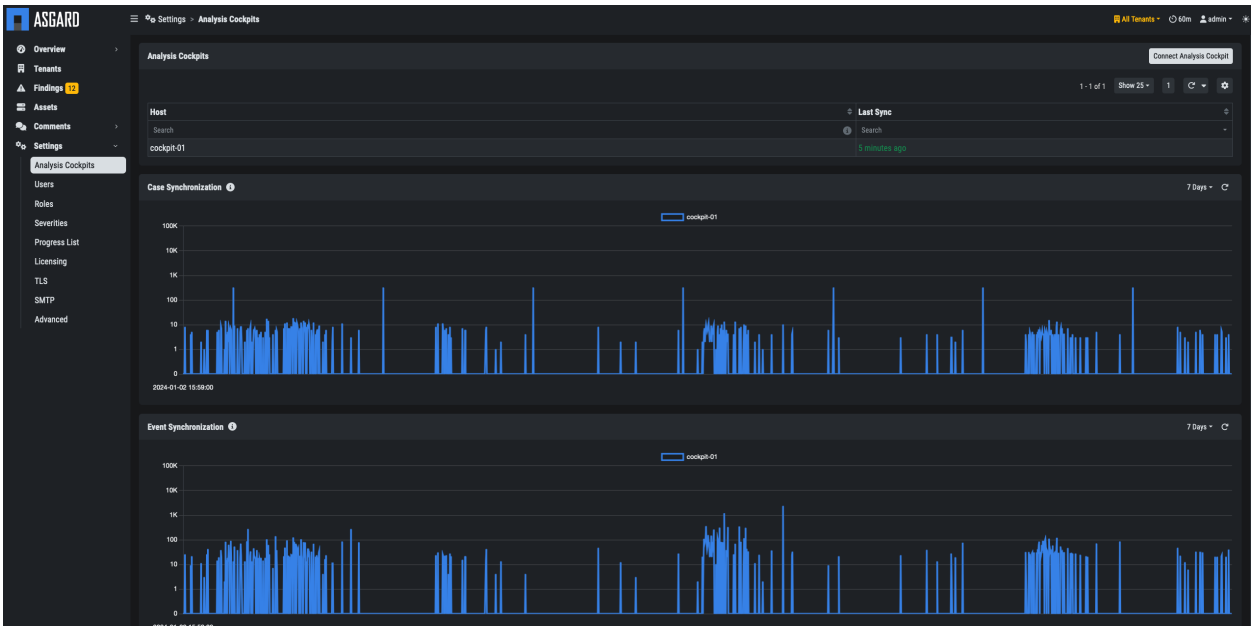


Fig. 5: Connected Analysis Cockpit

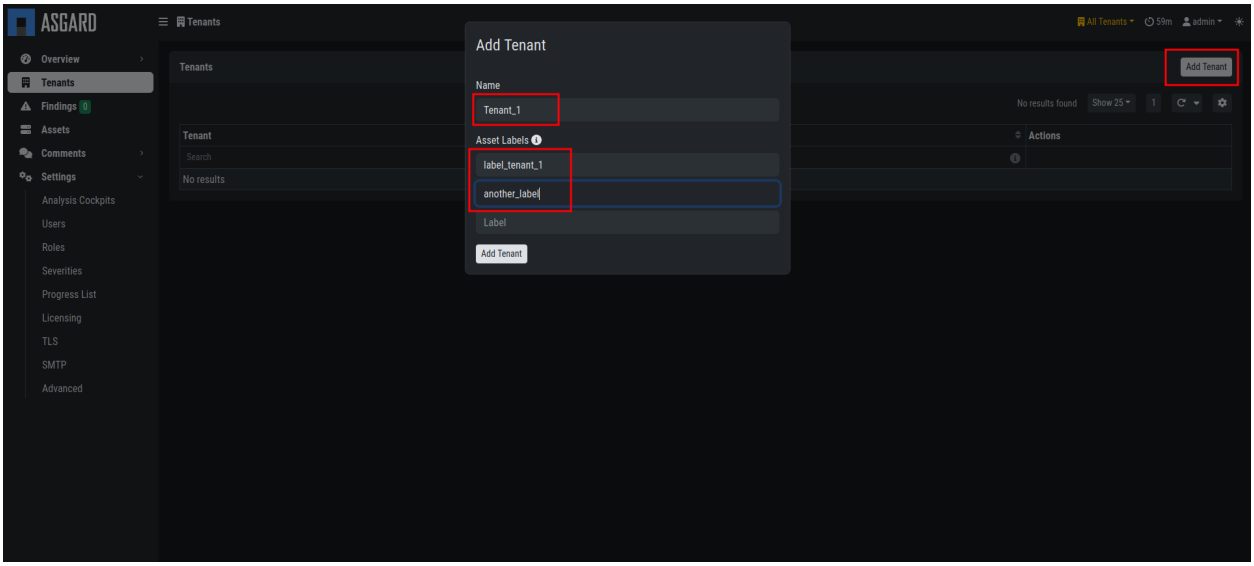


Fig. 6: Security Center new Tenant

provieded to the specific tenant for installation.

3.3.2 Create a User Group for your Tenant

You can create an optional `User` User Group for the Security Center. This can be used to assign to non-administrative users of the Security Center. Individual Users will be assigned to a tenant with those permissions.

To do this, navigate to `Settings` > `Roles` and click `Add Role` in the top right corner.

