Network Management Card 4

Security Handbook, Firmware Version 6.x and 12.x

990-6121J-001

Publication Date: March, 2023

Schneider Electric

Schneider Electric IT Corporation Legal Disclaimer

The information presented in this manual is not warranted by the Schneider Electric IT Corporation to be authoritative, error free, or complete. This publication is not meant to be a substitute for a detailed operational and site specific development plan. Therefore, Schneider Electric IT Corporation assumes no liability for damages, violations of codes, improper installation, system failures, or any other problems that could arise based on the use of this Publication.

The information contained in this Publication is provided as is and has been prepared solely for the purpose of evaluating data center design and construction. This Publication has been compiled in good faith by Schneider Electric IT Corporation. However, no representation is made or warranty given, either express or implied, as to the completeness or accuracy of the information this Publication contains.

IN NO EVENT SHALL SCHNEIDER ELECTRIC IT CORPORATION, OR ANY PARENT, AFFILIATE OR SUBSIDIARY COMPANY OF SCHNEIDER ELECTRIC IT CORPORATION OR THEIR RESPECTIVE OFFICERS, DIRECTORS, OR EMPLOYEES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL, OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS, CONTRACT, REVENUE, DATA, INFORMATION, OR BUSINESS INTERRUPTION) RESULTING FROM, ARISING OUT, OR IN CONNECTION WITH THE USE OF, OR INABILITY TO USE THIS PUBLICATION OR THE CONTENT, EVEN IF SCHNEIDER ELECTRIC IT CORPORATION HAS BEEN EXPRESSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SCHNEIDER ELECTRIC IT CORPORATION RESERVES THE RIGHT TO MAKE CHANGES OR UPDATES WITH RESPECT TO OR IN THE CONTENT OF THE PUBLICATION OR THE FORMAT THEREOF AT ANY TIME WITHOUT NOTICE.

Table of Contents

Introduction

Content and Purpose of this Guide

This guide documents security features for firmware version 6.x and 12.x for Schneider Electric® Network Management Card 4, which enables the devices to function remotely over the network.

This guide documents the following protocols and features, how to select which ones are appropriate for your situation, and how to set up and use them within an overall security system:

- Secure Shell v2 (SSH)
- Transport Layer Security (TLS) v1.1, v1.2, and v1.3
- RADIUS
- Extensible Authentication Protocol over LAN (EAPoL)
- SNMPv1 and SNMPv3

User Management

Types of User Accounts

The Network Management Card has five basic levels of access:

- A Super User: can use all of the management menus available in the Web interface and all of the commands in the command line interface.
- Administrative User: can use all of the management menus available in the Web interface and all of the commands in the command line interface.
- A Device User: can access the event log (but cannot delete the contents of the log), and can use the device-related menus and commands.
- Network-Only User: can only access information that is not device-related.
- A Read-Only User: can access the event log, and device-related menus, but cannot change configurations, control devices, delete data, delete the contents of the log, or use file transfer options.

Note: A Super User is an Administrator account which is persistent and cannot be deleted, but can still be enabled or disabled.

Security

Security Features

Protection of passwords and passphrases

No password or passphrases are stored on the Network Management Card in plain text.

- Passwords are hashed using a one-way hash algorithm.
- Passphrases, which are used for authentication and encryption, are encrypted before they are stored on the Network Management Card.

Summary of access methods

Local access to the command line interface.

Security Access	Description
Access by user name, user type, and password	Always enabled. Access level depends on user type.

Remote access to the command line interface

Security Access	Description
Available methods: • User name and password • Selectable server port • Access protocols that can be enabled or disabled. • Secure Shell (SSH)	For high security, use SSH. • Enabling SSH provides encrypted access to the command line interface, to provide additional protection from attempts to intercept, forge, or alter data during transmission.

SNMPv1 and SNMPv3

Security Access	Description
Available methods (SNMPv1)*: • Community Name • Host Name • NMS IP filters • Agents that can be enabled or disabled • Four access communities with read/write/disable capability	For both SNMPv1 and SNMPv3, the host name restricts access to the Network Management System (NMS) at that location only, and the NMS IP filters allow access only to the NMSs specified by one of the IP address formats in the following examples: • 159.215.12.1: Only the NMS at the IP address 159.215.12.1. • 159.215.12.255: Any NMS on the 159.215.12 segment. • 159.215.255.255: Any NMS on the 159.215 segment. • 159.255.255.255: Any NMS on the 159 segment. • 0.0.0.0: Any NMS. • SNMPv3 has additional security features that include the following: – An authentication passphrase to ensure that an NMS trying to access the Management Card or device is the NMS it claims to be. – Encryption of data during transmission, with a privacy passphrase required for encrypting and decrypting.
Available methods (SNMPv3): • Four User Profiles • Authentication through an authentication passphrase • Encryption through a privacy passphrase • SHA or MD5 authentication • AES or DES encryption algorithm • NMS IP filters	

* SNMPv2c can also be used using the configured SNMPv1 settings.

