

Secure NMC System (SNS) Tool

Table of Contents

Introduction.....	1
System Requirements	2
Prerequisites	2
Download the SNS Tool	4
Install the SNS Tool	4
Windows.....	4
Linux.....	4
macOS	5
Add/Remove Devices to the SNS Tool.....	6
Login.....	6
Activate NMC Subscription	7
Update NMC Firmware.....	7
Device Actions.....	9
Import/Export Data	10
Clear Cache.....	10
Configuration Settings	11

Introduction

The Secure NMC System (SNS) Tool allows you to manage firmware updates for your Network Management Card 3, including pre-installed and standalone SmartSlot cards (AP9640, AP9641, AP9643, AP9544) and embedded cards. The SNS Tool was designed to enhance cybersecurity and reduce exposure to security threats by ensuring that your NMC3 is running the latest and most secure firmware.

The SNS Tool supports five NMC3 applications including SU (Smart- UPS), SY (1-Phase Symmetra), SUCAN (Smart-UPS Ultra), RDP2G (Rack Power Distribution Units) and EU1P (Easy UPS On-Line). As part of Schneider Electric's new Secure NMC System, the SNS Tool provides support for activating your NMC subscriptions. A 1-year Secure NMC subscription is included with all NMC3 for UPS and PDU products, including the standalone NMC3s: AP9640, AP9641, AP9643 and AP9544.



It is highly recommended you run the Secure NMC System Tool on a sufficiently hardened and secure PC. The Secure NMC System Tool should be executed only by authorized users by verifying the Tool has the correct file permissions and it's accessible at a secure location.



If you are upgrading your NMC3 firmware from a firmware version prior to 2.3.1.1, see Knowledge Base article [FAQ000262012](#)

System Requirements

1. The NMC must have a valid IPv4 address.
2. The NMC must be available via the network to the SNS Tool.
3. To connect to Schneider Electric cloud services, the SNS Tool needs to be able to connect directly to TCP port 443 on [schneider-electric.flexnetoperations.com](#), [dsc-apps-prod.auth.eu-west-1.amazoncognito.com](#), [sds.se.com](#), and [se.com](#).

If the network of the SNS Tool is behind a proxy server (e.g., ZScaler), you must add a firewall rule that permits this connection to TCP port 443 and bypasses any proxy service packet inspection.

Consult with your Network Administrator to configure this firewall rule.

4. The system running the SNS Tool must have at least 4GB of memory.
5. The system running the SNS Tool must also have at least 4GB of storage space available.

Prerequisites

1. You must have a valid Secure NMC subscription.
2. If you do not have a valid or an included subscription, you can purchase one using the part numbers below.

Note: You must purchase the correct subscription for your application type to maximize the benefits of the SNS Tool.

Smart-UPS and 1-Phase Symmetra devices (SU, SY & SUCAN)	
Applicable Part Number	Secure NMC Subscription
SWNMC3SU-1Y-DIGI	NMC3 for Smart-UPS & 1-Ph Symmetra - 1 Year Secure NMC Subscription
SWNMC3SU-2Y-DIGI	NMC3 for Smart-UPS & 1-Ph Symmetra - 2 Year Secure NMC Subscription
SWNMC3SU-3Y-DIGI	NMC3 for Smart-UPS & 1-Ph Symmetra - 3 Year Secure NMC Subscription
SWNMC3SU-4Y-DIGI	NMC3 for Smart-UPS & 1-Ph Symmetra - 4 Year Secure NMC Subscription
SWNMC3SU-5Y-DIGI	NMC3 for Smart-UPS & 1-Ph Symmetra - 5 Year Secure NMC Subscription
SWNMC3SU-6Y-DIGI	NMC3 for Smart-UPS & 1-Ph Symmetra - 6 Year Secure NMC Subscription

Rack Power Distribution Units (RPDU2G)	
Applicable Part Number	Secure NMC Subscription
SWNMC3PDU-1Y-DIGI	NMC3 rPDU - 1 Year Secure NMC Subscription
SWNMC3PDU-2Y-DIGI	NMC3 rPDU - 2 Year Secure NMC Subscription
SWNMC3PDU-3Y-DIGI	NMC3 rPDU - 3 Year Secure NMC Subscription
SWNMC3PDU-4Y-DIGI	NMC3 rPDU - 4 Year Secure NMC Subscription
SWNMC3PDU-5Y-DIGI	NMC3 rPDU - 5 Year Secure NMC Subscription
SWNMC3PDU-6Y-DIGI	NMC3 rPDU - 6 Year Secure NMC Subscription

