
Connectivity Suite Documentation

Maurin Vögeli

Apr 26, 2024

CONTENTS

| | | |
|---|----------|---|
| 1 | Overview | 3 |
|---|----------|---|

Copyright: 2024 © NetModule AG

Modification date: 26.04.2024

Legal: *Legal Aspects*



OVERVIEW

| Installation | Operation | Maintenance |
|-------------------------------|------------------------------------|----------------------------|
| <i>Installation</i> | <i>User Management</i> | <i>Troubleshooting</i> |
| <i>First steps</i> | <i>Device Management</i> | <i>Update & Backup</i> |
| <i>Network architecture</i> | <i>Dashboard</i> | |
| <i>Network Management</i> | <i>Variables & Bulk Editor</i> | |
| <i>Certificate Management</i> | <i>Artifacts</i> | |
| | <i>Jobs</i> | |
| | <i>Remote Access</i> | |
| | <i>Child Device Access</i> | |
| | <i>User Traffic</i> | |

Content

1.1 Introduction

1.1.1 Key Features

Remote access with one click: Access all connected routers and clients of your routers within seconds via the web interface of the Connectivity Suite.

Configure & Control: Remote execute automated and scheduled remote over-the-air updates and configurations.

Communication via REST API: REST API to access functionalities from the Connectivity Suite via your own platform or application.

Scalable network: Adding new assets to your existing network can be done within a few minutes and without network configuration know-how required.

Organize & Control Access: Grouping assets based on a multitenancy capability with hierarchical access control to group your assets according to customers, regions, teams etc.

End-to-end Security: Auto-setup of encrypted VPN infrastructure for an end-to-end encryption to secure your communication and your network without any user intervention required.

Cloud based or On-Premise installation: Installation and operation is possible in a cloud environment but also on-premise on your in-house servers to keep control of your data.

1.1.2 System Architecture

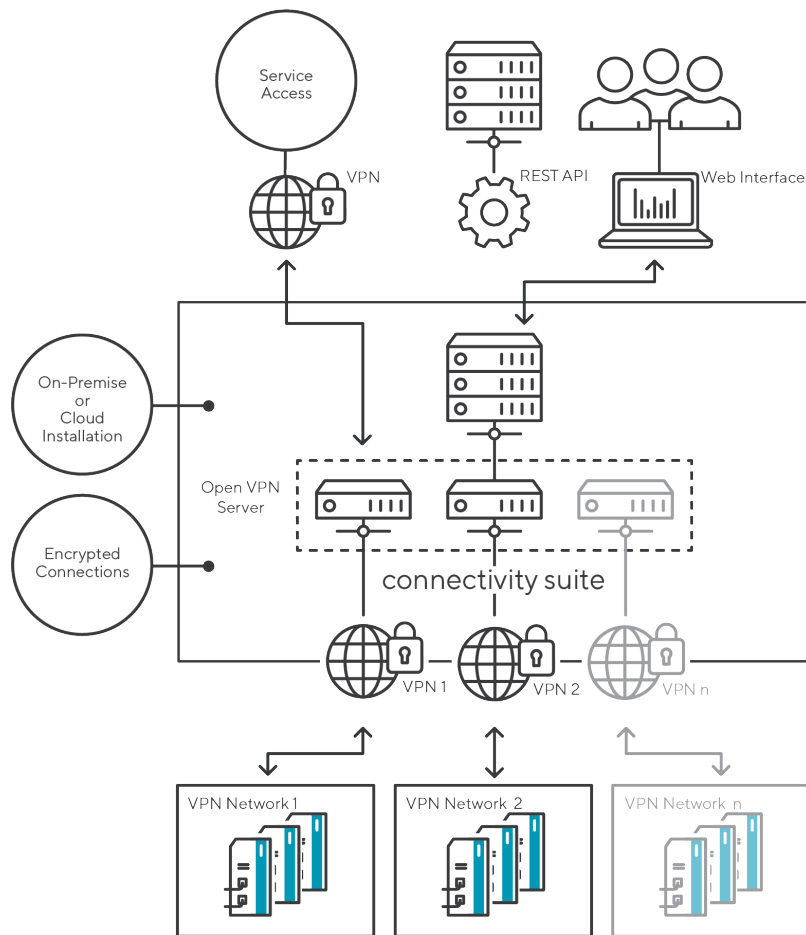


Fig. 1.1: System architecture

The Connectivity Suite is not only a software but also a network infrastructure. This means that when installing the software, you install a network infrastructure that must be integrated into your existing network. When the software is installed, the Connectivity Suite automatically sets up an OpenVPN network. Whenever a Device is connected with the Connectivity Suite this Device will be integrated in the OpenVPN Network of the Connectivity Suite. The [Fig. 1.1](#) shows a simplified representation of the Connectivity Suite infrastructure.

1.1.3 Web interface Connectivity Suite

The web interface of the Connectivity Suite provides the interface to configure and setup the Connectivity Suite incl. the Devices. Find below a description and general overview of the web interface.

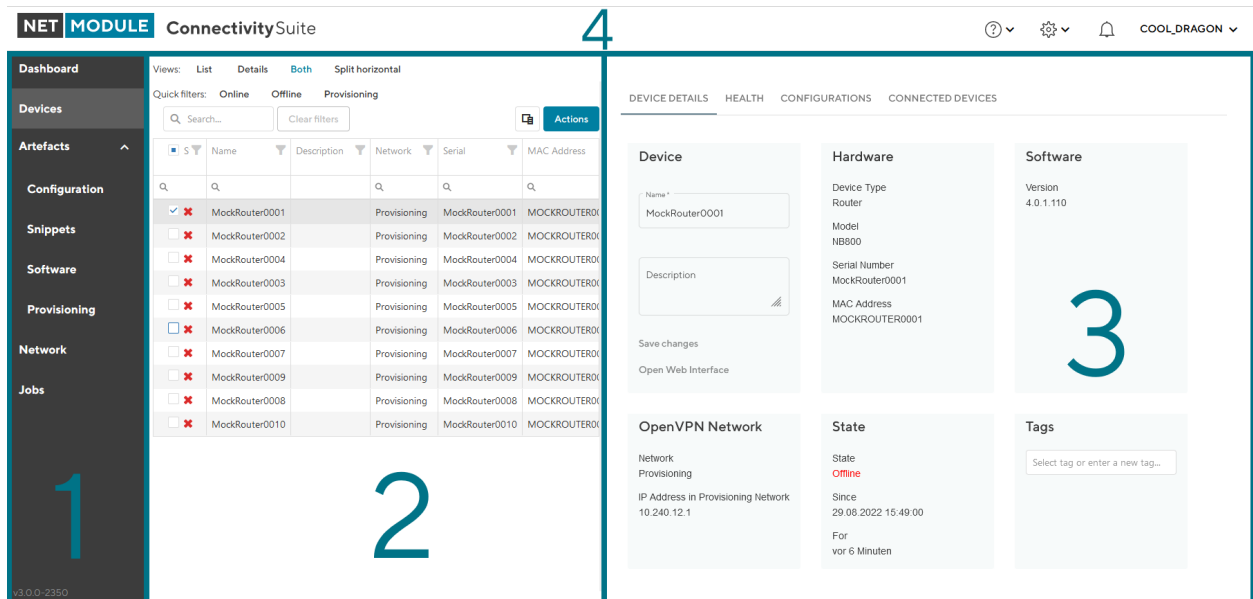


Fig. 1.2: UI overview

| 1 - Main menu | 2 - Main Dialogue | 3 - Detail Dialogue | 4 - Top menu |
|---|--|---|--|
| <p>The main menu gives access to the main features of the CS which are:</p> <ul style="list-style-type: none"> • Dashboard • Devices • Artefacts <ul style="list-style-type: none"> – Configuration – Snippets – Software – Provisioning • Network • Jobs | <p>Shows detailed lists of devices, artefacts, network and jobs, depending on chosen element in the Main menu.</p> | <p>Provides details of the selected element in the Main dialogue.</p> | <p>The top menu gives access to the following features:</p> <ul style="list-style-type: none"> • Help <ul style="list-style-type: none"> – User Manual – NetModule Wiki – NetModule Support – API Documentation – About • Settings <ul style="list-style-type: none"> – Manage Users – Download Logs • Notifications • User <ul style="list-style-type: none"> – Change Password – Log out |

1.2 Installation

Warning: It is assumed that the user who is installing and setting up the Connectivity Suite has read and understood the installation prerequisites (see [Section 1.2.1](#)), otherwise an installation won't be possible.

1.2.1 System requirements

Server Hardware

Server: Physical or virtual server, either hosted by the company or by an IAAS (Infrastructure as a Service) provider

CPU: 2 cores each running at 2.5 GHz

RAM: 16 GB

Disk space: 120 GB

Warning: Insufficient system resources can cause devices to lose connection and Connectivity Suite operation can no longer be guaranteed.

Server Software

Operating system: Ubuntu 20/22, Debian 10/11/12

Docker: Docker (v20+), Docker Compose Plugin (v2+)

- Instructions for Docker
 - **Debian:** <https://docs.docker.com/engine/install/debian/>
 - **Ubuntu:** <https://docs.docker.com/engine/install/ubuntu/>
- Instructions for Docker Compose
 - **Linux:** <https://docs.docker.com/compose/install/linux/>

Warning: Make sure that you are running at least **Docker v20.x.x**.

You can run `docker -v` to get your currently installed version. Example output: `Docker version 20.10.17, build 100c701`

Make sure that you are running at least **Docker Compose v2.x.x**.

You can run `docker compose version` to get your currently installed version. Example output: `Docker Compose version v2.10.2`

Note: NetModule does not provide a full OS installer. The customer must provide it's own, already secured, Ubuntu or Debian server with Docker and the Docker Compose plugin installed. NetModule only installs the containers.

Note: The user has to be added to the docker group. This can be done with `sudo usermod -aG docker $USER` and `sudo su $USER`

1.2.2 Devices Compatible with Connectivity Suite

Router Product Lines

- NetModule NB8xx
- NetModule NG8xx
- NetModule NB1xxx
- NetModule NB2xxx
- NetModule NB3xxx

Compatibility with Connectivity Suite is given with the following Router Models and corresponding Router Software.

- Router models: <https://wiki.netmodule.com/documentation/overview>
- Router Software versions: <https://wiki.netmodule.com/documentation/releases#active-releases>

WiFi Access Points

- NetModule AP3400

Switches

- NetModule ES3300
- Tronteq ROQSTAR 2GE+8FE M12 Managed Gigabit Switch (006-130-117)
- Tronteq ROQSTAR 2GE+8FE M12 Managed Gigabit *PoE* Switch (006-130-118)
- Tronteq ROQSTAR 4GE+12FE M12 Managed Gigabit Switch (006-130-124)
- Tronteq ROQSTAR 4GE+12FE M12 Managed Gigabit *PoE* Switch (006-130-125)

Discontinued Models are not supported by Connectivity Suite. The full list can be found here: <https://www.netmodule.com/en/support/portfolio-changes/>

1.2.3 DNS prerequisites

Domain name / FQDN

- A FQDN is needed which points to the IP address of the server where the Connectivity Suite is installed.
- If you want to use TLS certificates issued by Let's Encrypt, this FQDN must be publicly known and accessible.
- This same FQDN is also used by the routers to connect to the Connectivity Suite as well as for the users to access the Web UI.

Devices CNAMEs (Subdomains)

To be able to access a Device via the web proxy (see [Section 1.11.1](#)) a devices CNAME DNS record is necessary. Example:

| Name | Type | Value |
|--------------------------|-------|------------------|
| devices.cs.mycompany.com | CNAME | cs.mycompany.com |

If you want to use the Proxy Records feature (see [Section 1.11.1](#)) you need to create a CNAME DNS record with a wildcard in the front as well. Example:

| Name | Type | Value |
|----------------------------|-------|------------------|
| *.devices.cs.mycompany.com | CNAME | cs.mycompany.com |

DNS Example (with Proxy Records support)

| Name | Type | Value |
|----------------------------|-------|------------------|
| cs.mycompany.com | A | 10.42.42.42 |
| devices.cs.mycompany.com | CNAME | cs.mycompany.com |
| *.devices.cs.mycompany.com | CNAME | cs.mycompany.com |

1.2.4 Firewall

Incoming Ports

The following ports must be opened for incoming connections to the server:

| Protocol | Port | Description |
|----------|-----------|--|
| TCP | 80 1) | Certbot (for certificate renewal) |
| TCP | 443 2) | Traefik Web Proxy (for accessing the Web UI & API) |
| UDP | 50040 3) | OpenVPN Backend Server |
| UDP | 50041 3) | OpenVPN Provisioning Server |
| UDP | Custom 3) | OpenVPN VPN Servers (one port per VPN Network) |

- 1) Only required if you want to use TLS certificates issued by Let's Encrypt via TLS challenge (default), if you have enabled Proxy Records a DNS challenge is used and the port is not needed.
- 2) If all the users of the Connectivity Suite UI are located inside a company network, port 443 does not need to be opened to the outside world.
- 3) If all the routers managed by the Connectivity Suite are located inside a company network, these UDP ports do not need be opened to the outside world.

Note: The router through which the Connectivity Suites accesses the internet must support the NAT loopback functionality. If this is not the case, operation of the Connectivity Suite will not be possible. A list of routers that fulfil the functionality can be found at the following link: http://opensimulator.org/wiki/NAT_Loopback_Routers

Outgoing Ports

The following ports must be opened for outgoing connections to the internet:

| Protocol | Port | Description |
|----------|------|--|
| TCP | 21 | Used to download the latest version of the cs-cmd |
| TCP | 443 | Used to download the latest version of the docker images and plugins |

1.2.5 Network Address Blocks

The Connectivity Suite requires two Network Address Blocks **that do not overlap with each other or the existing company network address blocks**.

The Network Address Blocks must be specified during the installation of the Connectivity Suite.

- Core Address Block: must be a /20 network (4'096 addresses) used for Connectivity Suite internal services
- Platform Address block: The size can be defined by the user and is used to assign each Device a platform wide unique IP-address
- If there is no need to access the Child Devices, the minimum size of the Platform Address Block corresponds to the number of Parent Devices you want to connect to the Connectivity Suite.
- If you want to access the Child Devices, the minimum size of the Platform Address Block is [Parent Devices] * [Child Devices].
- Because the Platform Address Block will be divided into several VPN Network Address Blocks during the installation process (see [Network architecture](#)), its size cannot be smaller than 4096 addresses (a /20 network).

Fig. 1.3 shows how an infrastructure with two VPN networks and five routers including end devices can look.

Note: The Connectivity Suite supports only IPv4. IPv6 is currently not supported.

1.2.6 Installing the Connectivity Suite

Downloading the cs-cmd

1. Log into your server where the Connectivity Suite will be installed
2. Make sure that the latest docker version is installed
3. Make sure that the latest docker compose plugin is installed
4. We recommend to install the Connectivity Suite into ~/cs


```
mkdir cs
```
5. Change to the cs directory


```
cd cs
```
6. Download the *cs-cmd* console application from the NetModule repository by calling


```
curl -u cs-install ftp://ftp.netmodule.com/latest/cs-cmd -o cs-cmd --ssl-reqd
```

 The credentials for repository are provided by NetModule.
7. Add execution rights to the *cs-cmd* by calling `chmod +x ./cs-cmd`

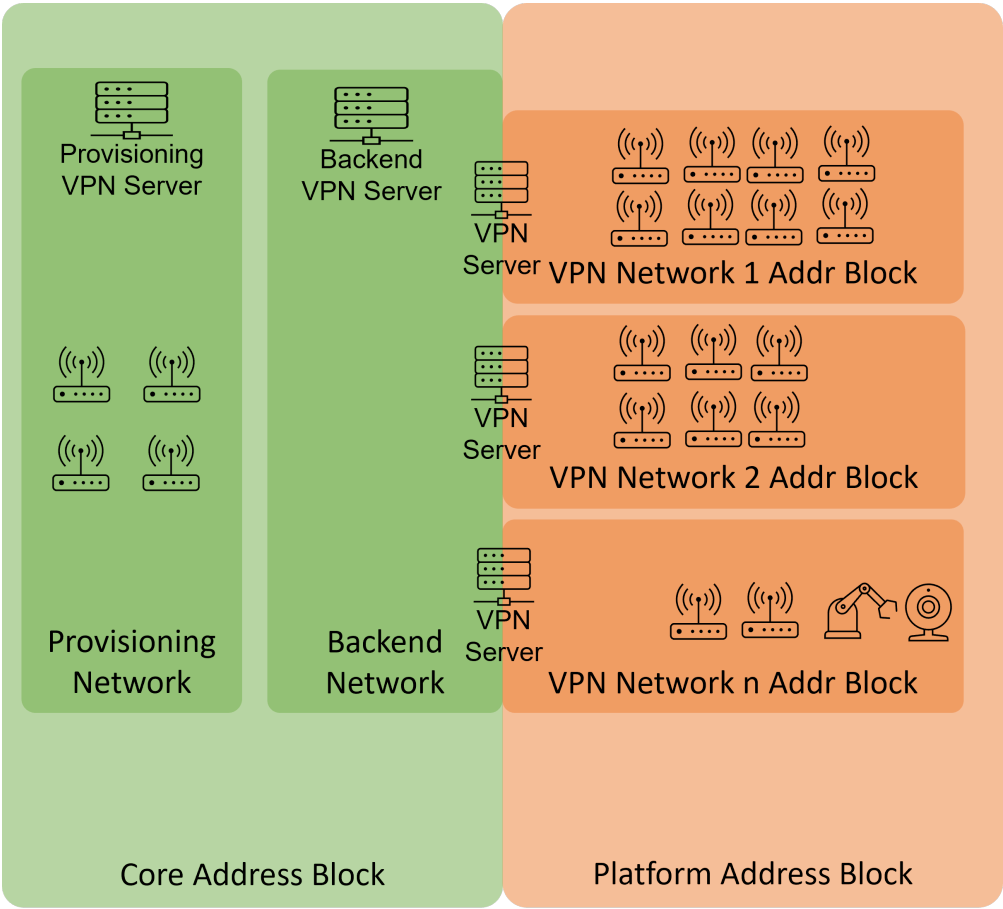


Fig. 1.3: Example system architecture

Running the cs-cmd Installation Assistant

1. Run the *cs-cmd* by calling `./cs-cmd`
2. Choose **Installation Assistant** and press [Enter]
3. Follow the instructions of the Installation Assistant

Warning: Attention! The following steps can only be configured during the installation and are only reversible by doing a re-installation (which means you will lose all the stored data).

4. Configure the Core Address Block in the format `xxx.xxx.xxx.xxx/20`. It is mandatory to use an address block mask of 20 (see [Section 1.12](#) for more detailed description).
5. Configure the Platform Address Block in the format `xxx.xxx.xxx.xxx/xx` and make sure the address block is greater than 20. Also be aware that as example a address block of 20 does not mean that you will be able to connect 4096 devices there is a big reduction based on the Network Architecture. (see [Section 1.12](#) for more detailed description).

Warning: Attention! The Platform Address Block restricts the amount of Devices which can be connected to the Connectivity Suite. Be aware that if the number set during this step is too small this cannot be changed afterwards.

6. When prompted choose between default settings for your Platform Address Block layout or create a layout by yourself. If you choose the default settings step 7-12 can be skipped. Be aware, that only experienced users should do the settings in step 7-12.
7. Choose your preferred Platform Address Block layout (you have the option of three given layouts).
8. Enter a name for the VPN subnet Pool type.
9. Enter the number of max. required VPN networks. Be aware that if the number set during this step is too small this cannot be changed afterwards.
10. Configure the size of the VPN Network Address Block in the format `xxx.xxx.xxx.xx/xx`.
11. Enter the number of max. required End Devices. Be aware that if the number set during this step is too small this cannot be changed afterwards.
12. Enter the number of concurrent Service Access sessions. Be aware that if the number set during this step is too small this cannot be changed afterwards.

Note: Step 8-12 may need to be repeated, depending on the chosen Platform Address Block layout in step 7.

13. Choose if you want Let's Encrypt or the Connectivity Suite certification authority to be used to issue the SSL certificate to access the UI. If you already have your own certificate infrastructure you can choose to use your own certificates for TLS.

Note: If you choose the Connectivity Suite certification authority to issue the SSL certificate, it is not required for port 80 to be open for incoming connections in your firewall! However, your browser is going to display a warning the first time you open the Connectivity Suite UI. This is normal behaviour. In order to make this warning disappear, your browser needs to trust the Connectivity Suite Root Certification Authority. The procedure varies for different browsers (see [Section 1.17.3](#)).

14. Advanced options: If you want to adjust the OpenVPN Default Ports or have some custom MTU sizes (OpenVPN fragment / MssFix)
15. Once the installation has finished, you can log into your newly installed Connectivtiy Suite instance with the *url*, *username* and *password* provided in the console output.
16. You will be asked to change the password. **Make sure to store the username and password in a save place**

Note: For details regarding the network configuration and layout see [Network architecture](#).

Note: The username is randomly generated. It is thought as the *main admin account*, used only to create personal users for each platform admin

1.3 First steps

1.3.1 License

- Starting from software version v3.5 and newer, a valid License Key is required for every Connectivity Suite instance to operate.
- License Keys are to be obtained through sales@netmodule.com

License Management

Click on the “+” button, select a previously received license key file (.lic) and hit import.

The status page (see [Fig. 1.4](#)) provides a comprehensive overview of the current licensing status.

Settings

| FEATURES DEVICE FILTER CERTIFICATES VARIABLES <u>LICENSES</u> | | | | |
|---|------------|------------|----------------------------|------------------------------------|
| Licenses | | | | |
| <div><div></div><p>This product requires an active subscription license for operation. Multiple licenses may be added in order to guarantee a seamless operation when transitioning to a new subscription. New licenses may be ordered through authorized channels or directly at sales@netmodule.com.</p></div> | | | | |
| <div><div></div><div><div>1</div><div>+</div></div></div> | | | | |
| License status | Not before | Not after | Devices (available used) | Fully qualified domain name (FQDN) |
| - License OK | 01.12.2023 | 30.11.2024 | 50 4 | myCSdomain.com |

Max. Devices

Registered Devices

Fig. 1.4: License Overview Table

| License Status | Explanation | Action |
|----------------|--|--|
| OK | License is valid and covers number of registered devices | Nothing required |
| Exceeded | Too many devices registered | Order new license for more devices |
| Expired | License has expired and is no longer valid. Not after date is in the past. | Renew license |
| Missing | No license found | Import license, by clicking “+” button |

A notification email will be sent ahead of time for licenses that are about to expire, allowing sufficient time for renewal.

1.3.2 First Login

After login users will be directed to the dashboard. This one will initially look pretty empty but start to fill up as soon as networks are created and devices are added to the platform.

The Provisioning Network and the Backend Network are already deployed during the installation. Therefore, the two networks must already be displayed in the dashboard at the beginning.

As a next step it is necessary to set up a VPN Network to which a Device can be assigned, as only devices in a VPN Network can be managed via the Connectivity Suite. The procedure how to add VPN Networks is described in [Add a Network](#).

1.3.3 Adding a Network

See [Section 1.4.1](#) on how to add a new Network

1.3.4 Adding a Provisioning Configuration

See [Section 1.9.6](#) on how to add a new Provisioning Device Configuration

1.3.5 Installing a Provisioning Configuration

See [Section 1.6.2](#) on how to add install a Provisioning Device Configuration on a Device

1.3.6 Move Device from Provisioning to Network

See [Section 1.6.3](#) on how to move a Device from the Provisioning to the newly created Network

1.4 Network Management

1.4.1 Add a Network

Note: For the following steps an account with **Platform Administrator** right is required.

When adding a new VPN Network between three VPN Network types can be chosen (see [Section 1.12](#) for more detailed explanation of the Network Architecture).

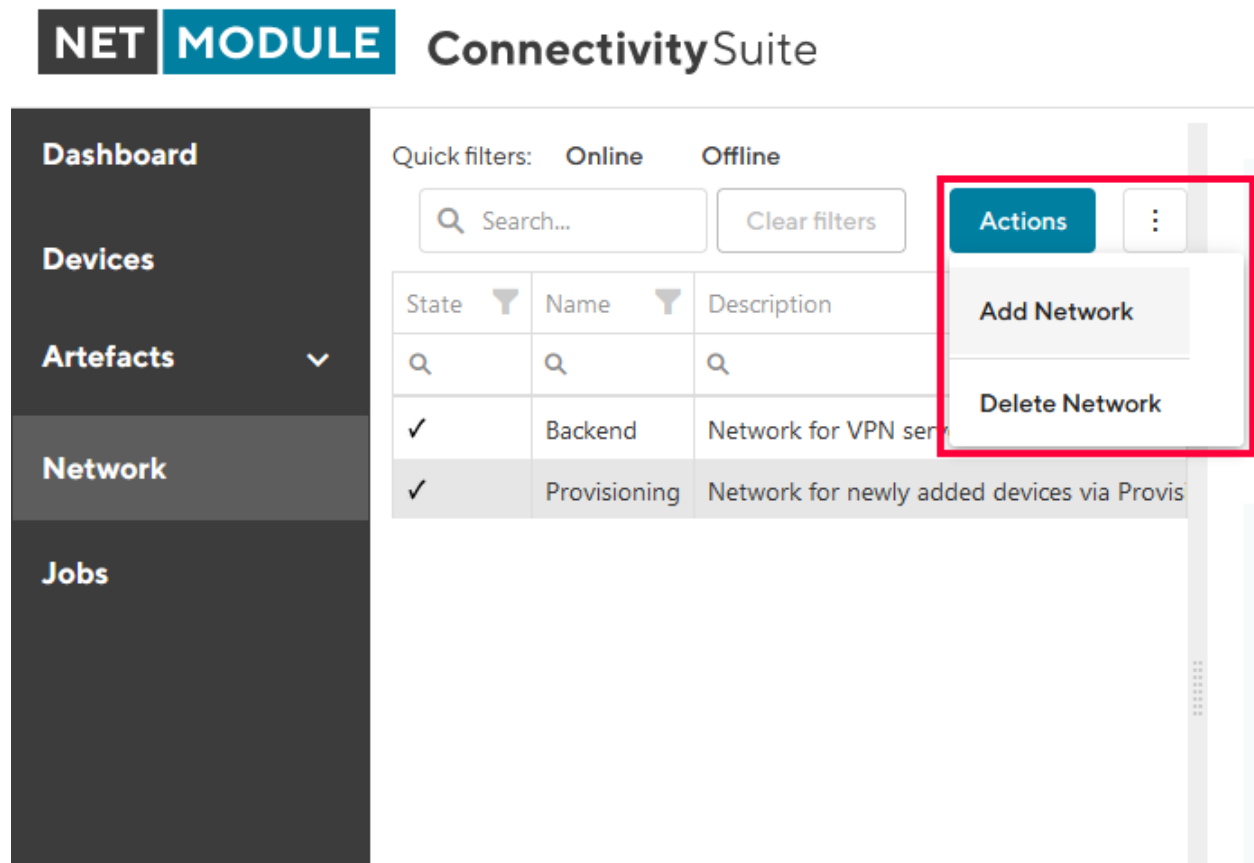


Fig. 1.5: Add Network

1. To add a VPN Network, navigate to the “Network” page of the Connectivity Suite UI. Click on “Actions” at the upper right corner of the Main dialogue and Click “Add Network”.
2. Fill out the required fields and click “Add Network” to start the assignment of a VPN Network. A confirmation message must pop up which confirms the assignment of the VPN Network.
3. The VPN Network will now be listed in the table in the Main dialogue. When the status shows a green tick, the VPN Network is ready for use. It can take up to two minutes until the VPN Network shows up in the table (see [Fig. 1.6](#)).