File transfer protocols

Security Access	Description
Available methods: • User name and password • Selectable server port • Access protocols that can be enabled or disabled. • Secure FTP (SFTP) • Secure Copy (SCP)	Available methods: • FTP – With FTP, the user name and password are transmitted as plain text, and files are transferred without encryption. • SFTP and SCP – Use SFTP and SCP to encrypt the user name and password and the files being transferred, such as firmware updates, configuration files, log files, Transport Layer Security (TLS) certificates, EAPoL certificates, and Secure Shell (SSH) host keys. If you choose SFTP or SCP as your file transfer protocol, enable SSH and disable FTP. **Note:** FTP is disabled by default.

Web Server

Security Access	Description
Available methods: • User name and password • Selectable server port • Web interface access that can be enabled or disabled • Transport Layer Security (TLS)	In basic HTTP authentication mode, the user name and password are transmitted as plain text (with no encoding or encryption). TLS is available on Web browsers supported for use with the Management Card or network-enabled device and on most Web servers. The Web protocol HyperText Transfer Protocol over Secure Sockets Layer (HTTPS) encrypts and decrypts page requests to the Web server and pages returned by the Web server to the user.

RADIUS

Security Access	Description
Available methods: • A server secret shared between the RADIUS server and the Management Card or device • The RADIUS server name or IP address (IPv4 or IPv6) and port	RADIUS (Remote Authentication Dial-In User Service) is an authentication, authorization, and accounting service used to centrally administer remote access for each Management Card or device. (Schneider Electric supports the authentication and authorization functions.)

EAPoL (802.1X Security)

Security Access	Description
Available methods: • Access to network ports based on RADIUS authorization	Extensible Authentication Protocol (EAP) over LAN (EAPoL) is a network port authentication protocol used in 802.1X (port-based Network Access Control). **Supported EAP methods:** EAP-TLS **Supported TLS versions:** v1.0, v1.1, and v1.2 with a recommendation to set-up minimum and maximum to v1.2 on the RADIUS server side.

Syslog

Security Access	Description
Available methods (standard): • Message transmission over TCP or UDP • Configurable server hostname or IP address • Selectable server port	Syslog is a message logging standard using the Syslog protocol, which was standardized by RFC 5424. It works using a client-server model, where the Network Management Card (NMC) is the client who sends message logs to your external Syslog server, using TCP or UDP.

Security Access	Description
Available methods (secure): • Configurable server hostname or IP address • Selectable server port • Transport Layer Security message transmission (over TCP only) • Allows one or two-way authentication	Secure Syslog behaves the same way as standard Syslog, except the messages are encrypted using Transport Layer Security (TLS) before being transmitted. The NMC supports both one-way and two-way authentication between the client (the NMC) and your external Syslog server. Secure Syslog can only be used with TCP.

Change default Super User password

At first login to the NMC, you will be prompted to change the default Super User password of `apc`. You cannot change the user name of the Super User. It is recommended that the Super User account is disabled, once any additional Administrator accounts are created.

Note: If you forget the Super User password, you can reset it back to its default of `apc` by holding down the Reset button on the NMC's faceplate for 15 seconds. The NMC's Status LED will flash orange three times in a short burst to indicate that the reset was successful. This action is logged to the Event Log.

Alternatively, you can reset the Super User password back to its basics in the Web UI (**Control > Network > Reset NMC Settings**) or through the CLI interface (`resetToDef`). To reset the Super User password, Administrator, or Network user privileges are required. Reset-related actions are logged to the Event Log.

Note: This will reset the Management Card to its default values and remove all information. If you are copying your configuration to another NMC, it is recommended you export your config.ini file before resetting the device.

Port assignments

If the FTP server, SSH/SFTP/SCP, or the Web server uses a non-standard port, a user must specify the port in the command line or Web address used to access the Management Card or device. A non-standard port number provides an additional level of security. The ports are initially set at the standard "well known ports" for the protocols. To increase security, change the ports to any unused port numbers from 5001 to 32768 for the FTP server and from 5000 to 32768 for the other protocols and servers. (The FTP server uses both the specified port and the port one number lower than the specified port.)

User names, passwords, and community names with SNMPv1

All user names, passwords, and community names for SNMPv1 are transferred over the network as plain text. A user who is capable of monitoring the network traffic can determine the user names and passwords required to log on to the accounts of the command line interface or Web interface of the Management Card or network-enabled device. If your network requires the higher security of the encryption-based options available for the command line interface and Web interface, disable SNMPv1 access or set its access to **Read**. (**Read** access allows you to receive status information and use SNMPv1 traps.)

SNMPv1 is disabled by default. To check SNMPv1 settings, go to **Configuration > Network > SNMPv1 > Access.** Clear the **Enable SNMPv1 access** check box and click **Apply**.

To set SNMPv1 access to **Read**, perform the following steps: On the **Configuration** tab select **Network**. Select **SNMPv1** and then **Access Control**. For each configured Network Management System (NMS), click the community names and set the Access Type to **Read**. Select **Apply**.

Watchdog Features

Automatic Logout

By default, users will be automatically logged out of the NMC Web UI and CLI interfaces after 3 minutes of inactivity. The default logout time for user accounts can be adjusted through the Web UI: **Configuration > Security > Local Users > Default Settings**.

Authentication

You can choose security features for the Management Card or network-enabled device that control access by providing basic authentication through user names, passwords, and IP addresses, without using encryption. These basic security features are sufficient for most environments in which sensitive data are not being transferred.

