Easy Rack PDU v1x.xx

Security Handbook

990–91473
Release date: 01/2021

by Schneider Electric

Legal Information

Table of Contents

Introduction

Content and Purpose

This guide documents security features devices with Easy Rack PDU, 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.

- Transport Layer Security (TLS) v1.2
- SNMPv1, SNMPv2c, and SNMPv3

User Management

Types of User Accounts

The Easy Rack PDU has 2 basic levels of access.

- A Super User: can use all of the management menus available in the Web interface.
- A General User: can access the device-related menus, but cannot change configurations, control devices, delete data, delete the content of logs, or use file transfer options.

  NOTE: A Super User is an Administrator account which is persistent and cannot be deleted.

  NOTE: General user accounts are disabled by default and cannot be enabled until a password is set for the account.

Security

Security Features

Protection of passwords and passphrases

No password or passphrase is stored on the Easy Rack PDU in plain text.

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

Summary of access methods
SNMPv1, SNMPv2c, and SNMPv3

Security Access	Description
Available methods (SNMPv1/SNMPv2c)*: • Community Name	For SNMPv1/SNMPv2c, only use one community name for read and write access (the default is “public”), and for SNMPv3, user name restricts access to the Network Management System (NMS).
Available methods (SNMPv3): • Authentication through an authentication passphrase • Encryption through a privacy passphrase • SHA or MD5 authentication • AES or DES encryption algorithm	SNMPv3 has additional security features that include the following: • An authentication passphrase to ensure that an NMS trying to access the device is the NMS it claims to be. • Encryption of data during transmission, with a privacy passphrase required for encrypting and decrypting.

Web Server

Security Access	Description
Available methods: • User name and password • 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 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.

Change default user names and passwords immediately

After installation and initial configuration of the device, immediately change the user names and passwords from their defaults to unique user names and passwords to establish basic security.

User names, passwords, and community names with SNMPv1

All user names, passwords, and community names for SNMPv1 are transferred over the network as plain text. A user who is capable of monitoring the network traffic can determine the user names and passwords required to log on to the accounts of the command line interface or Web interface of the device. If your network requires the higher security of the encryption-based options available for the Web interface, disable SNMPv1 access.

To disable SNMPv1 access on the **Configuration** tab, clear the **Enable SNMPv1 access** check box and click **Apply**.

Authentication

You can choose security features for 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.

SNMP GETS, SETS, and Traps

For enhanced authentication when you use SNMP to monitor or configure the device, choose SNMPv3. The authentication passphrase used with SNMPv3 user profiles ensures that a Network Management System (NMS) attempting to communicate with the 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 enabled by default.

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

Web interface

To ensure that data and communication between the device and the Web interface cannot be intercepted, you can provide a greater level of security by using the following encryption-based method: Transport Layer Security (TLS) 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 device, choose SNMPv3. The privacy passphrase used with SNMPv3 user profiles ensures the privacy of the data (by means of encryption, using the AES or DES encryption algorithm) that an NMS sends to or receives from the device.

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 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 device supports Transport Layer Security (TLS) versions 1.2.

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 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.

You can use a certificate generator 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 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 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.

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 device supports the use of digital certificates with the Transport Layer Security (TLS) protocol. Digital certificates can authenticate the device (the server) to the Web browser (the TLS client).

NOTE: While you can generate a 1024-bit RSA key, or 2048-bit RSA key, it is highly recommended you generate a 256-bit ECC key, which provides complex encryption and a higher level of security.

The sections that follow summarize the three 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 device (256-bit ECC key).
- Method 2: Use a certificate generator to create a CA certificate and a server certificate.
- Method 3: Use a certificate generator 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 certificate generator Method 3 if your company or agency operates its own Certificate Authority. Use the certificate generator in the same way, but use your own Certificate Authority. Use the certificate generator in the same way, but use your own Certificate Authority in place of a commercial Certificate Authority.

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 device

When you enable TLS, you must reboot the device. During rebooting, if no server certificate exists, the 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 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:

- The device takes up to 1 minute to create this 256-bit (ECC key) certificate, and the Web interface is not available during that time (This delay occurs the first time you log on after you enable TLS).
- 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 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 device, and each user must always use the fully qualified domain name of the server when logging on to the device.
- The default server certificate has the serial number of the device in place of a valid *Common Name* or *Subject Alt Name* (the DNS name or the IP address of the device). Therefore, although the device can control access to its Web interface by user name, password, and account type (e.g., **Super User**, or **General User**), the browser cannot authenticate which device is sending or receiving data.
- The length of the *public key* (ECC key) that is used for encryption when setting up a TLS session is 256 bits (equivalent to 3072 bits RSA), by default.

Method 2: Use a certificate generator to create a CA certificate and a server certificate

Use a certificate generator to create two digital certificates:

- *CA root certificate* (Certificate Authority root certificate) that a certificate generator 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 device.

- A *server certificate* that you upload to the device. When a certificate generator creates a server certificate, it uses the CA root certificate to sign the server certificate.

