Security Handbook

Network Management Card 3, Firmware Version 3.4.x

990-91251R-001

Publication Date: August, 2025

Schneider Electric

Table of Contents

Introduction 1

Content and Purpose of this Guide 1

User Management 1

Types of User Accounts 1
User Feature Privilege Table 2

Security. 2

Security Features 2
Authentication 7
Encryption 8
Secure SHell (SSH) and Secure CoPy (SCP) for the Command Line Interface 9
Transport Layer Security (TLS) for the Web interface 10
Creating and Installing Digital Certificates 11
Choosing a Method for your System 11
Firewalls 14

Vulnerability Reporting and Management 15

How to report a vulnerability 15

Using the NMC Security Wizard CLI Utility 16

Overview. 16

Authentication by Certificates and Host Keys 16
Files you Create for TLS and SSH Security 17

Create a Root Certificate and Server Certificates 18

Summary 18
Procedure for Creating the CA Root Certificate 18
Load the CA Root Certificate to your Browser 19
Create an SSL/TLS Server Certificate 19
Load the Server Certificate to the Management Card or Device 19

Create a Server Certificate and Signing Request. 20

Summary 20
Procedure for Creating the Certificate Signing Request (CSR) 20
Import the Signed Certificate 21
Load the Server Certificate to the Management Card or Device 21

Create an SSH Host Key 21

Summary 21
Procedure for Creating the Host Key 21
Load the Host Key to the Management Card or Device 22

Using the ssl command in the Command Line Interface .23

Overview 23

Configure the NMC's HTTPS certificate 23

Display the current NMC HTTPS certificate 23
Create a new private key 23
Configure the certificate 23

NMC Security Wizard CLI Utility Backwards Compatibility 24

Command Line Interface Access and Security 25

Introduction 25

Telnet and Secure SHell (SSH) 25

Web Interface Access and Security 26

HTTP and HTTPS (with TLS) 26

HSTS 26

RADIUS 28

Supported RADIUS Functions and Servers 28

Supported functions 28
Supported RADIUS Servers 28
Configure the Management Card or Device 28
RADIUS 29
Configure the RADIUS Server 29
Example using Service-Type Attributes 29
Examples using Vendor Specific Attributes 30
RADIUS Users file with VSAs 31
Example with UNIX shadow passwords 31

TACACS+ 32

Supported TACACS+ Functions and Servers 32

Supported functions 32
Supported TACACS+ Servers 32
Configure the Management Card or Device 32
TACACS+ 33
Configure the TACACS+ Server 33

LDAP 35

Supported LDAP Functions and Servers 35

Supported functions 35
Supported LDAP Servers 35
Configure the Management Card or Device 35
LDAP 35
Configure the LDAP Server 35

Secure Disposal Guidelines..... 36

Introduction. 36

Delete device contents 36
Dispose of physical device 36

Appendix 1: Network Management Card Security Deployment Guide 37

Overview. 37

Best Practices for the Network Management Card 37

Physical Security 37

Description of Risk 37
Recommendations 38

Device Security. 38

Software Patch Updates 38
Secure NMC System (SNS) Tool 38
Privileged Accounts 38
Certificates 38
Use of Authentication 39
Minimum Protocol 39
SSH Host Key 39
Logging 39
No Unattended Console Sessions 39
No Unnecessary Services 39

Network Security 39

Firewalls 39
Background and Description of Risk 40
Recommendations 40
Network Segmentation 40
Other Security Detection and Monitoring Tools 40
Validate Security Settings 41

Appendix 2: Network Management Card Security Hardening

Checklist 42

Appendix 3: Copyright Notices.....45

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.

Introduction

Content and Purpose of this Guide

This guide documents security features for firmware version 3.4.x of the Network Management Card 3 and for devices with embedded components of Schneider Electric Network Management Cards, which enable 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:

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

In addition, this guide documents how to use the NMC Security Wizard CLI utility, and the ssl and ssh commands in the Command Line Interface (CLI) to create the components required for the high security available through TLS and SSH.

NOTE: The NMC Security Wizard CLI utility can create security components for Management Cards or devices running firmware version 1.1.0.16 and higher. The ssl and ssh commands are available in firmware version 1.4 and higher.

NOTE: If you upgrade to firmware version 2.0.x or higher, you cannot downgrade to a firmware version lower than 2.0.x.

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.
- Administrator: 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 and data log (but cannot delete the contents of either log), and can use the device-related menus and commands.
- Network-Only User: can only access network-related information.
- A Read-Only User: can access the event log, data log, and device-related menus, but cannot change configurations, control devices, delete data, delete the content of logs, or use file transfer options.

NOTE: Some APC devices have additional user accounts, e.g., outlet users for Switched Rack PDUs and an A/C Manager for some NetworkAIR devices. For information on the additional account type, see the User's Guide provided with the device.

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

NOTE: The Administrator, Device, Network-Only, and Read-Only user accounts are disabled by default, and cannot be enabled until a password is set for each user account.

NOTE: Actions performed by users, such as logging in to any interface, changing configuration values, and modifying settings of the attached device are logged in the Event Log. These entries contain the username, a timestamp, and what action was taken by the user.

User Feature Privilege Table

	User Type				
Feature	**Super User**	**Administrator**	**Device User**	**Network-Only**	**Read-Only**
Network Status	✓	✓	X	✓	X
Network/ Security Configuration	✓	✓	X	✓	X
Network Control	✓	✓	X	✓	X
Device Status	✓	✓	✓	X	✓
Device Configuration	✓	✓	✓	X	X
Device Control	✓	✓	✓	X	X
User Management	✓	✓	X	X	X
View Event Log	✓	✓	✓	✓	✓
View Data Log	✓	✓	✓	X	✓
Delete Event Log	✓	✓	X	X	X
Delete Data Log	✓	✓	X	X	X
Configure Event Log	✓	✓	X	X	X
Configure Data Log	✓	✓	X	X	X
File Transfer	✓	✓	✓	X	X
NMC3 Firmware Update	✓	✓	X	X	X

Security

Security Features

Protection of passwords and passphrases

No password or passphrase is stored on the Network Management Card in plain text.

- Passwords are salted and hashed in accordance with NIST Special Publication 800-63B using PBKDF2-HMAC-SHA256.
- Passphrases, which are used for authentication and encryption, are encrypted before they are stored on the Network Management Card.

Summary of access methods

Serial access to the command line interface.

Security Access	Description
Access is by user name and password and by security level	Always enabled

An overview of the current configuration is available in the CLI banner displayed after log on, or in the Web UI at the following path: **Configuration > Network > Summary**.

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)	Available methods: • Telnet – With Telnet, the user name and password are transmitted as plain text. • SSH – For high security, use SSH. SSH provides encrypted access to the command line interface, to provide additional protection from attempts to intercept, forge, or alter data during transmission. If you select SSH as your remote access protocol, disable Telnet. **NOTE:** Telnet is disabled, and SSH is enabled by default.

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 or 255.255.255.255: 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. **NOTE:** SNMPv1 and SNMPv3 are disabled by default.
Available methods (SNMPv3): • Four User Profiles • Authentication through an authentication passphrase • Encryption through a privacy passphrase • SHA-256, SHA or MD5 authentication • AES-256, AES or DES encryption algorithm • NMS IP filters	

* SNMPv2c is also supported by SNMPv1 and its configuration 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 CoPy (SCP)	Available methods: • FTP – With FTP, the user name and password are transmitted as plain text, and files are transferred without encryption. • SCP – Use SCP to encrypt the user name and password and the files being transferred, such as firmware updates, configuration files, log files, .fwl files, Transport Layer Security (TLS) certificates, EAPoL certificates, and Secure SHell (SSH) host keys. If you choose SCP as your file transfer protocol, enable SSH and disable FTP. **NOTE:** FTP is disabled, and SCP is enabled 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)	Available methods: • HTTP – In basic HTTP authentication mode, the user name and password are transmitted as plain text (with no encoding or encryption). • TLS – 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. **NOTE:** HTTP is disabled, and HTTPS is enabled by default.