As an added layer of security, network-based port access via EAPoL can also be utilized to request network access at the individual port level via the network's switch or router (where applicable) which the Management Card is connected.

Password Requirements and Recommendations

Strong passwords are enabled by default for all NMC user accounts. Provided passwords must be between 8 and 64 characters in length. In addition, provided passwords cannot include:

- Your user name as part of the password
- Commonly-used sequences like qwerty1234 or passw0rd

Strong passwords can be disabled for user accounts in the Web UI (**Configuration > Security > Local Users > Default Settings**), however, this is not recommended.

For enhanced security, it is recommended that you also configure the Password Change Interval and Bad Login Attempts features in the Web UI (**Configuration > Security > Local Users > Default Settings**).

- **Password Change Interval:** If enabled, all user account passwords must be changed after a user-specified duration between 0 - 365 days. The default value is 0, never.
- **Bad Login Attempts:** This feature mitigates brute force attacks by locking user accounts after a user-specified number of unsuccessful logins between 0 - 99. The default value is 5. When a user account is locked, it must be re-enabled by the Super User account, or a user account with Administrator privileges.

SNMP GETS, SETS, and Traps

For enhanced authentication when you use SNMP to monitor or configure the Management Card or network-enabled device, choose SNMPv3. The authentication passphrase used with SNMPv3 user profiles ensures that a Network Management System (NMS) attempting to communicate with the Management Card or device is the NMS it claims to be, that the message has not been changed during transmission, and that the message was not delayed, copied, and sent again later at an inappropriate time. SNMPv3 is disabled by default.

The Schneider Electric implementation of SNMPv3 allows the use of the SHA-1 or MD5 protocol for authentication.

Web interface and command line interface

To ensure that data and communication between the Management Card or network-enabled device and the client interfaces (the command line interface and the Web interface) cannot be intercepted, you can provide a greater level of security by using one or more of the following encryption-based methods:

- For the Web interface, use the Transport Layer Security (TLS) protocol
- To encrypt user names and passwords for command line interface access, use the Secure Shell (SSH) protocol
- To encrypt user names, passwords, and data for the secure transfer of files, use the Secure FTP (SFTP) or Secure Copy (SCP) protocol.

Note: For more information on encryption-based security, see **Encryption**.

Encryption

SNMP, GETS, SETS, and Traps

For encrypted communication when you use SNMP to monitor or configure the Management Card or network-enabled device, choose SNMPv3. The privacy passphrase used with SNMPv3 user profiles ensures the privacy of the data (by means of encryption, using the AES or DES encryption algorithm) that an NMS sends to or receives from the Management Card or device.

Secure Shell (SSH), Secure FTP (SFTP) and Secure Copy (SCP) for the Command Line Interface

The Secure Shell protocol

SSH provides a secure mechanism to access computer consoles, or *shells,* remotely. The protocol authenticates the server (in this case, the Management Card or network-enabled device) and encrypts all transmissions between the SSH client and the server.

- SSH is a high-security alternative to Telnet. SSH protects the user name and password, which are the credentials for authentication, from being used by anyone intercepting network traffic.
- To authenticate the SSH server (the Management Card or network-enabled device) to the SSH client, SSH uses a host key unique to the SSH server. The host key is an identification that cannot be falsified, and it prevents an invalid server on the network from obtaining a user name and password by presenting itself as a valid server.

Note: For information on supported SSH client applications, see **Secure Shell (SSH)**.

The Management Card or device supports SSHv2, which provides protection from attempts to intercept, forge, or change data during transmission.

Secure FTP and Secure Copy

SFTP and SCP are secure file transfer applications that you should use instead of FTP. SFTP and SCP use the SSH protocol as the underlying transport protocol for encryption of user names, passwords, and files.

- When you enable and configure SSH, you automatically enable and configure SFTP and SCP. No further configuration of SFTP or SCP is needed.
- FTP is disabled by default. FTP settings can be reviewed at **Configuration > Network > FTP Server**. To disable FTP, clear the **Enable** check box and click **Apply**.

Transport Layer Security (TLS) for the Web interface

For secure Web communication, enable Transport Layer Security (TLS) by selecting HTTPS as the protocol mode to use for access to the Web interface of the Management Card or network-enabled device. HyperText Transfer Protocol over Secure Sockets Layer (HTTPS) is a Web protocol that encrypts and decrypts page requests from the user and pages that are returned by the Web server to the user. The Management Card or network-enabled device supports TLS versions 1.1, 1.2 and 1.3.

Note: Secure Socket Layer (SSL) version 3 is not supported.

Note: The Management Card automatically negotiates to use the highest supported protocol or cipher suite that is supported by the Management Card and the client.

Note: When TLS is enabled, your browser displays a small lock icon.

TLS uses a digital certificate to enable the browser to authenticate the server (in this case, the Management Card or device). The browser verifies the following:

- The format of the server certificate is correct.
- The expiration date and time of the server certificate have not passed.
- The DNS name or IP address specified when a user logs on matches the common name in the server certificate.
- The server certificate is signed by a trusted certifying authority. Each major browser manufacturer distributes CA root certificates of the commercial Certificate Authorities in the certificate store (cache) of its browser so that it can compare the signature on the server certificate to the signature on a CA root certificate.