Network Details OpenVPN Network

NET MODULE Connectivity Suite

Quick filters: **Online** **Offline**

Search... Clear filters

Actions

| State | Name | Description | Port | Tags |
|-------|--------------|--|------|----------------|
| ✓ | Backend | Network for VPN servers to communicate with the Backend VPN Server | 1194 | |
| ✓ | Provisioning | Network for newly added devices via Provisioning | 1195 | |
| ✓ | EMEA | Europe, Middle East & Africa | 1201 | EMEA Frankfurt |
| ✓ | APAC | Asia & Pacific | 1202 | APAC Tokyo |
| ✓ | NA | North America | 1203 | NA NewYork |

v3.0.0-2325

Fig. 1.6: Network added

| | |
|--|---|
| Alias | Name of the OpenVPN Server |
| Platform Address | IP address which is assigned to the network by the home server. |
| VPN Network Address Block in Platform Network | The address block of a specific VPN network inside the Platform Address Block |
| VPN Network Address Block | The address block of a specific VPN network |
| Port | The UDP port number of the server where the Connectivity Suite is running (needs to be open in the firewall to connect Devices to the Network). |

Network Details Devices

| | |
|---------------------------------|---|
| VPN Network Type | Defines the number of possible VPN Networks which can be added and number of Devices which can be connected to the VPN Network. |
| Max number of routers | The maximum numbers of routers which can be connected to the VPN Network. |
| Number of routers left | The number of routers that can be added to the VPN Network. |
| Child Devices per router | The number of End Devices that can be connected to the VPN Network. |

1.4.2 Add a Remote VPN Network

Note: A Remote VPN Network is an Open VPN Server which is not running on the Connectivity Suite server, but on a separate server.

1. To add a Remote VPN Network, navigate to the “Network” page of the Connectivity Suite UI. Click on “Actions” at the upper right corner of the Main dialogue box and Click “Add Network”.

2. Fill out the required fields including the field “Remote VPN Network” and add the domain name or IP address of the remote server, then click “Add Network” to start the assignment of a VPN Network.

The screenshot shows the 'Add Network' dialog box in the Connectivity Suite interface. The background shows a table with columns for State, Name, and Description. The dialog box has the following fields and values:

- Name: SA
- Description: South America
- Network Type: Medium
- VPN Network Address: 10.0.0.0
- Netmask: 19
- End Devices per Router: 16
- Maximum number of routers on this network: 512
- ☒ Remote Network (use only if you want to run this network on another server)
- Domain Name or IP address of remote network server: my-other-server
- Network Port: 1201

An 'Add Network' button is located at the bottom of the dialog.

Fig. 1.7: Add Remote VPN Network

3. Download the Remote Open VPN installer package (this can either be done directly from the pop-up displayed right after the VPN Network creation or later via the Network page by clicking on the download symbol under Remote VPN Network Installer next to the respective VPN Network (see Fig. 1.8).
4. After downloading the installer package, follow the instructions given in the README.txt which is included in the package.

NET

MODULE

ConnectivitySuite

?

CLEVER_CRAB

Dashboard

Devices

Artefacts

Network

Jobs

Quick filters: Online Offline

Actions

| State | Name | Description |
|-------|--------------|--|
| ✓ | Backend | Network for VPN servers to communicate with the Backend VPN Server |
| ✓ | Provisioning | Network for newly added devices via Provisioning |
| ✓ | EMEA | Europe, Middle East & Africa |
| ✓ | APAC | Asia & Pacific |
| ✓ | NA | North America |
| 🔄 | SA | South America |

Network Server

Name

SA

Description

South America

OpenVPN Network

Shortname

sa

VPN Network

10.0.0.0/19

VPN Network in Platform Network

10.232.0.0/19

Port

1201

Routers and End Devices

Network Type

Medium

Max number of routers

8192

Number of routers left

8192

End devices per router

16

Service Access

Download OpenVPN client configuration

Tags

State

State

Unknown

Since

For

Remote Network

Remote Network Address

my-other-server.local

Download Remote Network Installer

Fig. 1.8: Download Remote Network

1.5 Certificate Management

The built in Certificate Authority handles the Lifetime by issuing new Certificates as well as deploying them by replacing the old ones. This includes certificates of VPN Networks, Service Access, Devices and HTTPs for WEB access. This happens automatically in the background with no interaction needed.

1.5.1 Certificate Lifetimes

By default, when Connectivity Suite was installed with version 3.3.x or newer, the following certificate Lifetimes are in use:

| Certificate | Lifetime | Renewal before expiry |
|--------------|----------|-----------------------|
| Root | 1095d | 365d |
| HTTPS | 90d | 30d |
| Network | 730d | 243d |
| Device | 90d | 30d |
| Service Acc. | 90d | N/A |

Updating or migrating Connectivity Suite from a previous release, Certificate Lifetimes are carried over as follows.

| From | To | Lifetime |
|------|------|----------|
| v2.6 | v3.3 | 30 years |
| v3.x | v3.3 | 10 years |

1.5.2 Certificate Renewal

Using the standard settings for Certificate Management (Custom Certificate Settings switched off), Certificates are automatically renewed and deployed before they expire. The renewal process may happen at any time, with the condition that there is an active connection to the corresponding device / network, etc.

Note: Replacing the certificate, may cause a short connection interrupt.

1.5.3 Individual Settings

If desired, both the Certificate Lifetime as well as the period for renewal may be configured using individual values. The deployment window of the newly issued Certificates can also be specified if needed.

Warning: Modifying Certificate Lifetime values can cause disconnects and potential lockouts of devices no longer being able to re-connect to Connectivity Suite.

Before individual settings may be used, the auto function needs to be switched off. This is done, under Global Settings.

1. Enable Custom Settings for Certificate Management
2. Save before proceeding to the Certificates Tab

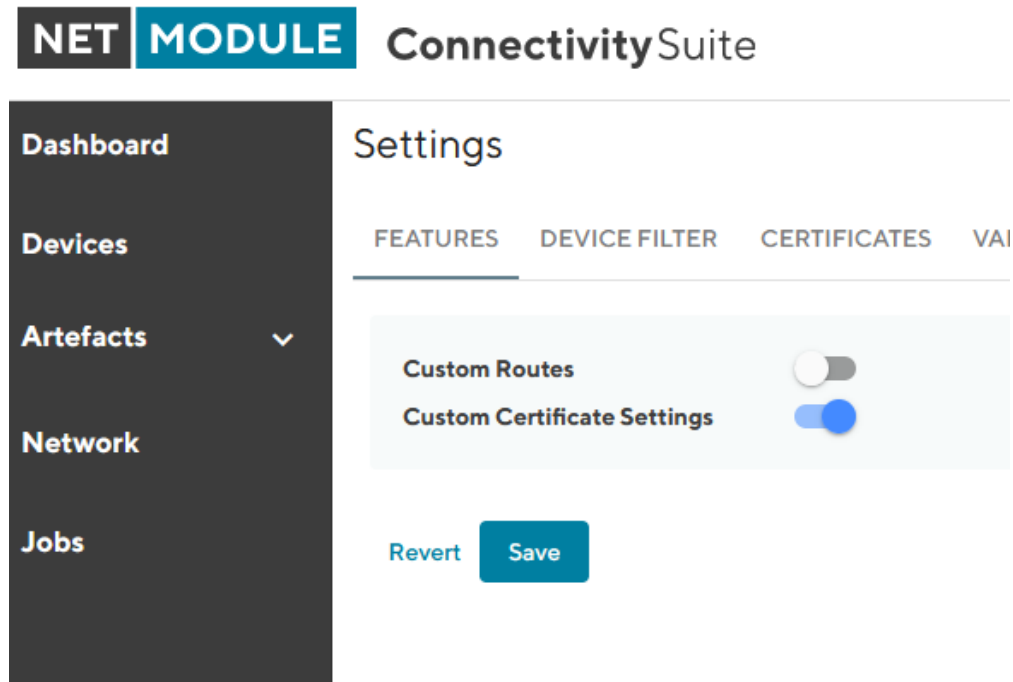


Fig. 1.9: Certificate Custom Settings

Custom Lifetime & Renewal Settings

With exception to the Root Certificate, which is on global level, there are two options to which level the settings apply to.

- Platform wide: Lifetime and renewal applies system wide
- Individual per Network: Settings can be modified on each Network individually

When changing the lifetimes, it is required that certificates on lower levels have a shorter lifetime than their parent certificates. The renewal period is derived by 1/3 of the certificate Lifetime but may be adjusted if desired.

On network level, the same Lifetime and renewal parameters can be found and adjusted, if “Individual per network” is set. For that, see the Certificate Settings Tab on each Network detail page.

Note: Depending on the changes to the Certificate Lifetime being made, there can be consequences, which need to be addressed beforehand, in order to not lose the connection to devices. Especially for pre-provisioned devices that have not yet established an active connection to Connectivity Suite may require a new Provisioning Configuration which is to be manually uploaded.

The following examples show the general behavior when changing the Certificate Lifetimes.

Impact When Shortening Lifetime

Changing the Certificate lifetime to be shorter than the current lifetime: As soon as the new Certificates have been deployed, the pre-existing ones will be revoked.

Warning: Provisioning and Service Access Certificates are revoked immediately, when a new lifetime is set, which is shorter than the existing one. Therefore, new provisioning-configs need to be issued and loaded into

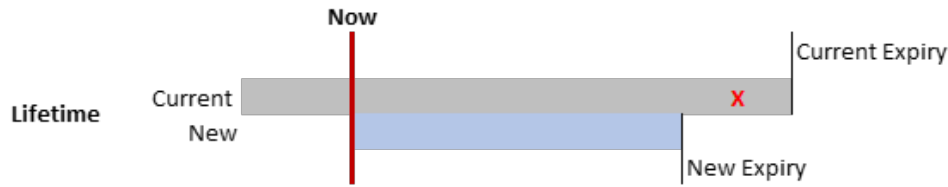


Fig. 1.10: Certificate Lifetime Shorter than Current

devices manually. The same for service access, for which the new Certificate needs to be distributed.

Impact When Increasing Lifetime



Fig. 1.11: Certificate Lifetime Longer than Current

When the Lifetime is increased, the current certificates remain unchanged active and valid as per their settings.

Custom Certificate Deployment Schedule

Newly generated Certificates need to be deployed before the current one expires. The renewal process may happen at any time when the certain entity (network, devices, etc.) is online. This behavior can be modified, and a specific schedule configured by when the deployment of newly issued certificates should be deployed. Given the target entity has an active connection to the system. When the effective deployment of these certificates should happen may be specified in the same manner as for config deployments see [Section 1.6.3](#)

1.6 Device Management

The Connectivity Suite can manage and administer different types of devices. Successfully onboarded devices are listed in the Device Inventory

1.6.1 Device Inventory & Status

A customizable table view provides an overview of all devices. The columns in the table can be configured using the column chooser. (see [Fig. 1.12](#))

Connection Status

The following codes indicating the connection states:

State Green: Connection is up and device can be accessed by Connectivity Suite.

State Red: Indicates that the device is not pingable from Connectivity Suite.

State Unknown: Devices that have been migrated from an older CS software version get “unknown” connection state. Once these devices have successfully established a connection, they become green and red respectively. Devices after a migration, that never establish a connection remain in “unknown” state.

The screenshot shows the Connectivity Suite interface. On the left is a sidebar with navigation links: Dashboard, Devices, Artefacts, Network, and Jobs. The main area displays a table of devices. At the top, there are tabs for Views (List, Details, Both) and Split vertical. Below the tabs are quick filters for Online, Offline, Unknown, and Provisioning. A search bar and a 'Clear filters' button are also present. A 'Column Chooser' icon is highlighted with a red box. The table has columns for State, Name, Network, Type, Model, and Software. The 'State' column is highlighted with a red box, and a callout points to it with the text 'Connection Status'. The table lists three devices: NB1600 (red dot), NB800-332 (green dot), and NB1800-5G (green dot).

| State | Name | Network | Type | Model | Software |
|-------|-----------|--------------|--------|------------|-----------|
| ● | NB1600 | Network1 | Router | NB1600 EOL | 4.6.0.105 |
| ● | NB800-332 | Network1 | Router | NB800 | 4.6.0.105 |
| ● | NB1800-5G | Provisioning | Router | NB1800 | 4.7.0.103 |

Fig. 1.12: Device List

Device Details Page

The device details page has multiple tabs with information about the device’s status and parameters.

Device Details Tab

The “Device Details” tab provides status information, hardware and software details, network information, tags, custom routes, storage information, mobile network module details, WLAN details, WAN & LAN interface details, VPN connections, GNSS module information, and enabled/disabled software features.

Device

Name
Tram_14

Description
ES3300

Save changes

Open Web Interface

Hardware

Device Type
SWITCH

Model
ES3300

Serial Number
4E4D520405020009

MAC Address
00112B02C3DD

Software

Version
2.2.0

OpenVPN Network

Tenant
test4

IP Address in Tenant Network
10.0.0.153

IP Address in Home Network
10.224.0.153

State

State
online

Since
11.05.2022 09:41:44

For
6 hours

Tags

Add tag...

Relations

Parent Device
00112B02558B

Fig. 1.13: Device Details overview

| | |
|----------------------|---|
| Device | Device name and description, which can be edited Direct Web UI access of device Refresh Device Data (Update Device Info) |
| Hardware | Device-specific information is displayed here which cannot be changed. |
| Software | Shows the firmware version which is running on the Device |
| Firmware | Firmware version |
| Network | Shows the assigned IP addresses of the Devices |
| State | Shows the status of the device connection with the Connectivity Suite |
| Tags | User-specific tags for further designations of Devices |
| Custom Routes | If enabled under global settings, custom routes may be set here. |
| Storage | If present, storage info to total size, used & available memory |
| Mobile | Indicates number of Mobile Network Modules, as well as corresponding statusinfo: - Modem operational Status - SIM card - IMEI, IMSI |
| WLAN | If present, it provides an overview on: - Module Type - Operation modes (WiFi Standards) |
| WAN & LAN | Interface details, with port count and relative status with IP Address info. |
| VPN | VPN connections, with type info, relative status, assigned IP Addresses |
| GNSS | If present, module information is listed here |
| Features | Overview of software features that are enabled or disabled |

Health

In the tab “Health” the connection status of the Device is displayed. The Connectivity Suite periodically pings whether the device is connected or not. If the connection is interrupted, the status switches from online to offline. The meaning of the colored status is as follows: Green = Connected / Online Yellow = Intermittent connection Red = Disconnected

The yellow state indicates intermittent reconnections within a given timeframe. Depending on the use-case, this may be a normal behavior (device is moving, e.g. installed on a train), in which no action is required.

Configurations

In the tab, the history of all configuration versions that the switch has applied is displayed. It is also possible to upload, download or retrieve the Configuration from the switch via this tab.

Connected Devices

Devices connected to the LAN, may be discovered using the scan function.

Certificate

In addition to the certificates validity being displayed on that tab, certificates can be either revoked or renewed. Revoking a certificate causes the device connection to be disconnected. This action might be useful when due to whatever reason the device has been compromised.

Logs

Device Logs viewer and export function.

1.6.2 Device Configuration Handling

Several actions related to the configuration of devices are available and described thereafter.

Variables

[Section 1.8.1](#)

Copy Device configurations

Using the Connectivity Suite, configurations can be copied from one Device to another Device of the same Model. To copy configurations across devices, follow the instructions below:

1. Navigate to the page “Devices” of the Connectivity Suite and select the Device in the table of the Main dialogue box from which the configuration is to be copied.
2. Click on “Actions” at the upper right corner of the Main dialogue box and click “Download this configuration” (configuration can be uploaded via the web manager) or “Download this Configuration as USB version” Configuration can be uploaded via an usb stick).
3. Select the Device in the table of the Main dialogue box to which the downloaded configuration is to be copied.
4. Click on “Actions” at the upper right corner of the Main dialogue box and click “Upload configuration”.
5. Select the downloaded configuration from step 2 and click “Upload Device Configuration”
6. Click on “Actions” at the upper right corner of the Main dialogue box and click “Deploy Configuration”.
7. Select the configuration version to be deployed from step 5.
8. Select whether you want to start the configuration immediately or whether it should be scheduled.
9. Confirm the deployment by click “Start deployment”. The job can be started (b) immediately or (a) scheduled.

Restore configuration

Each time a standard configuration is changed, a new configuration version is created rather than overwriting the current configuration. The different configuration versions can be seen on the page “Devices” in the Detail dialogue box in the tab “Configurations”.

DEVICE DETAILS

HEALTH

CONFIGURATIONS

CONNECTED DEVICES

CERTIFICATE

Configuration History

| Name | Created at |
|-------------------------------|------------|
| Added to provisioning network | 29.08.2022 |
| Added to provisioning network | 29.08.2022 |
| Before network move | 29.08.2022 |

Actions

Added to provisioning network

Description

This configuration was downloaded from the device once it was registre

Created at

29.08.2022 16:03:19

Content

```
config.version=1.16
config.product=3800
network.hostname=NB3800
wwan.0.status=1
wwan.0.card=0
wwan.0.sim=0
wwan.0.number=*99***1#
wwan.0.apn=netmodule.m2m.ch
wwan.0.auth=0
wwan.1.status=1
wwan.1.card=1
wwan.1.sim=1
wwan.1.number=*99***1#
wwan.1.apn=netmodule.m2m.ch
wwan.1.auth=0
usb.status=0
usb.0.enabled=0
usb.1.enabled=0
autorun.status=0
switch.port.1.status=0
switch.port.1.interface=1
switch.port.2.interface=1
switch.port.3.interface=1
switch.port.4.interface=1
wlan.0.regdom=EU
wlan.0.settings.channel=1
cliphp.status=0
network.lan.0.mode=wan
network.wan.0.interface=lan0
```

Fig. 1.14: Configuration versioning

The Connectivity Suite creates a configuration version when following happens:

- If a Device connects for the first time with the Connectivity suite
- If the Connectivity Suite has executed a configuration update
- When a Device is moved to a network
- Before the Connectivity Suite performs a configuration update (backup copy)

If you want to restore an old configuration follow the following steps:

1. Navigate to the page “Devices” of the Connectivity Suite and Select the Device on which an old configuration is to be restored.
2. Click on “Actions” at the upper right corner of the Main dialogue box and click “Deploy Configuration”.
3. A list of all configuration versions of the Device is displayed. Select the configuration version to be restored.
4. Select whether you want to start the configuration immediately or whether it should be scheduled.
5. Confirm the deployment by click “Start deployment”.

Manual configuration updates

There are a few cases where the Connectivity Suite does not capture a Device configuration change, with the current Configuration stored in the Connectivity Suite does not correspond to the one running on the Device and must be manually updated:

- If the change was made outside of the Connectivity Suite (e.g. via the web interface of a NM router or the router CLI)
- If an older configuration version has been deployed

In those cases, the user must manually trigger the import of the updated configuration to the Connectivity Suite.

1. Navigate to the page “Devices” and select in the Main dialogue the Device for which the configuration has changed
2. Open the tab “Configurations”, click on “Actions” at the upper right corner of the Detail dialogue box and click “Retrieve current configuraton from device”.

The screenshot shows the Connectivity Suite interface. On the left is a sidebar with navigation links: Dashboard, Devices, Artefacts, Configuration, Snippets, Software, Provisioning, Network, and Jobs. The main area displays a table of configurations. The 'Configuration History' table has columns for Name, Created at, and Actions. The 'Actions' menu is open, showing options like 'Download as file configuration', 'Download as USB configuration', 'Edit this configuration', 'Upload new configuration', and 'Retrieve current configuration from device' (highlighted with a red box). Below the menu, a snippet of configuration data is visible.

| Name | Created at | Actions |
|-------------------------------|------------|--|
| Added to provisioning network | 29.08.2022 | Download as file configuration Download as USB configuration Edit this configuration Upload new configuration Retrieve current configuration from device |
| Added to provisioning network | 29.08.2022 | |
| Before network move | 29.08.2022 | |

```

config.version=1.16
config.product=3800
network.hostname=NB3800
wwan.0.status=1
wwan.0.card=0
wwan.0.sim=0
wwan.0.number=*99**1#
wwan.0.apn=netmodule.m2m.c
h
wwan.0.auth=0
wwan.1.status=1
wwan.1.card=1
wwan.1.sim=1
  
```

Fig. 1.15: Retrieve user configuration

3. Choose “Import current device configuration into Connectivity Suite” in the pop-up window. The configuration is now listed in the configuration history table.

Install provisioning configuration on a device

1. Select the required configuration in the Main dialogue box.
2. Click on “Download this configuration as USB version” to download the provisioning configuration.

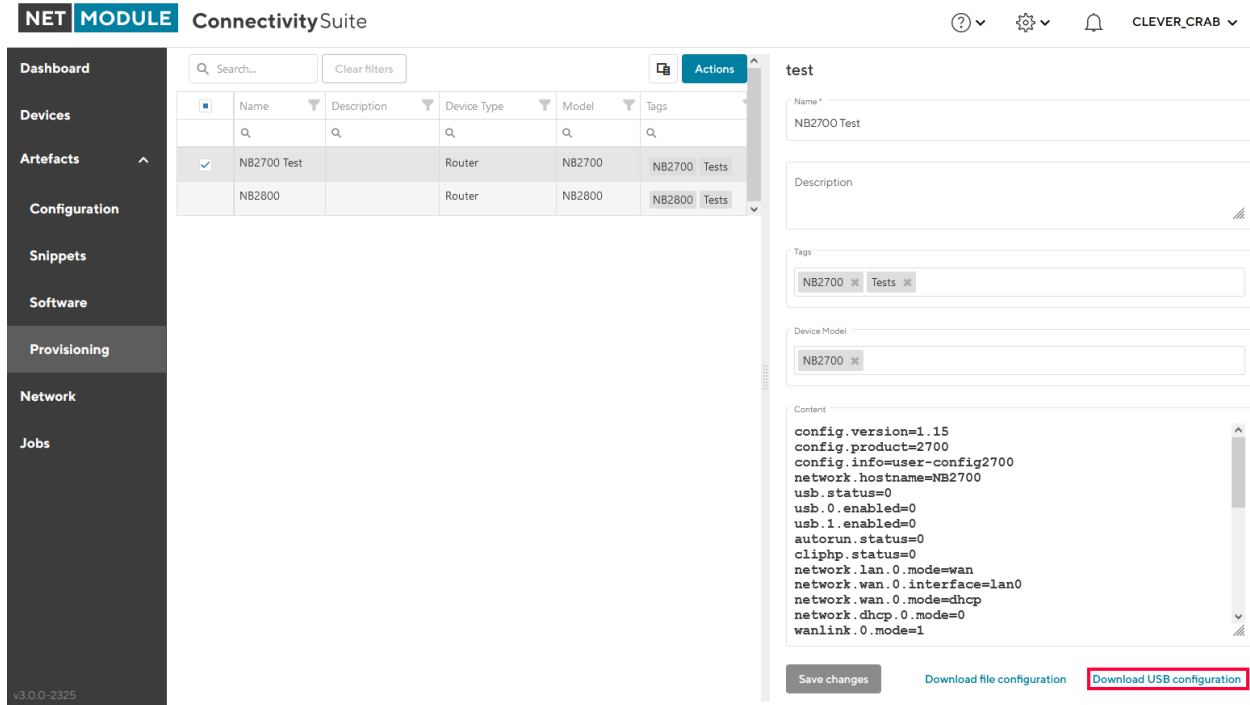


Fig. 1.16: Manual USB update

3. Unzip downloaded zip-file.
4. Copy the content of the extracted zip-file to an empty USB stick.

Warning: Make sure the USB port is activated. After your first login the USB port will be disabled per default.

5. Plug the USB stick into your router to start the configuration update.
6. The router will now automatically apply the provisioning configuration. As soon as all LEDs are blinking after connecting the USB stick, the USB stick can be removed.
7. The router connects now automatically to the Connectivity Suite.

Warning: The USB stick which is used to configure the NM router must be a FAT16/32 formatted USB stick.

Provisioning via the Web Manager

The screenshot shows the Connectivity Suite web interface. On the left is a sidebar with navigation links: Dashboard, Devices, Artefacts, Configuration, Snippets, Software, Provisioning (highlighted), Network, and Jobs. The main area displays a table of devices with columns for Name, Description, Device Type, Model, and Tags. Two devices are listed: 'NB2700 Test' and 'NB2800'. The 'NB2700 Test' device is selected, and its details are shown on the right. The details include fields for Name, Description, Tags, and Device Model. Below these fields is a 'Content' section containing a configuration file snippet. At the bottom of the details panel, there are three buttons: 'Save changes', 'Download file configuration' (highlighted with a red box), and 'Download USB configuration'.

| Name | Description | Device Type | Model | Tags |
|-------------|-------------|-------------|--------|--------------|
| NB2700 Test | | Router | NB2700 | NB2700 Tests |
| NB2800 | | Router | NB2800 | NB2800 Tests |

```

config.version=1.15
config.product=2700
config.info=user-config2700
network.hostname=Nb2700
usb.status=0
usb.0.enabled=0
usb.1.enabled=0
autorun.status=0
cliphp.status=0
network.lan.0.mode=wan
network.wan.0.interface=lan0
network.wan.0.mode=dhcp
network.dhcp.0.mode=0
wanlink.0.mode=1
  
```

Fig. 1.17: Manual file update

1. Click on “Download this Configuration” at the bottom of the Detail dialogue box to download the provisioning configuration.
2. Upload the file config.zip onto your NM router to start the configuration update. The configuration process starts.
3. The Device will now automatically connect to the Connectivity Suite.