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. (APC supports the authentication and authorization functions.)

TACACS+

Security Access	Description
Available methods: • A server secret shared between the TACACS+ server and the Management Card or device • The TACACS+ server name or IP address (IPv4 or IPv6) and port	TACACS+ (Terminal Access Controller Access-Control System Plus) is an authentication, authorization, and accounting service used to centrally administer remote access for each Management Card or device. (APC supports the authentication and authorization functions.)

LDAP

Security Access	Description
Available methods: Simple bind over TLS	LDAP (Lightweight Directory Access Protocol) is a protocol for accessing directory information services. It is commonly used for storing information about users and their group memberships. The NMC supports multiple LDAP schemas and can authenticate users given their username and password. It can determine the NMC permission level based on a user's group memberships in the LDAP directory.

EAPoL (802.1X Security)

Security Access	Description
Available methods: • Access to network ports based on RADIUS server authorization	Extensible Authentication Protocol (EAP) over LAN (EAPoL) is a network port authentication protocol used in 802.1X (port-based Network Access Control).

Syslog

Security Access	Description
Available methods (standard): • Message transmission over TCP or UDP. • Configurable server host name 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.
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 user names and passwords immediately

After installation and initial configuration of the Management Card or network-enabled device, immediately change the user names and passwords from their defaults to unique user names and passwords to establish basic security. You are required to change the default Super User password at first log in as a security measure. It is recommended you change the default Super User password before connecting the Management Card or network-enabled device to a network.

The password must be a minimum of 8 characters in length and must not appear in a list of 5000 known compromised passwords.

NOTE: 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.

Port assignments

If the Telnet, FTP, SSH/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.)

Usernames, 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.)

To disable SNMPv1 access on the **Configuration** tab, select **Network** on the top menu bar and select **Access** under the **SNMPv1** heading. 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**.

NOTE: SNMPv1 is disabled by default and the Community Names are blank.

Secure Boot with Root of Trust

Secure Boot with Root of Trust provides enhanced security at the NMC hardware level. The NMC's processor uses ECDSA (secp256r1) to verify the bootloader's signature using a known public key, and the bootloader also uses ECDSA (secp256r1) to verify firmware signatures using Schneider Electric's Firmware Signing CA public key stored in the bootloader.

Personally Identifiable Information (PII)

It is highly recommended that you do not enter Personally Identifiable Information (PII) into text fields, such as locations, descriptions, and labels. It is also recommended that you use generic email addresses instead of personal email addresses.

Authentication

You can choose security features for the Management Card or network-enabled device that control access by providing basic authentication through network port access, 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.

Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA) adds an additional layer of security to user logins by requiring a one-time password (OTP) sent via email after successful username and password authentication.

When MFA is enabled:

- Users must enter a 6-digit OTP sent to their configured email address to complete login.
- MFA applies to all login interfaces: Web UI, SSH/SCP, Telnet, FTP, Serial CLI, and UPS display.
- Local user accounts must have an email address configured.
- For remote users authenticated via LDAP, RADIUS, or TACACS+, the email address is retrieved from the respective protocol (see protocol-specific sections).
- If a remote user’s email cannot be determined, but the username is formatted as an email address, that will be used.
- If no email address is available, MFA will be skipped for local users and login will proceed normally. Remote users without an email will be unable to log in.

NOTE: An SMTP server must be configured for MFA to function.

Password Requirements and Recommendations

In firmware version 3.1 and higher, strong passwords are enabled by default. It is highly recommended that you enable strong passwords. The new passwords created for user accounts requires:

- Minimum 8 and maximum 64 characters in length
- Not found in a list of 5000 known compromised passwords.

For enhanced security, it is recommended that you also enable the Bad Login Attempts feature in the Web UI (**Configuration > Security > Local Users > Default Settings**). Additionally, the **Password Policy** setting may be enabled if required by your organization.

- **Bad Login Attempts:** This feature mitigates brute force attacks by locking user accounts for one hour after a user-specified number of unsuccessful logins between 0-99. When a user account is locked, it may also be manually re-enabled by the Super User account, or a user account with Administrator privileges. The default value is 10 from 3.0.x release.
- **Password Policy:** If enabled, all user account passwords must be changed after a user-specified duration between 0 - 365 days. The default value is 0, never.

NOTE: The active user sessions are terminated automatically after a password change.

If additional password policies or configurations are required, external authentication services such as, RADIUS, TACACS+, or LDAP are recommended. For example, a configurable user lockout time.

For Smart-UPS Modular Ultra systems, the User Mode for the UPS display is set to Authentication needed:

As special (non-alphanumeric) characters are not supported on the keyboard for the UPS display, it is recommended to create passwords at least 12 characters in length (using upper case, lower case, and numbers) for any user account that will be given UPS display access.

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 APC implementation of SNMPv3 allows the use of the SHA-256, 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 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-256, AES or DES encryption algorithm) that an NMS sends to or receives from the Management Card or device.

Configuration and Data Logs

Configuration and data logs are encrypted using AES-256 ESSIV and cryptographically authenticated with HMAC-SHA256 by the NMC before use.

Secure SHell (SSH) 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. Telnet does not provide encryption.
- 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 **Telnet and Secure SHell (SSH)**. To create a host key, see **Create an SSH Host Key**

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

- When you enable SSH, you should disable Telnet. **NOTE:** Telnet is disabled, and SSH is enabled by default.
- The interface, user accounts, and user access rights are the same whether you access the command line interface through SSH or Telnet.

Secure CoPy

SCP is a secure file transfer application that you can use instead of FTP. SCP uses 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 SCP. No further configuration of SCP is needed.
- You must explicitly disable FTP. It is not disabled by enabling SSH. To disable FTP, on the **Configuration** tab, select **Network** and then **FTP Server**. Clear the **Enable** check box and click **Apply**. **NOTE:** Telnet is disabled, and SSH is enabled by default.

NOTE: When the SCP command is used in OpenSSH version 9.0 or higher, SFTP is used by default for file transfers. This causes an issue as the NMC does not support SFTP. To use SCP with version 9.0 or higher, the -O option must be added to the SCP command in order to use the SCP protocol (scp -O <file> <user>@<remote>:<file>).

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 Transport Layer Security (TLS) versions 1.1, 1.2, or 1.3.

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. Use the client-side settings to enable/disable certain protocols or cipher suites. Alternatively, the various cipher suites/algorithms the Management Card supports can be configured via the CLI interface. The Minimum Protocol field can also be configured to be used to force the minimal protocol (TLS 1.1, TLS 1.2, or TLS 1.3) to use when negotiating a connection.

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 (or Subject Alt 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: It is recommended to use short certificate lifetimes as the NMC is unable to check the revocation status of certificates.

You can use the NMC Security Wizard CLI utility to create a certificate signing request to an external Certificate Authority, or if you do not want to use an existing Certificate Authority, you can create an APC root certificate to upload to the certificate store (cache) of the browser. You can also use the utility to create a server certificate to upload to the Management Card or device.

NOTE: See **Creating and Installing Digital Certificates** for a summary of how these certificates are used. To create certificates and certificate requests, see **Create a Root Certificate and Server Certificates** and **Create a Server Certificate and Signing Request.**

SSL/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: In firmware version 1.4.x and higher, you can generate ECDSA keys. It is highly recommended you generate ECDSA keys over RSA keys as they provide a higher level of security.