Note: See **Creating and Installing Digital Certificates** for a summary of how these certificates are used. TLS also uses various algorithms and encryption ciphers to authenticate the server, encrypt data, and ensure the integrity of the data, i.e., that it has not been intercepted and sent by another server.

Note: Web pages that you have recently accessed are saved in the cache of your Web browser and allow you to return to those pages without re-entering your user name and password. Always close your browser session before you leave your computer unattended.

Creating and Installing Digital Certificates

Purpose

For network communication that requires a higher level of security than password encryption, the Web interface of the Management Card or network-enabled device supports the use of digital certificates with the Transport Layer Security (TLS) protocol. Digital certificates can authenticate the Management Card or device (the server) to the Web browser (the TLS client).

Note: You can generate a 1024-bit key or a 2048-bit key - choose a 2048-bit key for increased security.

The sections that follow summarize the two methods of creating, implementing, and using digital certificates to help you determine the most appropriate method for your system.

- Method 1: Use the default certificate auto-generated by the Network Management Card or network-enabled device (2048-bit).
- Method 2: Generate your own certificate. The system requires a Privacy-Enhanced Mail (PEM) encoded public certificate and a PEM encoded private key. Both files should have a **.pem** file extension.

Choosing a Method for your System

Using the Transport Layer Security (TLS) protocol, you can choose any of the following methods for using digital certificates.

Method 1: Use the default certificate auto-generated by the Network Management Card or network-enabled device

TLS is enabled by default. During booting, if no server certificate exists, the Management Card or device generates a default server certificate that is self-signed but that you cannot configure.

Method 1 has the following advantages and disadvantages.

Advantages:

- Before they are transmitted, the user name and password and all data to and from the Management Card or device are encrypted.
- You can use this default server certificate to provide encryption-based security while you are setting up either of the other two digital certificate options, or you can continue to use it for the benefits of encryption that TLS provides.

Disadvantages:

- This method does not include the authentication provided by a CA certificate (a certificate signed by a Certificate Authority). There is no CA Certificate cached in the browser. Therefore, when you log on to the Management Card or device, the browser generates a security alert, indicating that a certificate signed by a trusted authority is not available, and asks if you want to proceed. To avoid this message, you must install the default server certificate into the certificate store (cache) of the browser of each user who needs access to the Management Card or device, and each user must always use the fully qualified domain name of the server when logging on to the Management Card or device.
- The default server certificate has the serial number of the Management Card or device in place of a valid *common name* (the DNS name or the IP address of the Management Card or device). Therefore, although the Management Card or device can control access to its Web interface by user name, password, and account type (e.g., **Super User, Administrator**, **Device-Only User**, **Network-Only**, or **Read-Only User**), the browser cannot authenticate which Management Card or device is sending or receiving data.
- The length of the *public key* (RSA key) that is used for encryption when setting up a TLS session is 2048-bit, by default.

Method 2: Add a valid certificate to the system

Generate a certificate signing request (CSR) file (a **.csr** file) to send to a Certificate Authority. This can be created using OpenSSL, Certreq.exe or any tool that generates a CSR. The Certificate Authority returns a signed certificate (a **.crt** file or **.cer** file typically) based on information you submitted in your request. If this file is not in **.pem** format, you must covert the file to **.pem** format. The below OpenSSL command takes a file in **.pfc** format and converts it to **.pem** format:

```
openssl pkcs12 -in client_ssl.pfx -out client_ssl.pem -clcerts
```

For a full list of commands, see the **OpenSSL documentation**. You can then upload the certificate to the Network Management Card together with its private key.

Note: You can also use Method 2 if your company or agency operates its own Certificate Authority. Use your own Certificate Authority in place of a commercial Certificate Authority.

Method 2 has the following advantages and disadvantages.

Advantages

Before they are transmitted, the user name and password and all data to and from the Management Card or device are encrypted.

- You have the benefit of authentication by a Certificate Authority that already has a signed root certificate in the certificate cache of the browser. (The CA certificates of commercial Certificate Authorities are distributed as part of the browser software, and a Certificate Authority of your own company or agency has probably already loaded its CA certificate to the browser store of each user's browser.)
- You choose the length of the *public key* (RSA key) that is used for setting up a TLS session (use 2048-bit which is the default setting, or use 4064-bit to provide complex encryption and a high level of security).
- The server certificate that you upload to the Management Card or device enables TLS to authenticate that data are being received from and sent to the correct Management Card or device. This provides an extra level of security beyond the encryption of the user name, password, and transmitted data.
- The browser matches the digital signature on the server certificate that you uploaded to the Management Card or device with the signature on the CA root certificate that is already in the browser's certificate cache to provide additional protection from unauthorized access.

Disadvantages

Setup requires the extra step of requesting a signed root certificate from a Certificate Authority.

- An external Certificate Authority may charge a fee for providing signed certificates.

Firewalls

Although some methods of authentication provide a higher level of security than others, complete protection from security breaches is almost impossible to achieve. Well-configured firewalls are an essential element in an overall security scheme.

Logs: The Active Firewall Policy Log lists the most recent firewall events, including the protocol, traffic, action, and rule priority, in reverse chronological order.

Note: This log is not persistent and can hold up to 2000 events.