Easy UPS On-Line devices (EU1P)	
FWENMC1P-ST1Y-DIGI	NMC3 for Easy UPS, 1-Phase - 1 Year Secure NMC Subscription
FWENMC1P-ST2Y-DIGI	NMC3 for Easy UPS, 1-Phase - 2 Year Secure NMC Subscription
FWENMC1P-ST3Y-DIGI	NMC3 for Easy UPS, 1-Phase - 3 Year Secure NMC Subscription
FWENMC1P-ST4Y-DIGI	NMC3 for Easy UPS, 1-Phase - 4 Year Secure NMC Subscription
FWENMC1P-ST5Y-DIGI	NMC3 for Easy UPS, 1-Phase - 5 Year Secure NMC Subscription
FWENMC1P-ST6Y-DIGI	NMC3 for Easy UPS, 1-Phase - 6 Year Secure NMC Subscription

3. Instructions for NMC3 devices with Multifactor Authentication (MFA) enabled

To ensure compatibility with the SNS Tool when MFA is enabled on an NMC3 device:

- a) **Create a Local User without MFA**
Make sure that at least one NMC3 local user account exists without an email address configured. This prevents MFA from being enabled for that local user.
- b) **Use the Local User Credentials in the SNS Tool**
When adding the device to the **Device List** in the SNS Tool, enter the credentials of the local user account that does **not** have an email address configured.
- c) **Update credentials for existing NMC3 devices with MFA enabled**
If existing devices in the **Device List** have MFA is enabled, update the credentials in the SNS Tool to use a local user account that does **not** have an email address configured, using the **Action Button** ... > **Edit**.

See Knowledge Base article [FAQ000276382](#) for details on NMC3 local user configuration.

Download the SNS Tool

1. Download the SNS Tool from the [Schneider Electric website](https://www.se.com) by navigating to the NMC product page, <https://www.se.com/secure-nmc> and selecting the **Secure NMC System Tool** from the **Category** list:

Applicable Part Number	SNS Tool
SFNM3SNST	Secure NMC System Tool

2. Click **See Software** to view the available downloads. The SNS Tool supports Windows, Linux, and macOS operating systems.
3. Select the software for your operating system and click the **Download** button.

Install the SNS Tool

Windows

Note: You must have administrator rights to run the SNS Tool installer.

1. Run the installer and click **Next**.
2. Enter an installation folder location or accept the default. Click **Install**.
3. Click **Finish** to exit the installer and open the Secure NMC System Tool.
4. Accept the End User License Agreement to proceed.

The default installation directory is:

```
C:\Program Files\Schneider Electric\SecureNMCSystemTool
```

Linux

Note: Sudo privileges are required to run the SNS Tool installer for Linux.

You must accept the End User License Agreement to run the SNS Tool.

Runtime Installation

The Secure NMC System Tool requires .NET 8.0 Runtime to be installed on your machine in order to run. The Runtime installation is handled during the Secure NMC System Tool installation once the Microsoft package source is configured.

Debian

This can be done with the following commands:

Debian 11

```
wget https://packages.microsoft.com/config/debian/11/packages-microsoft-prod.deb -O packages-microsoft-prod.deb
sudo dpkg -i packages-microsoft-prod.deb
rm packages-microsoft-prod.deb
sudo apt-get update
```

Debian 12

```
wget https://packages.microsoft.com/config/debian/12/packages-microsoft-prod.deb -O packages-microsoft-prod.deb
sudo dpkg -i packages-microsoft-prod.deb
rm packages-microsoft-prod.deb
sudo apt-get update
```

Or alternatively, visit <https://learn.microsoft.com/en-us/dotnet/core/install/linux-debian> to view Microsoft's instructions to set up the package sources.

Ubuntu

By default, .NET 8.0 Runtime is available in the Ubuntu package feed so no additional steps are required.

Verify .deb File Signature

Download the public key, SE_GPG.asc, from the Schneider Electric site at se.com/secure-nmc

Run the following commands:

```
gpg --import SE_GPG.asc
gpg --verify SecureNMCSysTool.sig snst_nmc3_X-X-X-X.deb
```

Installation

Run the following command from the same location as the Secure NMC System Tool .deb file:

```
sudo apt install ./snst_nmc3_X-X-X-X.deb
```

This will install the Secure NMC System Tool to the default installation directory:

```
/opt/Schneider Electric/SecureNMCSysTool
```

macOS

1. Place snst_nmc3_X-X-X-X.app in your Applications folder.
2. Search for Secure NMC System Tool in your applications library and launch it.
3. Accept the End User License Agreement to proceed.

Add/Remove Devices to the SNS Tool

You can add each device individually or add multiple devices at once.

Note: The SNS Tool supports up to 1000 NMC devices.

Add each device individually:

Click **Add Devices** and enter the following details:

- The NMC's IP address (IPv4 only), FQDN or Hostname.
- The communication protocol (FTP or SCP). SCP is selected by default.
Note: Your selected protocol should also be enabled on your NMC3 device.
- The port number for your selected protocol.
- The NMC username and password
- Once the device has successfully been queried, it will automatically be added to the **Device List** in the SNS Tool.