1.6.3 Generic Device actions

Deploy a Configuration

1. Navigate to the page “Devices” of the Connectivity Suite and select the Devices which should received a new Device Configuration.
2. Click on “Actions” at the upper right corner of the Main dialogue box and click “Deploy Configuration”.
3. Chose a configuration you want to deploy. If you have selected a single device, you can choose between previous configuration versions or Template Configurations. If you have chosen multiple devices, only Template Configurations are available for deployment.
4. Select the Configuration you want to deploy and click “Next”.
5. Chose if you want to start the deployment immediately or if you want to schedule it for later execution and click “Next”.

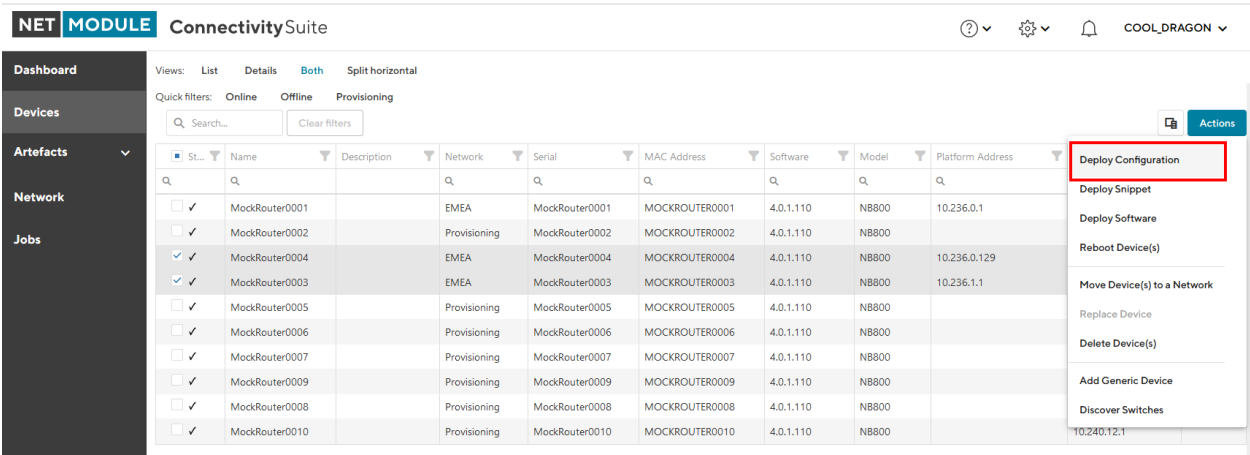


Fig. 1.18: Deploy Configuration Action

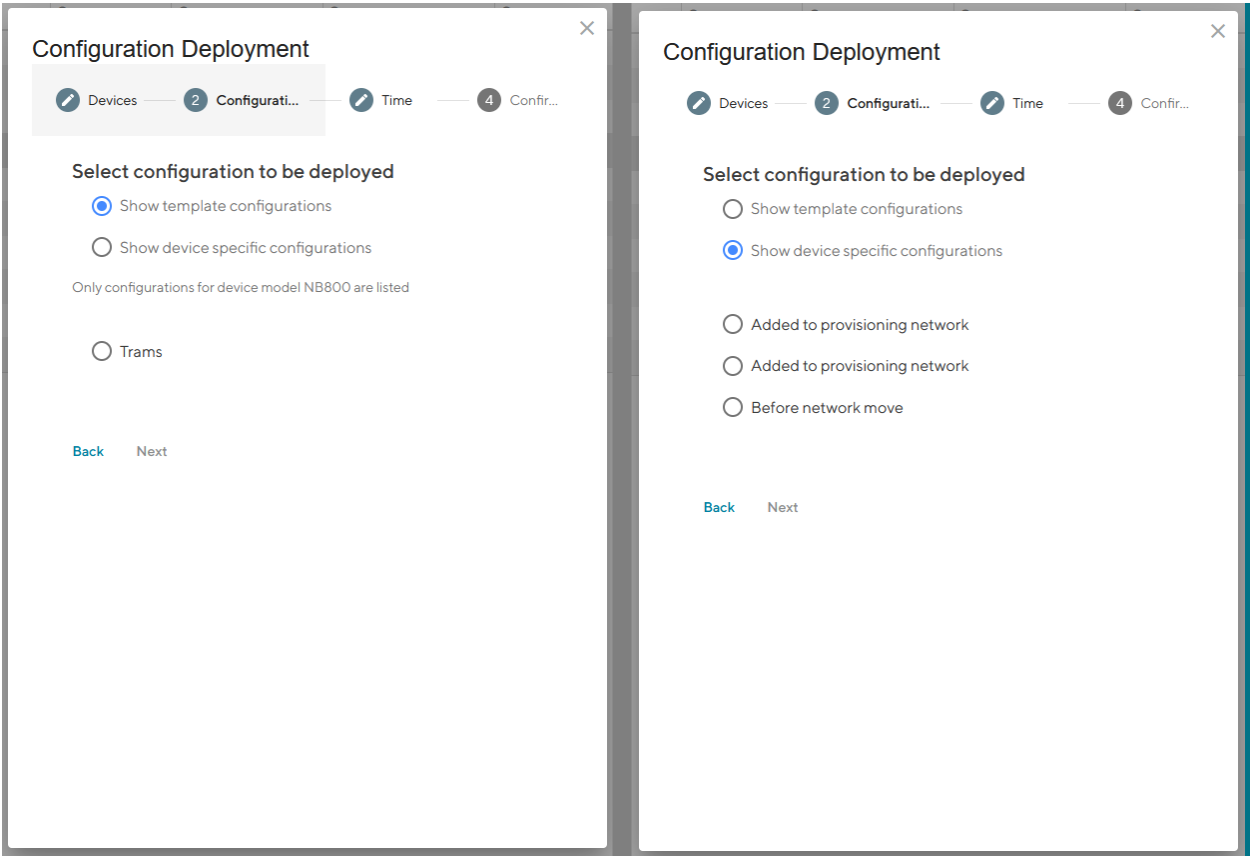


Fig. 1.19: Deploy Configuration Type Selection

Configuration Deployment

Devices

Configurati...

3 Time

4 Confir...

Select execution time

☐ Start deployment now

☒ Schedule deployment for later execution

Enter a date range

Weekdays this job is allowed to run

M

T

W

T

F

S

S

Time range this job is allowed to run
(in your local time zone)

Start Time

End Time

+

+

00

:

00

24

:

00

-

-

Back

Next

Fig. 1.20: Deploy Configuration Schedule

6. Check if the deployment details are correct and click “Schedule deployment”.

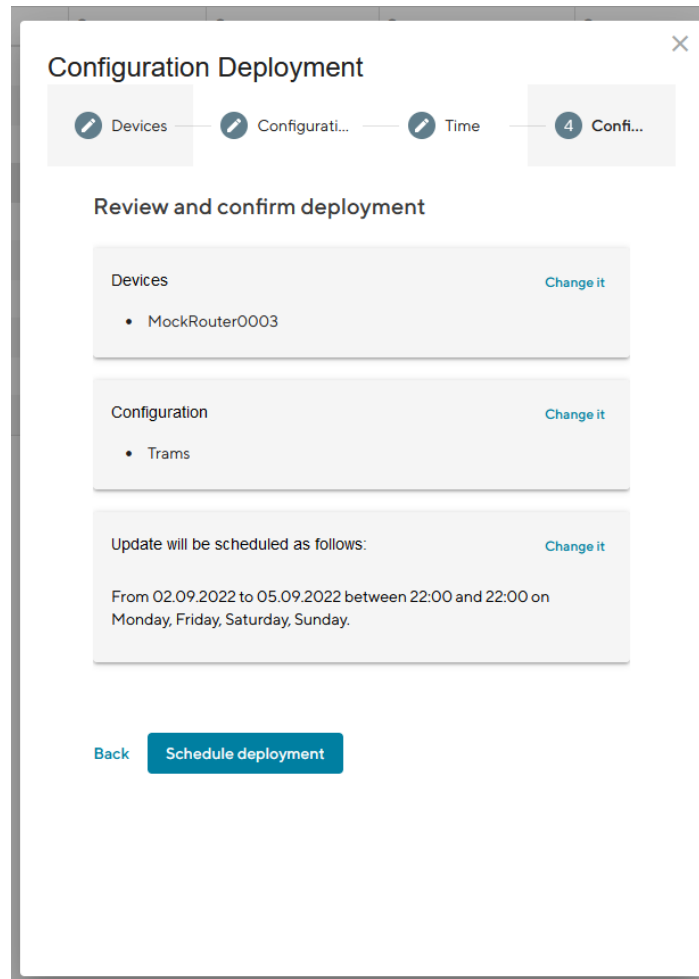


Fig. 1.21: Deploy Configuration Confirmation

Deploy a Snippet

1. Navigate to the page “Devices” and select the Devices in the main dialogue Box that are to be configured.
2. Click on “Actions” at the upper right corner of the Main dialogue box and click “Deploy Snippet”.
3. Select the Snippet to be deployed.
4. Select whether you want to start the configuration immediately or whether it should be scheduled.
5. Confirm the deployment by click “Start deployment”.

When a Snippet deployment has started it will be listed as a Job in the Jobs table (see [Section 1.10](#)). Jobs can be scheduled while creating them (see step 7). Therefore following scheduling options are possible:

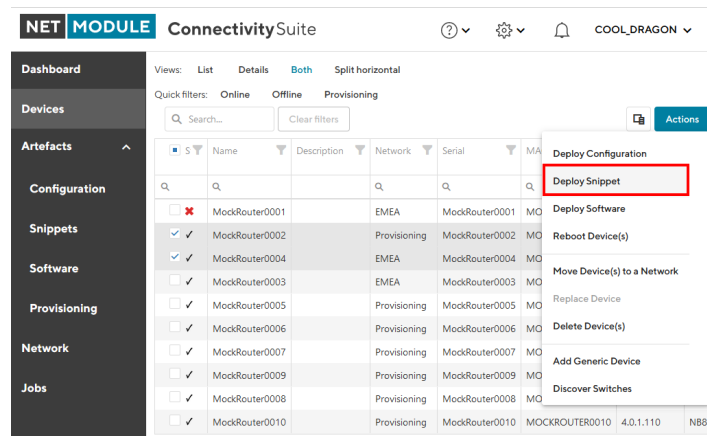


Fig. 1.22: Deploy Snippet Action

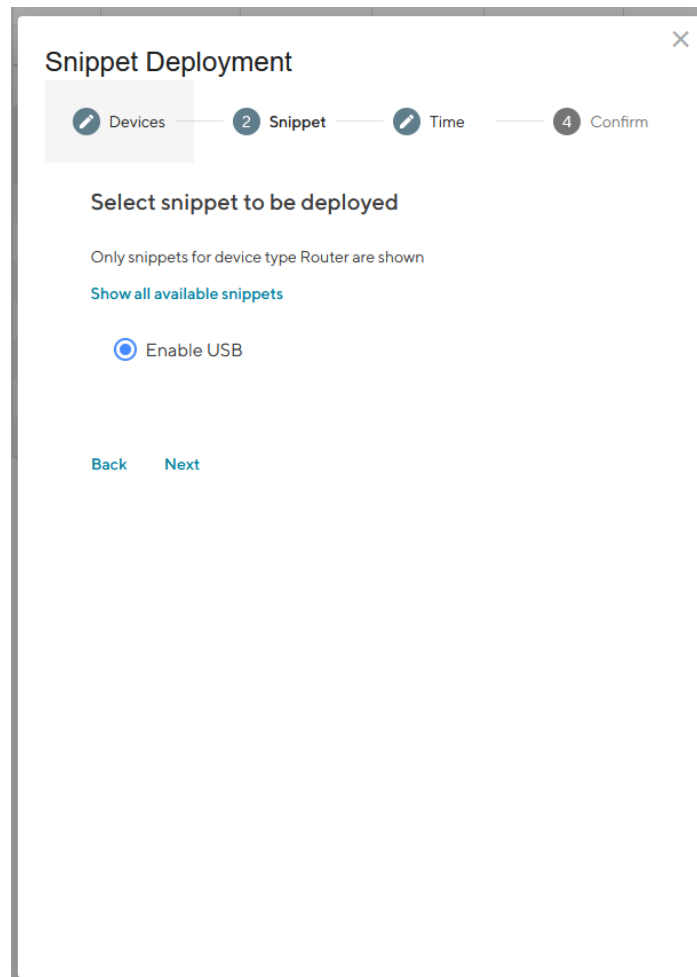


Fig. 1.23: Snippet Selection

Snippet Deployment

1

Devices

2

Snippet

3

Time

4

Confirm

Select execution time

☐ Start deployment now

☒ Schedule deployment for later execution

Enter a date range
9/22/2022 - 9/30/2022

Weekdays this job is allowed to run
M **T** **W** **T** F **S** **S**

Time range this job is allowed to run
(in your local time zone)
Start Time
+
22 : 00
-
End Time
+
23 : 00
-

Back

Next

Fig. 1.24: Snippet Deployment Schedule

Snippet Deployment

Devices

Snippet

Time

4 Confirm

Review and confirm deployment

Devices

Change it

- MockRouter0002
- MockRouter0004

Snippet

Change it

- Enable USB

Update will be scheduled as follows:

Change it

From 22.09.2022 to 30.09.2022 between 22:00 and 22:00 on Tuesday, Wednesday, Thursday, Saturday, Sunday.

Back

Schedule deployment

Fig. 1.25: Snippet Deployment Confirmation

| | |
|-------------------|---|
| Start Date | The first day on which the Connectivity Suite is going to try to execute the Job, if all conditions are met (time window, day of the week etc.). |
| End Date | The last day on which the Connectivity Suite is going to try to execute the Job, if all conditions are met (time window, day of the week etc.). |
| Days | Offers the possibility to constrain the execution of the Job to specific days of the week. By default, the execution is allowed for all days of the week (the blue color indicates a selected day) |
| Start Time | Offers the possibility to constrain the Job execution to a certain time frame within a day. Only the hour can be specified, higher precision is not supported currently. Allowed values are 0-23, the default value is 0 (midnight). |
| End Time | Offers the possibility to constrain the Job execution to a certain time frame within a day. Only the hour can be specified, higher precision is not supported currently. Allowed values are 1-24, the default value is 24 (midnight). |

Warning: Configuration changes made in the web interface of the Device will not be automatically added to the Connectivity Suite and can lead to connectivity issues. Any configuration changes made in the web interface of a NM router must be uploaded to the Connectivity Suite as described in *::manual_configuration_updates*.

Deploy Software

1. Navigate to the page “Devices” and select the Devices in the main dialogue Box that are to be updated.
2. Click on “Actions” at the upper right corner of the Main dialogue box and click “Deploy Snippet”.

The screenshot shows the Connectivity Suite web interface. On the left is a sidebar with navigation links: Dashboard, Devices, Artefacts, Configuration, Snippets, Software, Provisioning, Network, and Jobs. The main area displays a table of devices. At the top right of the main area are icons for help, settings, notifications, and a user profile (COOL_DRAGON). Below these are view filters (List, Details, Both, Split horizontal) and quick filters (Online, Offline, Provisioning). A search bar and 'Clear filters' button are also present. The 'Actions' button in the top right corner is clicked, opening a dropdown menu. The 'Deploy Software' option in this menu is highlighted with a red rectangle. The table below shows 10 mock routers with columns for Name, Description, Network, Serial, and MA.

| | Name | Description | Network | Serial | MA |
|-------------------------------------|----------------|-------------|--------------|----------------|----------------|
| <input type="checkbox"/> | MockRouter0001 | | EMEA | MockRouter0001 | MO |
| <input checked="" type="checkbox"/> | MockRouter0002 | | Provisioning | MockRouter0002 | MO |
| <input checked="" type="checkbox"/> | MockRouter0004 | | EMEA | MockRouter0004 | MO |
| <input type="checkbox"/> | MockRouter0003 | | EMEA | MockRouter0003 | MO |
| <input type="checkbox"/> | MockRouter0005 | | Provisioning | MockRouter0005 | MO |
| <input type="checkbox"/> | MockRouter0006 | | Provisioning | MockRouter0006 | MO |
| <input type="checkbox"/> | MockRouter0007 | | Provisioning | MockRouter0007 | MO |
| <input type="checkbox"/> | MockRouter0009 | | Provisioning | MockRouter0009 | MO |
| <input type="checkbox"/> | MockRouter0008 | | Provisioning | MockRouter0008 | MO |
| <input type="checkbox"/> | MockRouter0010 | | Provisioning | MockRouter0010 | MOCKROUTER0010 |

Fig. 1.26: Deploy Software Action

2. Select the Software to be deployed.

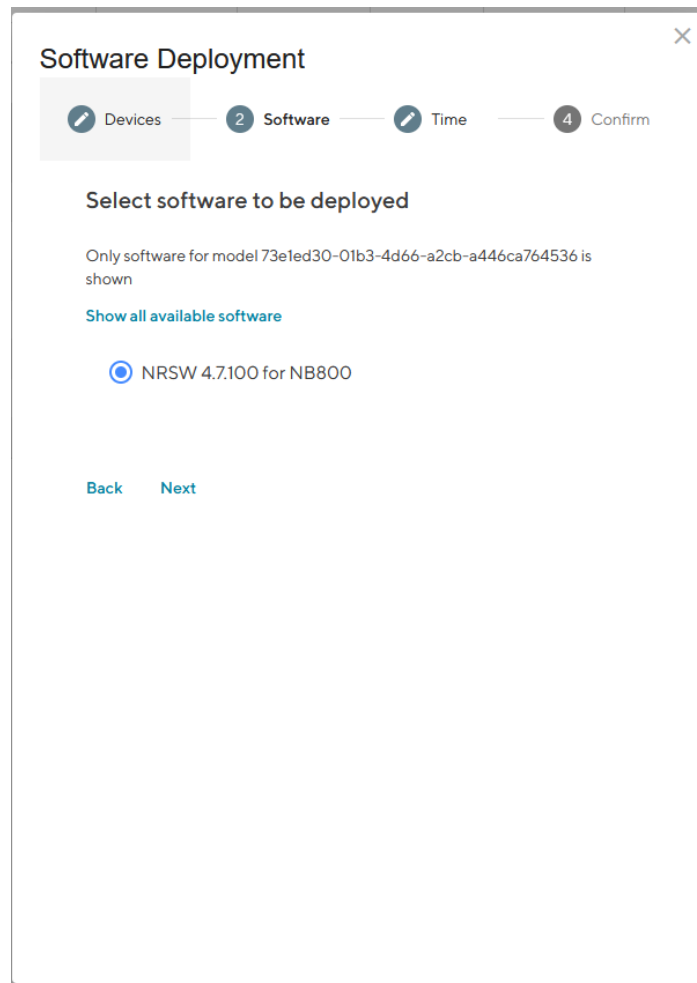


Fig. 1.27: Software Selection

3. Select whether you want to start the configuration immediately or whether it should be scheduled.
4. Confirm the deployment by click “Start deployment”.

When a Software deployment has started it will be listed as a Job in the Jobs table (see [Section 1.10](#)). Jobs can be scheduled while creating them (see step 7). Therefore following scheduling options are possible:

| | |
|-------------------|---|
| Start Date | The first day on which the Connectivity Suite is going to try to execute the Job, if all conditions are met (time window, day of the week etc.). |
| End Date | The last day on which the Connectivity Suite is going to try to execute the Job, if all conditions are met (time window, day of the week etc.). |
| Days | Offers the possibility to constrain the execution of the Job to specific days of the week. By default, the execution is allowed for all days of the week (the blue color indicates a selected day) |
| Start Time | Offers the possibility to constrain the Job execution to a certain time frame within a day. Only the hour can be specified, higher precision is not supported currently. Allowed values are 0-23, the default value is 0 (midnight). |
| End Time | Offers the possibility to constrain the Job execution to a certain time frame within a day. Only the hour can be specified, higher precision is not supported currently. Allowed values are 1-24, the default value is 24 (midnight). |

×

Software Deployment

✎

 Devices —

✎

 Software —

3

 Time —

4

 Confirm

Select execution time

☒ Start deployment now

☐ Schedule deployment for later execution

Back

Next

Fig. 1.28: Software Deployment Schedule

×

Software Deployment

✎ Devices

✎ Software

✎ Time

4 Confirm

Review and confirm deployment

Devices

Change it

- MockRouter0002
- MockRouter0004

Software

Change it

- NRSW 4.7.100 for NB800

Update will start now

Change it

Back

Start deployment

Fig. 1.29: Software Deployment Confirmation

Reboot a Device

1. Navigate to the page “Devices” and select the Devices in the main dialogue that are to be rebooted.
2. Click on “Actions” at the upper right corner of the Main dialogue box and click “Reboot Device(s)”.

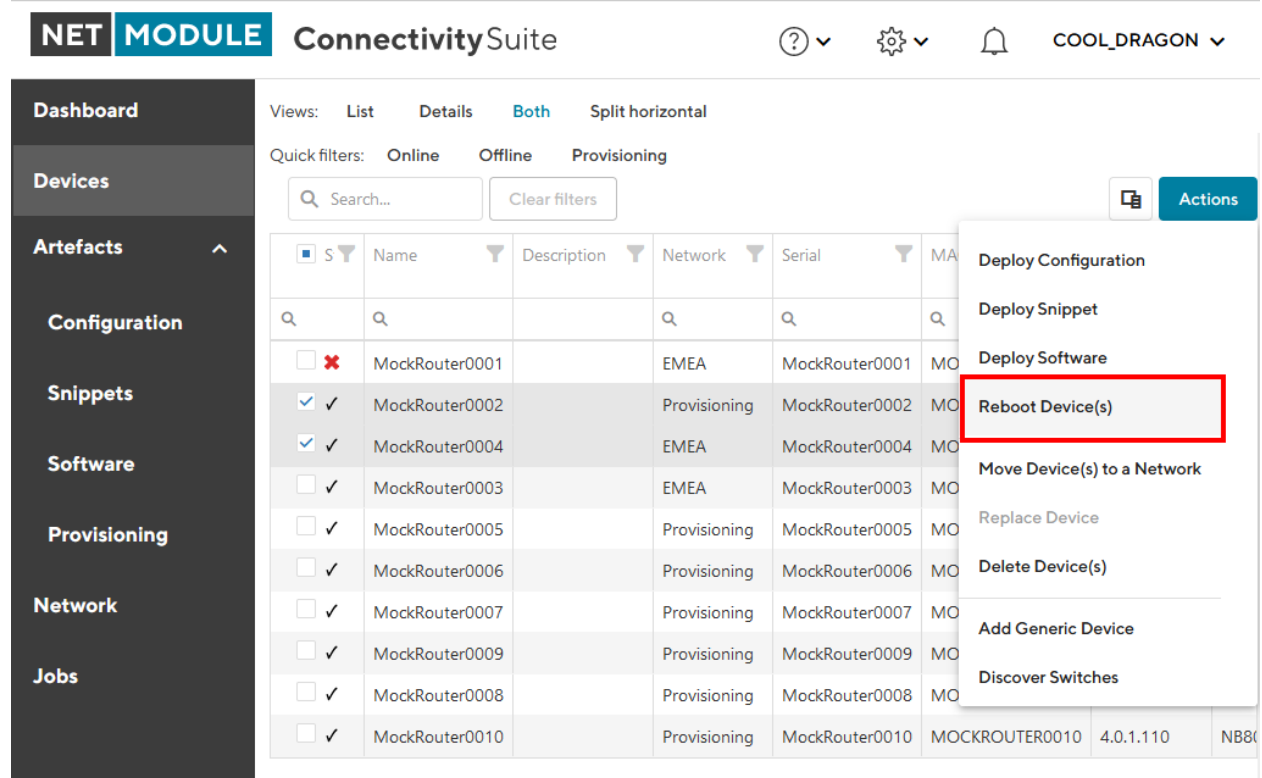


Fig. 1.30: Reboot Devices Action

3. Confirm the reboot by clicking “Reboot device(s)”.

When a Reboot has started it will be listed as a Job in the Jobs table (see [Section 1.10](#)).

Move Network

1. Navigate to the page “Devices” of the Connectivity Suite and select the Devices which have to be assigned to a VPN Network.
2. Click on “Actions” at the upper right corner of the Main dialogue box and click “Move Device(s) to a Network”.
3. Select the required VPN Network in the drop down list and click “Next”.
4. Click on “Start assignment” to assign the Devices to the VPN Network (this operation may take some time). A confirmation message must be pop up which confirms the assignment of the Devices to the VPN Network.
5. The applied VPN Network will be shown in the Main dialogue box in the table.