The Web browser authenticates the device sending or requesting data:

- To identify the device, the browser uses the *Common Name* or *Subject Alt Name* (IP address or DNS name of the 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 device are encrypted.

- You choose the length of the *public key* that is used for encryption when setting up a TLS session (use 256-bit ECC key to provide complex encryption and a high level of security).
- The server certificate that you upload to the device enables TLS to authenticate that data is being received from and sent to the correct 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 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 a certificate generator 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 a certificate generator 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 certificate generator to create a server certificate (a .**pem** file) that includes the signature from the root certificate returned by the Certificate Authority. Upload the server certificate to the 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.

Advantages:

Before they are transmitted, the user name and password and all data to and from the 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 device.
- You choose the length of the *public key* that is used for setting up a TLS session (use 256-bit ECC key to provide complex encryption and a high level of security).

- The server certificate that you upload to the device enables TLS to authenticate that data are being received from and sent to the 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 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.

Disadvantage:
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.

Using the OpenSSL Certificate Generator

Overview

The OpenSSL creates components needed for high security for a device on the network when you are using Transport Layer Security (TLS) and related protocols and encryption routines.

Authentication by Certificates and Host Keys

Authentication verifies the identity of a user or a network device. Passwords typically identify computer users. However, for transactions or communications requiring more stringent security methods on the Internet, the 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 device.

How certificates are used
Most Web browsers, including all browsers supported by devices, contain a set of CA root certificates from all of the commercial Certificate Authorities. Authentication of the server (in this case, the 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 (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 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 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 device.)

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.

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

- The file **ca.crt** is 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 device so that the browser can validate the server certificate of that device.
- Create a server certificate, which is stored in a file with a .**pem** suffix. During this task, you are prompted for the CA root certificate that signs the server certificate.
- Load the server certificate onto the device.

- For each 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 OpenSSL 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 OpenSSL files.
3. Issue the below command and complete the fields to create the **CA Root Certificate**:
   a. `Create CA key file: openssl ecparam -genkey -name prime256v1 -out ca.key`
   b. `Create CA Root Certificate: openssl req -new -x509 -key ca.key -out caroot.crt -subj "/C=<country>/ST=<state_province>/L=<locality>/O=<organization>/OU=<organization_unit>/CN=<common_name>"`

Load the CA Root Certificate to your Browser

Load the **.crt** file to the browser of each user who needs to access the 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 **openssl.exe** file.
2. Issue the below command and complete the fields to create the **SSL Server Certificate**:
   a. `Create server key file: openssl ecparam -genkey -name prime256v1 -out server.key`
   b. `Create server Certificate: openssl req -new -x509 -key server.key -out server.crt`
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 Device

1. Select: **Configuration > System > Network > Update tab**
2. Select **Choose File** and browse to the server certificate, the **server.crt** file you created in the procedure Create Server Certificates and apply.
3. Select **Choose File** and browse to the server certificate, the **server.key** file you created in the procedure Create Server Certificates and apply.
4. Select **User Certificate and Key** and apply. Reboot the device to take effect.

Create a Server Certificate and Signing Request

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.

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

- The file **ca.crt** is 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 device so that the browser can validate the server certificate of that device.
- Create a server certificate, which is stored in a file with a .**pem** suffix. During this task, you are prompted for the CA root certificate that signs the server certificate.
- Load the server certificate onto the device.
- For each 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 OpenSSL 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 OpenSSL files.
3. Issue the below command and complete the fields to create the **CA Root Certificate**:
   a. `Create CA key file: openssl ecparam -genkey -name prime256v1 -out ca.key`
   b. `Create CA Root Certificate: openssl req -new -x509 -key ca.key -out caroot.crt -subj "/C=<country>/ST=<state_province>/L=<locality>/O=<organization>/OU=<organization_unit>/CN=<common_name>"`

Load the CA Root Certificate to your Browser

Load the **.crt** file to the browser of each user who needs to access the 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 **openssl.exe** file.
2. Issue the below command and complete the fields to create the **SSL Server Certificate**:
   a. `Create server key file: openssl ecparam -genkey -name prime256v1 -out server.key`

b. `Create server Certificate: openssl req -new -x509 -key server.key -out server.crt`

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 Device

1. Select: **Configuration > System > Network > Update tab**
2. Select **Choose File** and browse to the server certificate, the **server.crt** file you created in the procedure Create Server Certificates and apply.
3. Select **Choose File** and browse to the server certificate, the **server.key** file you created in the procedure Create Server Certificates and apply.
4. Select **User Certificate and Key** and apply. Reboot the device to take effect.

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.

1. 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 **.key** suffix contains the private key of the device.
   b. The file with the **.csr** suffix contains the certificate signing request, which you send to an external Certificate Authority.
2. When you receive the signed certificate from the Certificate Authority, load the server certificate onto the device.
3. For each 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 OpenSSL 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 OpenSSL files.
3. Issue the below command and complete the fields to create the **Certificate Signing Request**:
   a. `Create server key file: openssl ecparam -genkey -name prime256v1 -out server.key`
   b. `Create CSR file: openssl req -new -sha256 -key server.key -out server.csr`
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.