Configuration: Enable or disable the overall firewall functionality.

Active Rules: Lists the individual rules that are being enforced based on the current active policy.

Test Policy: Temporarily enforce the rules of a policy.

Vulnerability Reporting and Management

How to report a vulnerability

Cybersecurity incidents and potential vulnerabilities can be reported via the Schneider Electric website - **Report a Vulnerability**.

Command Line Interface Access and Security

Introduction

Users with Super User, Administrator, Device User, Network-Only, Read-Only accounts can access the command line interface through Secure Shell (SSH). (A Super User or Administrator can enable these access methods by selecting the **Configuration > Network > Console > Access**.) SSH is enabled by default.

SSH for high-security access. If you use the high security of TLS for the Web interface, use Secure Shell (SSH) for access to the command line interface. SSH encrypts user names, passwords and transmitted data.

To use SSH, you must first configure SSH and have an SSH client program installed on your computer.

Secure Shell (SSH)

SSH is enabled by default. Enabling SSH automatically enables SFTP and SCP.

Note: When SSH is enabled and its port is configured, no further configuration is required to use Secure FTP (SFTP) or Secure Copy (SCP). SFTP and SCP use the same configuration as SSH. To use SSH, you must have an SSH client installed. Most Linux and other UNIX® platforms include an SSH client, but Microsoft Windows operating systems do not. SSH clients are available from various vendors.

To configure the options for Secure Shell (SSH):

- On the **Configuration** tab of the Web interface, select **Network** on the top menu bar, and select **Access** under the **Console** heading.
- Configure the port settings for SSH.

Note: For information on the extra security a non-standard port provides, see Port assignments.

- Select: **Configuration > Network > Console > SSH Host Key**. specify a host key file previously created with OpenSSL.
- If you do not specify a host key file here, if you install an invalid host key, or if you enable SSH with no host key installed, the Management Card or device generates a 2048-bit RSA host key.
- Display the *fingerprint* of the SSH host key for SSH version 2. Most SSH clients display the fingerprint at the start of a session. Compare the fingerprint displayed by the client to the fingerprint that you recorded from the Web interface or command line interface of the Management Card or device.

Web Interface Access and Security

HTTP and HTTPS (with TLS)

HyperText Transfer Protocol (HTTP) provides access by user name and password, but does not encrypt user names, passwords, and data during transmission. HyperText Transfer Protocol over Secure Sockets Layer (HTTPS) encrypts user names, passwords, and data during transmission, and provides authentication of the Management Card or device by means of digital certificates.

Note: See **Creating and Installing Digital Certificates** to choose among the several methods for using digital certificates.

To configure HTTP and HTTPS:

- On the **Configuration** tab, select **Network** on the top menu bar and **Access** under the **Web** tab.
- Enable either HTTP or HTTPS and configure the ports that each of the two protocols will use. Changes take effect the next time you log on. When TLS is activated, your browser displays a small lock icon.

Note: For information on the extra security a non-standard port provides, see Port assignments.

- Select: **Configuration > Network > Web > SSL Certificate** to determine whether a server certificate is installed on the Management Card or device.
- In the Web interface, browse to the certificate file and upload it to the Management Card or device.

Note: A certificate that the Management Card or device generates has some limitations. See **Method 1: Use the default certificate auto-generated by the Network Management Card or network-enabled device**.

- If a valid digital server certificate is loaded, the **Status** field displays the link **Certificate Valid**. Click the link to display the parameters of the certificate.

Parameter	Description
Issued To	**Common Name (CN)**: The IP Address or DNS name of the Management Card or device. This field controls how you must log on to the Web interface. • If an IP address was specified for this field when the certificate was created, use an IP address to log on. • If the DNS name was specified for this field when the certificate was created, use the DNS name to log on. If you do not use the IP address or DNS name that was specified for the certificate, authentication fails, and you receive an error message asking if you want to continue. For a server certificate generated by default by the Management Card or device, this field displays the serial number of the Management Card or device instead. **Organization (O)**, **Organizational Unit (OU**), and **Locality, Country:** The name, organizational unit, and location of the organization using the server certificate. For a server certificate generated by default by the Management Card or device, the **Organizational Unit (OU)** field displays “Internally Generated Certificate.” **Serial Number**: The serial number of the server certificate.
Issued By	**Common Name (CN)**: The Common Name as specified in the CA root certificate. For a server certificate generated by default by the Management Card or device, this field displays the serial number of the Management Card or device instead. **Organization (O)** and **Organizational Unit (OU**): The name and organizational unit of the organization that issued the server certificate. If the server certificate was generated by default by the Management Card or device, this field displays “Internally Generated Certificate.”
Validity	**Date Issued**: The date and time at which the certificate was issued. **Expiration Date**: The date and time at which the certificate expires.
Fingerprints	Each of the two fingerprints is a long string of alphanumeric characters, punctuated by colons. A fingerprint is a unique identifier to further authenticate the server. Record the fingerprints to compare them with the fingerprints contained in the certificate, as displayed in the browser. **SHA1 Fingerprint**: A fingerprint created by a Secure Hash Algorithm (SHA-1). **MD5 Fingerprint**: A fingerprint created by a Message Digest 5 (MD5) algorithm. **Note:** This does not represent the signature hash algorithm used on the certificate.