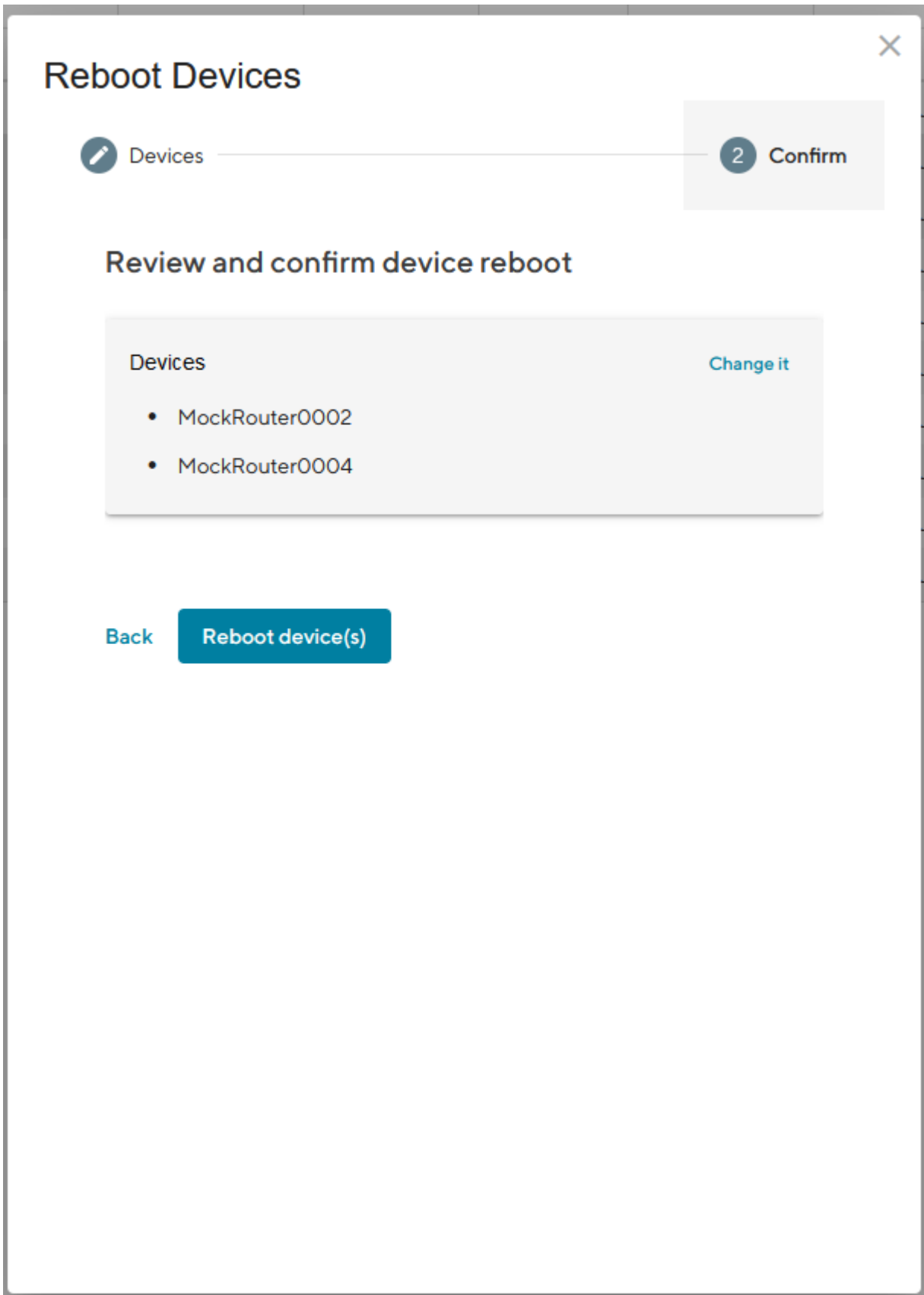


Fig. 1.31: Reboot Devices Confirmation

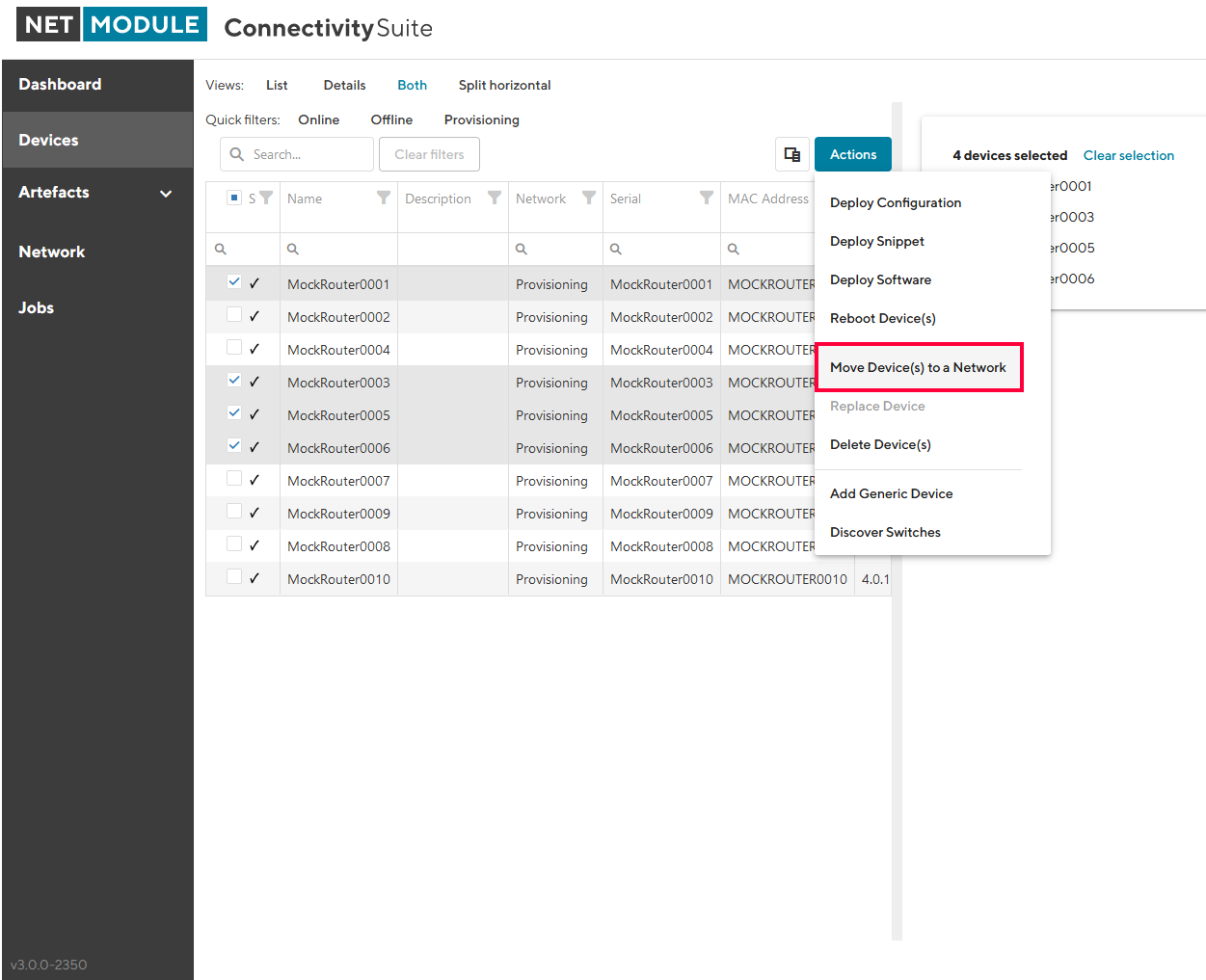


Fig. 1.32: VPN Network assignment

Delete a Device

1. Navigate to the page “Devices” and select the Devices in the main dialogue that are to be removed.
2. Click on “Actions” at the upper right corner of the Main dialogue box and click “Delete Device(s)”.

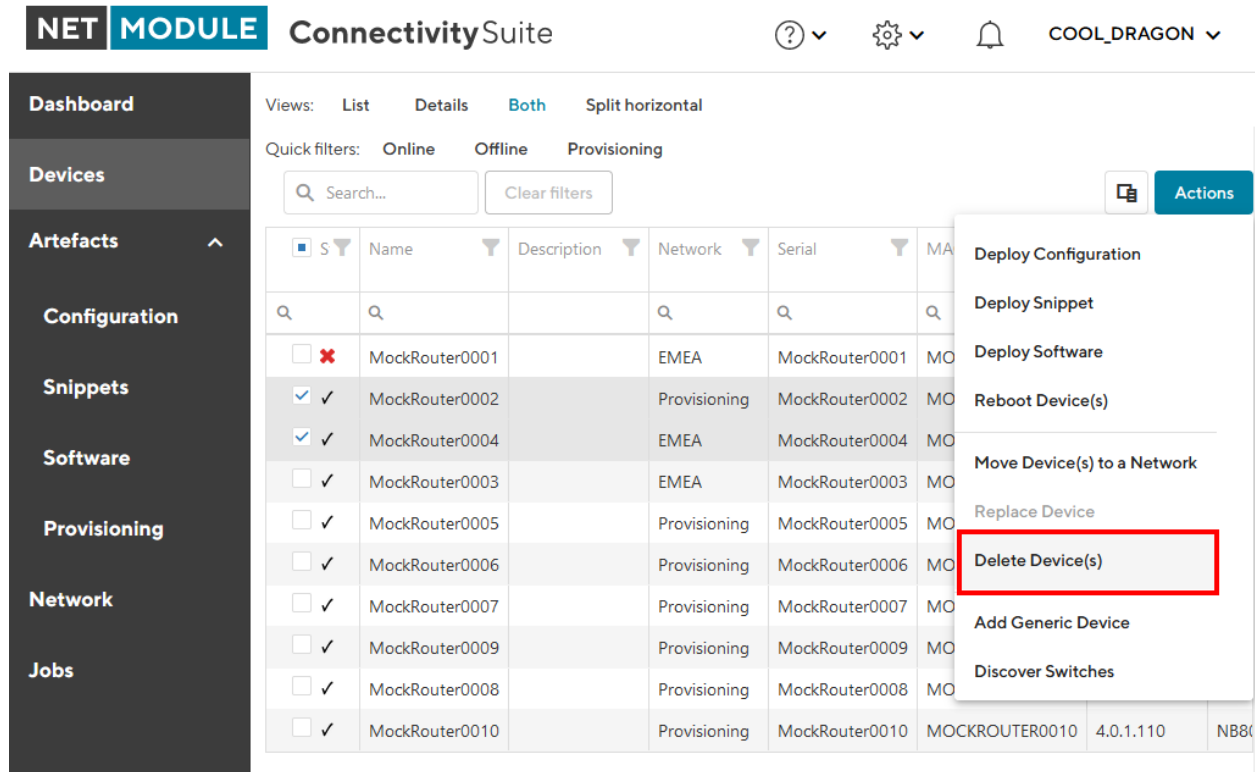


Fig. 1.33: Delete Devices Action

3. Confirm the deletion by clicking “Delete device(s)”.

Add a generic Device

1. Navigate to the page “Devices”
2. Click on “Actions” at the upper right corner of the Main dialogue box and click “Add generic Device”.
3. Add the device by clicking “Add Generic Device”.
3. You can download an OpenVPN configuration for the newly added device

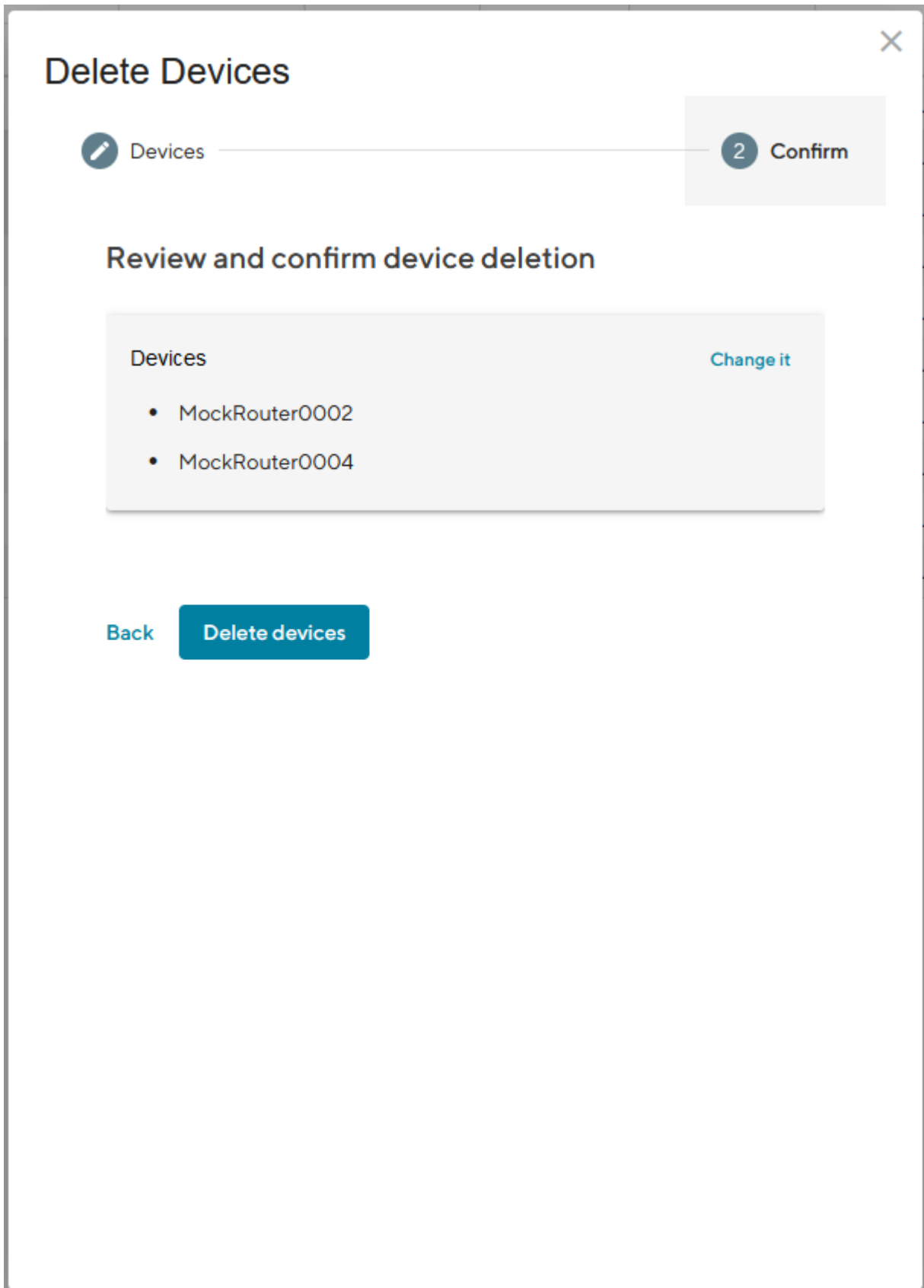


Fig. 1.34: Delete Devices Confirmation

NET MODULE ConnectivitySuite ? ⚙️ 🔔 COOL_DRAGON ▼

Views: List Details Both Split horizontal

Quick filters: Online Offline Provisioning

Search... Clear filters

| <input type="checkbox"/> S | Name | Description | Network | Serial | MAC Address | Software | Model | Tags |
|-------------------------------------|----------------|--------------|----------------|----------------|-------------|----------|-------|-------------|
| <input checked="" type="checkbox"/> | MockRouter0001 | Provisioning | MockRouter0001 | MOCKROUTER0001 | 4.0.1.110 | NB | | |
| <input type="checkbox"/> | MockRouter0002 | Provisioning | MockRouter0002 | MOCKROUTER0002 | 4.0.1.110 | NB | | |
| <input type="checkbox"/> | MockRouter0004 | Provisioning | MockRouter0004 | MOCKROUTER0004 | 4.0.1.110 | NB | | |
| <input type="checkbox"/> | MockRouter0003 | Provisioning | MockRouter0003 | MOCKROUTER0003 | 4.0.1.110 | NB | | |
| <input type="checkbox"/> | MockRouter0005 | Provisioning | MockRouter0005 | MOCKROUTER0005 | 4.0.1.110 | NB | | |
| <input type="checkbox"/> | MockRouter0006 | Provisioning | MockRouter0006 | MOCKROUTER0006 | 4.0.1.110 | NB | | |
| <input type="checkbox"/> | MockRouter0007 | Provisioning | MockRouter0007 | MOCKROUTER0007 | 4.0.1.110 | NB | | |
| <input type="checkbox"/> | MockRouter0009 | Provisioning | MockRouter0009 | MOCKROUTER0009 | 4.0.1.110 | NB | | |
| <input type="checkbox"/> | MockRouter0008 | Provisioning | MockRouter0008 | MOCKROUTER0008 | 4.0.1.110 | NB | | |
| <input type="checkbox"/> | MockRouter0010 | Provisioning | MockRouter0010 | MOCKROUTER0010 | 4.0.1.110 | NB800 | | 10.240.12.1 |

Actions

- Deploy Configuration
- Deploy Snippet
- Deploy Software
- Reboot Device(s)
- Move Device(s) to a Network
- Replace Device
- Delete Device(s)
- Add Generic Device**
- Discover Switches

Fig. 1.35: Add Generic Device Action

Add Generic OpenVPN Device ✕

Device Name *
my printer

Network *
EMEA

Add Generic Device

Fig. 1.36: Add Generic Device Dialog

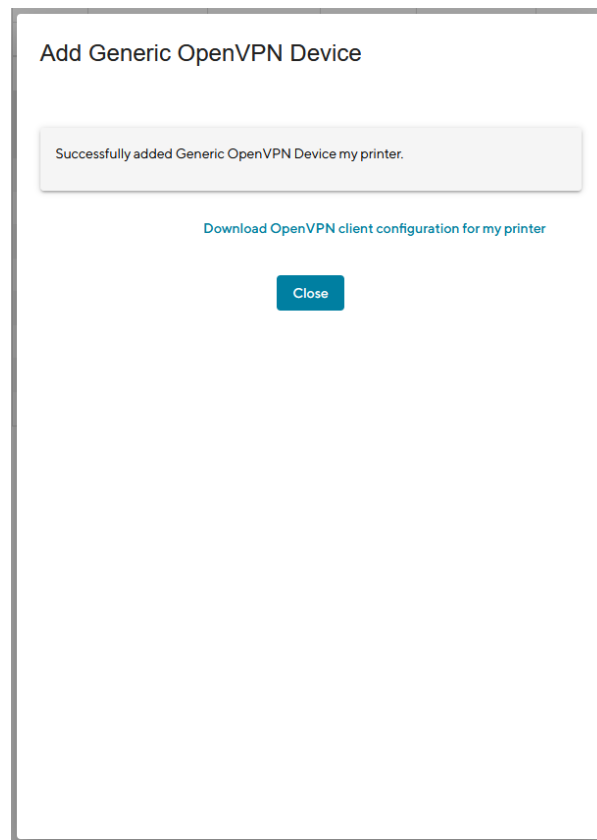


Fig. 1.37: Add Generic Device Confirmation

1.6.4 Router specific actions

Router Provisioning

Before the devices can be managed or accessed, they must be provisioned. Provisioning makes it possible to integrate the devices into the network infrastructure of the Connectivity Suite. The provisioning process is shown in Fig. 1.38 and described in the following chapters.

Caution: The Router Configuration must support the following, for proper operation through Connectivity Suite.
 | a. Open TCP port 22, for SSH access through VPN tunnel from CS | b. SSH Server listening on port 22 | c. root user with SSH access

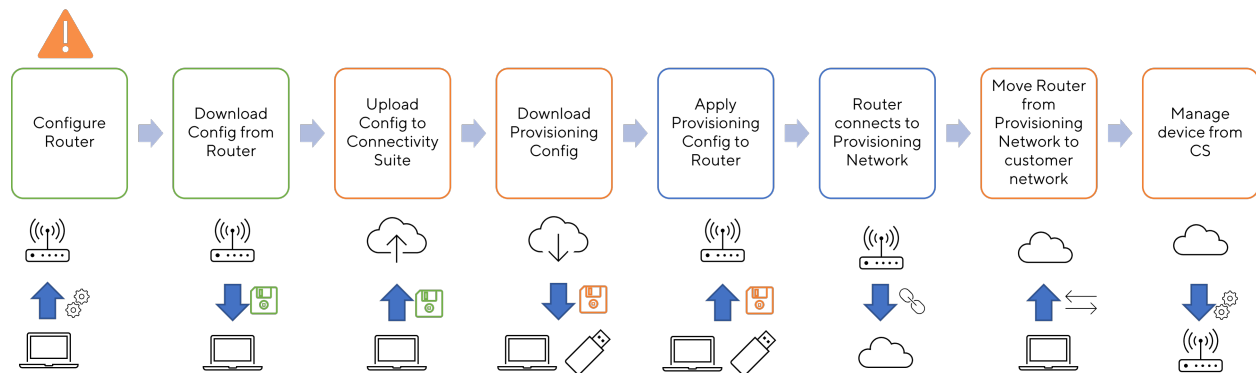


Fig. 1.38: Provisioning Process Router

Note: Only 250 devices can be connected to the Provisioning Network at once. If the provisioning server has no available space left move the Devices to a VPN Network before adding more.

For the following steps an account with **Platform Administrator** rights is required.

The CS can deploy configurations to Devices. The main feature here is mass configurations that can be rolled out for different types of Devices. In addition, configurations of individual devices can also be copied or adapted via the CS.

Router replacement

A NM router will be replaced due to a defect or a hardware update etc. If the replaced Device is not the same type as the replacement Device this procedure might won't work.

Note: Ensure that the firmware used on the replacement Device is the same or newer than the firmware version of the Device being replaced, otherwise the replacement will not work and both Devices will be lost.

1. Navigate to the page "Devices" and click on "Actions" and "Replace Device" to exchange a Device.
2. Click "Generate Replacement Device Configuration" to generate a configuration which can be uploaded to the replacement Device.
3. Click "Download this configuration" (configuration can be uploaded via the web manager) or "Download this Configuration as USB version" Configuration can be uploaded via an usb stick) to download the configuration.

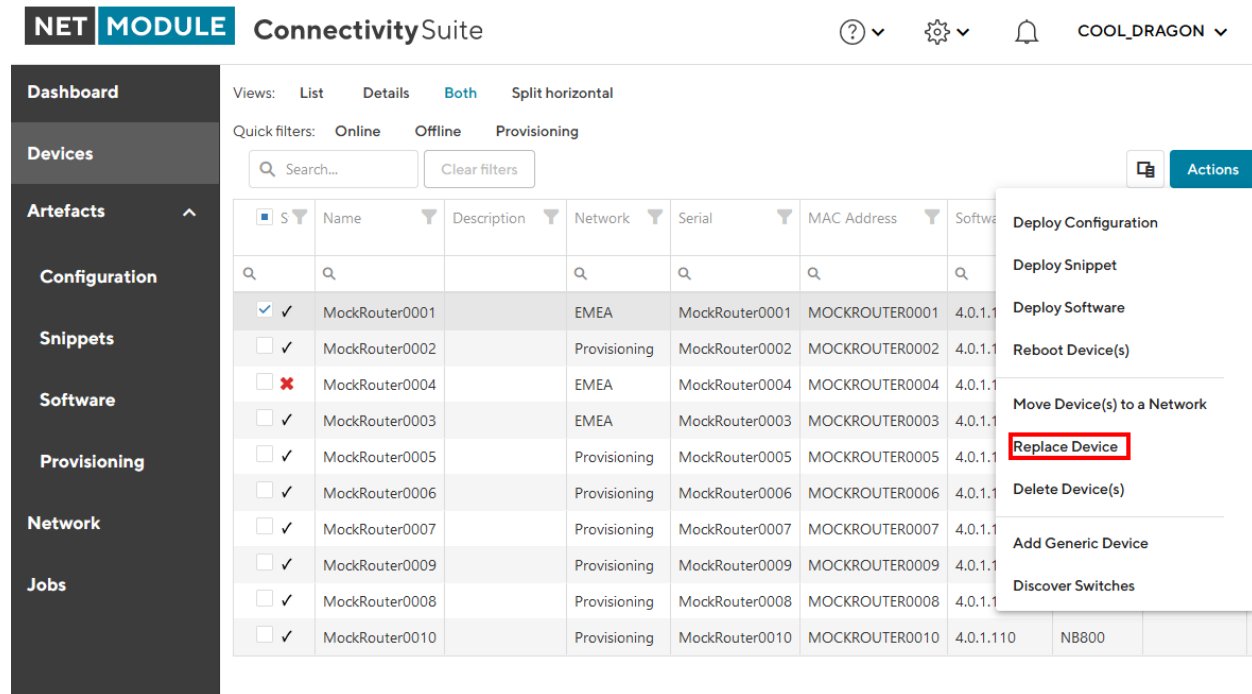


Fig. 1.39: Replace Device

4. Upload the configuration to the replacement Device via web manager or USB
5. The replacement Device will automatically connect to the Connectivity Suite and the Device which will be replaced will be automatically removed from the Connectivity Suite.
6. If the device has connected correctly you can see all the Device details by clicking on the replacement device in the table of the Main dialogue box.

Changes to replaced Device object:

- firmware version
- Serial number

Note: When the replacement device connects to the Connectivity Suite, the certificate of the defective device will be revoked and it won't be able to connect to the Connectivity Suite anymore.

1.6.5 Switch specific actions

Supported switch firmware releases

Before connecting a switch to the Connectivity Suite ensure that a supported switch firmware is running on the device. The Connectivity Suite guarantees support for all switch firmware releases which are supported by Tronteq. These can be checked at the following link: <https://www.tronteq.com/>

Switch provisioning

Before the switch can be managed or accessed, it has to be provisioned. Provisioning makes it possible to integrate the switch into the network infrastructure of the Connectivity Suite. The provisioning process is shown in Fig. 1.40 and described in the following chapters.

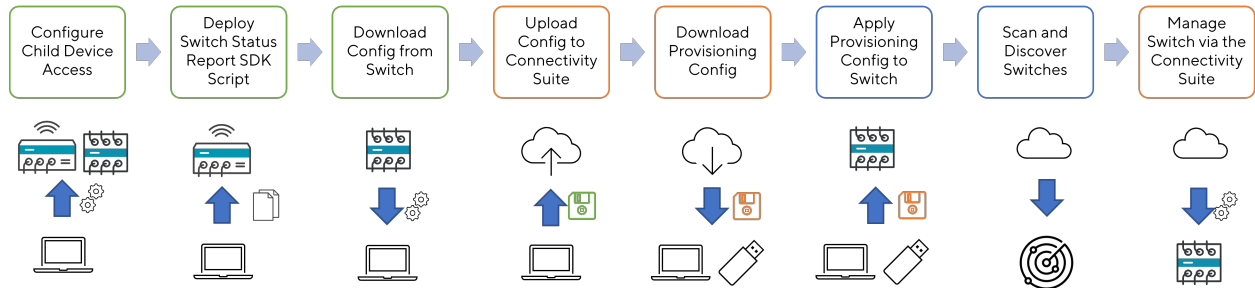


Fig. 1.40: Provisioning Process Switch

For the following steps an account with **Platform Administrator** rights is required.

1. **Configure child Device Access:** Configure a Child Device Access on the router for the switch as described in [Section 1.13](#). Note that LLDP discovery must be enabled on the router before provisioning (LLDP sending is enabled on the switch by default).
2. **Deploy Switch Status Report SDK Script:** On each router where a switch is connected, the SDK script must be executed. The SDK script is provided by NetModule and can be downloaded from here: <https://repo.netmodule.com/repository/cs/cs-stable/sdk-scripts/cs-status-reporting.are>. See [Section 1.9.4](#) on how to deploy this script via the Connectivity Suite. Choose “openvpn-up” as Event Trigger. After deployment, reboot the router to activate the script.
3. **Download Config from Switch:** Once the switch is configured the configuration can be downloaded from the switch. The file should be a .cfg file.
4. **Upload Config to Connectivity Suite:** Navigate to the page Provisioning and Upload the configuration (see [Fig. 1.41](#)). Fill out the required fields, upload the configuration and click “Generate Provisioning Configuration”.
5. **Download Provisioning Config:** If the provisioning configuration is uploaded to the switch via a usb stick click on “Download USB configuration” or if its uploaded via the web interface of the switch click “Download file configuration” (see [Fig. 1.42](#)).
1. **Apply Provisioning Config to Switch:** Upload the provisioning configuration to the switch, as mentioned before this can be done via usb stick or via web interface of the switch.
2. **Scan and Discover Switches:** Select the routers where the switches are connected to, open the “Actions” menu, select “Register Connected Devices”, and start the scan process. If switches are discovered they will be shown in the Devices List.