The sections that follow summarize the four 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 (ECDSA P-256-bit).
  NOTE: AOS 1.1.0.16 and higher use a SHA-2 signature algorithm.
- Method 2: Use the NMC Security Wizard CLI utility to create a CA certificate and a server certificate.
- Method 3: Use the NMC Security Wizard CLI utility to create a certificate-signing request to be signed by the root certificate of an external Certificate Authority and to create a server certificate.
  NOTE: You can also use Method 3 if your company or agency operates its own Certificate Authority. Use the NMC Security Wizard CLI utility in the same way, but use your own Certificate Authority in place of a commercial Certificate Authority.
- Method 4: Use the `ssh` and `ssl` commands in the CLI. See **Using the ssl command in the Command Line Interface** for more information.

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.

When you enable TLS, you must reboot the Management Card or device. During rebooting, 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) that Methods 2 and 3 provide. 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* or *Subject Alt 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**, or **Read-Only User**), the browser cannot authenticate which Management Card or device is sending or receiving data. **NOTE:** The Common Name will be the hostname of the NMC after it completes its reset operation.

Method 2: Use the NMC Security Wizard CLI utility to create a CA certificate and a server certificate

Use the NMC Security Wizard CLI utility to create two digital certificates:

- *CA root certificate* (Certificate Authority root certificate) that the NMC Security Wizard CLI utility uses to sign all server certificates and which you then install into the certificate store (cache) of the browser of each user who needs access to the Management Card or device.
- A *server certificate* that you upload to the Management Card or device. When the NMC Security Wizard CLI utility creates a server certificate, it uses the CA root certificate to sign the server certificate.

The Web browser authenticates the Management Card or device sending or requesting data:

- To identify the Management Card or device, the browser uses the *Common Name* or *Subject Alt Name* (IP address or DNS name of the Management Card or device) that was specified in the server certificate's *distinguished name* when the certificate was created.
- To confirm that the server certificate is signed by a "trusted" signing authority, the browser compares the signature of the server certificate with the signature in the root certificate cached in the browser. An expiration date confirms whether the server certificate is current.

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 choose the length of the *public key* (RSA key) that is used for encryption when setting up a TLS session (use 2048-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 is 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 root certificate that you install to the browser enables the browser to authenticate the server certificate of the Management Card or device to provide additional protection from unauthorized access.

Disadvantage

Because the certificates do not have the digital signature of a commercial Certificate Authority, you must load a root certificate individually into the certificate store (cache) of each user's browser. (Browser manufacturers already provide root certificates for commercial Certificate Authorities in the certificate store within the browser, as described in Method 3.)

Method 3: Use the NMC Security Wizard CLI utility to create a certificate-signing request to be signed by the root certificate of an external Certificate Authority and to create a server certificate

Use the NMC Security Wizard CLI utility to create a request (a .csr file) to send to a Certificate Authority. The Certificate Authority returns a signed certificate (a .crt file or .cer file typically) based on information you submitted in your request. You then use the NMC Security Wizard CLI utility to create a server certificate (a .p15 file) that includes the signature from the root certificate returned by the Certificate Authority. Upload the server certificate to the Management Card or device.

NOTE: You can also use Method 3 if your company or agency operates its own Certificate Authority. Use the NMC Security Wizard CLI utility in the same way, but use your own Certificate Authority in place of a commercial Certificate Authority.

Method 3 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.) Therefore, you do not have to upload a root certificate to the browser of each user who needs access to the Management Card or device.
- You choose the length of the *public key* (RSA key) that is used for setting up a TLS session (use 2048-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 50 events.

Configuration: Enable or disable the overall firewall functionality.

Active Policy: Select an active policy from the available firewall policies.

Active Rules: Lists the individual rules that are being enforced based on the current active policy. **NOTE**: This option is only available when the firewall is enabled.

Create/Edit Policy: Create a new policy or edit an existing one.

Load Policy: Load a policy file (.fwl suffix) from a source external to this device.

Test Policy: Temporarily enforce the rules of a chosen policy.

Vulnerability Reporting and Management

How to report a vulnerability

Please direct your submission to **Technical Support** and include the following information:

- Product Line
- Vulnerable version
- Vulnerability type [CWE ID, if available]
- Organization name
- Email
- Phone number
- Country

Using the NMC Security Wizard CLI Utility

Overview

The NMC Security Wizard CLI utility creates components needed for high security for a Management Card or network-enabled device on the network when you are using Transport Layer Security (TLS) and related protocols and encryption routines.

NOTE: The NMC Security Wizard CLI utility can create security components for Management Cards or devices running firmware 1.1.0.16 or higher.

Authentication by Certificates and Host Keys

Authentication verifies the identity of a user or a network device (such as a Network Management Card or network-enabled device). Passwords typically identify computer users. However, for transactions or communications requiring more stringent security methods on the Internet, the Management Card or device supports more secure methods of authentication.

- Transport Layer Security (TLS), used for secure Web access, uses digital certificates for authentication. A digital *CA root* certificate is issued by a Certificate Authority (CA) as part of a public key infrastructure, and its digital signature must match the digital signature on a server certificate on the Management Card or device.
- Secure SHell (SSH), used for remote terminal access to the command line interface of the Management Card or device, uses a public *host key* for authentication.

How certificates are used

Most Web browsers, including all browsers supported by Network Management Cards or network-enabled devices, contain a set of CA root certificates from all of the commercial Certificate Authorities. Authentication of the server (in this case, the Management Card or device) occurs each time a connection is made from the browser to the server. The browser checks to be sure that the server's certificate is signed by a Certificate Authority known to the browser. For authentication to occur:

- Each server (Management Card or device) with TLS enabled must have a server certificate on the server itself.
- Any browser that is used to access the Web interface of the Management Card or device must contain the CA root certificate that signed the server certificate. If authentication fails, a browser message asks you whether to continue even though it cannot authenticate the server.

If your network does not require the authentication provided by digital certificates, you can use the default certificate that the Management Card or device generates automatically. The default certificate's digital signature will not be recognized by browsers, but a default certificate enables you to use TLS for the encryption of transmitted user names, passwords, and data. (If you use the default certificate, the browser prompts you to agree to unauthenticated access before it logs you on to the Web interface of the Management Card or device.)

How SSH host keys are used

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.

Files you Create for TLS and SSH Security

Use the NMC Security Wizard CLI to create these components of a TLS and SSH security system:

- The server certificate for the Management Card or network-enabled device, if you want the benefits of authentication that such a certificate provides. You can create either of the following types of server certificate:
    a. A server certificate signed by a custom CA root certificate also created with the NMC Security Wizard CLI. Use this method if your company or agency does not have its own Certificate Authority and you do not want to use an external Certificate Authority to sign the server certificate.
    b. A server certificate signed by an external Certificate Authority. This Certificate Authority can be one that is managed by your own company or agency or can be one of the commercial Certificate Authorities whose CA root certificates are distributed as part of a browser's software.
- A certificate signing request containing all the information required for a server certificate except the digital signature. You need this request if you are using an external Certificate Authority.
- A CA root certificate
- An SSH host key that your SSH client program uses to authenticate the Management Card or device when you log on to the command line interface.

NOTE: All private keys are encrypted by the firmware before storage on the device. The encryption key is unique for each device.

NOTE: You define whether the public keys for TLS certificates and the host keys for SSH that are created with the NMC Security Wizard CLI are 2048-bit RSA keys (the default setting), or 1024-bit RSA keys, which provide complex encryption and a higher level of security.

NOTE: NMC Security Wizard CLI uses the SHA-2 signature algorithm.

NOTE: If you do not create and use TLS server certificates and SSH host keys with the NMC Security Wizard CLI, the Management Card or device generates 2048-bit RSA keys using the SHA-2 signature algorithm.

Only APC server management and key management products can use server certificates, host keys, and CA root certificates created by the NMC Security Wizard CLI. These files will not work with products such as OpenSSL® and Microsoft® Internet Information Services (IIS).

Create a Root Certificate and Server Certificates

Summary

Use this procedure if your company or agency does not have its own Certificate Authority and you do not want to use a commercial Certificate Authority to sign your server certificates.