RADIUS

Supported RADIUS Functions and Servers

Supported functions

Schneider Electric supports the authentication and authorization functions of Remote Authentication Dial-In User Service (RADIUS). Use RADIUS to administer remote access for each Management Card or network-enabled device centrally. When a user accesses the Management Card or device, an authentication request is sent to the RADIUS server to determine the permission level of the user.

Note: For more information on permission levels, see Types of user accounts.

Supported RADIUS Servers

FreeRADIUS v2.x and v3.x, and Microsoft Server 2012 and 2019 Network policy Server (NPS) are supported. Other commonly available RADIUS applications may work, but may not have been fully tested.

Configure the Management Card or Device

Authentication

On the **Configuration** tab, select **Security** on the top menu bar. Then, under **Remote Users** on the left navigation menu, select **authentication** to define an authentication method:

- **Local Authentication Only**: RADIUS is disabled. Local authentication is enabled.
- **RADIUS, then Local Authentication**: Both RADIUS and local authentication are enabled. Authentication is requested from the RADIUS server first; local authentication is used only if the RADIUS server fails to respond.
- **RADIUS Only**: RADIUS is enabled. Local authentication is disabled.

Note: RADIUS configuration supports Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) only.

Note: If **RADIUS Only** is selected, and the RADIUS server is unavailable, improperly identified, or improperly configured, remote access is unavailable to all users. You must use a direct connection, via a micro-USB cable (part number 960-0603), to change the RADIUS access setting to **Local Authentication Only** or **Radius, then Local Authentication** to regain access.

To login serially to RADIUS, **Remote Authentication Override** (**Configuration > Security > Session Management**) and **Serial Remote Authentication Override** (**Configuration > Security > Local Users > Management**) must be enabled. If **Override** is not enabled, you cannot login serially.

Please see the “Local access to the web interface” section in the **NMC 4 Installation Guide** for more information on how to gain local access to the command line interface. These instructions can also be used to gain local access to the internal NMC using the IP address `169.254.251.1`.

RADIUS

To configure RADIUS, on the **Configuration** tab, select **Security** on the top menu bar. Then, under **Remote Users** on the left navigation menu, select **RADIUS**.

Settings	Description
RADIUS	The server name or IP address of the RADIUS server.
Port	The port of the RADIUS server (1812 by default). The NMC also supports ports 1645, 1646, and 5000 - 32768.
Secret	The secret shared between the RADIUS server and the Management Card or device.
Reply Timeout	The time in seconds that the Management Card or device waits for a response from the RADIUS server.
Authentication Method	Protocol to be used when authorizing a user with the RADIUS server. This is CHAP by default. The NMC also supports PAP.

Configure the RADIUS Server

You must configure your RADIUS server to work with the Management Card or device. The server configuration is specific to the server in use and is out of the scope of this document.

RADIUS-based Authentication Authorization Accounting (AAA) is supported by the range of Schneider Electric devices, and only a subset of Vendor Specific Attributes (VSAs) are applicable.

- Add the IP address of the Management Card or device to the RADIUS server-client (NAS) list.
- Users should be configured with Service-Type attribute unless Vendor Specific Attributes (VSAs) are defined. If no Service-Type attribute is configured, the user has read-only access.

Supported IETF (RFC2865) Attributes

Idle-Timeout

Configures a time in seconds that a user can remain idle for before being logged off.

Service-Type

Only the values listed in the below table are supported.

Name	Value	Description
Login	1	Equivalent of ReadOnly.
Administrative	6	Equivalent of Admin.
Providing any other value will result in the user having read-only access.		

Supported APC Vendor Specific Attributes

Vendor Specific Attributes (VSAs) take precedence over IETF RADIUS attributes. For an example of a RADIUS dictionary file, please see **dictionary.apc**. The dictionary can be used in RADIUS server configurations.

APC vendor identifierdisct

Vendor Identifier for APC is 318.

APC-Service-Type

APC-Service-Type VSA is of identifier equals to 1.

The attribute values supported by the Management Card or device are listed in the below table.

Name	Value	Description
Admin	1	Full access to the Management Card or device.
Device	2	Read-write access to the device-related menus only.
ReadOnly	3	ReadOnly access.
Card	5	Synonym of the Super User. Full access to the Management Card or device and can delete Administrator accounts.
NetworkOnly	6	Read-write access to the network-related menus only. The Administrator account can enable or disable the Network-Only user account.
Providing any other value will result in the user having read-only access.		

Please see Knowledge Base article **FA156083** for information on how to configure a RADIUS server to authenticate with a Network Management Card.

Secure Disposal Guidelines

Introduction

This topic outlines how to wipe the Network Management Card of all information and configurations.

Delete device contents

To wipe the Network Management Card or network-enabled device, hold down the Reset button on the NMC's faceplate for 60 seconds. The NMC's Status LED will slowly flash green three times to indicate that the reset was successful.

NOTE: This will reset the Management Card to its default values and remove all information. If you are copying your configuration to another NMC, it is recommended you export your config.ini file before resetting the device.

These secure disposal guidelines only apply to the external AP9644 card and **not** the internal Network Management Card. Performing a 60-second reset on the internal NMC will render the NMC and UPS device inoperable, and a field service engineer will be required to recover the UPS.