Note: The same provisioning configuration can be used for several switches as long as they belong to the same Device Model

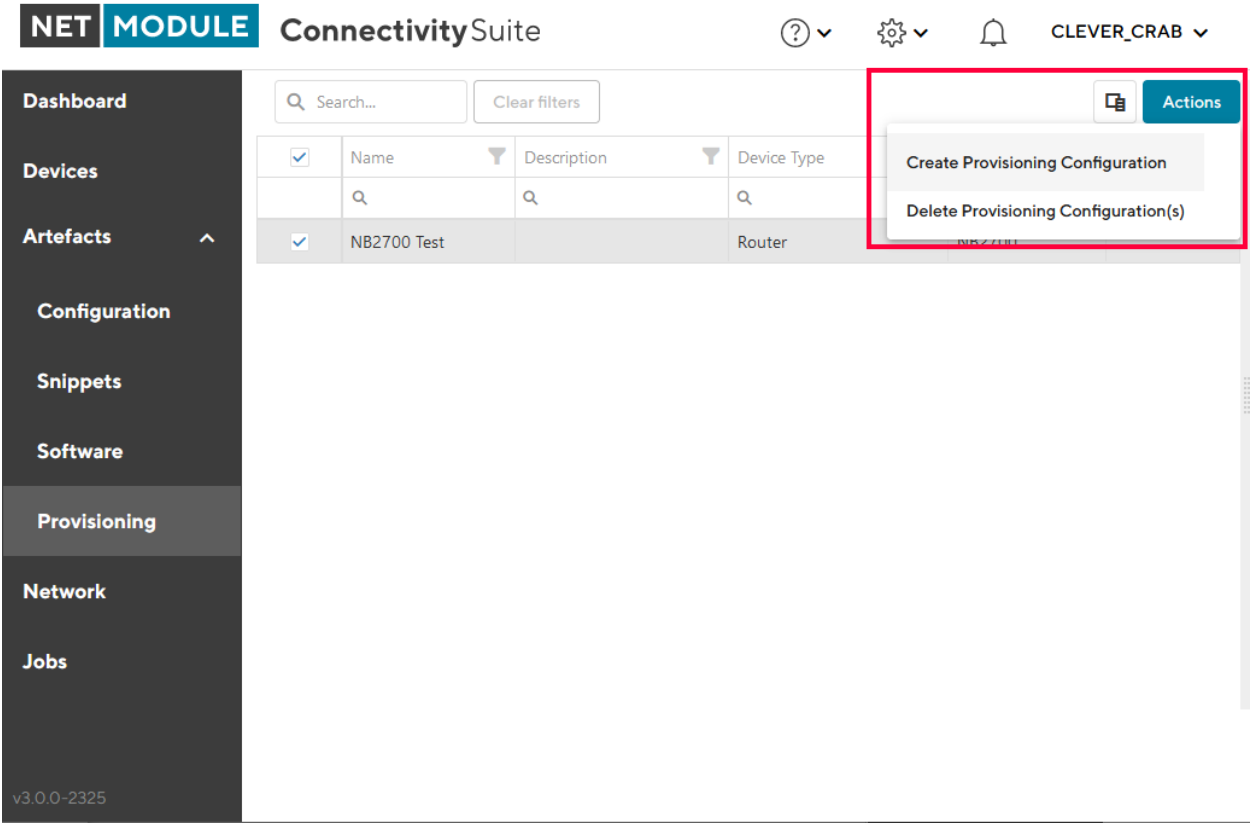


Fig. 1.41: Add Switch Provisioning Configuration

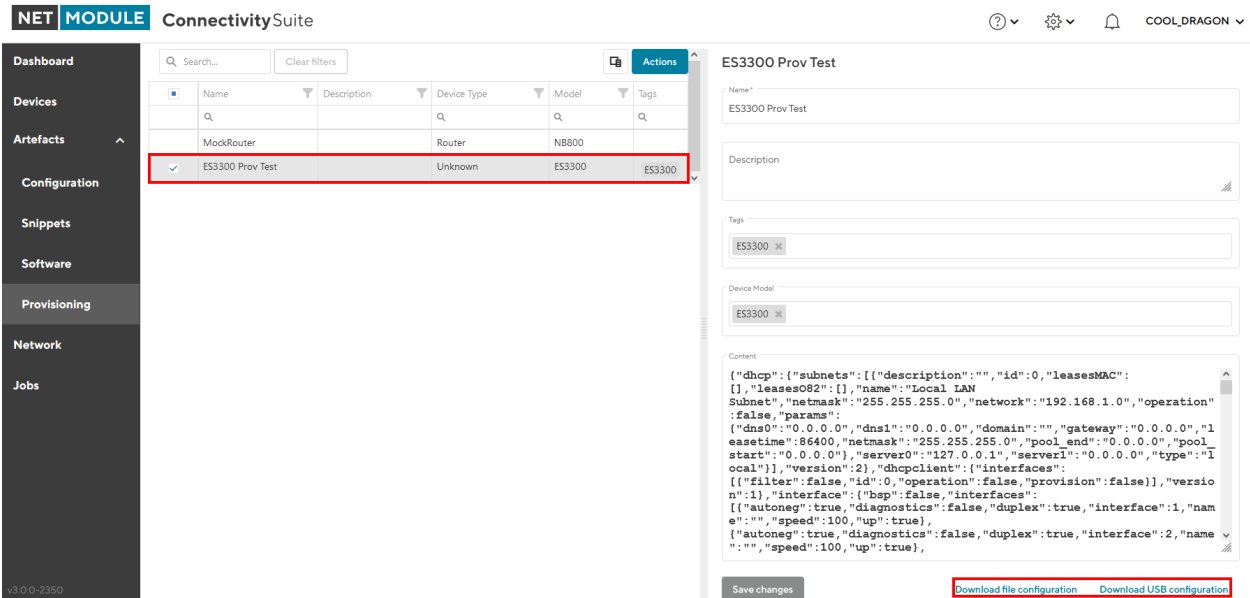


Fig. 1.42: Manual Switch USB update

1.6.6 WLAN Access Point specific actions

The AP3400 is being managed the same way as the ethernet switches.

Note: Once an accesspoint has been commissioned to Connectivity Suite, it is strongly advised to no longer manage the access point locally.

Firmware releases

All the firmware releases for AP3400, listed in the NetModule Soft- & Firmware repository are supported.

Provisioning

The provisioning of AP3400 is following the same process as for switches.

1.7 Dashboard

The Dashboard is supposed to give a quick status overview of the Connectivity Suite and its devices.



Fig. 1.43: Dashboard

1.7.1 Tiles

There are multiple tiles providing different information.

Devices in Networks

This tile shows all not hidden devices assigned to a network (i.e. no longer in provisioning) grouped by their current status.

The following status-grouping is applied:

- Offline (<5m): offline less than 5 minutes
- Offline (<1h): offline less than 1 hour
- Offline (<24h): offline less than 24 hours
- Offline (>24h): offline more than 24 hours
- Online
- Unknown

By clicking on the corresponding status in the status list, the user will be directed to the Devices page and the corresponding filter will be applied.

Devices in Provisioning

This tile shows all not hidden devices in provisioning (i.e. not yet assigned to a network) grouped by their current status.

The same status-grouping is applied as for the [Section 1.7.1 *Devices in Networks*](#) tile.

By clicking on the corresponding status in the status list, the user will be directed to the Devices page and the corresponding filter will be applied.

Device Models

This tile shows all not hidden devices grouped by their device model.

By clicking on the corresponding device model in the device model list, the user will be directed to the Devices page and the corresponding device model filter will be applied.

VPN Networks

This tile shows all VPN networks including the Backend and the Provisioning networks grouped by their status (online, offline, unknown).

By clicking on the corresponding status in the status list, the user will be directed to the Networks page and the corresponding filter will be applied.

Jobs

This tile shows the most recent jobs grouped by their status.

The date range to cover can be changed in the tile. The following date ranges are available:

- Last hour
- Today
- Last 24 hours
- Last 3 days
- Last 7 days (default)
- Last 30 days

By clicking on the corresponding status in the status list, the user will be directed to the Jobs page and the corresponding filter will be applied.

Software

This is a series of tiles, one per device type (e.g. Router, Switch, etc.). They show the software versions currently used. It covers only devices providing this information. Only not hidden devices are incorporated.

By clicking on the corresponding software version in the software version list, the user will be directed to the Devices page and the corresponding filter will be applied.

1.8 Variables & Bulk Editor

The main advantage of Variables is to reduce time required for deployments, especially for many devices to be configured at the same time, with each device having individual parameters being unique.

1.8.1 System & Custom Variables

Variables consist of a parameter key & value pair, which is available system wide, to be used in device template configs and snippets.

The administration of Variables is done on a global level under systems settings. In addition to Variables provided by the system, custom ones may be created as desired.

Custom Variables

Follow the steps below, to create custom variables

1. Create a new table entry
2. Enter Custom Variable
3. Save entry

For custom Variables, a default value must be set. In addition, either the network or device specific value, can be set. This is done on the corresponding detail page under the tab “Variables”, by clicking the save icon once entered.

Note: Once a variable is created, its name cannot be changed afterwards.

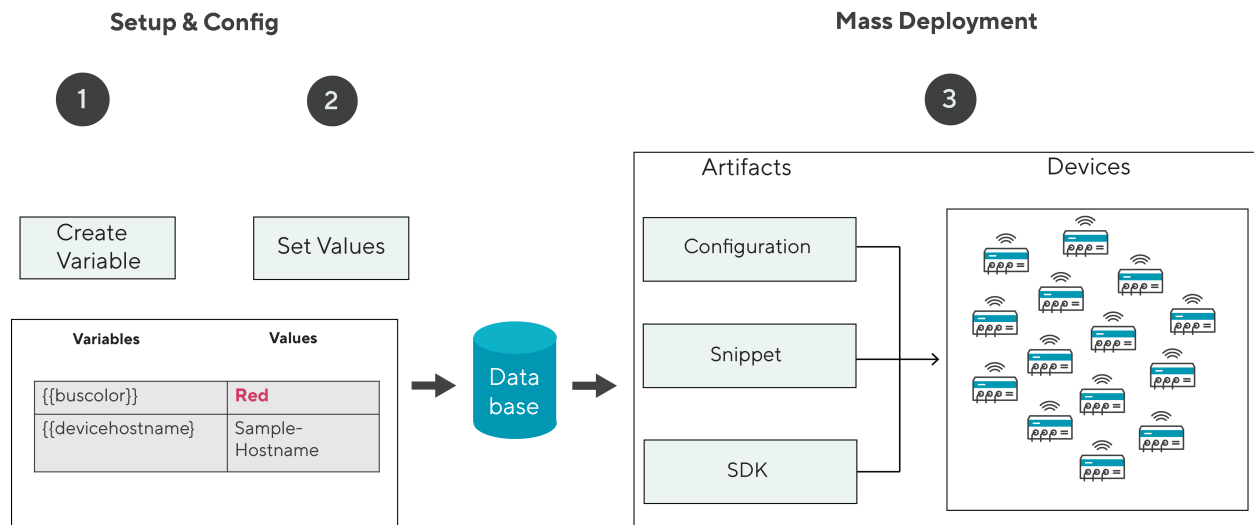


Fig. 1.44: Workflow Variables

The screenshot shows the **ConnectivitySuite** interface. The left sidebar contains navigation links: **Dashboard**, **Devices**, **Artefacts**, **Network**, and **Jobs**. The main content area is titled **Settings** and has tabs for **FEATURES**, **DEVICE FILTER**, and **VARIABLES**.

Custom Variables:

- Buttons: **+** (Add), **🗑️** (Delete), **↺** (Refresh).
- Table:

| Name | Default value | Description | Delete |
|----------|---------------|----------------|--------|
| color | green | vehicle color | |
| hostname | name | devicehostname | |

System Provided Variables:

| Name | Example value |
|---------------------------|--|
| system-device-name | My Router |
| system-device-description | A description for the device My Router |
| system-device-platform-ip | 10.224.0.1 |
| system-device-vpn-ip | 10.0.0.1 |
| system-device-subnet-mask | 255.255.255.0 |
| system-device-subnet-cidr | 24 |

Right Panel:

- Admin menu: **Manage Users**, **Logs**, **Settings** (highlighted), **Event Viewer**.
- Information box: "Along with the system provided variables, there may be custom ones created, which then can be inserted in configurations, snippets, etc. using the editor plane on the corresponding detail page. The default values of the variables defined here can be overwritten on network and/or device level."
- Warning box: "Deleting a variable here has the following consequences:
 - The variable is deleted on all Networks and Devices!
 - The variable is NOT removed from configuration files where it was used, you will have to do this manually!"

Fig. 1.45: Variables Global Settings

Default value and description of a variable can be modified once created. When doing so, the new value will be propagated down to Network and Device level, where no custom value has been configured before (See Fig. 1.46). With the consequence that all values which have been set individually (override) on either network and/or device level, do not change when the default value for a variable is being modified. Both, system provided and custom created Variables, are distributed to Networks and Devices and therefore available for deployments.

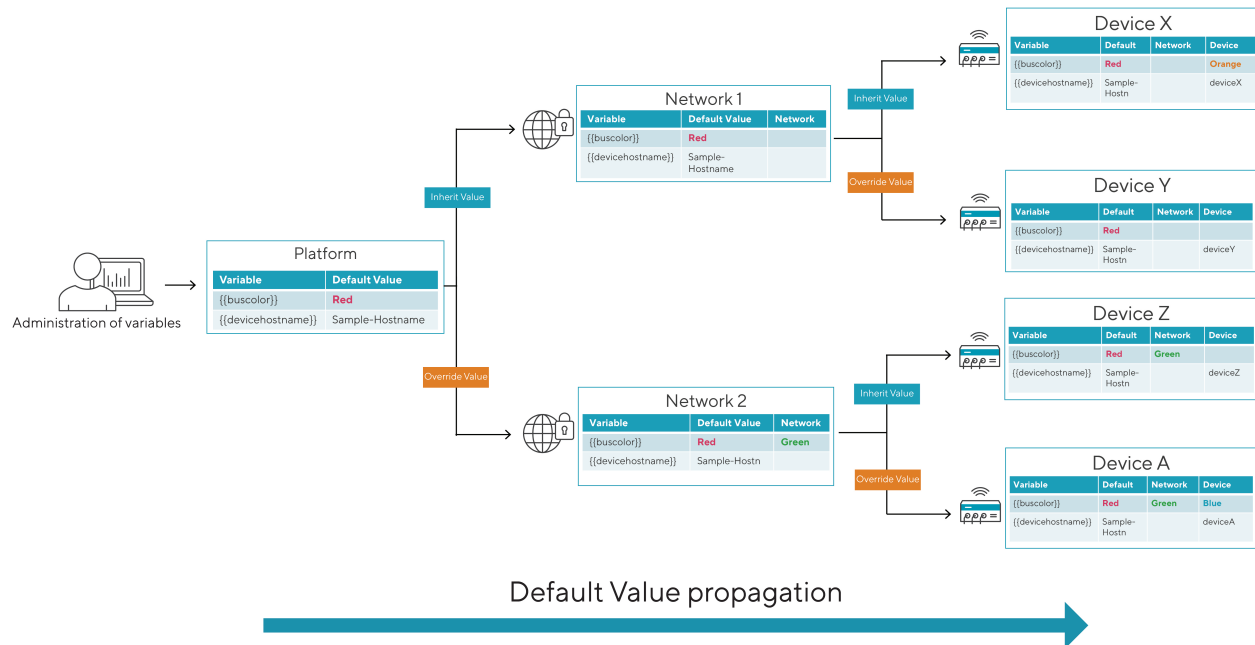


Fig. 1.46: Variables Values Propagation

1.8.2 Bulk Import

In addition to managing the values of Variables through the WEB interface, they can be edited in an .xlsx document and be imported in one batch. It is recommended to export a device list first (see Section 1.8.3) and start editing parameters there before importing it. The greyed-out fields in the .xlsx sheet previously exported, must not be edited as these are non-configurable items. Either the column "DeviceID" or "MacAddress" is required for the device identification when importing the .xlsx sheet. Fields that are kept blank cause no action when importing.

1.8.3 Device List Export

Device lists with custom parameters can easily be generated using the Export function. In a first step, select the devices, followed by “Export Device List” under Actions, which opens a Modal Dialog. Chose which fields to be included in the .xlsx formatted list. By selecting “Standard” the commonly used parameters are included. This list may be edited, by adding device specific values for the given variables and for a later import to Connectivity Suite.

1.8.4 Deployments using Variables

Variables can be used system wide for different deployments, such as Configuration, Snippets, etc. Using an example of a configuration deployment, the following steps are required. Under the menu item Artifacts, select Configuration.

1. Add a new Configuration, which serves as a template for mass deployments
2. Once created navigate to the Editor tab of the Configuration
3. Replace Configuration values which should be device dependent (see [Fig. 1.47](#)) by inserting a Variable.
4. Choose a variable in the drop-down list a. Repeat for additional Variables to be set

In the example below, the system hostname uses a variable which means the corresponding value will be inserted which is set for the device.

Note: Make sure the config is saved before continuing to the next step

For the deployment of the configuration, follow the instructions documented under [Section 1.6.3](#)

1.9 Artifacts

1.9.1 Snippets

Add Snippets

A snippet is an excerpt from the configuration parameters that configures a specific function of the router, e.g. activating the USB port or switching off WLAN. Snippets can be used to configure an infinite number of Devices, regardless of the Device type (only applies to NM devices). They are not complete Device Configurations (in comparison to Template Device Configurations as described under [Template Device Configurations](#))

Note: Switches currently do not support Snippets.

All configuration parameters which can be used for a Snippet are documented and can be found in the NM Wiki using following link: [https://wiki.netmodule.com/documentation/config-parameters?s{\[\]}{}}=parameter](https://wiki.netmodule.com/documentation/config-parameters?s{[]}{}}=parameter)

Example of a complete Snippet that originates from a configuration with version 1.8 and enables the USB port 0:

```
config.version=1.8
usb.status=1
usb.0.enabled=1
```

Before the configuration can be deployed for a massconfiguration a Snippet must be created:

1. Navigate to the page “Snippets” and click on “Actions” and “Add Snippet” to add a snippet.
1. Fill out the required fields and click “Add Snippet” to save the Snippet.

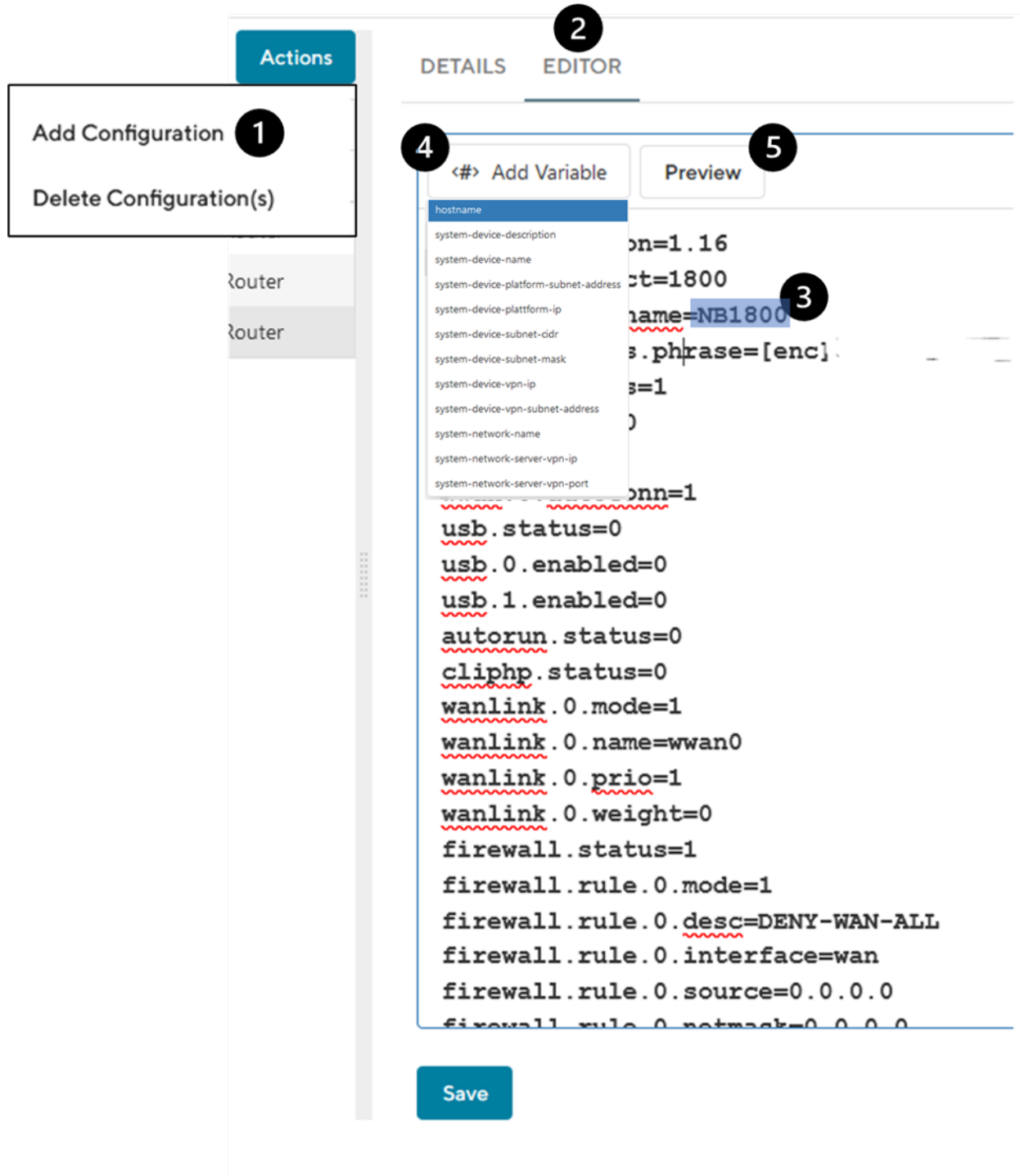


Fig. 1.47: Variables Configuration Editor

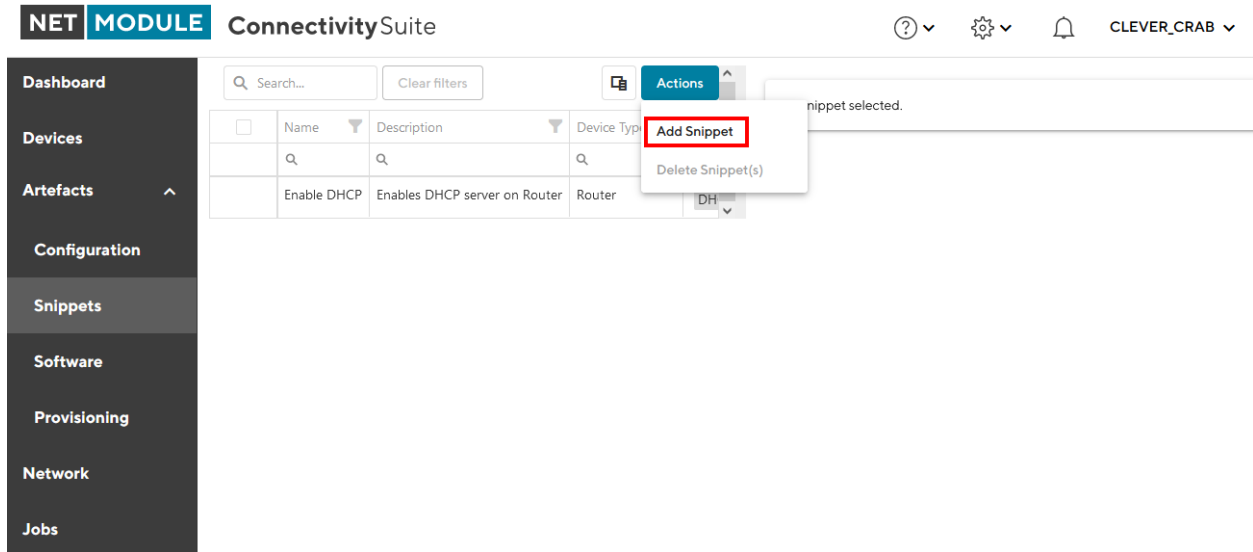


Fig. 1.48: Add Snippet Action

When creating the Snippet following parameters can be set:

| | |
|--------------------|--|
| Name | Name of the Snippet |
| Description | Description of the Snippet to be executed |
| Tag | Tag to identify the Snippet |
| Device Typ | Device type can be a NM switch or router |
| Content | Subset of configuration parameters taken from a user-config.cfg file can be filled in this field |

2. A confirmation message will pop up. The added Snippet will be listed in the Main dialogue box in the table.

Deploying Snippets


See [Section 1.6.3](#) on how to deploy Snippets

1.9.2 Template Device Configurations

Template Device Configurations are complete Device Configurations (in comparison to Snippets as described under [Section 1.9.1](#)) which get patched before a deployment to each Devices needs (certificate, keys etc).

Add Template Device Configuration

1. Navigate to the page “Configuration” and click on “Actions” and “Add Template Device Configuration” to add a configuration.
2. Fill out the required fields, upload the switch configuration file and click “Add” to save the configuration.
3. The added configuration will be listed in the Main dialogue box in the table.
4. Navigate to the page “Devices” and select the switches in the main dialogue Box that are to be configured. Click on “Actions” at the upper right corner of the Main dialogue box and click “Deploy Configuration”.



The image shows a 'Add Snippet' dialog box with a close button (X) in the top right corner. The dialog contains several input fields and a list of tags. The 'Name' field is labeled 'Name *' and contains the text 'Enable USB'. The 'Description' field is empty. The 'Tags' field is labeled 'Tags' and contains a single tag 'USB' with a close button (X). The 'Device Model' field is labeled 'Device Model' and contains four tags: 'NB1810', 'NB2700', 'NB2800', and 'NB2810', each with a close button (X). The 'Config Version' field is labeled 'Config Version *' and contains the text '1.13'. The 'Content' field is labeled 'Content *' and contains the text 'usb.status=1'. At the bottom left of the dialog is a blue button labeled 'Add Snippet'.