NOTE: Define the size of the public RSA key that is part of the certificate generated by the NMC Security Wizard CLI. You can generate a 1024-bit key, or you can generate a 2048-bit key, which provides complex encryption and a higher level of security. (The default key generated by the Management Card or network-enabled device, if you do not use the NMC Security Wizard CLI, is 2048 bits.)

Create a CA root certificate that will sign all server certificates to be used with Management Cards or devices. During this task, two files are created:

- The file with the **.p15** suffix is an encrypted file that contains the Certificate Authority's private key and public root certificate. This file signs server certificates.
- The file with the **.crt** suffix contains only the Certificate Authority's public root certificate. Load this file into each Web browser that will be used to access the Management Card or device so that the browser can validate the server certificate of that Management Card or device.
- Create a server certificate, which is stored in a file with a .**p15** suffix. During this task, you are prompted for the CA root certificate that signs the server certificate.
- Load the server certificate onto the Management Card or device.
- For each Management Card or device that requires a server certificate, repeat the tasks that create and load the server certificate.

Procedure for Creating the CA Root Certificate

1. If the NMC Security Wizard CLI is not already extracted to a folder on your computer, double-click the self-extracting archive to extract the necessary files.
2. Open a command prompt and navigate to the folder containing the extracted NMC Security Wizard CLI files.
3. Issue the below command and complete the fields to create the **CA Root Certificate**:

```
NMCSecurityWizardCLI --caroot -o <file> -n <common_name> -c <country> [-m
<state_province> -l <locality> -g <organization> -u <organizational_unit> -e
<email> -f <validity_from> -t <validity_to> -i <uri_name> -d <dns_name> -a
<ip_address>]
```

NOTE: Enter a name for this file using the -o flag, which will contain the certificate authority's public root certificate and private key. The file must not contain a suffix/file extension and, by default, will be created in the current folder.

NOTE: You can use the **-k** flag to specify the length of the key to generate (use 1024 bits or 2048 bits, which is the default setting, to provide complex encryption and a high level of security).

NOTE: When you provide the information to an internal/public CA, the **Country** and **Common Name** fields are the only required fields. For the Common Name field, enter an identifying name of your company or agency. Use only alphanumeric characters, with no spaces.

NOTE: By default, a CA root certificate is valid for 4 years from the current date, but you can edit the **Validity Period Start** and **Validity Period End** fields.

Load the CA Root Certificate to your Browser

Load the **.crt** file to the browser of each user who needs to access the management card or device.

NOTE: See the help system of the browser for information on how to load the **.crt** file into the browser's certificate store (cache). Following is a summary of the procedure for Microsoft Internet Explorer.

1. Select **Tools**, then **Internet Options** from the menu bar.
2. In the dialog box, on the **Content** tab click **Certificates** and then **Import**.
3. The Certificate Import Wizard guides you through the rest of the procedure. The file type to select is X.509, and the CA Public Root Certificate is the **.crt** file created in the procedure Create a Root Certificate and Server Certificates.

Create an SSL/TLS Server Certificate

1. Open a command prompt and navigate to the folder containing the extracted NMC Security Wizard CLI files.
2. Issue the below command and complete the fields to create the **SSL Server Certificate**:

   ```
   NMCSecurityWizardCLI --sslcert -o <file> -r <file> -n <common_name> -c
   <country> [-m <state_province> -l <locality> -g <organization> -u <organiza-
   tional_unit> -e <email> -f <validity_from> -t <validity_to> -i <uri_name> -d
   <dns_name> -a <ip_address>]
   ```

   NOTE: Enter a name for this file using the **-o** flag, which will contain the SSL server certificate and corresponding browser certificate. The file must not contain a suffix/file extension and, by default, will be created in the current folder with the **.p15** and **.crt** extensions respectively.

   NOTE: Enter the name for the **CA Public Root Certificate** using the **-r** flag. The value must not contain the suffix/file extension of the actual file.

   NOTE: You can use the **-k** flag to specify the length of the key to generate (use 1024 bits or 2048 bits, which is the default setting, to provide complex encryption and a high level of security).

   NOTE: When you provide the information to configure the CA root certificate, the **Country** and **Common Name** fields are the only required fields. For the **Common Name** field, enter an identifying name of your company or agency. Use only alphanumeric characters, with no spaces.

   NOTE: By default, a CA root certificate is valid for 4 years from the current date, but you can edit the **Validity Period Start** and **Validity Period End** fields.

   NOTE: Because the configuration information is part of the signature, the information for every certificate must be unique. The configuration of a server certificate cannot be the same as the configuration of the CA root certificate. (The expiration date is not considered part of the unique configuration. Some other configuration information must also differ.

3. The output will then display the certificate issuer and certificate subject information. If any information is incorrect, rerun the command with the correct values.

Load the Server Certificate to the Management Card or Device

1. Select: **Configuration > Network > Web > SSL Certificate tab**
2. Select **Add or Replace Certificate File**, and browse to the server certificate, the **.p15** file you created in the procedure Create a Root Certificate and Server Certificates.

NOTE: You can use FTP or Secure CoPy (SCP) instead to transfer the server certificate. An example command for SCP to transfer a certificate named **cert.p15** to a Management Card or device with an IP address of 156.205.6.185 would be: **scp cert.p15 apc@156.205.6.185:ssl/cert.p15**. Then, import the server certificate using the `ssl` command in the CLI. For example: `ssl key -i ssl/cert.p15`. For more information, see the **CLI Guide**.

NOTE: SCP utilities may have different command syntax.

Create a Server Certificate and Signing Request

Summary

Use this procedure if your company or agency has its own Certificate Authority or if you plan to use a commercial Certificate Authority to sign your server certificates.

- Create a Certificate Signing Request (CSR). The CSR contains all the information for a server certificate except the digital signature. This process creates two output files:
  a. The file with the **.p15** suffix contains the private key of the Management Card or device.
  b. The file with the **.csr** suffix contains the certificate signing request, which you send to an external Certificate Authority.
- When you receive the signed certificate from the Certificate Authority, import that certificate. Importing the certificate combines the **.p15** file containing the private key and the file containing the signed certificate from the external Certificate Authority. The output file is a new encrypted server certificate file with a **.p15** suffix.
- Load the server certificate onto the Management Card or device.
- For each Management Card or device that requires a server certificate, repeat the tasks that create and load the server certificate.

Procedure for Creating the Certificate Signing Request (CSR)

1. If the NMC Security Wizard CLI is not already extracted to a folder on your computer, double-click the self-extracting archive to extract the necessary files.
2. Open a command prompt and navigate to the folder containing the extracted NMC Security Wizard CLI files.
3. Issue the below command and complete the fields to create the **Certificate Signing Request**:

   ```
   NMCSecurityWizardCLI --csr -o <file> -n <common_name> -c <country>
   [-m <state_province> -l <locality> -g <organization> -u <organization-
   al_unit> -e <email> -i <uri_name> -d <dns_name> -a <ip_address>]
   ```

   NOTE: Enter a name for this file using the **-o** flag, which will contain the certificate signing request and corresponding private key. The file must not contain a suffix/file extension and, by default, will be created in the current folder with the **.csr** and **.p15** extensions respectively.

   NOTE: You can use the **-k** flag to specify the length of the key to generate (use 1024 bits or 2048 bits, which is the default setting, to provide complex encryption and a high level of security).

   NOTE: When you provide the information to configure the CA root certificate, the **Country** and **Common Name** fields are the only required fields. For the **Common Name** field, enter an identifying name of your company or agency. Use only alphanumeric characters, with no spaces.

   NOTE: By default, a CA root certificate is valid for 4 years from the current date, but you can edit the **Validity Period Start** and **Validity Period End** fields.
4. Send the certificate signing request to an external Certificate Authority, either a commercial Certificate Authority or, if applicable, a Certificate Authority managed by your own company or agency.