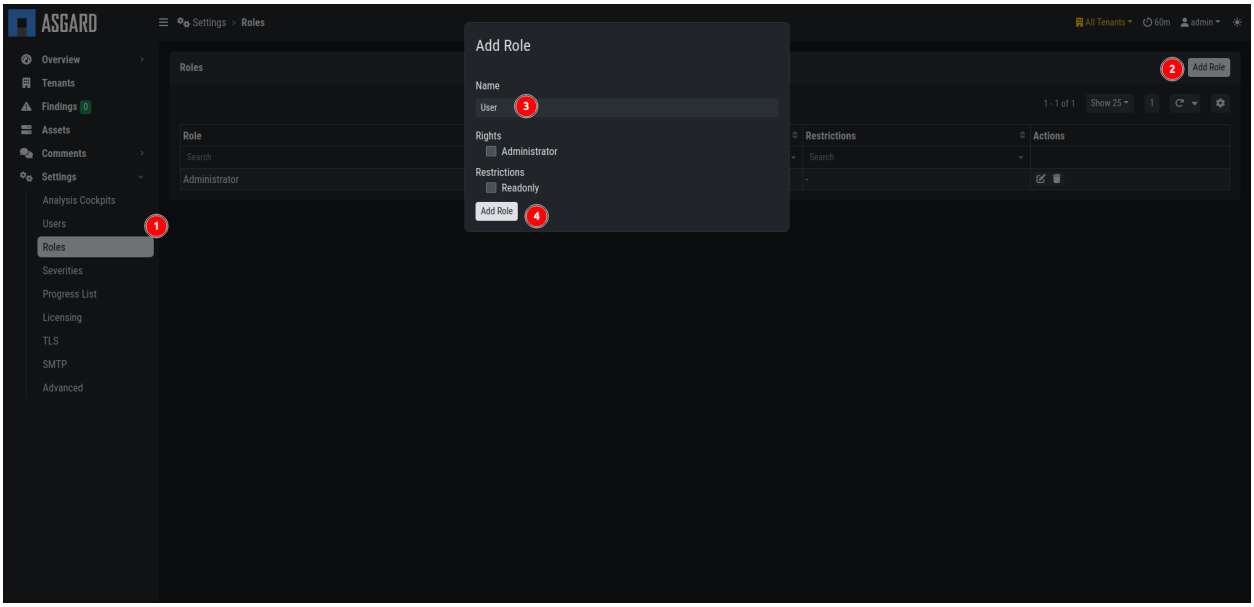


Fig. 7: Security Center User Group

3.3.3 Create a User for your Tenant

You can find all the users in `Settings` > `Users`. Here you can create new users for your tenants. You will also find the admin user, which is assigned to `All Tenants`. Create a new user by clicking `Add User` in the top right corner.

Make sure to use the correct role and tenant for this user, as this will determine what the user can access.

Hint: Currently you can only create normal user accounts for a tenant. In future version you will be able to create tenant-specific administrative accounts, which will be able to create users for their own tenant.

The tenant users should use the Security Center Frontend to access their data. See *Customer Access*.

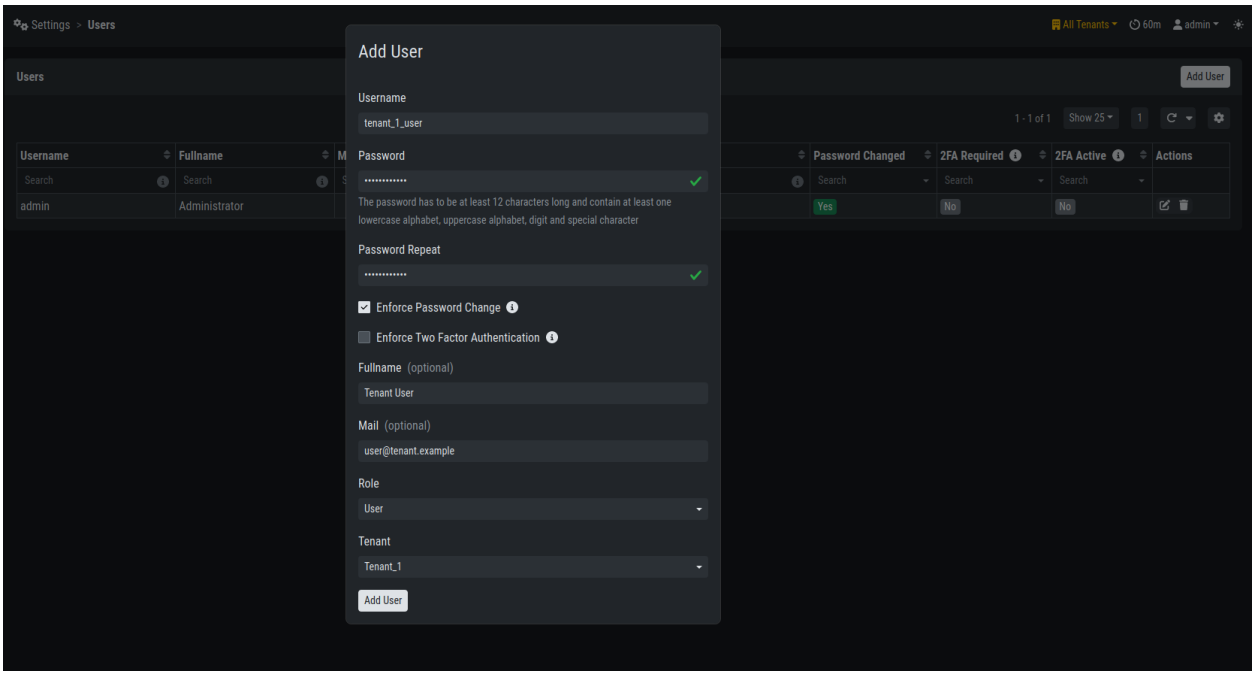


Fig. 8: Security Center new User

CHAPTER

FOUR

FINDINGS, ASSETS AND TENANTS

In this chapter we will explain how to work with the Security Center. We will explain how to manage findings, how to work with your assets and how to manage tenants.

4.1 Working Model

For simplicity's sake, let's consider a scenario where a service provider scans all endpoints of all connected tenants on a weekly basis. In our scenario, the tenants are named EMEA, USA, Customer_XYZ, and ASIA_CORP.

The service provider has a team of analysts (Analyst Team), which is working on the `Analysis Cockpit` and is providing tenant independent valuation of events by building cases. A second team of security specialists (Customer Service Team), which is more focused on the individual tenants/customers, is working on the `Security Center`. They provide guidance to individual customers where needed.