Add Snippet

Name *
Enable USB

Description

Tags
USB

Device Model
NB1810 NB2700 NB2800 NB2810

Config Version *
1.13

Content *
usb.status=1

Add Snippet

Fig. 1.49: Add Snippet Dialog

DEVICE DETAILS
HEALTH
CONFIGURATIONS
CONNECTED DEVICES
CERTIFICATE

Configuration History

Name

Created at

Added to provisioning network

29.08.2022

Added to provisioning network

29.08.2022

Before network move

29.08.2022

Added to provisioning network

Description

This configuration was downloaded from the device once it was registered

Created at

29.08.2022 15:14:14

Content

```

config.version=1.16
config.product=3800
network.hostname=NB3800
wwan.0.status=1
wwan.0.card=0
wwan.0.sim=0
wwan.0.number=*99**1#
wwan.0.apn=netmodule.m2m.ch

```

Fig. 1.50: Configuration version

- Select the configuration to be deployed and whether you want to deploy the configuration immediately or if it should be scheduled.
- Confirm the deployment by click “Start deployment”.

When a configuration deployment has started it will be listed as a Job in the Jobs table (see [Section 1.10](#)). Jobs can be scheduled while creating them (see step 7). Therefore following scheduling options are possible:

| | |
|-------------------|---|
| Start Date | The first day on which the Connectivity Suite is going to try to execute the Job, if all conditions are met (time window, day of the week etc.). |
| End Date | The last day on which the Connectivity Suite is going to try to execute the Job, if all conditions are met (time window, day of the week etc.). |
| Days | Offers the possibility to constrain the execution of the Job to specific days of the week. By default, the execution is allowed for all days of the week (the blue color indicates a selected day) |
| Start Time | Offers the possibility to constrain the Job execution to a certain time frame within a day. Only the hour can be specified, higher precision is not supported currently. Allowed values are 0-23, the default value is 0 (midnight). |
| End Time | Offers the possibility to constrain the Job execution to a certain time frame within a day. Only the hour can be specified, higher precision is not supported currently. Allowed values are 1-24, the default value is 24 (midnight). |

Deploying Template Device Configurations

See [Section 1.6.3](#) on how to deploy Template Device Configurations

1.9.3 License File Management

NetModule licenses may enable extra functions on the router. Some licenses are tied to specific hardware components the router must be equipped with. A breakdown of licensed features can be found here: <https://wiki.netmodule.com/faq/licenses> With the corresponding Artefact, such software license files can be deployed to the routers at scale. Doing so, the following steps are to be executed.

Add License Files

1. Navigate to “Licenses” under the “Artefacts” section.
2. Upload one or more license files under Actions “Add License(s)”
 - Single licenses in either .lic or .zip format
 - Multiple licenses in .zip format

Deploy Licenses

There are two ways of how licenses may be deployed. Either starting from the Licenses Artefacts or from device list, where several filtering options are available.

Artefacts

1. Navigate to “Licenses”
2. Select the desired license files to be deployed.
3. Under Actions, select “Deploy License(s)”.
4. Choose “Now” or “Scheduled”, depending on when the execution should happen.
5. Review and Start or Schedule deployment.

Devices

1. Filter & select the desired devices for which a license is to be deployed.
2. Under Actions, select “Deploy License(s)”.
3. Choose “Now” or “Scheduled”, depending on when the execution should happen
4. Review and Start or Schedule deployment.

Note: Only licenses of devices that have been provisioned to the Connectivity Suite can be deployed.

1.9.4 Scripts

NetModule Routers come with a built in Software Development Kit (SDK), which offers a simple and fast way to implement customer-specific functions and applications using arena scripts. These scripts can be managed and deployed via Connectivity Suite.

Note: More information about SDK and Scripting can be found here: <https://wiki.netmodule.com/sdk/sdk>

Add a new Script

Scripts are added to the Connectivity Suite in the same manner as for Configurations, which requires the following steps to be done:

1. Navigate to “Scripts” under the “Artefacts” section.
2. Under “Actions”, select “Add Script”.
3. Complete the corresponding fields.
4. Select “New” and click “Add” for an empty script to be created.

Import existing Scripts

Already existing scripts may be imported in the following way:

1. Navigate to “Scripts” under the “Artefacts” section.
2. Under “Actions”, select “Add Script”.
3. Complete the corresponding fields.
4. Select “Import” and browse the file to be imported.
5. Click “Add” for the script to be imported

Editing Scripts

The detail page of every script consists of three tabs.

| | |
|------------------|--|
| De-tails | Overview of script, which details may be modified |
| Edi-tor | A new script can be composed, or existing and imported scripts may be edited. The editor supports Section 1.8.1 as well as the preview function. |
| Trig-gers | When the script is triggered / started – See details on triggers below |

Configuration & management of Triggers

1. Add new triggers
2. Save entry
3. Discard changes
4. Delete existing triggers

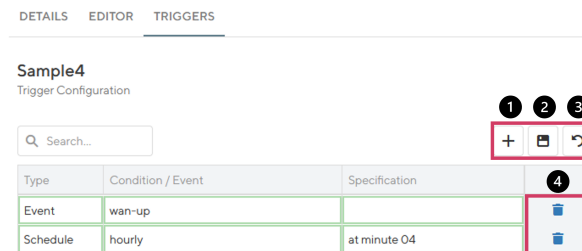


Fig. 1.51: Triggers Configuration

Script Triggers

| Type | Condition /Event | Specification |
|------------------|---|---|
| Event | Select an event from the dropdown menu when the script is triggered | Stays empty |
| Sched-ule | From the dropdown, select the frequency when the script is triggered. E.g. hourly | Enter the corresponding value. E.g. 4, means at 4 mins past the full hour |

Deployment of Scripts

Deploy Scripts

1. Navigate to “Devices”.
2. Select the devices for which a script is to be deployed
3. Under “Actions”, select “Deploy Script”.
4. Select the script to be deployed
5. Review the content of the Script.
6. Choose immediate or scheduled deployment.
7. Review and Start or Schedule deployment.

1.9.5 Software/Firmware

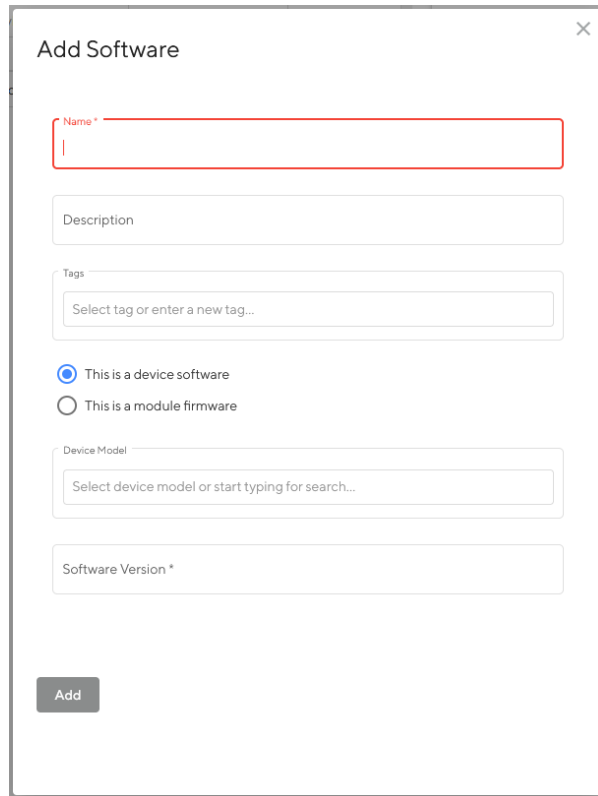
To get the latest software for your router go to <http://netmodule.com/support/downloads.html>

To get the latest firmware for your switch contact Tronteq

Add Software / Firmware

To execute a NRSW Router Software, or a Module-Firmware update, the Soft-/Firmware image needs to be loaded into Connectivity Suite first, before executing the update. Doing so, the following steps are to be taken:

1. Under Artifacts, Actions, select the item “Add Software”.



The screenshot shows a modal dialog box titled "Add Software" with a close button (X) in the top right corner. The dialog contains several input fields and radio buttons. The "Name *" field is highlighted with a red border. Below it is a "Description" field. Then a "Tags" section with a dropdown menu showing "Select tag or enter a new tag...". Below the tags are two radio buttons: "This is a device software" (selected) and "This is a module firmware". Below the radio buttons is a "Device Model" dropdown menu showing "Select device model or start typing for search...". Below that is a "Software Version *" field. At the bottom left is an "Add" button.

Fig. 1.52: Add Software

2. Fill out the required fields
3. Select if this is a Software for the Router or a Module Firmware and click “Add”
4. A confirmation message will pop up. The added Soft-/Firmware will be listed in the software table of the main dialogue box.

Note: It can take a while until the firmware has been uploaded.

| NET MODULE | | ConnectivitySuite | | | |
|-------------------------------------|-----------------------------|--|-------------|---------|-------------------|
| Dashboard | | <input type="text" value="Search..."/> <input type="button" value="Clear filters"/> <input type="button" value="Actions"/> | | | |
| | Name | Description | Device Type | Version | Tags |
| | Tronteq 2.3.0 for 006-130-x | | Unknown | 2.3.0 | Tronteq 006-130-x |
| <input checked="" type="checkbox"/> | NRSW 4.7.100 for NB800 | | Router | 4.7.100 | NB800 NRSW |

Fig. 1.53: Software overview

Deploying Software

See [Section 1.6.3](#) on how to deploy Software / Firmware

1.9.6 Provisioning Configurations

Supported NM router firmware releases

Before connecting a router to the Connectivity Suite ensure that a supported firmware is running on the device. The Connectivity Suite guarantees support for all supported NM router firmware releases. These can be checked at the following link: [https://wiki.netmodule.com/documentation/releases?s\[{}\]=nrsw](https://wiki.netmodule.com/documentation/releases?s[{}]=nrsw)

This chapter describes how to create the configuration required by the NM router to connect to the Connectivity Suite for the first time.

Steps to be executed on the web interface of the router:

1. Only required if the router is in factory state: Go to the Web Manager of your NM router and set an administrator password.
2. Only required if the router is in factory state: Set the NM router to WAN mode and change the firewall settings accordingly.
3. **Configure the router accordingly so that it can establish a connection to the Connectivity Suite Server.**
 - 3.1. Open TCP port 22, for SSH access through VPN tunnel from CS
 - 3.2. SSH Server listening on port 22
 - 3.3. root user with SSH access
4. Download the current configuration (Provisioning Configuration) from the NM router via the web interface.

Steps to be executed on the web interface of the Connectivity Suite:

1. For the initial NM router provisioning navigate to the page “Provisioning” on the Dashboard. Click on “Actions” at the upper right corner of the Main dialogue box and Click “Create Provisioning Configuration”.
2. Fill out the required fields and Import the configuration file that has been downloaded from the NM router by click on “Browse...”.

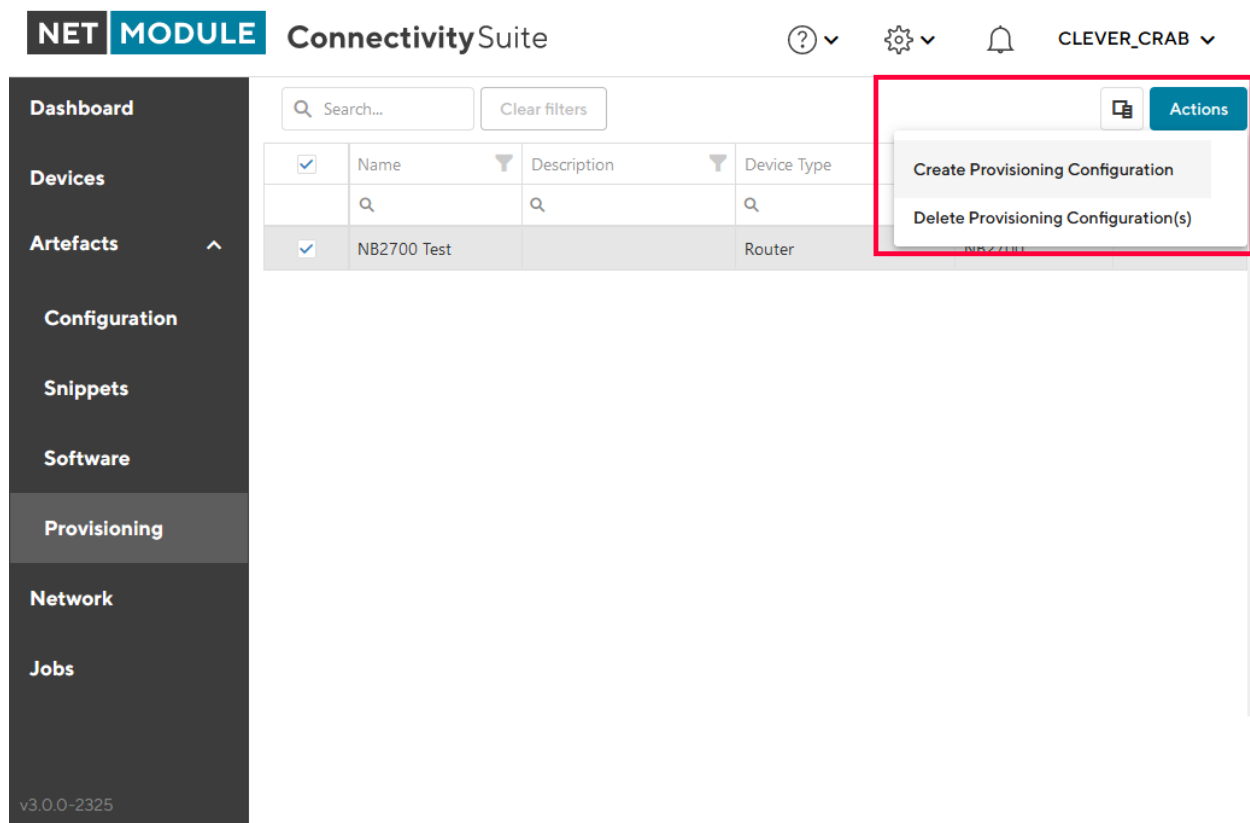
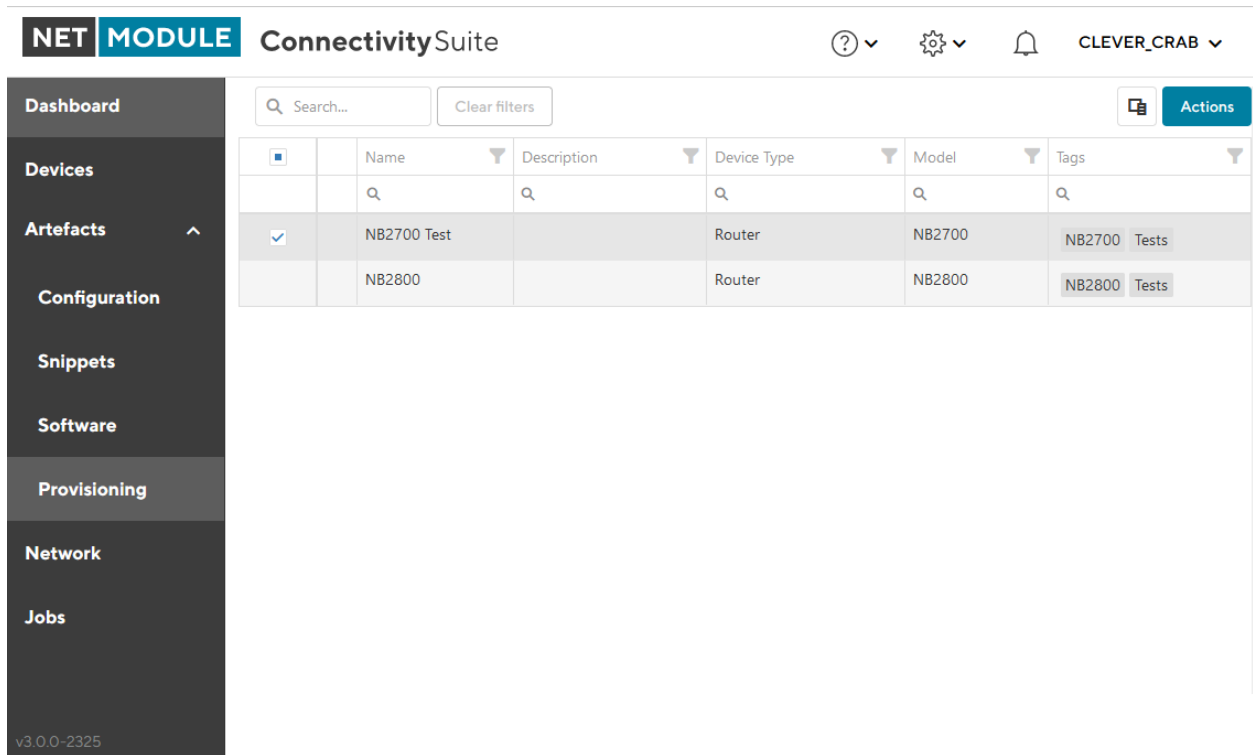


Fig. 1.54: Create Provisioning Configuration

- Click “Generate Provisioning Configuration” to upload the configuration to the Connectivity Suite. The uploaded configuration will be shown in the Main dialogue box in the table:



The screenshot shows the 'ConnectivitySuite' interface. On the left is a dark sidebar with navigation links: Dashboard, Devices, Artefacts (expanded), Configuration, Snippets, Software, Provisioning, Network, and Jobs. The main content area has a search bar and a table of provisioning configurations. The table has columns: Name, Description, Device Type, Model, and Tags. Two rows are shown: 'NB2700 Test' and 'NB2800', both with 'Router' as the Device Type. The 'NB2700 Test' row is selected, indicated by a blue checkmark in the first column. The 'Tags' column shows 'NB2700 Tests' and 'NB2800 Tests'.

| | Name | Description | Device Type | Model | Tags |
|-------------------------------------|-------------|-------------|-------------|--------|--------------|
| <input checked="" type="checkbox"/> | NB2700 Test | | Router | NB2700 | NB2700 Tests |
| | NB2800 | | Router | NB2800 | NB2800 Tests |

Fig. 1.55: Provisioning overview

Note: The same provisioning configuration can be used for several Devices as long as they belong to the same Device Model

1.10 Jobs

An overview table featuring all Jobs is available on the *Jobs* page, facilitating the management of pending and failed Jobs. In the list part of the page, you can find all jobs, complete with their status and overall progress. Upon selecting a specific job from the list, the corresponding job details are presented in the detail part of the page (see [Fig. 1.56](#)).

NET

MODULE

ConnectivitySuite

Dashboard

Devices

Artefacts

Configuration

Snippets

Scripts

Licenses

Software

Provisioning

Network

Jobs

Views: List Details Both Split horizontal

Quick filters: Succeeded Partially Succeeded Failed Running Paused Scheduled System Job

Q Search...

Clear filters

Actions

| | Name | State | Type | Schedule Type | Last Triggered | Created At | Tags | System Job | Tasks | Expires At |
|---|---|-------|---------------------|---------------|---------------------|---------------------|------|------------|-------|---------------------|
| | Q | Q | Q | Q | Q | Q 06.03.202... | Q | (All) | Q | Q |
| | Device info update job for ES3300 | ✓ | Device Info Update | FireAndForget | 06.03.2024 16:11:30 | 06.03.2024 16:11:28 | | | 1/1 | 06.03.2024 16:41:28 |
| | Device info update job for ticket-automat | ✓ | Device Info Update | FireAndForget | 06.03.2024 16:11:31 | 06.03.2024 16:11:30 | | | 1/1 | 06.03.2024 16:41:30 |
| ✓ | NB800 4.8.0.102 | 🚶 | Software Deployment | Scheduled | 06.03.2024 16:15:13 | 06.03.2024 16:11:24 | | | 0/1 | 10.03.2024 23:59:59 |

Fig. 1.56: Jobs overview

1.10.1 Job Details

In the *Detail* part of the page the Job Details are displayed:

| | |
|------------------|---|
| Job | Shows the name and the type of the Job. |
| State | Shows the state of a Job, the progress of its tasks and the Schedule. The different states are described in Section 1.10.3 and the Schedule Types in Section 1.10.2 . |
| Job Tasks | Shows each Task, often associated with a specific device, the Tasks State, when it was last triggered, the current Step (if applicable) and the progress of its steps (if applicable). The different states are described in Section 1.10.4 . |
| Steps | Certain tasks consist of multiple steps. Those steps indicate where a task might got stuck and how to manually fix an issue with the device. Steps have a Status and they have <i>Started At</i> , <i>Skipped At</i> and <i>Completed At</i> dates indicating their progress. |

1.10.2 Job schedules

Fire and forget

The Job will be executed immediately after it was created. If it fails, it will retry every 5 minutes until the Expires At date is reached. Fire and forget Jobs expire after 30min.

Scheduled

The Job will be executed during the specified *date range* under the consideration of the specified *time window* and *weekdays*. If the Job fails, it will retry every 5minutes during those windows until the end of the specified date range (Expires at).

JOB DETAILS

Job
Name
Certificate renewal job for devices of network Real Devices 1
Type
Certificate Renewal

State
State
Partially Succeeded
Tasks

1/2

Schedule
From 23.01.2024 to 22.02.2024 between 1:00 and 1:00 on Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday.

Tags

Select tag or enter a new tag...

Job Tasks

Q Search...

| Device Name | Task State | Last Triggered | Current Step | Steps |
|---|------------|---------------------|---|------------|
| Q | Q | Q | Q | |
| cs-nb1800-1 | ✓ | 26.01.2024 12:00:15 | | 4 / 4 |
| | | | | |
| Step | | Status | Started - Completed | Skipped At |
| Generate a new certificate | | ✓ | 23.01.2024 03:00:02 - 23.01.2024 03:00:04 | |
| Deploy the new certificate | | ✓ | 26.01.2024 12:00:15 - 26.01.2024 12:02:52 | |
| Wait for device to go online with new certificate | | ✓ | 26.01.2024 12:02:52 - 26.01.2024 12:03:17 | |
| Revoke the old certificate | | ✓ | 26.01.2024 12:03:17 - 26.01.2024 12:03:18 | |
| | | | | |
| cs-nb2700-1 | ✗ | 22.02.2024 12:25:09 | Deploy the new certificate | 1 / 4 |
| | | | | |
| Step | | Status | Started - Completed | Skipped At |
| Generate a new certificate | | ✓ | 23.01.2024 03:00:02 - 23.01.2024 03:00:03 | |
| Deploy the new certificate | | 🚶 | 22.02.2024 12:25:10 | |
| Wait for device to go online with new certificate | | 🕒 | | |
| Revoke the old certificate | | 🕒 | | |

Fig. 1.57: Job Details

Select execution time

☐ Now

☒ Scheduled

Select a date range
13.3.2024 - 31.3.2024

Weekdays this job is allowed to run

M

T

W

T

F

S

S

Time range this job is allowed to run
(in your local time zone)

Start Time

End Time

+

+

23

:

00

03

:

00

-

-

Fig. 1.58: Jobs Schedule

1.10.3 Job States

Indicates in which state a **Job** is, between creation and completion.

| Job Status | Description |
|---------------------|---|
| Scheduled | Pending for execution. Typically due to the start date has not been reached yet or the execution time window is currently closed (the current time is not between start and end time and/or the date of the week does not allow the execution). |
| Running | Job is being executed. |
| Paused | The paused state typically occurs when the schedule window has closed. |
| Succeeded | Successfully completed with all tasks processed as expected. |
| Failed | Due to an error or failure the job was not completed. |
| Partially Succeeded | Not all of the tasks belonging to a job were completed successfully processed. |
| Cancelled Manually | Manually cancelled before completion. |
| Replaced | A different Job has replaced the current Job. |
| Unknown | The state of the Job is not known or has not been set. |

1.10.4 Task States

Represents the various states a **Job Task** can have during its lifecycle.

| Status | Description |
|-------------|--|
| Scheduled | Scheduled to run at a specified time. |
| Running | The Job Task is currently in progress. |
| Rescheduled | Rescheduled to run at a different time. |
| Succeeded | Completed successfully. |
| Failed | An error was encountered during execution, therefore it not complete successfully. |
| Cancelled | It was cancelled before it could complete. |

1.10.5 System Jobs

The system generates various Jobs that are automatically excluded from the Jobs List by default. These jobs are created to guarantee the proper functioning of the Connectivity Suite, such as updating Device Certificates or retrieving the most recent Device Information.

1.11 Remote Access

Connectivity Suite offers two options for remote access to Devices (incl. end/child-devices).

- **Web Proxy Access via Browser** The Web Interface of Devices can be reached through a Web Proxy. In addition there you can enable Proxy Records [Section 1.11.1](#), which allow a static and direct web access to devices as well as to end-devices.
- **Service Access via VPN** As per the chapter [Section 1.11.2](#), a full network service access allows managing devices and end-devices.

1.11.1 Device access via Web Proxy

The Connectivity Suite web proxy enables access to the web interface of the Child Devices to the Connectivity Suite OpenVPN servers without having to run an OpenVPN client locally.

Default Option (basic)

Accessing the web interface of the devices click on the “Open Web Interface” button in the Device Details (see [Fig. 1.59](#)).

The screenshot shows the Connectivity Suite interface. On the left is a sidebar with navigation options: Dashboard, Devices, Artifacts, Configuration, Snippets, Software, Provisioning, Network, and Jobs. The main area displays a table of devices. The 'MockRouter0001' device is selected, and its details are shown on the right. The 'Open Web Interface' button is highlighted with a red box.

| Views: | List | Details | Both | Split horizontal | | |
|--|---------------|----------------|----------------|------------------|----------|-------|
| Quick filters: | Online | Offline | Provisioning | | | |
| Search... | Clear filters | | | Actions | | |
| Name | Description | Network | Serial | MAC Address | Software | Model |
| <input checked="" type="checkbox"/> MockRouter0001 | EMEA | MockRouter0001 | MOCKROUTER0001 | 4.0.1.110 | NB800 | |
| <input checked="" type="checkbox"/> MockRouter0002 | Provisioning | MockRouter0002 | MOCKROUTER0002 | 4.0.1.110 | NB800 | |
| <input checked="" type="checkbox"/> MockRouter0003 | EMEA | MockRouter0003 | MOCKROUTER0003 | 4.0.1.110 | NB800 | |
| <input checked="" type="checkbox"/> MockRouter0004 | Provisioning | MockRouter0004 | MOCKROUTER0004 | 4.0.1.110 | NB800 | |
| <input checked="" type="checkbox"/> MockRouter0005 | Provisioning | MockRouter0005 | MOCKROUTER0005 | 4.0.1.110 | NB800 | |
| <input checked="" type="checkbox"/> MockRouter0006 | Provisioning | MockRouter0006 | MOCKROUTER0006 | 4.0.1.110 | NB800 | |
| <input checked="" type="checkbox"/> MockRouter0007 | Provisioning | MockRouter0007 | MOCKROUTER0007 | 4.0.1.110 | NB800 | |
| <input checked="" type="checkbox"/> MockRouter0008 | Provisioning | MockRouter0008 | MOCKROUTER0008 | 4.0.1.110 | NB800 | |
| <input checked="" type="checkbox"/> MockRouter0009 | Provisioning | MockRouter0009 | MOCKROUTER0009 | 4.0.1.110 | NB800 | |
| <input checked="" type="checkbox"/> MockRouter0010 | Provisioning | MockRouter0010 | MOCKROUTER0010 | 4.0.1.110 | NB800 | |

Device Details for MockRouter0001:

- Device:** Name: MockRouter0001, Description: (empty)
- Hardware:** Device Type: Router, Model: NB800, Serial Number: MockRouter0001, MAC Address: MOCKROUTER0001
- Software:** Version: 4.0.1.110
- OpenVPN Network:** Network: EMEA, IP Address in VPN Network: 10.0.0.1, IP Address in Platform Network: 10.236.0.1
- State:** State: Online, Since: 29.08.2022 16:03:07, For: vor 1 Stunde
- Tags:** Select tag or enter a new tag...