NOTE: See the instructions provided by the Certificate Authority regarding the signing and issuing of server certificates.

Import the Signed Certificate

When the external Certificate Authority returns the signed certificate, import the certificate. This procedure combines the signed certificate and the private key into an SSL/TLS server certificate that you then upload to the Management Card or device.

1. Open a command prompt and navigate to the folder containing the extracted NMC Security Wizard CLI files
2. Issue the below command and complete the fields to create the **SSL/TLS Server Certificate**:

   ```
   NMCSecurityWizardCLI --import -o <file> -s <file> -p <file>
   ```

   NOTE: Enter a name for this file using the **-o** flag, which will contain the SSL/TLS server certificate. The file must not contain a suffix/file extension and, by default, will be created in the current folder with the **.p15** extension.

   NOTE: Enter a name for this file using the **-s** flag, which contains the signed server certificate. The file must contain a suffix/file extension of **.cer** or **.crt**.

   NOTE: Enter a name for this file using the **-p** flag, which contains the private key. The file must not contain a suffix/file extension, but locally will have the **.p15** extension.
3. The output will then display the **Issuer Information** on the summary screen which confirms that the external Certificate Authority signed the certificate.

Load the Server Certificate to the Management Card or Device

1. Select: **Configuration > Network > Web > SSL Certificate**
2. Select **Add or Replace Certificate File**, and browse to the server certificate, the **.p15** file you created in the procedure Create a Root Certificate and Server Certificates.

NOTE: You can use FTP or Secure CoPy (SCP) instead to transfer the server certificate. An example command for SCP to transfer a certificate named **cert.p15** to a Management Card or device with an IP address of 156.205.6.185 would be: **scp cert.p15 apc@156.205.6.185:ssl/cert.p15**. Then, import the server certificate using the `ssl` command in the CLI. For example: `ssl key -i ssl/cert.p15`. For more information, see the **CLI Guide**.

NOTE: SCP utilities may have different command syntax.

Create an SSH Host Key

Summary

This procedure is optional. If you select SSH encryption, but do not create a host key, the Management Card or device generates a 2048-bit RSA key when it reboots. You define whether the host keys for SSH that are created with the NMC Security Wizard CLI are 1024-bit or 2048-bit RSA keys.

NOTE: You can generate a 1024-bit key, or you can generate a 2048-bit key, which provides complex encryption and a higher level of security.

- Use the NMC Security Wizard CLI to create a host key, which is encrypted and stored in a file with the **.p15** suffix.
- Load the host key onto the Management Card or device.

Procedure for Creating the Host Key

1. If the NMC Security Wizard CLI is not already extracted to a folder on your computer, double-click the self-extracting archive to extract the appropriate files.
2. Open a command prompt and navigate to the folder containing the extracted NMC Security Wizard CLI files.
3. Issue the below command and complete the fields to create the **SSH Server Host Key**:

   ```
   NMCSecurityWizardCLI --sshkey -o <file>
   ```

NOTE: Enter a name for this file using the **-o** flag, which will contain the SSH server host key. The file must not contain a suffix/file extension and, by default, will be created in the current folder with the **.p15** extension.

NOTE: You can use the **-k** flag to specify the length of the key to generate (use 1024 bits or 2048 bits, which is the default setting, to provide complex encryption and a high level of security).

Load the Host Key to the Management Card or Device

1. Select: **Configuration > Network > Console > SSH Host Key**
2. Select **Add or Replace Host Key**, and browse to the host key, the **.p15** file you created in the procedure Create the host key.
3. At the bottom of the **User Host Key** page, note the SSH fingerprint. Log on to the Management Card or device through your SSH client program and verify that the correct host key was uploaded by verifying that these fingerprints match the fingerprints that the client program displays.

NOTE: Alternatively, you can use FTP or Secure CoPy (SCP) to transfer the host key file to the Management Card or device. An example command for SCP to transfer a host key named **hostkey.p15** to a Management Card or device with an IP address of 156.205.6.185 would be: **scp hostkey.p15 apc@156.205.6.185:ssh/hostkey.p15**. Then, import the server certificate using the ssh command in the CLI. For example: ssh key -i ssh/cert.p15. For more information, see the **CLI Guide**.

NOTE: SCP utilities may have different command syntax.

Using the ssl command in the Command Line Interface

Overview

The topic details how to use the ssl command in the Command Line Interface (CLI) to configure the NMC's Web UI (HTTPS) certificate. It can be used as an alternative to the NMC Security Wizard CLI utility.

NOTE: The ssl command is available in firmware version 1.4 and higher.

The examples provided assumes that:

- "apc" is the NMC admin user
- "192.168.1.204" is the NMC IPv4 address
- "nmc.csr" is the created Certificate Signing Request (CSR)
- "nmc.crt" is the certificate signed by a Certificate Authority (CA)

The examples below show a shorthand syntax where the NMC CLI command follows an SSH invocation. All the commands following "ssh apc@192.168.1.204" are NMC CLI commands and may be typed at any NMC CLI command prompt. For more information, see the **CLI Guide**.

NOTE: You will be prompted to enter your NMC user name and password.

Configure the NMC's HTTPS certificate

Display the current NMC HTTPS certificate

Display the currently configured NMC HTTPS certificate:

```
ssh apc@192.168.1.204 ssl cert -s
```

Create a new private key

1. Delete the existing NMC HTTPS key:

   ```
   ssh apc@192.168.1.204 ssl key -d
   ```

2. Generate a new NMC HTTPS key:

   ```
   ssh apc@192.168.1.204 ssl key -ecdsa 256
   ```

Configure the certificate

Configuring the certificate is a three step process:

1. Create a Certificate Signing Request (CSR) and download it from the NMC:
   a. Create a Certificate Signing Request (CSR) from active configuration:
      ```
      ssh apc@192.168.1.204 ssl csr -q
      ```
   b. Download the created CSR:
      ```
      scp apc@192.168.1.204:ssl/nmc.csr nmc.csr
      ```

2. Create a certificate signed by a Certificate Authority (CA). How a CA creates a certificate from a CSR is beyond the scope of this example. There are many examples online on how to use Certificate Authorities to sign certificates, including how to create your own CA.
   – The Certificate Authority (CA) creates a signed certificate (nmc.crt) from the CSR (nmc.csr).
3. Upload and import the signed certificate. **NOTE:** The NMC certificate to be imported must match the NMC key used to create the NMC CSR in step 1.
   a. Upload the NMC certificate using Secure Copy:
      `scp nmc.crt apc@192.168.1.204:ssl/nmc.crt`
   b. Import the certificate:
      `ssh apc@192.168.1.204 ssl cert -i ssl/nmc.crt`

The NMC HTTPS certificate configuration is complete and the NMC HTTPS interface is available for immediate use.

NMC Security Wizard CLI Utility Backwards Compatibility

The ssl and ssh commands in the Command Line Interface (CLI) provide backwards compatibility with the NMC Security Wizard CLI Utility.

- Upload an NMC Security Wizard CLI utility nmc.p15 file:

  ```
  scp nmc.p15 apc@192.168.1.204:ssl/nmc.p15
  ```

- Import an NMC Security Wizard CLI utility nmc.p15 file:

  ```
  ssh apc@192.168.1.204 ssl key -i ssl/nmc.p15
  ```

Command Line Interface Access and Security

Introduction

All user accounts can access the command line interface through Telnet or Secure SHell (SSH), depending on which is enabled. (A Super User or Administrator can enable these access methods by selecting the **Configuration > Network > Console > Access**. By default, Telnet is disabled, and SSH is enabled.

The CLI commands available will depend on the user account accessing the command line interface. For example: the console command is only available to the Super User, Administrator, and Network Only User accounts.

Telnet for basic access: Telnet provides the basic security of authentication by user name and password, but not the high-security benefits of encryption.