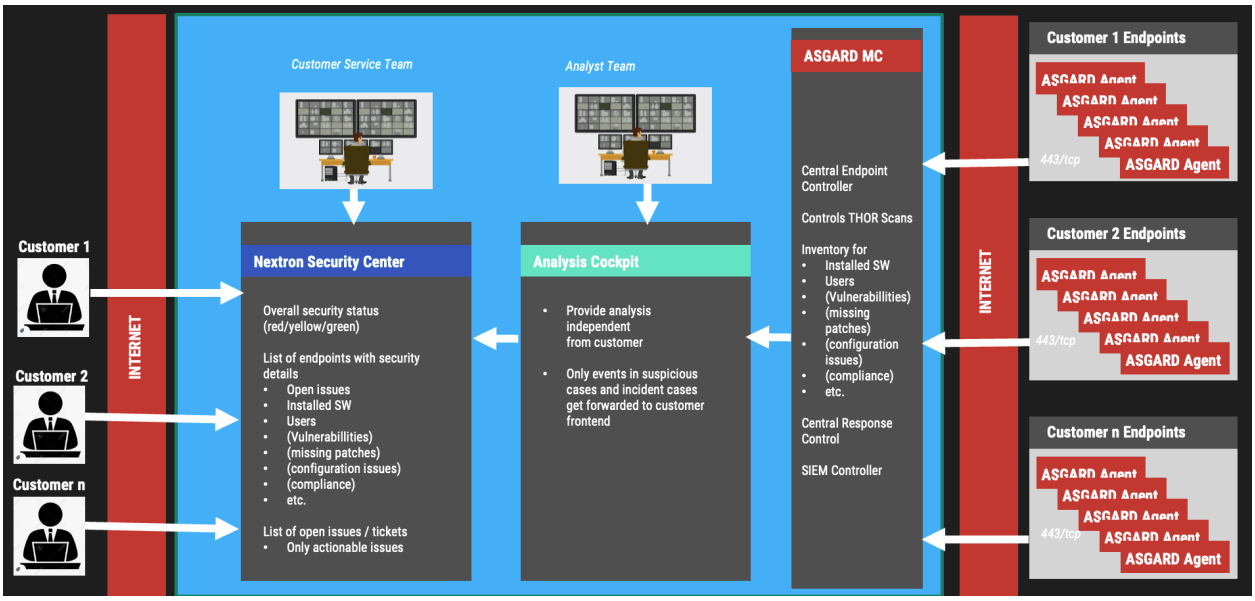


Fig. 1: Working Model

4.2 Synchronization

In this chapter we will explain how data is being synchronized between the different components.

4.2.1 Synchronization between Analysis Cockpit and Security Center

This chapter contains the synchronization of data between the Analysis Cockpit and the Security Center.

Asset Data

Asset data contains endpoint related data like operating system version, IP addresses, hostname, local users (windows only) and installed software (windows only).

An endpoint is assigned to a particular tenant based on the **label set in the ASGARD Management Center**. It is recommended to prepare custom agent installers for every tenant with a built-in label. Please see the ASGARD MC manual for details. This is to ensure an endpoint is automatically assigned to the correct tenant and human error cannot lead to an endpoint being assigned to the wrong customer. The mapping between tenant and label can be found in the chapter *Setting up your first Tenant*.

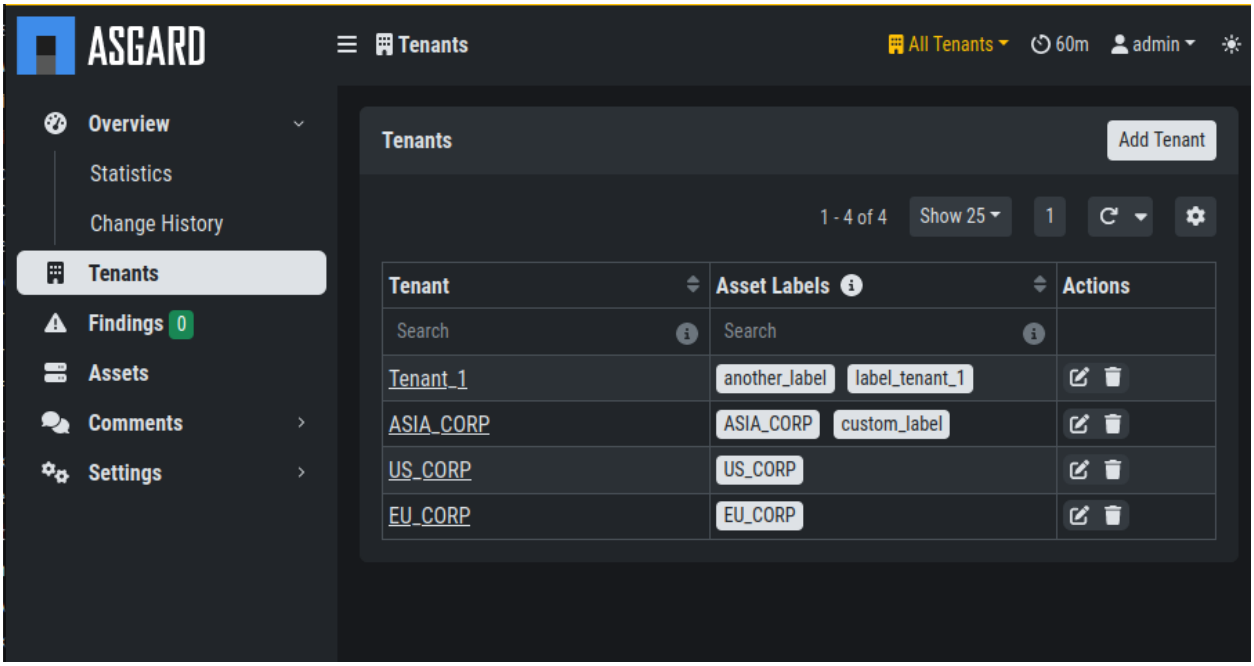


Fig. 2: Tenant Overview

An asset will be assigned to a tenant in the very first moment an asset shows up with a mappable label. Once mapped to a tenant, the asset will remain with this tenant forever – even if an asset's label is changed to another mappable label.

Event Data

Event data synchronization is defined in the Analysis Cockpit (see *Configure your Analysis Cockpit*). Once a case with the defined type has been set to the defined status, the case data will be synchronized to the Security Center and a `Finding` will be opened for all assets within this case – regardless of the affected tenant.

As it is recommended to only synchronize events that are actionable **AND** fully analyzed, the default criteria for synchronization are "Incident", "Suspicious" and "Vulnerability" in regards the case type. By default, only cases with status "Closed" – which stands for "Analysis is finalized" – are synchronized. However, **the service provider is free to configure this according to their needs and processes**.

Important: It is not uncommon that a single case triggers multiple findings for multiple assets and multiple tenants. As case data will be copied to every finding regardless of the tenant, the analysts must avoid storing tenant specific information into the cases' `assessment` fields, `summary` fields and `custom recommendation` fields.

4.3 Managing Findings

In this chapter we will describe our **recommended workflow** for managing findings within your Security Center.

4.3.1 High Level Workflow

The default progresses for findings are `New`, `In Progress`, `Remediated` and `Closed`. They can be amended or changed under `Settings` > `Progress List` to meet the organization's needs.