Add multiple devices at once:

- Open the `devices.csv` file at the following location:
 - **Windows:** `C:\Users\\AppData\Local\Schneider Electric\SecureNMCSysTool`
 - **Linux:** `/home/<user>/.local/share/Schneider Electric/SecureNMCSysTool`
 - **macOS:** `/Users/<user>/Library/Application Support/Schneider Electric`

Add the device details in a comma-separated format. **Note:** Only valid comma-separated format will be accepted, and lines that start with a semi-colon ; symbol will not be processed by the SNS Tool.

- Save and close the `devices.csv` file.
- Return to the SNS Tool and click **Add Devices**.
- Click **Import Device File**.
- Select **Query Devices** to verify the NMC.
- In the Query Devices dialog, proceed with querying all devices by selecting **Query Devices** again.
- Once all devices are successfully queried, select **Add Devices** to add them to the SNS Tool.

Remove Devices:

To remove your NMC from the SNS Tool, select your NMC device from the **Device List** and click **Remove Devices**.

Login

Log in to your Schneider Electric account to license devices and update firmware. To log in:

1. Click on the user icon in the upper right-hand corner and click **Log in**.
Select the Stay Logged In checkbox to allow the SNS Tool to keep your session active beyond the current visit.
2. In the login window, complete your login to your Schneider Electric account.

Activate NMC Subscription

You can activate your Secure NMC subscription **online**, when the NMC is on a public internet facing network, or **offline**, when the NMC is on an air-gapped private network.

Activate Online

1. In the SNS Tool, select the device you want to license. To license more than one NMC in the **Device List**, hold CTRL (Windows/Linux) or Command (macOS) and click each NMC to be licensed.
2. Select **License Devices** and click **Check License**. If you are not logged in, you will be prompted to log in.
3. If you have a 1-year included subscription or a previously activated subscription, the SNS Tool will retrieve the license details.
4. If your NMC does not have an included subscription or is not already licensed, click **Continue** and enter the Activation ID from your purchased Secure NMC subscription.
5. Click **Confirm and Activate**.



If the SNS Tool does not retrieve an included Secure NMC subscription for your NMC, but it was purchased after April 1st 2024, contact the [Customer Care Center](#).

Activate Offline

- To activate your Secure NMC subscription in an offline scenario, i.e. your NMCs are on an air-gapped private network, please see Knowledge Base article [FAQ000268166](#) for instructions.

See also: [Import/Export Data](#)

If you have an active subscription that you want to reuse on a similar NMC, contact the [Customer Care Center](#). Once your subscription is activated, you can update the firmware on your device(s).

Update NMC Firmware

The bell icon provides notification of a new firmware update available. When new firmware is available for your device(s), the **Target Application** column will display the latest firmware with a **New** icon.

To update the NMC firmware:

1. In the **Device List**, the NMCs that are eligible for update will have a status displayed as “Ready for Update”.
2. Select the NMC you want to update.
3. Click **Update Firmware**.

You can also update an NMC device with a status such as “Newer Firmware Installed” or “At Current Version” by manually selecting the devices in the Device List.



Note: If you click **Update Firmware** without selecting an NMC, the SNS Tool will automatically update the firmware of **all** eligible NMC devices.

Note: If a warning icon is displayed next to a device, it may be rebooting, offline, or unresponsive to pings. If the device is offline, firmware updates will be unsuccessful. To turn on ping responses, log into the NMC3 Web UI and navigate to **Configuration > Security > Ping Response** and enable the **IPv4 Ping Response** checkbox.

Change Firmware Version

By default, the SNS Tool will update to the latest firmware available for your device(s). To change the firmware version, select [View Details](#).

Download Firmware

You can choose to download the firmware files only, useful for custom firmware deployment scenarios. Select **Update Firmware > Download Only**.

Device Status

On the Device List page, you can view device status per NMC. See the table below for a description of each status type.

Device Status	Description
Activate Subscription to Update	The device must be activated with the correct subscription to perform update.
At Current Version	The NMC has the latest firmware available installed.
Backing Up Device	The NMC Event Log, Data Log and Configuration files are backed up before the firmware is updated. See Configuration Settings
Download Complete	The firmware has successfully downloaded.
Download Unsuccessful	The firmware has not successfully downloaded.
Download Pending	The firmware is pending download.
Downloading Firmware	The firmware is being downloaded.
Firmware Unavailable	The firmware update service is currently unavailable.
Incorrect Credentials	The NMC credentials provided are incorrect.
Newer Firmware Installed	The device has newer firmware than what is available for download.
Not Accessible	The device is not accessible via the network. Check the connection to the NMC.
Preparing Device	The device is checked for suitability to update.
Querying	The SNS Tool is communicating with the NMC device.
Queued for Update	The device is queued to be updated at the next availability.
Ready for Update	The device has passed all pre-update checks and requirements and is ready to update.
Restarting Interface	The device is restarting.