Fig. 1.59: Open web interface via web proxy

Note: Make sure that you have added a **devices** CNAME DNS record. See (see [Section 1.2.3](#)) for more details.

Proxy Records Option (advanced)

Besides the basic option of accessing devices and end-devices one at a time, the feature **Proxy Records** can be configured. This offers two benefits:

- Multiple sessions open at once by using the following url pattern `xxx-xxx-xxx-xxx.devices.mycs.com`, e.g. `10-240-3-45.devices.mycs.com`.
- Proxy Records mapping an *Alias* to a specific *IP* and *Port* of any Device, such as a CCTV camera, e.g. `camera-1-bus-23.devices.mycs.com`.

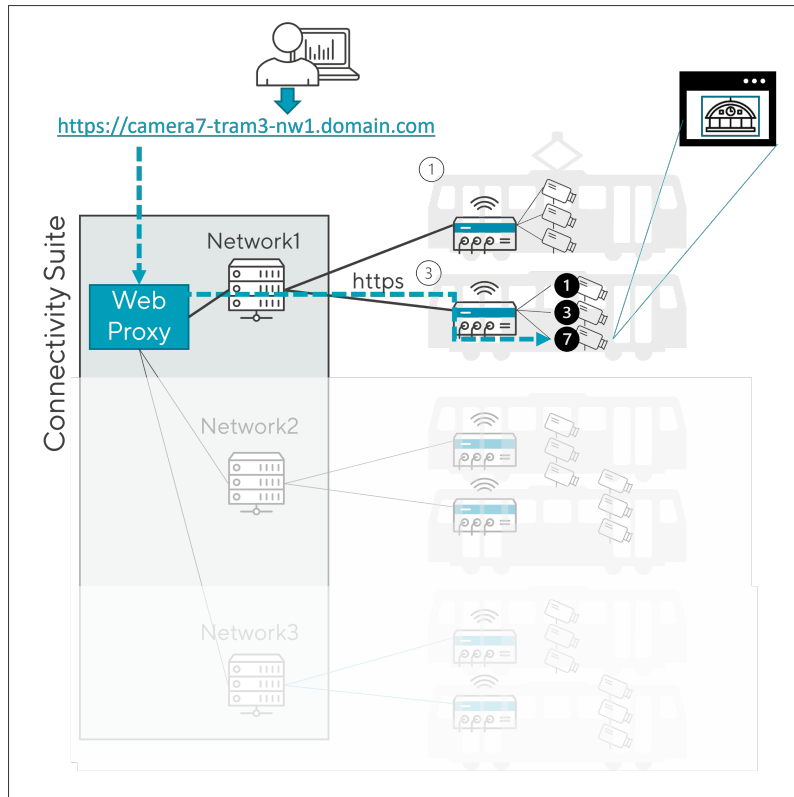


Fig. 1.60: Proxy Records Principle

Enable Proxy Records

You must use the `cs-cmd` tool to enable or disable the Proxy Records feature. This can be done through the command line interface by navigating to the `> Configure Proxy Records Feature` menu and setting the status to `> enable`.

Depending on which HTTPS CA is being used, the corresponding configurations need to be made.

- **LetsEncrypt**

- Add CNAME according to instructions provided in `cs-cmd`.
- Configure the DNS challenge
- Set the Provider Code and Variables, corresponding to [Traefik Let's Encrypt Documentation](#) `> set provider / > edit provider`
- Environment Variables `> add variable / > edit variable / > delete variable`

- Save settings with `> save` and `exit`
- **Own HTTPS Certificates**
 - Add CNAME according to instructions
 - Generate new certificates including the given wildcard SAN
 - Replace the certificates
- **Generated Certificates**
 - Add CNAME according to instructions

Configure Proxy Records

Proxy Records are managed under Global Settings. For each Device or End-Device that needs to be reached through a custom DNS record, a Proxy Record is required, as illustrated in the image below. Each record covers only one TCP Port, so two or more records are required if multiple targets on a device using different ports need to be reached.

Settings

| FEATURES DEVICE FILTER CERTIFICATES VARIABLES LICENSES PROXY | | | | | | | |
|---|----------------|-------------|----------|--------|---|--------|--|
| Proxy Records | | | | | | | |
| <div> <input type="text" value="Search..."/> <div> 1 2 3 </div> <div> + ⌂ ↺ </div> </div> | | | | | | | |
| Alias | Target Address | Target Port | Network | Device | Link | Delete | |
| camera7-tram3-nw1 | 10.236.0.154 | 443 | Network1 | Tram3 | https://camera7-tram3-nw1.domain.com | | |
| camera3-tram3-nw1 | 10.236.0.195 | 443 | Network1 | Tram3 | https://camera3-tram3-nw1.domain.com | | |

Fig. 1.61: Proxy Records Configuration

Table Controls

1. Create a new Proxy Record
2. Save entry / entries
3. Update table

Note: Changes may take up to 5 Minutes to take effect.

Explanation & meaning of table entries:

| Column | Explanation | Example |
|----------------|---|-------------------|
| Alias | Alias name, used for accessing the corresponding device via DNS through HTTPS | camera7-tram3-nw1 |
| Target Address | Specify the target IP of the corresponding device or end-device | 10.236.1.38 |
| Target Port | Specify the target port of the corresponding device or end-device | 443 |
| Network | Corresponding VPN Network, owning the matched IP Address Block | Network1 |
| Device | Corresponding Device, owning the matched IP Address Block | tram3 |

1. Proxy Records are not updated automatically, if a router gets a different address (e.g., by moving to another network), the corresponding proxy records will no longer work or must be updated manually (Target Address).

2. For proxy records that point to a connected device, we recommend configuring the router to assign a fixed IP to the connected device. Otherwise, the proxy record can also become invalid suddenly if the connected device receives a different IP.

1.11.2 Device access via OpenVPN client

To access the Devices, Connectivity Suite provides OpenVPN to access. A VPN connection to the Provisioning, the Backend or any custom VPN Network Server must be established. This means the user needs to run an OpenVPN client. The configuration and certificates needed for the VPN connection can be downloaded from the Connectivity Suite via the Service Access function.

Installing OpenVPN Client

The OpenVPN client to access the devices can be downloaded from <https://openvpn.net/community-downloads/>.

Warning: While the VPN Connect client often works, make sure you are using the **Community Edition** of the OpenVPN client. The commercial version of the OpenVPN client is not officially supported by the Connectivity Suite.

OpenVPN access

There are three types of Service Access:

1. VPN Network: The user can access any Device within the VPN Network by using the VPN Address of the Device. This is helpful if the user shall access only Devices of a specific VPN Network.
2. Platform Network: The user can access any Device within the Platform Network by using the Platform Address of the Device. This is helpful if the user shall access Devices of different VPN Networks.
3. Provisioning Network: The user can access any Device within the Provisioning Network by using the Provisioning Address of the Device.
4. Navigate to the page “Network” of the Connectivity Suite. Select the Network where the required Device is assigned.
5. Click on “Download OpenVPN client configuration” at the Detail dialogue box to download the OpenVPN client configuration.
3. Start the OpenVPN client on your client pc and upload the downloaded file from step 1 into the OpenVPN client to establish a connection with the Connectivity Suite.
4. After the connection has been established Navigate to the page “Devices” and select the required Device in the main dialogue table.
5. Use the IP-address shown in the Detail dialogue box to access the Device.

NET MODULE ConnectivitySuite ? ⚙️ 🔔 CLEVER_CRAB

Dashboard

Devices

Artefacts

Configuration

Snippets

Software

Provisioning

Network

Jobs

Quick filters: Online Offline

Search... Clear filters

Actions

| State | Name | Description |
|-------|--------------|--|
| ✓ | Backend | Network for VPN servers to communicate with the Backend VPN Server |
| ✓ | Provisioning | Network for newly added devices via Provisioning |
| ✓ | EMEA | Europe, Middle East & Africa |
| ✓ | APAC | Asia & Pacific |
| ✓ | NA | North America |
| ✓ | SA | South America |

Network Server

Name: APAC

Description: Asia & Pacific

OpenVPN Network

Shortname: test2

VPN Network: 10.0.0.0/18

VPN Network in Platform Network: 10.224.64.0/18

Port: 1202

Routers and End Devices

Network Type: Large

Max number of routers: 16384

Number of routers left: 16384

End devices per router: 256

Service Access

[Download OpenVPN client configuration](#)

State

State: Online

Since: For

Tags

APAC Tokyo

Fig. 1.62: Download VPN config

NET MODULE ConnectivitySuite ? ⚙️ 🔔 COOL_DRAGON

Dashboard

Devices

Artefacts

Configuration

Snippets

Software

Provisioning

Network

Jobs

Views: List Details Both Split horizontal

Quick filters: Online Offline Provisioning

Search... Clear filters

Actions

| Name | Description | Network | Serial | MAC Address | Software | Model |
|----------------|--------------|----------------|----------------|-------------|----------|-------|
| MockRouter0001 | EMEA | MockRouter0001 | MOCKROUTER0001 | 4.0.1.110 | NB800 | |
| MockRouter0002 | Provisioning | MockRouter0002 | MOCKROUTER0002 | 4.0.1.110 | NB800 | |
| MockRouter0004 | EMEA | MockRouter0004 | MOCKROUTER0004 | 4.0.1.110 | NB800 | |
| MockRouter0003 | EMEA | MockRouter0003 | MOCKROUTER0003 | 4.0.1.110 | NB800 | |
| MockRouter0005 | Provisioning | MockRouter0005 | MOCKROUTER0005 | 4.0.1.110 | NB800 | |
| MockRouter0006 | Provisioning | MockRouter0006 | MOCKROUTER0006 | 4.0.1.110 | NB800 | |
| MockRouter0007 | Provisioning | MockRouter0007 | MOCKROUTER0007 | 4.0.1.110 | NB800 | |
| MockRouter0009 | Provisioning | MockRouter0009 | MOCKROUTER0009 | 4.0.1.110 | NB800 | |
| MockRouter0008 | Provisioning | MockRouter0008 | MOCKROUTER0008 | 4.0.1.110 | NB800 | |
| MockRouter0010 | Provisioning | MockRouter0010 | MOCKROUTER0010 | 4.0.1.110 | NB800 | |

DEVICE DETAILS HEALTH CONFIGURATIONS CONNECTED DEVICES CERTIFICATE

Device

Name: MockRouter0001

Description:

Save changes

[Open Web Interface](#)

Hardware

Device Type: Router

Model: NB800

Serial Number: MockRouter0001

MAC Address: MOCKROUTER0001

Software

Version: 4.0.1.110

OpenVPN Network

Network: EMEA

IP Address in VPN Network: 10.0.0.1

IP Address in Platform Network: 10.236.0.1

State

State: Online

Since: 29.08.2022 16:03:07

For: vor 1 Stunde

Tags

Select tag or enter a new tag...

Fig. 1.63: Open web interface

1.11.3 Child Device Remote Access

To access Child Devices the router must perform a network NAT. In order to carry out a NAT, following router settings are necessary:

1. Open the web interface of the router, open the Firewall/Inbound Rules page and create a new rule
2. Select “network” for the mapping to execute a network NAT.
3. Select the interface. The interface must be the OpenVPN tunnel which is used to connect to the Connectivity Suite.
4. Add the Device VPN Network Block Address. If its unclear what the Device VPN Network Block Address ist check chapter [Section 1.13](#).
5. Add the LAN as Redirect address/netmask and apply the settings.

HOME INTERFACES ROUTING **FIREWALL** VPN SERVICES SYSTEM

Firewall
Administration
Address / Port Groups
Filtering Rules

NAPT
Masquerading
Inbound Rules 1
Outbound Rules

Edit NAPT Rule For Inbound Packets

Description: 1-to-1-NAT 2

Map: ☐ host ☒ network 2 ☐ port range

Packet Selection 3

Incoming interface: TUN1 3

Source: ☒ ANY ☐ specify 3

Target address: 10.0.0.0 4

Target netmask: 255.255.255.0 4

Redirect to

Redirect address: 172.16.0.0 5

Redirect netmask: 255.255.255.0 5

Apply Cancel

2021-08-18 15:28 job 0 is already running

NB2800 NetModule Router
Hostname NB2800
Software Version 4.3.0.107
© 2004-2020, NetModule AG

Fig. 1.64: NAT Settings NetModule Router

6. Select now the router in the Device Liste and open the tab Child Device in the Detail dialogue box and click on the “Scan again” button. The Child Devices are now displayed in the table.

| DEVICE DETAILS | HEALTH | CONFIGURATIONS | CONNECTED DEVICES | CERTIFICATE | VARIABLES | LOGS |
|--|-------------|----------------|-------------------|------------------|-------------|------|
| Name | MAC Address | LAN Address | VPN Address | Platform Address | Description | |
| No connected devices found on this router. | | | | | | |
| <div> Scan again 6. </div> | | | | | | |

Fig. 1.65: End Devices View Connectivity Suite

1.12 Network architecture

The Connectivity Suite requires two Network Address Blocks that do not overlap with each other or the existing company network address blocks. The Network Address Blocks:

- Core Address Block: must be a /20 network (4'096 addresses) used for Connectivity Suite internal services
- Platform Address block: Can be defined by the user and is used to assign each Device a platform wide unique IP-address. It can be roughly estimated like this:

Maximum number of Devices X average number of End Devices behind a single Device. For example, a /16 network (65'536 addresses) can address 4096 Parent Devices with 16 Child Devices each or 2048 routers with 32 Child Devices each.

1.12.1 System architecture IP overview

1.12.2 Setting the number of VPN Networks

During the installation the user must define how many VPN networks he wants to create and how many Devices he wants to assign to a VPN network. Depending on the use case, this can be very different. See below two examples of different use cases (see Fig. 1.3):

Example 1: A user who wants to manage all devices in one VPN network would choose the fragmentation so that only one VPN Network is created, but this VPN network can contain a large number of Devices.

Example 2: A user who, for example, has several customers and creates one VPN Network per customer would probably want to create many VPN Networks, but the VPN Networks only contain a small number of Devices.

To ensure flexibility the user can fragment the Platform Address Block during the installation according to his use case.

1-to-1 NAT on VPN Networks and Routers

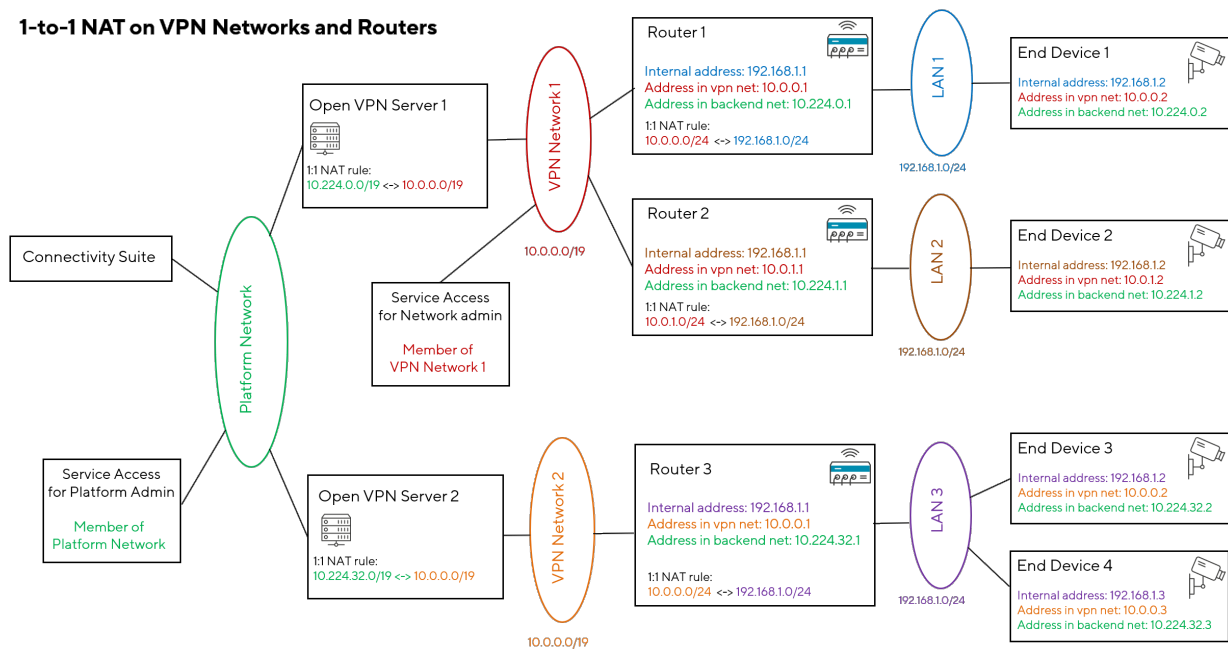


Fig. 1.66: Network Architecture

VPN Subnet Pools

For various reasons (network fragmentation, routing complexity), it would be impractical to set the size for each VPN Network separately. Instead, different types of VPN Subnet Pools can be defined. three layouts:

Layout 1: One VPN Subnet Pool

The whole address space of the Platform Address Block is evenly distributed among the VPN Network Address Blocks, resulting in one VPN Subnet Pool:

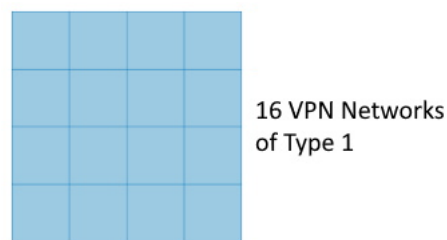


Fig. 1.67: Network type 1

Layout 2: Two VPN Subnet Pools

The address space of the Platform Address Block is split in two halves, one for each VPN Subnet Pool type. Each of these halves' address space is evenly distributed among the VPN Network Address Blocks of the respective type, resulting in two VPN Subnet Pools:

Layout 3: Three VPN Subnet Pools

The Platform Address Block space of the Home Network is split into three parts, one for each VPN Subnet Pool type. One part contains half of the Platform Address Block space, the other two parts a quarter of the Platform Address Block

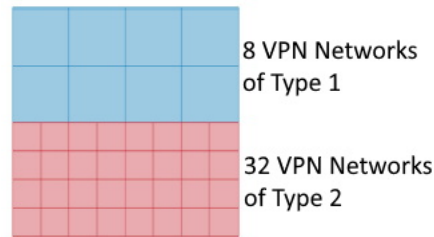


Fig. 1.68: Network type 2

space each. Each of these parts Platform Address Block space is evenly distributed among the VPN Network Address Blocks of the respective type, resulting in three VPN Subnet Pools:

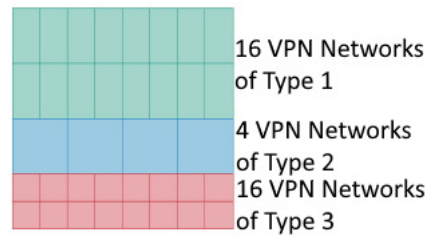


Fig. 1.69: Network type 3

Configure the VPN Subnet Pools

Once a layout for the Platform Address Block has been chosen, the VPN Network Address Block types must be configured. Depending on the layout, there are one, two or three of them.

For each VPN Network Address Block type, the following properties must be specified:

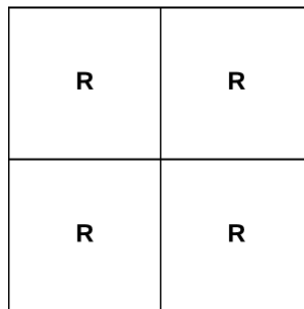
- A name to identify the VPN Network Address Block type in the UI.
- The size (number of IP addresses) of a VPN Network Address Block of this type. As the size of the relevant VPN Subnet Pool is fixed, the larger the size of a VPN Network Address Block type is, the less VPN Network Address Blocks of this type will be available. As an example, the [Fig. 1.69](#) shows that the same VPN Subnet Pool size can be distributed among 4 VPN Network Address Blocks of type 2 or 16 VPN Network Address Blocks of type 3.
- The default network specifies the VPN Network Address Block of a VPN Network of this type.
- The default number of Child Devices per router is explained in chapter [Section 1.12.2](#).
- The default maximum number of concurrent Service Access users accessing a single VPN Network of this type.

Setting the number of Child Devices

As a VPN Network Address Block has a fixed amount of IP addresses, the less Child Device addresses are needed, the more Parent Devices can be attached to that VPN Network and vice versa. If one doesn't need to access any Child Device at all, then each address of the VPN Network Address Block can be assigned to a Parent Device.

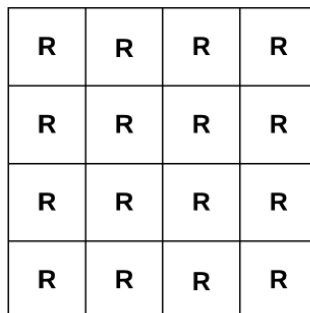
It would be impractical to set the amount of Child Device addresses for each Parent Device individually. Instead, this amount is configured when a new VPN Network is created (see chapter [Section 1.4.1](#)). All routers assigned to the same VPN Network share the same amount of accessible Child Devices.

As an illustration, this figure shows two VPN Network Address Blocks of the same size (i.e. they are of the same VPN Network Address Block type), but with a different amount of Child Devices per Parent Device:



Few routers with many End Devices each

Fig. 1.70: Few routers with many End Devices each per VPN Network Address Block



Many routers with few End Devices each

Fig. 1.71: Many routers with few End Devices each per VPN Network Address Block

1.13 Child Device Access

1.13.1 Overview

Accessing Child Devices by utilizing Connectivity Suite can be done in two different ways.

- Network Address Translation (NAT) on Parent Device
- Custom Routes on Parent Device

Given by the network architecture, Connectivity Suite, the Parent Device and the Child Device reside in different IP Networks. In order to access (end)devices, located in Local Area Networks behind routers (as per Fig. 1.72), either a NAT Table or Custom Routes are required to be setup. (see Fig. 1.72).

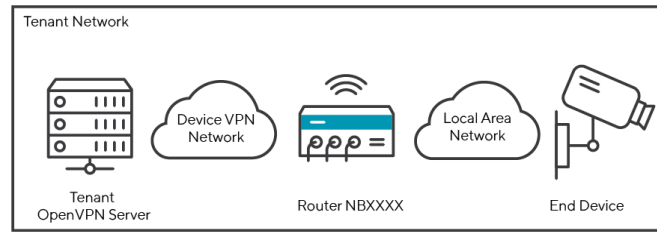


Fig. 1.72: Network Setup Devices and Connectivity Suite

1.13.2 Network Address Translation (NAT)

To access Child Devices, such as CCTV Cameras, WiFi Access Points, etc., the Device VPN Network address needs a Network Address Translation (NAT) to the Local Area Network address. For example, the Device VPN Network 10.0.0.0/24 is translated into the Local Area Network 172.16.0.0/24, as per the illustration in Fig. 1.73.

Note: The Subnetmasks of both, VPN Network and the Local Area Network, have to be identical in order for the NAT to work.

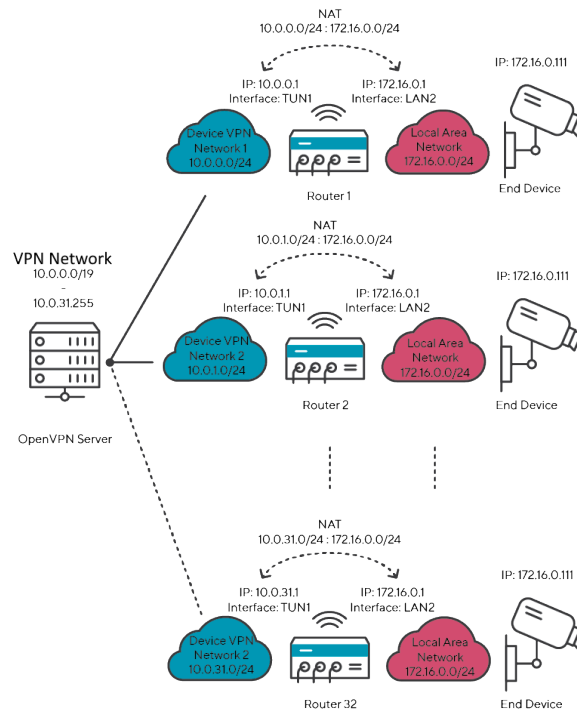


Fig. 1.73: Network Setup in Network Network

NAT Example Use Case

Network Architecture:

- VPN Network using an IP Address Block of /19
- Device VPN Networks using IP Subnetmasks of /24
- Local Area Networks using the same IP Subnetmask size of /24
- The Child Device is given the IP address of 172.16.0.111
- A Network NAT from LAN (17.0.0.0/24) to the Device VPN Network (10.0.0.0/24) is setup

Benchmark Data / Limitations of NAT Example Use Case:

- Max. 32 routers can be connected to a VPN Network
- Max. 256 Child Devices that may be connected to a router

Router Settings for NAT

In order to carry out a NAT, various steps are necessary which are explained in this chapter [Section 1.11.3](#)

1.13.3 Custom Routes

For the same purpose of setting up direct access to Child Devices, Custom IP Routes may be setup as an alternative to NAT or on top of it. The working principle of Custom Routes is depicted in the illustration [Fig. 1.74](#) below. In contrast to a NAT based Network Design, direct Routes require the LAN Addressing to be unique within a VPN Network. Custom Routes are configured on top of other Routes, such as those required by the System of Connectivity Suite. Furthermore Custom Routes can be configured on a “as needed” basis and do not require the entire system to be configured with them.