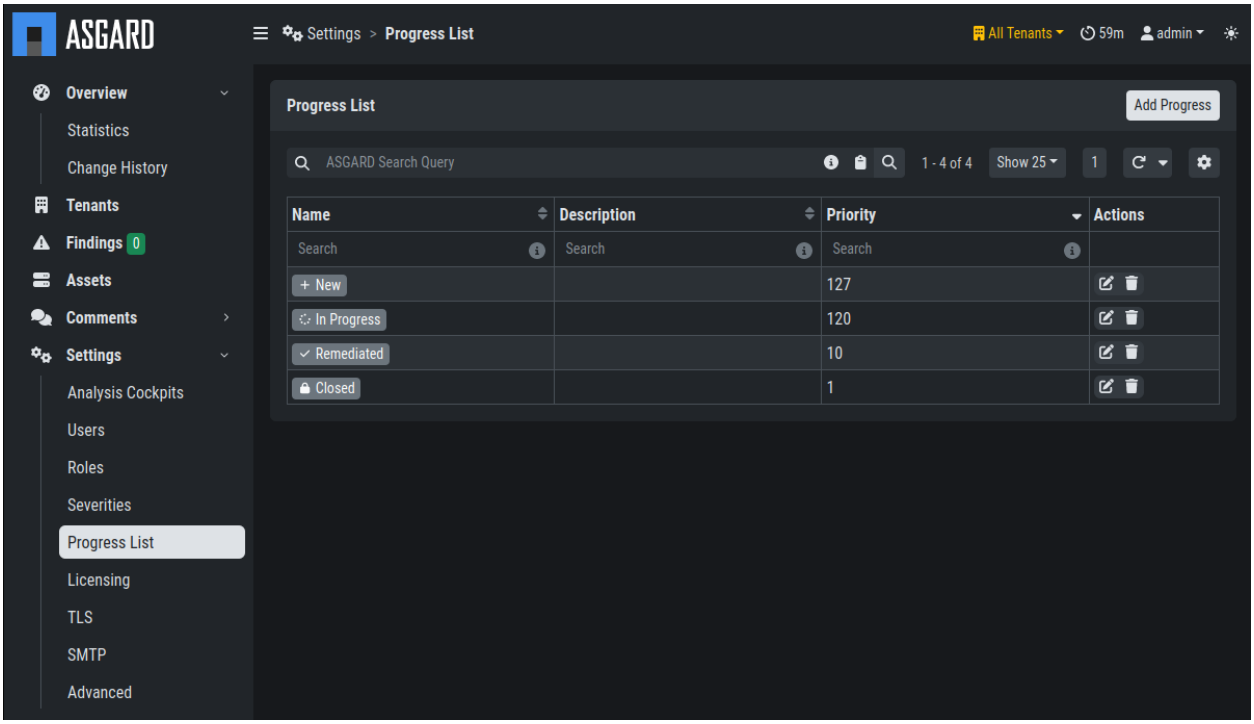


Fig. 3: Progress List

The `Priority` has to be a unique value between **1** and **127**. The progress with the highest priority will be treated as **Open**, the progress with the lowest priority will be treated as **Closed**.

4.3.2 Basic Workflow

A basic workflow could look like the following.

- Step 1:

  A tenant's security analyst opens a particular finding. Now all affected assets are shown in the sidebar. They set the status to `In Progress` for one or multiple assets within the finding, as they are now working on this issue.

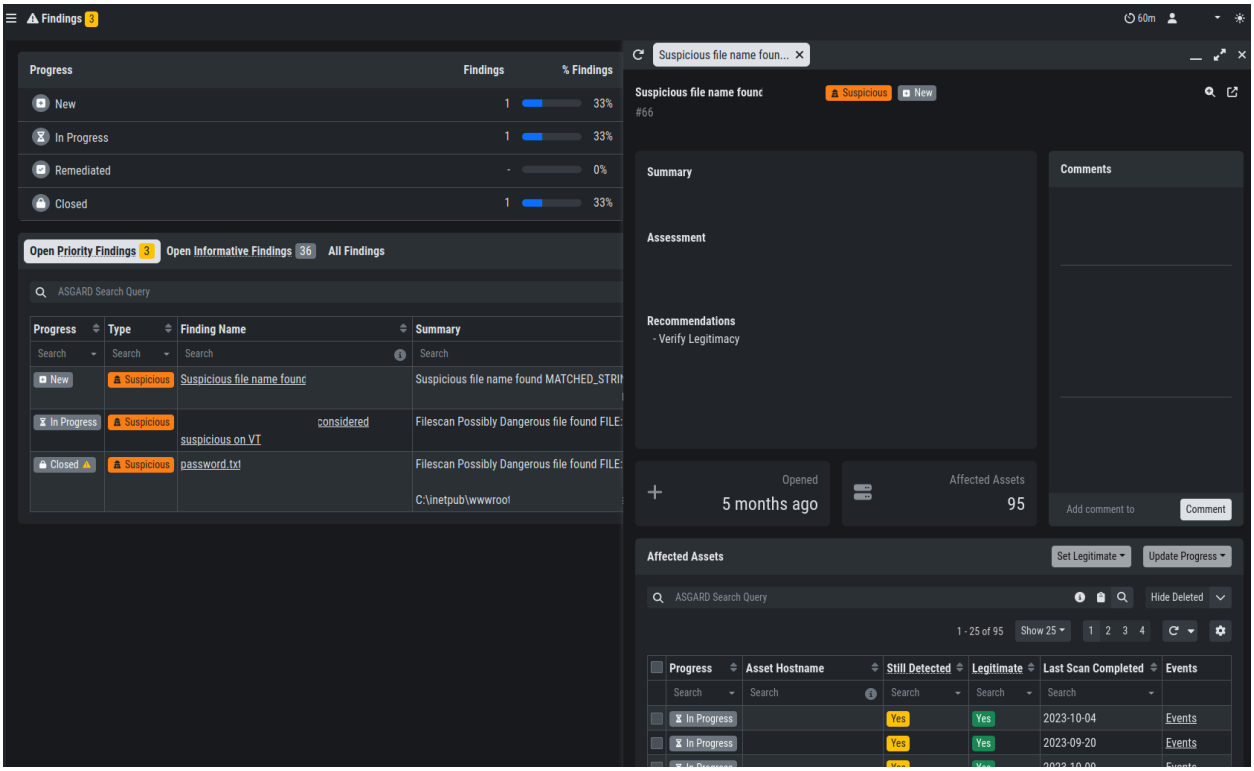


Fig. 4: Findings

- Step 2:

  Now the organization works on remediating the finding. Once remediated, the status should be changed to `Remediated`.