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.

The interface, user accounts, and user access rights are the same whether you access the command line interface through SSH or Telnet, but to use SSH, you must first configure SSH and have an SSH client program installed on your computer.

Telnet and Secure SHell (SSH)

If SSH is enabled, you should disable Telnet access the command line interface, for improved security. Enabling SSH enables SCP automatically.

NOTE: When SSH is enabled and its port is configured, no further configuration is required to use Secure CoPy (SCP). SCP uses 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 Telnet and 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 Telnet and 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 the APC Security Wizard, and load it to the Management Card or device.
- Import the SSH key using the `ssh` command in the CLI. For example: `ssh key -i ssh/cert.p15`. For more information, see the **CLI Guide**.

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 an ECDSA host key of 256 bits. For the Management Card or device to create a host key, it must reboot. The Management Card or device can take up to 1 minute to create this host key, and SSH is not accessible during that time.

NOTE: Alternatively, from a command line interface such as the command prompt on Windows operating systems, you can use FTP or Secure CoPy (SCP) to transfer the host key file.

- 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. By default, HTTP is disabled, and HTTPS is enabled.

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. If a certificate was created with the NMC Security Wizard CLI utility but is not installed:
  - In the Web interface, browse to the certificate file and upload it to the Management Card or device.
  - Alternatively, use the Secure CoPy (SCP) protocol or FTP to upload the certificate file to the `/ssl` folder of the Management Card or device. Then, import the certificate using the `ssl` command in the CLI. For example: `ssl key -i ssl/cert.p15`. For more information, see the **CLI Guide**.

NOTE: Creating and uploading a server certificate in advance reduces the time required to enable HTTPS. If you enable HTTPS with no server certificate loaded, the Management Card or device creates one when it reboots.

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 Valid Certificate. Click the link to display the parameters of the certificate.

HSTS

HSTS (HTTP Strict Transport Security) is an HTTP header used to redirect insecure HTTP requests to an HTTPS version of the page. This is more secure than simply using a redirect, as it is not susceptible to man-in-the-middle attacks as it does not use an insecure HTTP channel. HSTS can be enabled in the CLI using the web `-hs` command and it is highly recommended that this is enabled.

This feature sets the Strict-Transport-Security header in the browser the first time a user visits an HTTPS page on the NMC and is only available when both HTTP and HTTPS are enabled. It instructs the browser to never visit an insecure version of the page if the header is valid.

HSTS will only operate if a non-self-signed certificate is loaded on the NMC, so it is necessary to load a certificate trusted by the browser on to the NMC.

For more information on the `-hs` option, see the **CLI Guide**.

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. **NOTE:** Full certificate properties can be verified via the browser. 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 “N/A.” **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 is the host name of the device. **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:	**Issued on**: The date and time at which the certificate was issued. **Expires on**: 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). **NOTE:** This does not represent the signature hash algorithm used on the certificate.

RADIUS

Supported RADIUS Functions and Servers

Supported functions

APC 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 2008 and 2012 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

NOTE: RADIUS user names used with Network Management Cards or devices are limited to 64 characters.

To define an authentication method, navigate to **Configuration > Security > Remote Users > Authentication** in the Web UI. Select RADIUS for “Remote User Authentication” to use RADIUS.

NOTE: The Network Management Card provides a mechanism for remote authentication to be overridden on a per-user basis. This allows a specific account to login serially even when Local User Authentication is set to Off. To enable this feature, navigate to **Configuration > Security > Session Management** and enable the **Remote Authentication Override** feature. Now you can go into each user account (**Configuration > Security > LocalUsers > Management**) and enable the **Serial Remote Authentication Override** check box for each user you want to allow this override for.

NOTE: If **Local User Authentication** is set to Off, and the RADIUS server is unavailable, improperly identified, or improperly configured, remote access is unavailable to all users. You must use a serial connection to the command line interface, log in with a user that has Serial Remote Authentication Override enabled, and change the Local User Authentication access setting to first or last to regain access.

For example, the command to change the local user authentication setting to first would be: `userauth -l first`

NOTE: RADIUS configuration supports Password Authentication Protocol (PAP) only.

RADIUS

To configure RADIUS, navigate to **Configuration > Security > Remote Users > RADIUS** on the Web UI.

NOTE: You can configure two RADIUS servers i) primary server, and ii) secondary server.

Settings	Description
RADIUS Server	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 1-65535.
Secret	The secret shared between the RADIUS server and the Management Card or device.
Require Message-Authenticator	Enabling this setting (disabled by default) will require the NMC to receive a valid Message-Authenticator attribute in the response from the RADIUS server.
Reply Timeout	The time in seconds that the Management Card or device waits for a response from the RADIUS server.
Test Settings	Enter the Administrator user name and password to test the RADIUS server configuration.
Skip Test and Apply	Do not test the RADIUS server configuration.

Configure the RADIUS Server

You must configure your RADIUS server to work with the Management Card or device. The examples in this section may differ somewhat from the required content or format of your specific RADIUS server. In the examples, any reference to outlets applies only to APC devices that support outlet users.

- Add the IP address of the Management Card or device to the RADIUS server client list (file).
- Users must be configured with Service-Type attributes unless Vendor Specific Attributes (VSAs) are defined instead. If no Service-Type attribute is configured, then the user will be granted read-only access. The two acceptable values for Service-Type are Administrators (6), which gives the user Administrator permissions, and Login-User (1), which gives the user Device permissions.
- When **Multi-Factor Authentication (MFA)** is enabled, each user's email address must be specified with the APC-Contact VSA (26.318.5).

NOTE: See your RADIUS server documentation for information about the RADIUS users file.

Example using Service-Type Attributes

In the following example of a RADIUS users file:

– **UPSAdmin** uth-Type = corresponds to **Service-Type: Administrative, (6)**

– **UPSDevice** corresponds to **Service-Type: Login-User, (1)**

– **UPSReadOnly** corresponds to **Service-Type: null**

UPSAdmin Cleartext-Password = "admin"

Service-Type = Administrative

UPSDevice Cleartext-Password = "device"

Service-Type = Login-User

UPSReadOnly Cleartext-Password = "readonly"

Examples using Vendor Specific Attributes

Vendor Specific Attributes (VSAs) can be used instead of the Service-Type attributes provided by your RADIUS server. This method requires a dictionary entry and a RADIUS users file. In the dictionary file, you can define the names for the ATTRIBUTE and VALUE keywords, but not the numeric values. If you change the numeric values, RADIUS authentication and authorization will not work correctly. VSAs take precedence over standard RADIUS attributes.

Dictionary file. Following is an example of a RADIUS dictionary file (dictionary.apc):

```
# dictionary.apc
VENDOR          APC                     318
BEGIN-VENDOR    APC
ATTRIBUTE       APC-Service-Type        1       integer
ATTRIBUTE       APC-Outlets             2       string
ATTRIBUTE       APC-Perms               3       string
ATTRIBUTE       APC-Username            4       string
ATTRIBUTE       APC-Contact             5       string
ATTRIBUTE       APC-ACCPX-Doors         6       string
ATTRIBUTE       APC-ACCPX-Status        7       string
ATTRIBUTE       APC-ACCPX-Access1       8       string
ATTRIBUTE       APC-ACCPX-Access2       9       string
ATTRIBUTE       APC-ACCPX-Access3       10      string
ATTRIBUTE       APC-ACCPX-Access4       11      string
ATTRIBUTE       APC-ACCPX-Access5       12      string
ATTRIBUTE       APC-ACCPX-Access6       13      string
ATTRIBUTE       APC-ACCPX-Access7       14      string

VALUE           APC-Service-Type        Admin       1
VALUE           APC-Service-Type        Device      2
VALUE           APC-Service-Type        ReadOnly    3
VALUE           APC-Service-Type        Outlet      4
VALUE           APC-Service-Type        Card        5
VALUE           APC-Service-Type        NetworkOnly 6
END-VENDOR      APC
```