Device Status	Description
Retrying Update	The device could not be updated. The firmware update process is starting over from the beginning.
Unknown	Status is unknown.
Update Complete	The device has completed the firmware update process.
Update Error	The device experienced an error during the firmware update process.
Updating Bootloader	The bootloader of the device is updating.
Updating Firmware	The device is currently updating its firmware.
Verifying Update	The device is verifying the new firmware.

Cancel Firmware Update

To cancel a firmware update that is in progress:

1. Select the device in the **Device List**.
2. Click **Cancel Update**. A dialog will indicate if the firmware update has progressed beyond the point of cancellation.
3. If it is possible to cancel the firmware update, click **Confirm**.

Device Actions

Certain actions can be performed on a per-device basis. Select an NMC in the **Device List** and click on the three horizontal dots for more options.

View Details

The **Profile** tab provides an overview of the NMC, including information available on the **Device List**.

Note: The System Information is displayed here if configured on the NMC Web UI.

The **Firmware** tab allows you to specify which firmware version to install on your NMC. You can also change the firmware application running on your NMC. By default, a standalone NMC (AP9640, AP9641, AP9643) includes the Smart-UPS firmware pre-installed. If you want to update an NMC to be used in a Symmetra or Smart-UPS Ultra device, you can update the firmware to match the device requirements:

1. From the **Application Type** menu, select the firmware type of the new device.
2. From the **Application Version** menu, select the firmware version to which you want to update. The release notes for each application version are linked beside the menu.

Note: Changing application type will reset the NMC to factory settings.

3. Return to the **Device List** where the new application version and type is visible, and the device status is **Ready to Update**.
4. To complete the firmware update to the new application type, click **Update Firmware**.

Note: NMCs used with RDP2G (Rack Power Distribution Units) and EU1P (Easy UPS On-Line) cannot change firmware application type, as no other application type is supported by the device.

Edit

If the username or password of your NMC has changed, you can edit the details using the **Edit** option.

Refresh Details

This will query your NMC and retrieve the latest information.

Log in to NMC

This will open a web browser to log in to the NMC's Web UI.

Remove

This will remove the device from the Device List.

Import/Export Data

You can import and export application data for use on another Secure NMC System Tool, for example when licensing and updating NMCs on an air-gapped network:

1. Click the **Options** button on the upper right-hand corner of the SNS Tool.
2. Click **Import/Export Application Data**.
3. Select all or specific **Devices**, **Licenses** and **Firmware** to import/export.

Note: For export, there are two file type options:

- a. **CSV:** This option exports the minimal amount of device data required for licensing and downloading firmware.
- b. **SNST Bundle:** This option allows you to export all **Device details**, **Licenses** and **Firmware**.



Note: The exported application data will contain sensitive information like NMC username and password. **Password-protect the export file and store it securely.**

See Knowledge Base article [FAQ000268166](#) for instructions on licensing and updating NMC devices on an air-gapped network.

Clear Cache

This will delete all local firmware files stored at the following location on your operating system:

- **Windows:** C:\Users\\AppData\Local\Schneider Electric\SecureNMCSysTool
- **Linux:** /home/<user>/local/share/Schneider Electric/SecureNMCSysTool
- **macOS:** /Users/<user>/Library/Application Support/Schneider Electric

Configuration Settings

Configuration Setting	Description
Theme	<p>Select your preferred appearance:</p> <ul style="list-style-type: none"> • System theme – match the theme of your operating system. • Light theme – bright background with dark text for well-lit environments. • Dark theme – dark background with light text for low-light environments.
Back up configuration and log files prior to update	<p>Select this checkbox to back up the NMC configuration and log files before a firmware update. These files will be stored in the application data folder of the operating system:</p> <ul style="list-style-type: none"> – Windows C:\Users\<username>\AppData\Local\Schneider Electric\SecureNMCSysTool\Backup</username> – Linux: /home/<UserName>/./local/share/Schneider Electric/SecureNMCSysTool/Backup – macOS: /Users/<UserName>/Library/Application Support/Schneider Electric/SecureNMCSysTool/Backup
Check for Secure NMC System Tool software updates automatically	<p>The Secure NMC System Tool will notify you when there is a newer version available to download. Select this checkbox to check the update server when the SNS Tool is run. You can also click Options > Check for Updates to check the update server at any time.</p>
Advanced Settings	
Number of Concurrent Requests	<p>Specify the number of concurrent requests for NMC devices, e.g. firmware updates.</p>
Maximum Number of Firmware Update Attempts	<p>Specify the maximum number of times the SNS Tool will attempt a firmware update. The default value is 3.</p>