- Step 3:

  Ideally the remediation should be confirmed by waiting for the next scan – in our working model this is one week as a maximum. If the finding is not detected anymore, the `Still Detected` flag changes to `No`. Now the finding`s status can be changed to `Closed`. Once the finding is set to `Closed` for all endpoints within the finding, the finding`s status will automatically change to `Closed`.

Starting from the Asset View

Alternatively, it is possible to start from an asset-based view and start working on potentially multiple findings on this endpoint. The figure below shows two different findings on the system windows06-pg01. The findings can now be selected, and their status can be changed and/or they can be set to legitimate.

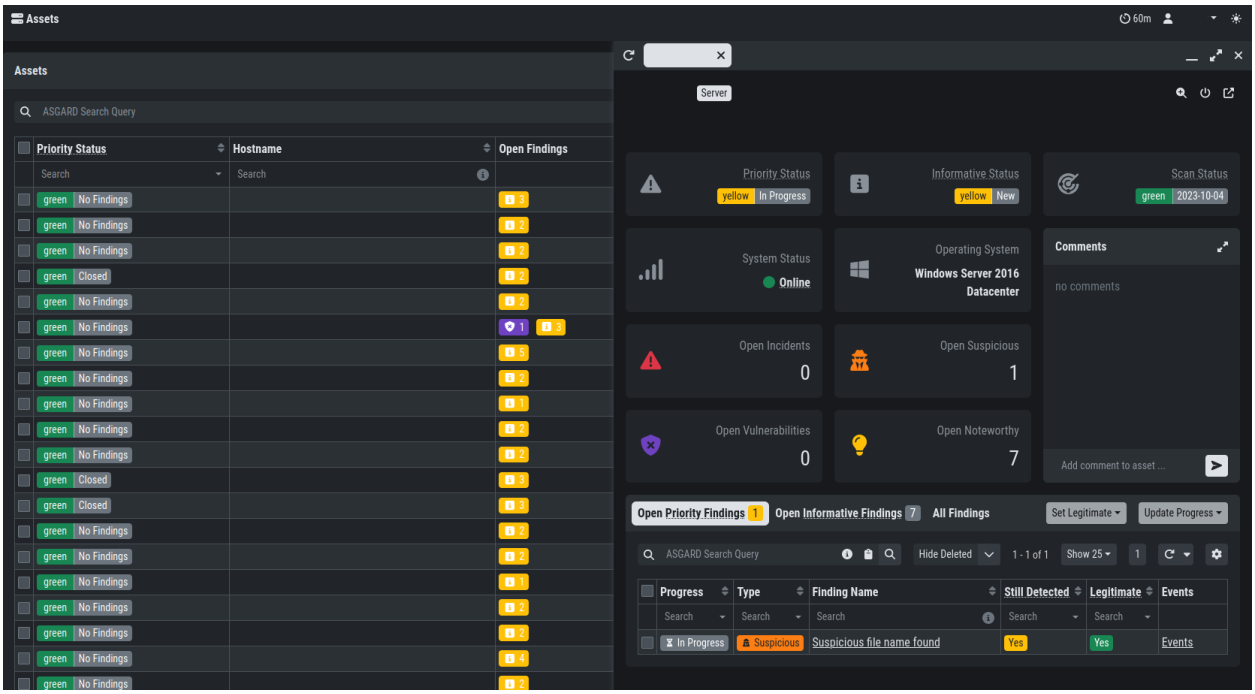


Fig. 5: Start from Asset View

4.3.3 Using the "Legitimate" Flag

Sometimes the same finding represents an incident for one customer while another customer finds the same thing to be legitimate – or at least legitimate for this particular endpoint. For this reason, a finding that is not intended to be remediated can also be flagged `Legitimate`. This can be done by clicking on the finding and selecting the `Affected Assets` tab. One can now select one or multiple assets and change their status or set the finding to legitimate.

4.3.4 The "Call for Action" Flag

Let's consider a situation where a finding has been closed but the next scan finds the very same issue on one endpoint within the finding. In this case the entire case will be flagged with `Call for Action`. The picture below shows a finding that has been set to closed, but we find it highlighted and the `Call for Action` column states `Yes`.

However, if a finding has been flagged to be legitimate the `Call for Action` flag will not be set. The picture below shows a finding regarding `Laudanum` that was detected on two endpoints.

As we can see, the finding is closed and not highlighted, although it is still detected on the second asset. The reason for this is that it has been set to `Legitimate`.