Load the Server Certificate to the Device

1. Select: **Configuration > System > Network > Update tab**
2. Select **Choose File**, and browse to the server certificate, the file signed by own company or agency and apply.
3. Select **Choose File**, and browse to the server certificate, the **key** file you created in the procedure Create Server Certificates and apply.
4. Select **User Certificate and Key**, and apply, reboot the device to take effect.

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 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 **System** on the top menu bar and under the **Network** 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 reboot the device and log on. When TLS is activated, your browser displays a small lock icon.

  NOTE: If a certificate was created but is not installed: In the Web interface, browse to the certificate and key file and upload it to the device.

  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 device creates one when it reboots.

Parameter	Description
Issued To:	**Common Name (CN)**: The IP Address or DNS name of the 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 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 device, the **Organizational Unit (OU)** field displays “Internally Generated Certificate.” **Serial Number**: The serial number of the server certificate.
Issued By	**Common Name (CN)**: The Common Name as specified in the CA root certificate. For a server certificate generated by default by the device, this field displays the serial number of the device instead. **Organization (O)** and **Organizational Unit (OU**): The name and organizational unit of the organization that issued the server certificate. If the server certificate was generated by default by the 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). **MD5 Fingerprint**: A fingerprint created by a Message Digest 5 (MD5) algorithm. **NOTE:** This does not represent the signature hash algorithm used on the certificate.

Secure Disposal Guidelines

Introduction

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

Delete device contents

To reset the device:

- Hold down the Reset button on the device for 10 seconds, release the Reset button to allow the format function to complete and for the device to complete its reboot process.

  NOTE: This will reset the device to its default values and remove all information.

Dispose of physical device

For information on how to physically dispose of the device and destroy its volatile memory, please consult the **Statement of Volatility document** available on the APC by Schneider Electric website **www.apc.com**.

Appendix 1: Easy Rack PDU Security Deployment Guide

Overview

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

Best Practices for the Network Management Card

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

- Physical Security
- Device Security
- Network Security

NOTE: Different deployments may require different security considerations.

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

Physical Security

Deploy the equipment in a secure location:
Custodians should secure equipment from unauthorized physical access.

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

Secure access to the device front panel and console port:
Deploy the device in a rack or cage that can be locked with a suitable key, or other physical methods. This will prevent access to the physical ports of the device.

Description of Risk

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

Recommendations

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

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

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

Device Security

NOTE: For more information on Device Security options, see **Appendix 2: Easy Rack PDU Security Hardening Checklist**.

Software Patch Updates

APC by 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 APC by Schneider Electric products. For information on new and updated security bulletins, visit the **Schneider Electric Security Bulletins** Web page on **www.se.com** or **www.apc.com**.

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

Privileged Accounts

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

Also minimize the number of local accounts.

Certificates

Replace the Default SSL/TLS Certificate

Default SSL/TLS certificates are created during the initial configuration of the device. These certificates are not intended for use in production deployments and should be replaced. APC by 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.

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. Easy Rack PDU only supports TLS 1.2.

Network Security

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

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.

Network Segmentation

APC by 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

APC by 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 SIEM solutions.

Appendix 2: Easy Rack PDU Security Hardening Checklist

Upgrade to the latest firmware version

Visit the 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.

Disable HTTP and enable HTTPS

By default, HTTP is disabled on products. Disable HTTP if it is enabled and enable HTTPS for a more secure and encrypted channel for web communication.

Upload a custom HTTPS certificate

Your device creates an internally generated HTTPS certificate. It is recommended that you use the certificate tool to create a custom certificate to help strengthen authenticity.

Disable older versions of TLS

Transport Layer Security (TLS) is a cryptographic protocol that provides communication security over the internet, only TLS 1.2 is available for the Easy Rack PDU.

Disable SNMPv1, SNMPv2c, 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 and SNMPv2c.

Configure SNMPv3 to use AES/SHA

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

Use custom network ports where applicable

By using a non-standard port, your device can be confused by scans looking only at standard ports. These apply to protocols such as HTTPS, SNMP, 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.

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)

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

Source Code Copyright Notice

cryptlib copyright Digital Data Security New Zealand Ltd 1998.

Copyright © 1990, 1993, 1994 The Regents of the University of California. All rights reserved.

This code is derived from software contributed to Berkeley by Mike Olson.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:
   This product includes software developed by the University of California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Radio Frequency Interference

USA—FCC

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. these limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with this user manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference. The user will bear sole responsibility for correcting such interference.

Canada—ICES

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada

Taiwan—BSMI

警告使用者：
這是甲類的資訊產品，在居住的
環境中使用時，可能會造成射頻
干擾，在這種情況下，使用者會
被要求採取某些適當的對策。

APC by Schneider Electric
70 Mechanic Street
02035 Foxboro, MA
USA

www.se.com

As standards, specifications, and design change from time to time, please ask for confirmation of the information given in this publication.

990–91473