RADIUS Users file with VSAs

Following is an example of a RADIUS users file with VSAs:

nmc_admin Cleartext-Password := "admin"

APC-Service-Type = Admin,

APC-Contact = user1@example.se.com

nmc_device Cleartext-Password := "device"

APC-Service-Type = Device

nmc_network Cleartext-Password := "networkonly"

APC-Service-Type = NetworkOnly

nmc_readonly Cleartext-Password := "readonly"

APC-Service-Type = ReadOnly

Give an Outlet user access to outlets 1, 2, 3 and 6-8 on a Rack PDU

pdu-user001 Cleartext-Password := "outlet"

APC-Service-Type = Outlet,

APC-Outlets = "1,2,3,6-8"

NOTE: The information below applies to AP8xxx SKUs when using the Network Port Sharing (NPS) feature.

give user access to outlets 1,2, and 3 on unit 1,

outlet 7 on unit 2, outlets 1 through 6

on unit 3, and outlets 1,2,4 through 6, 7 through 10,

and 20 on unit 4

pdu-user001 Cleartext-Password := "outlet"

APC-Service-Type = Outlet,

APC-Outlets = "1[1,2,3];2[7];3[1-6];4[1,2,4-6,7-10,20];"

NOTE: See the following related topics:

- ***Types of User Accounts*** for information on the three basic user permission levels (Super User/ Administrator, Device User, and Read-Only User). If your APC device has an additional user account type, e.g., outlet user for a Switched Rack PDU, see the *User's Guide* provided with your device for information on the additional account type.
- ***Supported RADIUS Servers*** for information on RADIUS servers tested and supported by APC.

Example with UNIX shadow passwords

If UNIX shadow password files are used **(/etc/passwd)** with the RADIUS dictionary files, the following two methods can be used to authenticate users:

- If all UNIX users have Administrator privileges, add the following to the RADIUS "user" file. To allow only Device Users, change the APC-Service-Type to **Device**.
  DEFAULT Auth-Type = System
  APC-Service-Type = Admin
- Add user names and attributes to the RADIUS "user" file, and verify the password against **/etc/passwd**. The following example is for users **bconners** and **thawk**:
  bconners Auth-Type = System
  APC-Service-Type = Admin
  thawk Auth-Type = System

TACACS+

Supported TACACS+ Functions and Servers

Supported functions

APC supports the authentication and authorization functions of the Terminal Access Controller Access-Control System Plus (TACACS+) protocol as defined in **RFC 8907**. Use TACACS+ to administer remote access for each Management Card or network-enabled device centrally. When a user accesses the Management Card or device, authentication and authorization requests are sent to the TACACS+ server to determine the permission level of the user.

NOTE: For more information on permission levels, see **Types of User Accounts**.

Supported TACACS+ Servers

All TACACS+ servers that conform to RFC 8907 should be compatible with the Management Card. The tac_plus daemon from Cisco's TACACS+ developer's kit has been fully tested and verified to work correctly.

Configure the Management Card or Device

Authentication

NOTE: TACACS+ usernames used with Network Management Cards or devices are limited to 64 characters.

To define an authentication method, navigate to **Configuration > Security > Remote Users > Authentication** in the Web UI. Select TACACS+ for "Remote User Authentication" to use TACACS+.

NOTE: The Network Management Card provides a mechanism for remote authentication to be overridden on a per-user basis. This allows a specific account to login serially even when Local User Authentication is set to Off. To enable this feature, navigate to **Configuration > Security > Session Management** and enable the **Remote Authentication Override** feature. Now you can go into each user account (Configuration > Security > Local Users > Management) and enable the Serial Remote Authentication Override check box for each user you want to allow this override for.

NOTE: If **Local User Authentication** is set to Off, and the TACACS+ server is unavailable, improperly identified, or improperly configured, remote access is unavailable to all users. You must use a serial connection to the command line interface, log in with a user that has Serial Remote Authentication Override enabled, and change the Local User Authentication access setting to first or last to regain access.

For example, the command to change the local user authentication setting to first would be: `userauth -l first`

TACACS+

To configure TACACS+, navigate to **Configuration > Security > Remote Users > TACACS+**.

NOTE: You can configure two TACACS+ servers i) primary server, and ii) secondary server.

Settings	Description
TACACS+ Server	The server name or IP address of the TACACS+ server.
Port	The port (49 by default) that the TACACS+ server listens on. You can change the port setting to any port from 1 to 65535.
Secret	The secret shared between the TACACS+ server and the device.
Reply Timeout	The time in seconds that the device waits for a response from the TACACS+ server.
Test Settings	Enter the username and password of any account on the server to test the newly configured settings before applying them.
Skip Test and Apply	Applies the settings without first performing a test authentication using the provided username and password.

Additionally, there are two settings that apply to both servers that determine an authorized user's permission level.

NOTE: The TACACS+ client implementation currently only supports the Administrator and Read-Only User permission levels.

Settings	Description
Read-Only User Privilege Level	Specify a value between 0 and 15. If an authorized user's privilege level (priv-lvl authorization argument) is greater than or equal to this, and less than the Administrator Privilege Level, then the user will be granted read only access. This value must be less than the Administrator Privilege Level.
Administrator Privilege Level	Specify a value between 0 and 15. If an authorized user's privilege level (priv-lvl authorization argument) is greater than or equal to this then the user will be granted administrator access. This value must be greater than the Read-Only User Privilege Level.

Configure the TACACS+ Server

You must configure your TACACS+ server to work with the Management Card or device.

- The Management Card requires that the TACACS+ server be configured with a shared secret. All TACACS+ packets sent by the device have the TAC_PLUS_UNENCRYPTED_FLAG flag in the header set to 0 and are obfuscated using the shared secret.
- The Management Card only supports the Password Authentication Protocol (PAP) authentication method, and so requires users on the TACACS+ server be configured with a PAP password. This allows the TACACS+ server to store user passwords using current best practices.

- The Management Card requires that the TACACS+ server configure users for session-based shell authorization with a specified privilege level to determine the level of access. This means that the Management card requests authorization for the “shell” service with the mandatory “cmd” argument set to the empty value. The server must reply with the same service and cmd arguments, as well as with the “priv-lvl” set to a value between 0 and 15. The server may also reply with optional argument “idletime” with a value between 1 and 60 to set the user’s idle time.
- When **Multi-Factor Authentication (MFA)** is enabled, each user’s email address must be specified with the optional custom attribute ‘mail’.

NOTE: If the Management Card receives any authorization arguments other than “service”, “cmd”, “priv-lvl”, or “idletime” the authorization request will be unsuccessful.

Example configuration for tac_plus server

It sets the shared secret to “shared_secret” and configures a single user with the username “nmc_user”, the password as “password”, the email address “nmc_user@company,com”, a privilege level of 15, and an idle time of 30 minutes:

```
key = shared_secret
user = nmc_user
{
  pap = cleartext "password"
  service = exec {
    priv-lvl = 15
    idletime = 30
    mail = nmc_user@company.com
  }
}
```

LDAP

Supported LDAP Functions and Servers

Supported functions

APC supports the Lightweight Directory Access Protocol (LDAP) protocol as defined in **RFC 4510** to search for users, perform simple bind authentication over TLS, and to find a user's group membership in the LDAP directory to determine NMC permission level. Multiple common LDAP schemas are supported, including the default Microsoft Active Directory schema for users and groups. Use LDAP to administer remote access for each Management Card or network-enabled device centrally. When a user accesses the Management Card or device, LDAP requests are sent to the LDAP server to determine the permission level of the user.

NOTE: For more information on permission levels, see **Types of User Accounts**.