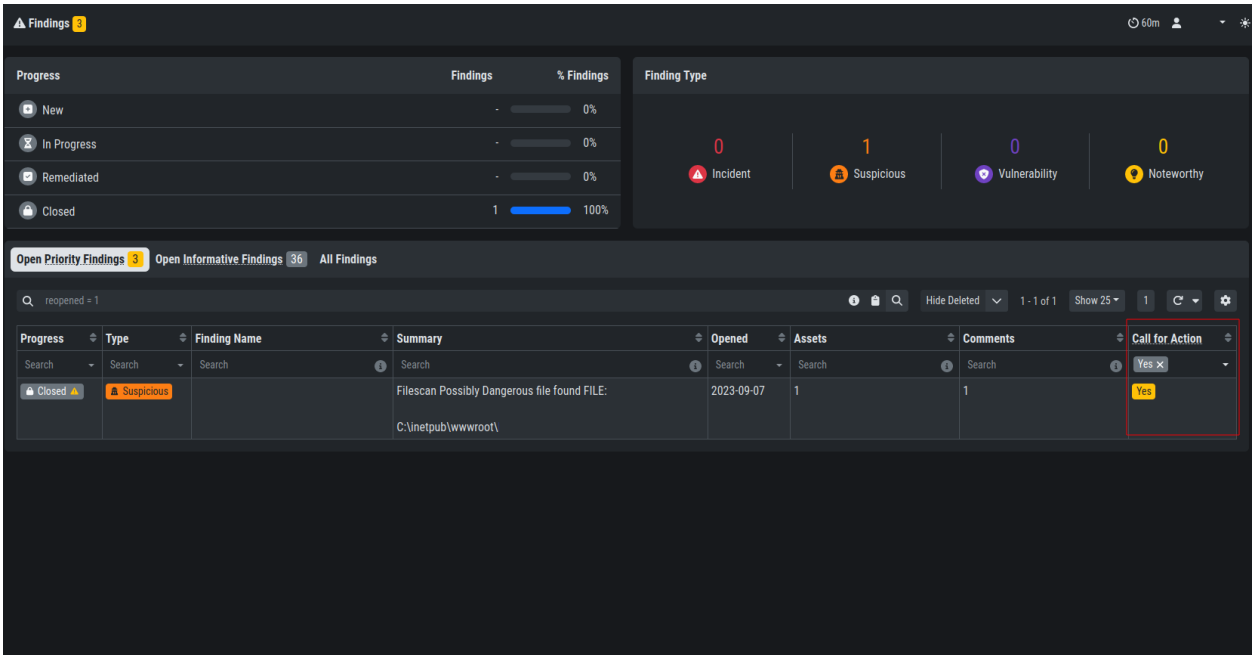


Fig. 6: Call for Action

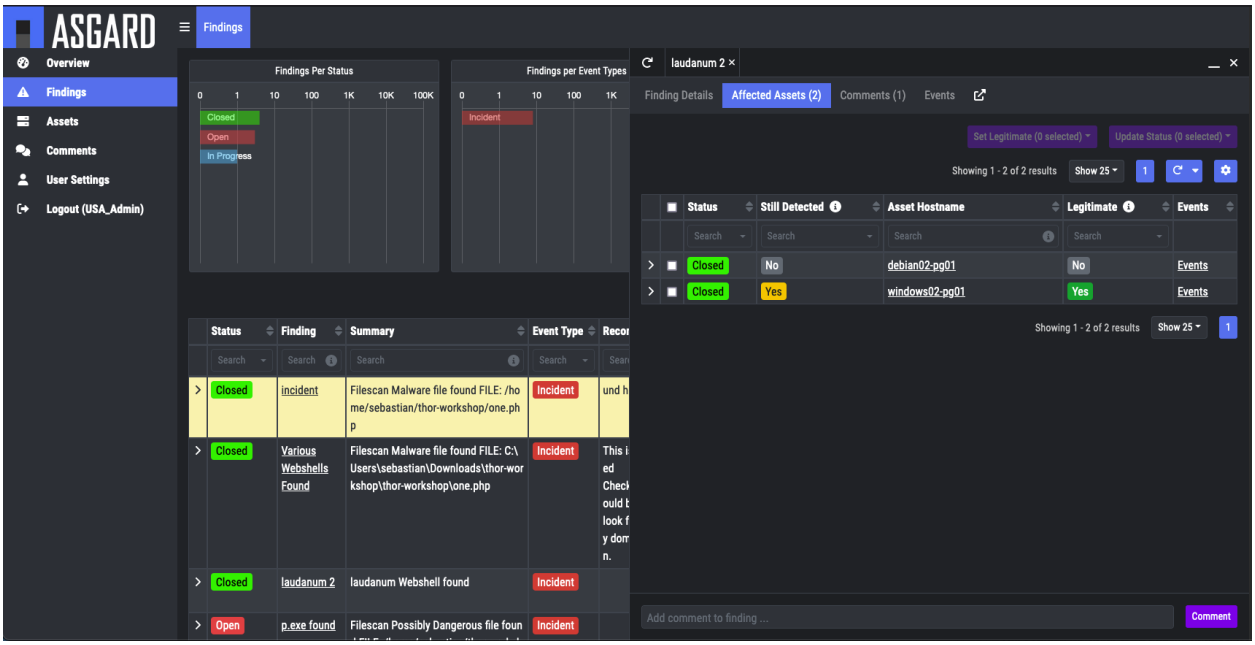


Fig. 7: Example Finding

4.3.5 Using the Comment Function

Comments are intended to be used for communication between a tenant's employees and the service providers' customer care team. Comments can be assigned to an asset or to a case.

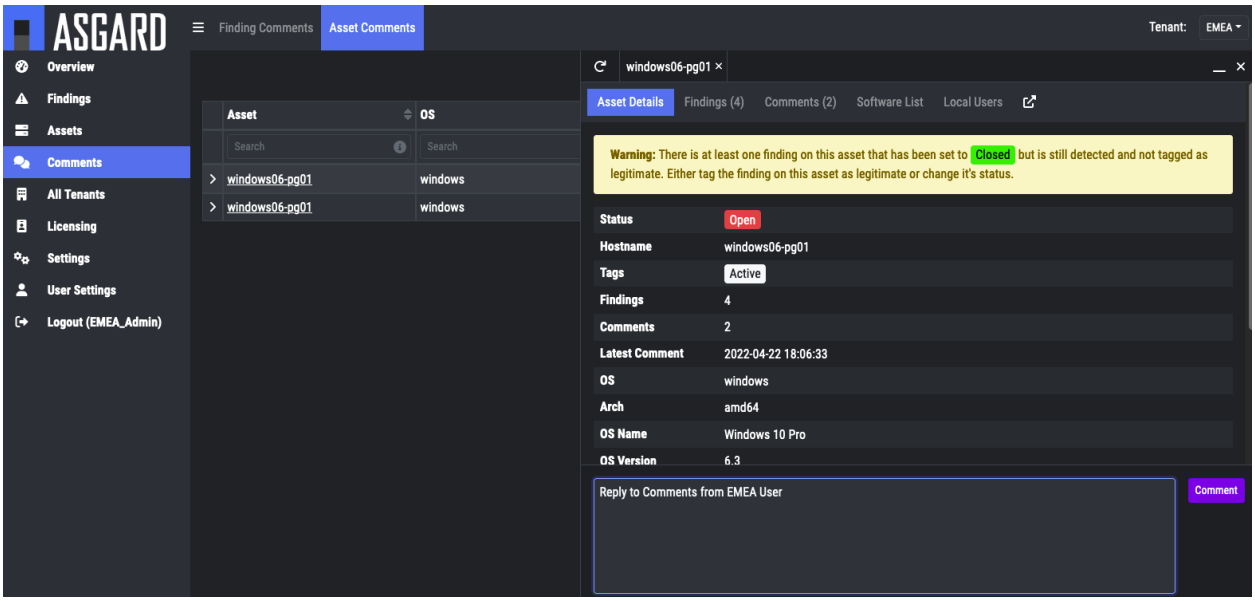


Fig. 8: Center Comments

Comments are visible to all users assigned to the particular tenant and to the service provider's administrative users.

4.4 Service Provider

Service Providers can use the Security Center by logging into the administrative backend system on port 8443 and setting the desired tenant in the upper right corner of the overview tab.