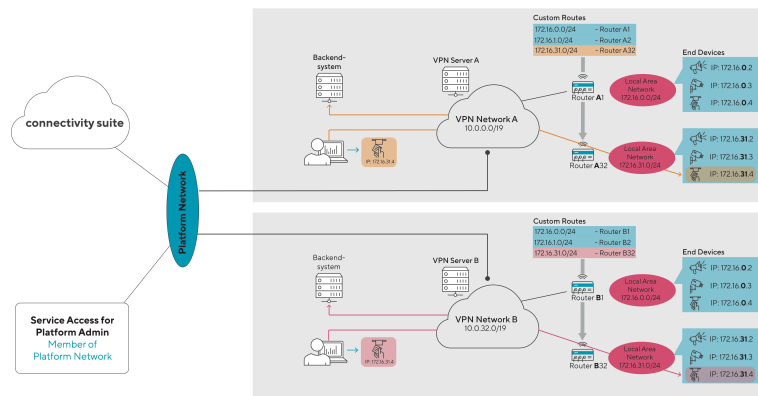


Fig. 1.74: Custom Routes Principle

Configuration

Enabling custom routes, requires the feature to be switched on under the general settings. In a second step, the effective custom routes are to be configured per device under the device details tab.

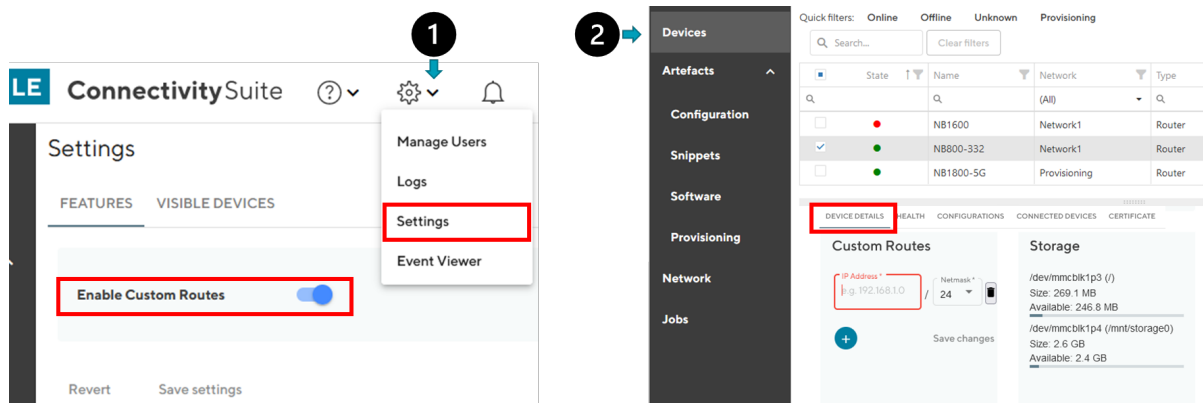


Fig. 1.75: Enabling of Custom Routes

1.14 User Traffic

By enabling and configuring the User Traffic feature, the Connectivity Suite acts as a router between the (end) devices and the customer's backend systems. This allows for instance to connect a ticket vending machine to an accounting application via the VPN infrastructure operated by the Connectivity Suite. This is achieved by additional rules being pushed to the routers, so that in addition to the device management traffic, also specific User Traffic is routed over the same VPN tunnel/infrastructure.

User Traffic must initially be enabled in the Command Line Tool; further settings for routing and masquerading can then be configured through the CS UI/API.

1.14.1 Enabling User Traffic

The User Traffic feature must first be enabled in the Command Line Tool (cs-cmd), by selecting "Configure User Traffic Feature".

By doing so, the firewall on the CS server is set to allow incoming traffic destined to the Platform Network.

Apart from the configuration in Connectivity Suite, corresponding routes in the Backendsystems are required, pointing to the CS Platform Network.

1.14.2 Traffic from the company network to routers and end devices

By following the steps above, the routers are accessible from the company network.

Accessing end devices behind the routers, NAT rules on the routers are required (see [Section 1.14.4](#) below).

Routers and end devices are reachable via their platform address.

1.14.3 Traffic from routers and end devices to company network

Which traffic to be sent through the VPN infrastructure, originating from routers and end devices & destined to the company network, is configured as follows:

- **Routing:** which traffic to be routed through CS to company network
- **Masquerading:** how the source IP address of user-traffic is formed

Reminder: For end devices to access the company network, NAT rules on the routers are required (see [Section 1.14.4](#) below).

Routing

The logic which traffic is to be sent through the CS VPN infrastructure is managed by routes on the routers itself. These routes are pushed by CS, according to the setting below.

| | |
|--------------------|---|
| None | No routes are pushed to the router. The device's traffic is routed to its existing default gateway. |
| None Except | Only traffic destined for specific networks is routed through the CS. All other traffic is routed to the device's existing default gateway. |
| All | All traffic is routed through the CS, i.e. the CS acts as the device's default gateway. |

The routing options can be managed on platform level as well as on individual VPN Networks.

Masquerading

Traffic originating from routers and end devices, destined to a backend network may have one of the following source IP addresses:

- device's platform address, if the source address is **not** masqueraded
- CS server IP address, if source address **is** masqueraded

Masquerading options:

| | |
|--------------------|--|
| None | No masquerading is done. |
| None Except | Traffic destined for specific networks is masqueraded. All other traffic is not masqueraded. |
| All | All traffic is masqueraded. |
| All Except | Traffic destined for specific networks is not masqueraded. All other traffic is masqueraded. |

The masquerading options can only be managed on platform level.

1.14.4 NAT Rules

For the User Traffic to work, NAT rules must be configured on the routers.

Incoming direction - Backend to end devices - "VPN IP address block" to "LAN IP address block" NAT rule

Outgoing direction - End devices to Backend - "LAN IP address block" to "VPN IP address block" NAT rule

Note: These NAT rules are not part of the User Traffic Settings; they have to be configured separately. See [Section 1.13.2](#) for more information on NAT.

1.14.5 Disabling User Traffic

Disabling the User Traffic feature in the Command Line Tool (cs-cmd) has the following consequence

- The firewall on the CS server no longer accepts incoming traffic that is directed to the Platform Network.
- No routes are pushed to the routers anymore.
- All masquerading rules are removed.

1.15 User Management

The Connectivity Suite user hierarchy consists of three different user roles.

1.15.1 Platform Admin

The Platform Admin is the highest in the role hierarchy. A Platform Admin can administer the complete Connectivity Suite instance. This means he can administer VPN Networks, Devices and users.

1.15.2 Network Admin

A Network Admin can only administer Devices connected to a specific VPN Network. A Network Admin can assign the Network Admin and Network user roles for VPN he administrates to other users.

1.15.3 Network user

The Network user only can access and monitor Devices within specific VPN Network. However, a Network user is not allowed to manipulate Devices via the Connectivity Suite.

1.15.4 User rights table

1.15.5 Assigning user rights

1. Navigate to the page “User Management” of the Connectivity Suite UI by clicking on the tool icon in the Support bar.
2. Click on “Actions” at the upper right corner of the Main dialogue box and click “Add user” to add a user.
3. Fill out the required fields and click on “Add user” to add the user.
4. The added user must now be shown in the Main dialogue box in the table.

When creating the user following parameters can be set

| | |
|-------------------|--------------------------------------|
| Username | Name of the user (Login credential) |
| Email | Email of the user |
| Password | Password to login (Login credential) |
| First Name | First name of the user |
| Last Name | Last name of the user |
| Address | Address of the user |
| Company | Company the user works for |
| Phone | Company phone number |

| User rights | Platform administrator | Tenant administrator | Tenant user |
|---|------------------------|----------------------|-------------|
| Can view Devices | X | X | X |
| Can access Devices via Service Access and Webproxy | X | X | X |
| Can access Connected Devices via Service Access | X | X | X |
| Can view health data | X | X | X |
| Can manipulate Devices | X | X | |
| Can modify configurations | X | X | |
| Can execute Device updates (firmware and configuration) | X | X | |
| Add new Device via provisioning | X | | |
| Revoke router certificate | X | X | |
| Exchange Devices | X | X | |
| Can create /delete Networks | X | | |
| Can assign / revoke Platform Admin role | X | | |
| Can assign / revoke Network Admin role for Network X | X | X | |
| Can assign / revoke Network user role for Network X | X | X | |
| Can create / delete a user | X | X | |

Fig. 1.76: User rights table

NET

MODULE

ConnectivitySuite

?

⚙

🔔

COOL_DRAGON

Dashboard
Devices
Artefacts
Configuration
Snippets
Software
Provisioning
Network
Jobs

Users

Search...

Clear filters

| | Username | First Name | Last Name | Email Address | Company | Address | Phone | Created At |
|---|-------------|------------|-----------|-------------------|-------------|----------------------|----------------|-------------|
| | cool_dragon | | | | | | | 2022-08-29T |
| ✓ | john_smith | John | Smith | smith@company.com | Company Ltd | Some Rd 123, My City | 0041 123 45 67 | 2022-08-29T |

Actions

Add user
Delete user(s)
Reset password

Fig. 1.77: Manage users

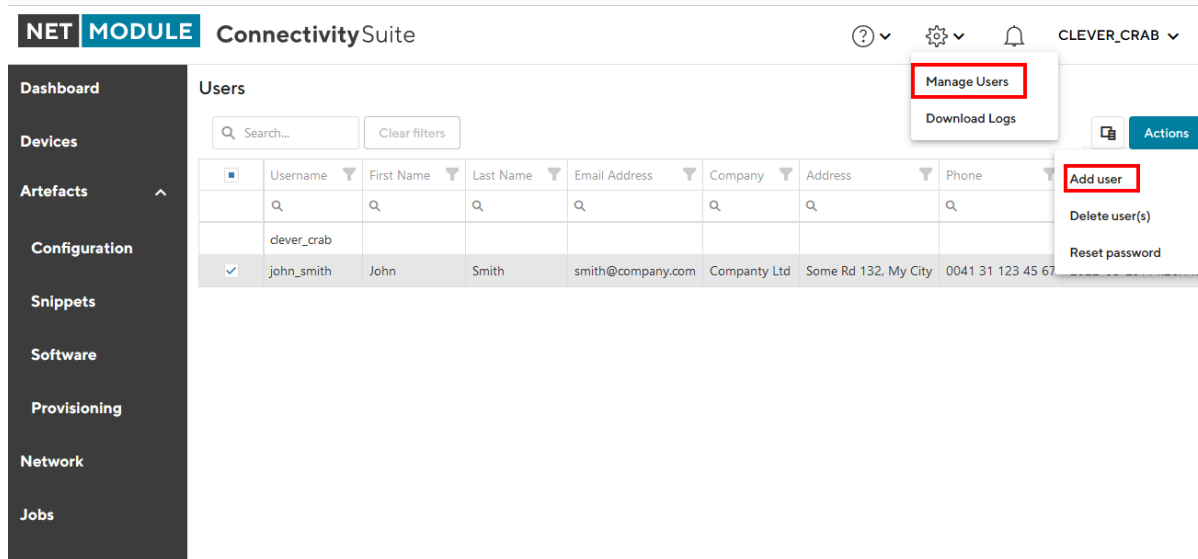


Fig. 1.78: Added user

When the tab “User Roles” is opened in the Main dialogue box, the user rights can be assigned there.

The following settings can be made:

| | |
|-----------------------|--|
| Platform Admin | If the checkbox is set the new user will have platform admin rights |
| Network Admin | Select the VPN Network of which the user will have admin rights (if no selection is taken the user won't be a Network admin). See Fig. 1.76 for the different user rights. |
| Network User | Select the VPN Network the user can access. See Fig. 1.76 for the different user rights. |

1.16 Customizations

There are several ways to customize Connectivity Suite to meet specific needs. The following chapter contains some options and examples of how to realize things that provide an additional value for certain applications.

Warning: While many of those options are being used in the field, they can break the system or reduce its performance. Please make sure to test your changes in a staging environment before deploying them to production. NetModule does not provide support for customisations.

The screenshot shows the Connectivity Suite interface. On the left is a dark sidebar menu with options: Dashboard, Devices, Artefacts, Configuration, Snippets, Software, Provisioning, Network, and Jobs. The main area is titled 'Users' and contains a table with columns: Username, First Name, Last Name, and Email Address. The table lists users 'dever_crab' and 'john_smith'. The 'john_smith' row is selected. To the right of the table is a panel for 'john_smith' with tabs: USER DETAILS, USER ROLES (highlighted in red), and CERTIFICATES. Under the 'USER ROLES' tab, there are sections for 'Platform Admin Role' (with a checkbox 'This user is a platform administrator'), 'Network Admin Roles' (showing 'EMEA' with a dropdown 'Change selection'), and 'Network User Roles' (showing 'NA' with a dropdown 'Change selection'). A 'Save changes' button is at the bottom.

Fig. 1.79: User roles

1.16.1 Additional Docker Containers

Additional containers can be operated in Connectivity Suite by adding them to the `cs/app/compose.override.yml` file. This file is not part of the standard installation, but can be added manually.

NTP Server

The following example adds an NTP server to the Connectivity Suite. The NTP server is a simple container running the *chrony* NTP server. The container is added to the Connectivity Suite by adding the following lines to the `compose.override.yml` file:

```
services:
  ntp:
    image: dockurr/chrony
    container_name: ntp
    ports:
      - 123:123/udp
    restart: always
    networks:
      - cs-net
```

Grafana

With the following example Grafana server may be added to Connectivity Suite.

The Grafana UI is exposed via the Connectivity Suite Web Proxy Service called *Traefik* under */grafana*. This is done with the help of labels. More about Traefik's use of labels can be found here: <https://doc.traefik.io/traefik/providers/docker/>.

The container is added to the Connectivity Suite by adding the following lines to the *compose.override.yml* file:

```
services:
  grafana:
    image: grafana/grafana:latest
    container_name: grafana01
    restart: always
    environment:
      - GF_SERVER_ROOT_URL=/grafana
      - GF_SERVER_SERVE_FROM_SUB_PATH=true
    labels:
      - "traefik.enable=true"
      - "traefik.http.routers.grafana-router.entryPoints=websecure"
      - "traefik.http.routers.grafana-router.rule=PathPrefix(`/grafana/`)"
    networks:
      - cs-net
```

Warning: This is a simplified example. The Grafana container should be configured with a persistent storage for the data and the configuration. The example does not include a persistent storage.

Start or update instance with extra services

After changes to the *compose.override.yml* file, the Connectivity Suite needs to be restarted. This can be done by running the following command in the *cs/app* directory:

```
docker-compose up -d
```

1.16.2 Customising the Connectivity Suite API / Proxy settings

The Connectivity Suite *API* and the *Proxy* settings can be customised by changing the following file *cs/app/app-data/api/custom.json*. The following example shows how to add a override the certificate renewal schedule (default 2am UTC) to 10pm UTC:

```
{
  "App": {
    "Certificate": {
      "DailyCertificateRenewalAndCleanupHour": 22
    }
  }
}
```

1.16.3 Triggering scripts on VPN servers

Warning: You can easily break the VPN Servers or make them more vulnerable by running custom scripts. Please make sure to test your scripts in a staging environment before deploying them to production.

In rare cases a user might want to trigger some custom scripts running on the VPN servers. This can be done via the API by using the following endpoint:

```
PUT /api/v3/Devices/{id}/staticScripts
```

Note: The {id} above is **not the NetworkId**. To find the Id of the VPN Server Device, you can have a look at the `vpnServerId` property in the response of the GET `/api/v3/Networks` endpoint.

The following 4 script hooks are available:

- **preStartup**

This is run before the official startup script is run.

- **postStartup**

This is run after the official startup script is run.

- **preReconfigure**

This is run before the server reconfigure script is run which happens with every change on the network (e.g. new Device is added etc.)

- **postReconfigure**

This is run after the server reconfigure script is run which happens with every change on the network (e.g. new Device is added etc.)

You can retrieve the current scripts by using the following endpoint:

```
GET /api/v3/Devices/{id}/staticScripts
```

If you want to see the logs of the scripts, you can use the following endpoints:

```
GET /api/v3/Devices/{id}/logs/readable
```

 or

```
GET /api/v3/Devices/{id}/logs
```

 to get a zip file with all logs.

1.17 Troubleshooting

For the following steps an account with **Platform Administrator** or **VPN Network Administrator** right is required.

1.17.1 Troubleshoot a Device

If there are problems with a Device, there are several things that you can check:

- Is the Device online?
 - No: Check when it was last online by navigating to the Health page and selecting the specific Device
 - * Is the Device powered on?
 - Yes: Try to access the Device directly by downloading the Service Access VPN configuration and establishing a VPN connection to the Core Network
 - No: Power on the Device
- Yes, do a direct Device access by first downloading the Service Access VPN configuration and troubleshooting the Device outside of the Connectivity Suite

1.17.2 Troubleshoot the Connectivity Suite

1. Click on the wrench icon in the upper right corner
2. Select “Logs”
3. Click on “DOWNLOAD LATEST” to download the latest log file or choose one or multiple older log file from the list and click on “DOWNLOAD SELECTED”. The name of the file in the table indicates the timestamp of the last log entries in the file
4. Download the file and send it to the Connectivity Suite support

1.17.3 Browser settings Connectivity Suite SSL Certificate

Downloading the Connectivity Suite Root CA certificate using Microsoft Edge

1. Click on Certificate Error to the left of the address bar
2. Choose the Connectivity Suite Root CA from the menu on the right
3. Click on Export to file, this is the file that needs to be imported using one of the import procedures described below

Making your browser trust the Connectivity Suite Root CA

The client operating system or browser now needs to have the CA certificate added to its list of trusted CAs. The instructions vary by operating system and browser but instructions for a few major browsers are listed below.

| Client (Operating System, Browser) | Instructions |
|------------------------------------|--|
| Microsoft Windows | Right click the CA certificate file and select 'Install Certificate'. Follow the prompts to add the certificate to the trust store either for the current user only or all users of the computer. |
| Firefox | Firefox does not use the operating systems trust store so the CA needs to be added manually. Manually add certificates and manage added certificates through Firefox's Privacy & Security preferences. More information can be found on Mozilla Wiki |
| Chrome | If Chrome is configured to use the Windows trust store, adding the certificate to Windows (see above) is sufficient to add trust to the browser as well. Otherwise the certificate can be added manually using the following procedure: Open Settings > Advanced > Manage Certificates > Authorities, and select Import. |
| Edge/Internet Explorer | Edge/Internet Explorer uses the Windows trust store so adding the certificate to Windows (see above) is sufficient to add trust to the browser as well. |

1.18 Update & Backup

1.18.1 Update v3.a.b > v3.x.y

1. Connect to your server via SSH
2. Create a backup of the current version using the following command:

```
sudo cp -pr cs cs_backup
```
3. Change to the cs directory

```
cd ./cs
```
4. Download the latest Connectivity Suite console application. The credentials for repository are provided by Net-Module.

```
curl -u cs-install ftp://ftp.netmodule.com/latest/cs-cmd -o cs-cmd
```
5. Run the cs-cmd tool and select "update assistant"

```
./cs-cmd
```

1.18.2 Upgrade v2.6 > v3.0

Since v3.0 is based on a different software architecture than v2.6, this is not only an update but also a migration.

Warning: In case any of the following steps fail we advice to **snapshot the Virtual Machine** where the Connectivity Suite is installed so that a roll back is possible.

Warning: To install and run the Connectivity Suite v3 you need to have an **up to date Ubuntu 20/22 or Debian 10/11** with **Docker v20+** and the **Docker Compose v2+** plugin installed. See [Section 1.2.1](#) for details.

Warning: Routers with NRSW older than 4.3 will not be able to connect to a Connectivity Suite v3.x. Make sure to update the outdated Router Software before upgrading the Connectivity Suite.

Note: The following steps assume that you have installed your CS v2.6 in your home directory under ~/cs. If this is not the case, please adjust the paths below accordingly.

1. Connect to your server via SSH
2. Download the Connectivity Suite Backup script

```
curl https://repo.netmodule.com/repository/cs/v2.6/scripts/export_cs_v2.py -o
export_cs_v2.py
```
3. Export Connectivity Suite v2.6 data with the Backup script and note the location of the cs_export.zip file. You will need this later.

```
python ./export_cs_v2.py
```
4. Change to the ~/cs/docker-prod directory

```
cd ./cs/docker-prod
```
5. Stop the v2.6 instance

```
docker-compose down
```
6. Change directory back to home

```
cd ~
```
7. Rename the cs directory to cs_v2x

```
mv cs cs_v2x
```
8. Create new cs directory

```
mkdir cs
```
9. Change to new cs directory

```
cd ./cs
```
10. Run a ls command to make sure the directory is empty

```
ls
```
11. Download Connectivity Suite console application. The credentials for repository are provided by NetModule.

```
curl -u cs-install ftp://ftp.netmodule.com/latest/cs-cmd -o cs-cmd
```
12. Add execution permission to newly downloaded cs-cmd

```
sudo chmod +x ./cs-cmd
```
13. Run the cs-cmd tool and select “v2.x migration assistant”

```
./cs-cmd
```
14. The requested path to the cs_export.zip was printed out at step 3 and is similar to

```
/home/ubuntu/cs_export.zip
```
15. Optional: Remove v2.6

```
rm -rf ~/cs_v2x
```

Warning: When updating from v2.6 to v3.0, certain restrictions must be observed which are noted in chapter [Section 1.18.2](#)

Migration Notes

The migration to v3.0 will not migrate the full data of v2.6. The following list shows the affected entities:

- Replacement Devices
Devices which should replace an existing device and their replacement provisioning config will not be migrated. Make sure to finish all your device replacement jobs before you upgrade.
- Provisioning Devices
Devices currently connected to the provisioning network will **not be migrated**. Make sure to move all devices to their tenant before you upgrade.
- Logs
The plain-text logs will no be migrated.
- Jobs
Jobs will not be migrated. Make sure that there are no open jobs before you migrate.
- Provisioning Configurations
Already downloaded configurations from CS v2.6 will no longer work for CS v3.0.
- Device metric data
6 Months Online/Offline device state changes per Device will be migrated.

1.19 Appendix

1.19.1 Abbreviations

| | |
|------|-----------------------------------|
| API | Application Programming Interface |
| AWS | Amazon Web Services |
| CLI | Command Line interface |
| CS | Connectivity Suite |
| FQDN | Fully Qualified Domain Name |
| HMI | Human Machine Interface |
| NM | NetModule |
| OTA | Over the Air |
| REST | Representational State Transfer |
| SSH | Secure Shell |
| UI | User interface |
| VPN | Virtual Private Network |

1.19.2 Glossary

| v3 | v2.x | Meaning |
|---|--|----------------|
| | Tenant Network, Tenant-internal Network | Name of a |
| External Address | | The address |
| (Parent) Device | Device | Anything t |
| Alias | Shortname | |
| Artifact | | An artifact |
| Backend Network | Home Network | The VPN n |
| Backend VPN Server | Home Server | A VPN ser |
| Child Device | End Device, Connected Device, Managed Devices, Client Devices | Devices co |
| Connectivity Suite infrastructure | | The infrast |
| Connectivity Suite Networks | | Name for a |
| Container | LXC Container | |
| Core Address Block | Core Network | The Core A |
| Device Access Routes | | Routes tha |
| Device Configuration | Configuration | The Config |
| Device Information | | Information |
| Device information | | The inform |
| Device Health | | Information |
| Device Model | Model | Specific pr |
| Device specific configuration parameters | | Configurat |
| Device Status | | Information |
| Device Type | Device Type | Product ca |
| Device VPN Address Block | | The subnet |
| End Device | | Any Device |
| Firmware | Software, Firmware, Application | |
| Generic configuration parameters | | Configurat |
| Generic Device | Generic Device | Any device |
| Job | Job | Can be use |
| LAN | | Local Area |
| Lan Address | IP in LAN | The IP/Add |
| Managed Devices | | It distingui |
| Module | | A module |
| Open VPN Server | Tenant | An Open V |
| Platform Address | IP Address in Home Network, IP in Home | The platfor |
| Platform Address Block | Home Network | A VPN sub |
| Provisioning Configuration | Provisioning Configuration | The Provis |
| Provisioning Network | Provisioning Server | Newly add |
| Provisioning VPN Server | Provisioning Server | A VPN ser |
| Readable Configuration (internal use only) | Configuration | A Readabl |
| Repository | Files | The collect |
| Script | SDK Script | Script whic |
| Service Access | Service Access | The Servic |
| Snippet | Snippet | Refers to a |
| Task | Task | A Job can |
| VPN Address | IP Address in Tenant Network, IP in Tenant, Tenant-internal IP | The IP assi |
| VPN Network | Tenant, Tenant Net Internal | A VPN Ne |
| VPN Network Address Block | Tenant-internal Network | The address |
| VPN Network Address Block in Platform Network | Tenant Network in Home Network | The address |

| v3 | v2.x | Meaning |
|-----------------|-------------|------------|
| VPN subnet Pool | Tenant Pool | Collection |

1.19.3 Legal Aspects

Legal Considerations

This document contains proprietary information of NetModule AG. No part of the work described herein may be reproduced. Reverse engineering of the hardware or software is prohibited and is protected by patent law. This material or any portion of it may not be copied in any form or by any means, stored in a retrieval system, adopted or transmitted in any form or by any means (electronic, mechanical, photographic, graphic, optic or otherwise), or translated in any language or computer language without the prior written permission of NetModule AG.

The information in this document is subject to change without notice. NetModule AG makes no representation or warranties with respect to the contents herein and shall not be responsible for any loss or damage caused to the user by the direct or indirect use of this information. This document may contain information about third party products or processes. This third-party information is out of influence of NetModule AG therefore NetModule AG shall not be responsible for the correctness or legitimacy of this information. If you find any problems in the documentation, please report them in writing by email to info@netmodule.com at NetModule AG. While due care has been taken to deliver accurate documentation, NetModule AG does not warrant that this document is error-free.

NetModule AG is a trademark and the NetModule logo is a service mark of NetModule AG.

All other products or company names mentioned herein are used for identification purposes only and may be trademarks or registered trademarks of their respective owners.

The following description of software, hardware or process of NetModule AG or other third-party provider may be included with your product and will be subject to the software, hardware or other license agreement.

NetModule AG

Maulbeerstrasse 10

3011 Bern

Switzerland

info@netmodule.com

Tel +41 31 985 25 10

Fax +41 31 985 25 11

<https://www.netmodule.com>