Supported LDAP Servers

All LDAP servers that conform to RFC 4510 should be compatible with the Management Card. Open LDAP's slapd server, and Microsoft Active Directory have both been fully tested and verified to work correctly.

Configure the Management Card or Device

Authentication

NOTE: LDAP usernames used with Network Management Cards or devices are limited to 64 characters.

To define an authentication method, navigate to **Configuration > Security > Remote Users > Authentication** in the Web UI. Select LDAP for "Remote User Authentication" to use LDAP.

NOTE: The Network Management Card provides a mechanism for remote authentication to be overridden on a per-user basis. This allows a specific account to login serially even when Local User Authentication is set to Off. To enable this feature, navigate to **Configuration > Security > Session Management** and enable the **Remote Authentication Override** feature. Now you can go into each user account (Configuration > Security > Local Users > Management) and enable the Serial Remote Authentication Override check box for each user you want to allow this override for.

NOTE: If **Local User Authentication** is set to Off, and the LDAP server is unavailable, improperly identified, or improperly configured, remote access is unavailable to all users. You must use a serial connection to the Command Line Interface (CLI), log in with a user that has Serial Remote Authentication Override enabled, and change the Local User Authentication access setting to first or last to regain access.

For example, the command to change the local user authentication setting to first would be: `userauth -l first`

LDAP

To configure LDAP, navigate to **Configuration > Security > Remote Users > LDAP**.

NOTE: For more information on settings, see **NMC3 User Guide**.

Configure the LDAP Server

The configuration of an OpenLDAP, Active Directory, or other LDAP server is beyond the scope of this document. However, many common schemas are supported by default, including Active Directory users and groups, the POSIX schema defined in RFC 2307, the User Schema defined in RFC 4519, and the inetOrgPerson user class defined in RFC 2798. When configuring a new server, it is recommended that one of these schema is chosen. Ensure that groups are created for each NMC user type that you want to support and that users are added to them, accordingly.

When **Multi-Factor Authentication (MFA)** is enabled, the standard LDAP attribute 'mail' (0.9.2342.19200300.100.1.3) is used to determine the user's email address. This attribute is defined for the inetOrgPerson schema in RFC 2798 and is used by Active Directory.

Secure Disposal Guidelines

Introduction

This topic outlines how to reset the Network Management Card to its default settings and erase all user information and configurations.

Delete device contents

To reset the Network Management Card or network-enabled device:

- **Method 1:** Hold down the Reset button on the NMC's faceplate for 20 seconds, ensuring the NMC's Status LED is pulsing green during this time. When the LED changes to amber or orange, release the Reset button to allow the format function to complete and for the NMC to complete its reboot process.
- **Method 2:** Log in to the command line interface as a Super User or Administrator and issue the `format` command, followed by the `reboot` command. For more information on these commands, see the **CLI Guide**.

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. See Knowledge Base article **FA156131** for information on how to retrieve the config.ini file.

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**.

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. To increase physical security, it is recommended to add tamper resistance mechanisms to the NMC or the device it is installed in. This ensures that visible or electronic evidence remains when a tampering event occurs. For UPS devices, is recommended to place tamper-proof stickers or seals on the SmartSlot to detect unauthorized access to 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: Network Management Card 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.

Secure NMC System (SNS) Tool

The Secure NMC System (SNS) Tool provides an easy-to-use interface for remotely managing and updating your NMC3 firmware, so you never become outdated or exposed to additional risk. The SNS Tool provides access to independently certified IEC 62443-4-2 firmware.

The SNS Tool supports multiple applications and allows you to manage firmware updates for your Network Management Card 3, including pre-installed and standalone SmartSlot cards (AP9640, AP9641, AP9643) and embedded cards. For more information, see **apc.com/secure-nmc**.

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. Schneider Electric supports the authentication and authorization functions of Remote Authentication Dial-In User Service (RADIUS), Terminal Access Controller Access-Control System Plus (TACACS+), and Lightweight Directory Access Protocol (LDAP). You can configure the device to use RADIUS, TACACS+, or LDAP to authenticate remote users. [**Configuration > Security > Remote Users > Authentication**]

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 either TLS 1.2 or TLS 1.3 depending on your requirements. [**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 or generate it using the ssh command in the CLI. For more information, see **Using the ssl command in the Command Line Interface**.

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 **Configuration** > **Logs** > **Syslog**. Use the available functionality to integrate with Syslog. Use TCP/IP only for logging.

NOTE: NTP should be enabled on the device.

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 > Default Settings**] but can be individually configured for each local user [**Configuration > Security > Local Users > Management**]

No Unnecessary Services

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

Validate Security Settings

It is considered a best practice to validate configured security settings to ensure they work as intended. Schneider Electric strongly recommends making this practice mandatory whenever security configurations are modified. For example:

- Verify the configured firewall rules work by attempting to make a connection that is configured to be denied and ensuring it is denied.
- Attempt to log in with an invalid user name or password and validate that the unsuccessful login attempt is logged.
- Attempt to access the NMC via an insecure protocol (e.g. HTTP) and verify it's inaccessible.
- Attempt to change password to less than 8 characters.
- Ensure that you are logged out of NMC interfaces after the specified Session Timeout value, e.g. 5 minutes.

Appendix 2: Network Management Card Security Hardening Checklist

Upgrade to the latest firmware version

Visit the **Schneider Electric website** to verify you are running the latest firmware for your device. This will help ensure security vulnerabilities and features are up-to-date for your protection. **NOTE:** If you upgrade to firmware version 2.0.x or higher, you cannot downgrade to a firmware version lower than 2.0.x.

Disable HTTP and enable HTTPS

By default, HTTP is disabled on Network Management Card-enabled products. Disable HTTP if it is enabled, and enable HTTPS for a more secure and encrypted channel for web communication. If both HTTP and HTTPS are enabled, enable HTTP Strict Transport Security (HSTS). See **HSTS** for more information.

Upload a custom HTTPS certificate

Your Network Management Card-enabled device creates an internally-generated HTTPS certificate. It is recommended that you use the NMC Security Wizard CLI utility or the ssl command in the CLI to create a custom certificate to help strengthen authenticity. For more information, see **Using the NMC Security Wizard CLI Utility** and Using the ssl command in the Command Line Interface.

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 Telnet and enable SSH

By default, Telnet is disabled on Network Management Card-enabled products. Disable Telnet if it is enabled, and enable SSH for a more secure and encrypted channel for remote CLI communication.

Disable FTP

Disable FTP when it is not in use to help harden security on your device. If SSH is enabled, SCP, which is more secure than FTP, can be used for file transfers. **NOTE**: By default, FTP is disabled.

Disable SNMPv1 and enable SNMPv3

If enabled and configured, your device can be accessed via SNMP. It is recommended to use SNMPv3 as it is more secure than SNMPv1. By default, SNMPv1 and SNMPv3 are disabled.

Configure SNMPv3 to use AES-256/SHA-256

Configure SNMPv3 to use the most secure algorithms, AES-256 and SHA-256, 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, immediately change the default Super User account password. **NOTE**: You will be prompted to change the Super User password at first login to the NMC.

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.

Delete Read-Only/Device User accounts (if applicable)

Read-Only and Device User accounts are automatically created on your Network Management Card-enabled device. If not required, disable or delete these accounts to manage access control. **NOTE**: The Read-Only and Device user accounts are disabled by default.

Enable Strong Passwords

Enable this feature to ensure strong passwords are created. All passwords will be required to be a minimum length and shall not appear in a list of passwords known to be compromised.

Enable Multi-Factor Authentication (MFA)

Enable this feature to require a one-time password (OTP) via email for user logins across all interfaces.

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, disable 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.

Appendix 3: Copyright Notices

To view Copyright Notices for the Network Management Card 3, see **here**.

Worldwide Customer Support

Access to customer support terms may vary by product. 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 > Support > Operations around the world** for contact information.

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

990-91251R-001 **08/2025**