Now the sections `Assets`, `Findings`, and `Comments` only show information related to this tenant. The picture below shows allocation to the tenant `USA`.

Hint: You can customize the corresponding tenant view, i.e. if you have selected a tenant, only the information about this tenant will be displayed (Findings, Assets ...). If you switch to `All Tenants` you will see all information. This applies to the entire navigation tree.

4.5 Security Monitoring

The Security Center writes detailed logs for all relevant actions. The log files can be found here:

- `/var/lib/nextron/securitycenter/log/securitycenter.log`
- `/var/lib/nextron/securitycenter-model/log/securitycenter-model.log`

Audit events within the log files are flagged with `AUDIT: true`.

Fig. 9: Specific Tenant

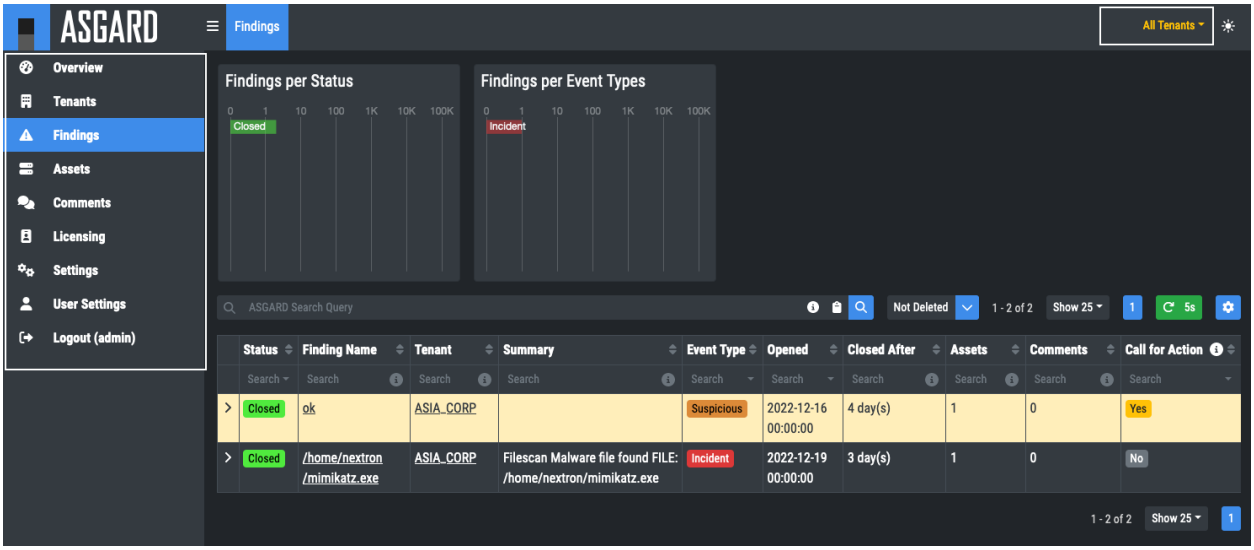


Fig. 10: All Tenants

CHAPTER

FIVE

ADMINISTRATIVE TASKS

In this chapter we will walk through some administrative tasks you might need when working with your Security Center. You will need access to the command line, the Web UI, or both to perform those tasks, so make sure you have access before continuing.

5.1 Updates

Since the Security Center does not contains an "Update" menu in your Web UI, you need to update the verions via the command line.

To do this, connect to your Security Center Frontend and Backend via SSH. If you are running the Frontend and Backend on the same server, you only need to perform the next step once.

We run the following command to update the minor version of your Security Center:

```
nextron@asgard-sc:~$ sudo apt update
nextron@asgard-sc:~$ sudo apt dist-upgrade
```

After the updates have been installed, you can check if the services are up and running again. Make sure the status is in the `active (running)` state:

Frontend:

```
nextron@asgard-sc:~$ sudo systemctl status asgard-security-center-frontend.service
 asgard-security-center-frontend.service - ASGARD Security Center Frontend
     Loaded: loaded (/lib/systemd/system/asgard-security-center-frontend.service;␣
↪enabled; preset: enabled)
     Active: active (running) since Thu 2023-11-16 12:42:47 CET; 38s ago
[...]
```

Backend:

```
nextron@asgard-sc:~$ sudo systemctl status asgard-security-center-backend.service
 asgard-security-center-backend.service - ASGARD Security Center Backend
     Loaded: loaded (/lib/systemd/system/asgard-security-center-backend.service; enabled;
↪ preset: enabled)
     Active: active (running) since Thu 2023-11-16 12:42:47 CET; 31s ago
[...]
```

5.2 Upgrade your Security Center from v1 to v2

In this chapter we will explain how to upgrade your Security Center v1 to the newest version. Since we mainly focus on the new Version 2 of the Security Center in this document, we want to help you through the upgrade process from your older Version 1 of Security Center the newest one, so you can make use of the newest features.

If you are running your Security Center Frontend and Backend on two separate servers, you will have to do the steps below for both servers. You can upgrade them at the same time to reduce downtime.

5.2.1 New Update Servers

We are using a new update server for the new versions of the Security Center. Please make sure the following server is reachable by both your Frontend and Backend server:

Description	Port	Source	Destination
Product Updates	443/tcp	Security Center Frontend & Backend	update-301.nextron-systems.com

Please make sure your local firewall allows the connection to the new update server, otherwise the upgrade will not work.

5.2.2 Preparing for the Upgrade

To prepare for the upgrade, make sure that you have an up to date backup of both your Security Center backend (sometimes referred to as "model") and the frontend. We advise to take a snapshot of the VMs with your hypervisor.

After you created a backup/snapshot, we need to update both frontend and backend servers to the newest version. If you have the frontend and backend installed on the same system, you need to run the next commands only once. If you have two separate servers, repeat the next steps for each of them.

Connect to your Security Center v1 via SSH. Update your current Security Center v1 to the newest version:

```
nextron@seccenter:~$ sudo apt update && sudo apt dist-upgrade
[...]
Do you want to continue? [Y/n] y
```

Please confirm the linux upgrade by pressing **y** and **enter**. This will not upgrade your Security Center, only the underlying linux operating system.

Hint: This process might take a while.