Dispose of physical device

For information on how to physically dispose of the Network Management Card or network-enabled device and destroy its volatile memory, please consult the **Statement of Volatility document** available on the Schneider Electric website.

Appendix 1: Network Management Card Security Deployment Guide

Overview

As network security continues to grow and change in the fast-paced IT industry, user requirements for security solutions are becoming a requirement for system delivery. The Network Management Card (NMC) interfaces are implemented to provide users with as much flexibility as possible. Industry standard security implementation coupled with the flexibility of the Network Management Card, enables products to exist in different user environments.

Best Practices for the Network Management Card

To maintain security throughout the deployment lifecycle, Schneider Electric recommends reviewing the following considerations for:

- Physical Security
- Device Security
- Network Security

Note: Different deployments may require different security considerations.

This document provides general security guidance to help you decide on an appropriate secure deployment based on your specific security requirements.

Physical Security

Deploy the equipment in a secure location

Custodians should secure equipment from unauthorized physical access.

- Access should be restricted to those who require access to maintain the equipment.
- Restricted areas should be clearly marked for authorized personnel only.
- Restricted areas should be secured by locked doors.
- Access to the restricted areas should produce a physical or electronic audit trail.

Secure access to the device front panel and console port

Deploy the device in a rack or cage that can be locked with a suitable key, or other physical methods. This will prevent access to the physical ports of the device.

Description of Risk

Attackers with physical access to covered equipment can access the device without authorization.

Recommendations

Physical security must be in place to control physical access to restricted areas and facilities containing devices. Devices should be locked behind cabinets or protected by physical restraints that prevent unauthorized access or removal from restricted areas. Access to areas containing covered equipment should only be granted to personnel who require access based on their job function.

Restricted areas should display signs that clearly indicate access is for authorized personnel only. Facilities containing covered devices should give minimum indication of their purpose, with no obvious signs identifying the presence of related functions.

Physical access control devices, such as key card readers, doors and cabinet locks, should be tested prior to use and on a periodic basis (e.g. annually). Resource custodians should produce physical or electronic audit trails to record all personnel's physical access to restricted areas for security incident investigation. Inventory of who has physical access to control devices should be regularly reviewed, and any inappropriate access identified during the review should be promptly removed.

Device Security

Note: For more information on Device Security options, refer to **Appendix 2: Security Hardening Checklist**.

Software Patch Updates

Schneider Electric strongly recommends that, prior to deployment, customers ensure their devices have been updated with the latest firmware versions.

Customers are also strongly advised to review security bulletins that relate to their Schneider Electric products. For information on new and updated security bulletins, visit the **Schneider Electric Security Bulletins web page**.

Network Management Card devices must only run software for which security patches are made available in a timely fashion. All currently available security patches must be applied on a schedule appropriate to the severity of the risk they mitigate.

Privileged Accounts

Privileged and super-user accounts (Administrator, root, etc.) must not be used for non-administrator activities. Network services must run under accounts assigned the minimum necessary privileges.

Also minimize the number of local accounts.

Certificates

Replace the Default SSL/TLS Certificate

Default SSL/TLS certificates are created during the initial configuration of the device. These certificates are not intended for use in production deployments and should be replaced. Schneider Electric recommends that customers configure the device to use certificates either from a reputable Certificate Authority (CA) or appropriate certificates from your enterprise CA.

Use of Authentication

Network services and local (console) device access must require authentication by means of passphrases or other secure authentication mechanisms unless the explicit purpose of the service/device is to provide unauthenticated access.

Minimum Protocol

Set the minimum allowed Transport Layer Security Protocol that Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS) uses to secure the communication between the browser and the device. This should be set to TLS 1.2. (**Configuration > Network > Web > Access**)

SSH Host Key

Schneider Electric recommends the use of an SSH host key. An SSH host key authenticates the identity of the server (the Management Card or device) each time an SSH client contacts that server. Each server with SSH enabled must have an SSH host key on the server itself. Use the NMC Security Wizard CLI utility to create this key.

Logging

Schneider Electric recommends enabling the generation (and therefore, the logging) of Syslog messages for events that have Syslog configured as a notification method. To configure notification methods for events, navigate to the Event Actions screen (**Configuration > Notifications > Event Actions**). Use the available functionality to integrate with Syslog.

No Unattended Console Sessions

Devices must be configured to “lock” or log out and require a user to re-authenticate if left unattended for more than a specified number of minutes. By default, this is set to 3 minutes. (**Configuration > Security > Local Users > Management - General User**)

No Unnecessary Services

If a network service is not necessary for the intended purpose or operation of the device, ensure that service is not running.

Network Security

When deploying a Network Management Card to a production environment, Schneider Electric strongly recommends that the below key configuration changes are made.

Firewalls

Deploy a Network Layer Firewall

Schneider Electric strongly recommends that the device is not exposed to the public Internet and is deployed behind an appropriate Stateful Packet Inspection (SPI) firewall.

Enable Device Firewall Software

The device’s Firewall software must be running and configured to block all inbound traffic that is not explicitly required for the intended use of the device (default: deny). Use of a network-based firewall does not obviate the need for host-based firewalls.

Use a ‘Default Deny’ policy.