5.2.3 Performing the Upgrade

After we prepared the system(s) for the update, we can run the following command to install the version 2 of the Security Center. Please note that this step can not be reversed, and your Security Center will be running with the newest version after the update has finished.

```
nextron@seccenter:~$ start-asgard-update
Created symlink /etc/systemd/system/multi-user.target.wants/asgard-updater.service → /
↪lib/systemd/system/asgard-updater.service.
Successfully started the ASGARD update process.
To monitor the update progress and view log files, you can use the following command:
sudo tail -f /var/log/asgard-updater/update.log
```

Warning: Your server will restart multiple times during the upgrade process. Do not restart the server manually. You can log into the server and run the following command to monitor the progress:

```
nextron@seccenter:~$ sudo tail -f /var/log/asgard-updater/update.log
```

Once your update is finished, you should find the following message in the update log:

```
nextron@seccenter:~$ sudo tail /var/log/asgard-updater/update.log
[...]
2023-10-31T08:57:14.834079+01:00 security-center asgard-updater[731]: Upgrade finished.␣
↪Deactivating service...
2023-10-31T08:57:14.843136+01:00 security-center asgard-updater[731]: Removed "/etc/
↪systemd/system/multi-user.target.wants/asgard-updater.service".
```

You can now connect to your Security Center's Web UI as usual.

5.3 Password Reset

Since the password for the admin user is stored only on the Backend, you have to reset the password via console. To reset the password for the `admin` user on the **Security Center Backend**, run the following command via console:

```
nextron@sc-back:~$ sudo asgard-security-center-backend set-password
Please enter password for user `admin`:
Please re-enter password for user `admin`:
nextron@sc-back:~$
```

CHAPTER

SIX

KNOWN ISSUES

You can find a list of known issues in this section. There are no known issues at this point.

6.1 ASC#001: Backend is down after Upgrade to v2

Introduced Version	Fixed Version
2.x	N/A

There is currently a rare issue where the backend is not starting after upgrading to v2. This is due to insufficient permissions for the MySQL Trigger.

If you upgraded your Security Center to version 2 and everything seems to be working fine, you can ignore this advisory.

We are currently working on a more robust upgrade process to prevent this from happening in the future.

6.1.1 ASC#001: Workaround

After a successful upgrade to version 2 ("Upgrade finished" message can be seen, see *Performing the Upgrade*), you might encounter the following error message in `/var/log/asgard-security-center-backend/server.log`:

```
{
  "level": "FATAL",
  "time": "2024-04-03T18:49:16+02:00",
  "message": "failed to init database schema",
  "error": "Error 1142 (42000): TRIGGER command denied to user 'securitycenter-model'@
↪'localhost' for table `asgard-security-center-backend`.`assets`"
}
```

To fix this problem, run the following commands on your backend.

Drop the MySQL trigger (no data will be lost):

```
nextron@backend:~$ sudo mysql asgard-security-center-backend -e "DROP TRIGGER IF EXISTS␣
↪assets_updated_fields;"
```

Restart the backend service. This will recreate the trigger with the correct permissions automatically:

```
nextron@backend:~$ sudo systemctl restart asgard-security-center-backend.service
```

Check if the service is running:

```
nextron@backend:~$ sudo systemctl status asgard-security-center-backend.service
```

CHAPTER

SEVEN

CHANGELOG

In this chapter you can find all the changes of the Security Center.

7.1 Security Center v2

This chapter contains all the changes made to the Security Center **Version 2**.

7.1.1 Security Center 2.0.3

Type	Description
Bugfix	Fixed scroll to top when selecting dropdown items
Bugfix	Fixed temporarily wrong 'call for action' indicator
Bugfix	Fixed wrong table shown when clicking on some counts in the overview page

7.1.2 Security Center 2.0.2

Type	Description
Change	Upgraded Debian from 10 to 12
Feature	Support ASGARD Installer

7.2 Security Center v1

This chapter contains all the changes made to the Security Center **Version 1**.

7.2.1 Security Center 1.2.9

Type	Description
Feature	Differentiate between 'Open Findings' and 'All Findings'
Feature	Differentiate between 'Priority Findings' and 'Informative Findings'
Feature	Configure severity of findings per type and tenant
Feature	Receive E-Mails for updates on findings and assets
Feature	Added more change events to change history
Feature	Support Aurora (requires Analysis Cockpit 3.8)
Feature	Baselining count for THOR and Aurora events per asset (requires Analysis Cockpit 3.8, configurable)
Feature	API keys (Backend only)
Feature	API documentation (Backend only)
Change	Refactored the UI
Change	Wordings
Bugfix	Fixed case with id 1 to be assigned to wrong finding
Bugfix	Fixed some missing audit logs
Bugfix	Fixed missing findings for assets that had no initial tenant assigned on first sync with Analysis Cockpit

7.2.2 Security Center 1.1.1

Warning:

- This release refactored the architecture between tenant-based UI, administrative UI and the servers. This also implies a full refactor of the API.
- If you have installed the Security Center and the Security Center Model on same servers, you can upgrade those components without any implications
- If you have installed the Security Center and the Security Center Model on different servers, the following things will change for you:
  1) The administrative UI is no more available from the Security Center server, the administrative UI will be instead served on the Security Center Model server.
  2) The administrative UI can no longer use the same https TLS certificate as the tenant-based UI, you will have to generate a new certificate for the admin UI in the administrative UI settings section.
  3) The license has to be re-imported in the administrative UI

Type	Description
Feature	All sections are now cross tenant.
Feature	Added a new 'ASGARD Query' search bar to most tables to support more complex searches
Feature	Added 'Change History' for assets and findings
Feature	Added charts in overview page for assets/findings per status, assets per day, ...
Feature	Automatically close all findings that are 'Legitimate Anomaly' or 'False Positive'
Feature	Automatically delete and close findings on case deletion or if an asset has been removed from a case
Feature	Light Mode
Feature	Manage frontend TLS certificate and backend TLS certificate separately
Feature	Create users that do not have to change their password
Change	Moved administrative UI from the Security Center server to the Security Center Model server
Change	Removed 'Call for Action' for findings in 'False Positive' or 'Legitimate Anomaly' state

7.2.3 Security Center 1.0.4

Type	Description
Bugfix	Fixed non-working QR code for 2FA in enforced 2FA mode

7.2.4 Security Center 1.0.3

Type	Description
Bugfix	Fixed hard coded limit of max. 40 tenants
Bugfix	Fixed non-working QR code for 2FA

7.2.5 Security Center 1.0.2

Type	Description
Bugfix	Fixed missing scroll bar for tenant selection
Bugfix	Fixed logout
Bugfix	Exclude backup directory from backup

7.2.6 Security Center 1.0.1

Type	Description
Security	OS Security Fix

CHAPTER

EIGHT

INDEX

- genindex

INDEX