Schneider Electric recommends that administrators configure the Application Firewall with a deny all policy at the global level to block all requests that do not match the Application Firewall policy.

Background and Description of Risk

Insufficient restrictions on system access over the network increases exposure to attacks from viruses, worms, and spyware, and may also facilitate undesired access to resources. Not having a rule in place that denies incoming traffic unnecessarily exposes a system to compromise.

Recommendations

Log firewall activity

A firewall will reduce the likelihood of compromise, but cannot prevent all attacks. Firewall logs, if enabled, can be used to identify successful attacks. In the event of a system compromise, these logs are used in forensic analysis to determine the extent of the compromise and nature of the attack.

Enable logs; retain at least 30 days of data; and collect at least source and destination IP addresses and ports, application, protocol, direction, date and time, and rule.

Log files should be read-only, and with write access granted only to the firewall service account.

Allow incoming traffic from Information Security scanners

Configure your firewalls to allow network-based scanning by Information Security (IS) vulnerability scanners. IS should scan hosts on the network and determine if hosts are vulnerable to common network threats, or if a system appears to have been compromised.

Network Segmentation

Schneider Electric strongly recommends that network traffic to the device's management interface is separated, either physically or logically, from normal network traffic. A flat network architecture makes it easier for malicious actors to move around within the network; whereas with network segmentation, organizations can enhance network security by controlling access to sensitive data in the form of enabling or denying network access. A strong security policy entails segmenting the network into multiple zones, with varying security requirements, and rigorously enforcing the policy on what is allowed to move from zone to zone.

Other Security Detection and Monitoring Tools

Schneider Electric recommends that the environment is protected and monitored by appropriate physical, technical and administrative tools for network intrusion and monitoring such as IDS/IPS and appropriate SIEM solutions.

Appendix 2: Security Hardening Checklist

This checklist contains recommended configuration changes to help provide a security hardening profile for Network Management Card-enabled products.

Upload a custom HTTPS certificate

Your Network Management Card-enabled device creates an internally-generated HTTPS certification. It is recommended that you create a custom certificate to help strengthen authentication.

Disable older versions of TLS

Transport Layer Security (TLS) is a cryptographic protocol that provides communication security over the internet. Ensure that older versions of TLS are disabled on your Network Management Card-enabled device, and use the latest version available.

Disable FTP

Disable File Transfer Protocol (FTP) when it is not in use to help harden security on your device. If SSH is enabled, SFTP and SCP, which are more secure than FTP, can be used for file transfers.

Configure SNMPv3 to use AES/SHA

Configure SNMPv3 to use the most secure algorithms, AES and SHA, to provide encryption and authentication.

Use custom network ports where applicable

By using a non-standard port, your device may not be detected by scans looking only for standard ports. This applies to protocols such as HTTPS, SSH, SMTP, Syslog, etc.

Change the Super User account password

After installation and initial configuration of your Network Management Card-enabled device, you will be prompted to enter a new password for the Super User account.

Disable Super User account

Ensure there is at least one Administrator account enabled on your device. Once an Administrator account is configured, it is recommended that the Super User account is disabled. The Administrator account has the same privileges as the Super User account.

Enable Strong Passwords

Enable this feature to ensure strong passwords are created. All passwords will be required to be a minimum length and contain special characters to make passwords harder to guess.

Enable Force Password Change

Enable this feature to force all passwords to be changed after a user-specified number of days.

Disable unused network addressing protocols (IPv4/IPv6)

To help secure your device, disabled unused addressing protocols such as IPv4 and IPv6.

Disable Ping Response (IPv4)

IPv4 Ping Response allows your device to respond to network pings. Disable this feature to help make your device undetectable.

Enable internal firewall with appropriate access rules

Your Network Management Card-enabled device has an inbuilt firewall that can be used to restrict access to and from your device for various protocols and addresses.

Disable IPv6 auto-configuration

When the NMC is configured for IPv6 auto-configuration, it is vulnerable to IPv6 router advertisement flood attacks on the local network segment. If your network is susceptible to these type of attacks, it is recommended you configure the NMC with a static IPv6 address or add protection for such attacks.

Enable Syslog Mutual Authentication over TLS

Enable the NMC to send Syslog messages to a Syslog server using Mutual Authentication. Note: Your Syslog server must be configured to use Mutual Authentication.

Disable Modbus TCP

By default, Modbus TCP is disabled as it is an insecure protocol and needs to be protected at the network level. If Modbus TCP is required, we recommend that it is protected using the NMC's firewall to restrict the clients that can connect to the Modbus server.

Worldwide Customer Support

Customer support for this or any other product is available at no charge in any of the following ways:

- Visit the Schneider Electric Web site to access documents in the Schneider Electric Knowledge Base and to submit customer support requests.
  - **www.schneider-electric.com** (Corporate Headquarters)
    Connect to localized Schneider Electric Web sites for specific countries, each of which provides customer support information.
  - **www.schneider-electric.com/support/**
    Global support searching Schneider Electric Knowledge Base and using e-support.
- Contact the Schneider Electric Customer Support Center by telephone or e-mail.
  - Local, country-specific centers: go to **www.schneider-electric.com** click > Support > Contact Support for contact information.

For information on how to obtain local customer support, contact the representative or other distributors from whom you purchased your product.