Easy Micro Data Center

C-Series & S-Series

Security Handbook

990-91544
Release date 8/2021

Legal Information

Table of Contents

Content and Purpose of This Guide

This guide documents security features for firmware version __ of the Easy MDC Monitor, which enables devices connected to the Easy MDC to function remotely over the network.

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

- Secure SHell v2 (SSH) (for Service Engineers only)
- Transport Layer Security (TLS) 1.1 and 1.2
- SNMPv1, SNMPv2c and SNMPv3

Types of User Accounts

The Easy MDC has three basic levels of access

- The **Super User** can use all of the menus in the Web UI and manage other accounts. The Super User cannot be deleted.
- An **Administrator** can use all of the menus in the Web UI except for **Configuration > General > User Management**.
- A **Read-only User** does not have access to **Control**, **Configuration**, or **Tests** menus. The **Home**, **Status**, **Logs**, and **About** tabs are visible, but Read-only users receive “Access denied” messages if they try to clear the logs.

Security

Security Features

Protection of Passwords and Passphrases

No password or passphrase is stored on the Monitor 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 Monitor.

Summary of Access Methods

Security Access: available methods	Description
Serial access to the Command Line Interface (CLI)	
• User name • Password	Always enabled. **NOTE:** Only service engineers have the password required to change settings.
Remote Access to the Command Line Interface (CLI) **NOTE:** The CLI access account is for use by the service team. The user name and password are not provided to customers.	
• User name and password • Selectable server port • Access protocols that can be enabled or disabled. • Secure SHell (SSH)	For high security, use SSH. SSH provides encrypted access to the CLI to provide additional protection from attempts to intercept, forge, or alter data during transmission.
SNMPv1, SNMPv2c and SNMPv3	
SNMPv1/SNMPv2c: Community Name	For SNMPv1/ SNMPv2c, the default community name for read access is “public.” The default community name for write access is “private.”
SNMPv3: • Up to four user profiles • 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 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.
Web Server	
User name and password	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 the Default Password Immediately

After installation and initial configuration of the Micro Data Center, you are required to change the default password for the Super User to establish basic security. It is recommended that you use a strong password that complies with your company’s password requirements.

Port Assignments

If 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 Monitor. A non-standard port number provides an additional level of security. The ports are initially set at the standard “well known ports” for the HTTP and HTTPS protocols. To increase security, change the ports to any unused port numbers from 5000 to 32768 in the Web UI under **Configuration > Network > Web** (see the of the *User Guide* on www.apc.com for more detailed information.

User Names, Passwords, and Community Names with SNMPv1

All user names, passwords, and community names for SNMPv1/SNMPv2c 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 CLI or Web UI of the Monitor. If your network requires the higher security of the encryption-based options available for the Web UI, disable SNMPv1/SNMPv2c access.

To disable SNMPv1/SNMPv2c access from the Web UI, go to **Configuration > Network > SNMPv1/2c**. Clear the **Enable SNMPv1/v2c 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.

Encryption

Transport Layer Security (TLS) for the Web UI

For secure Web communication, HyperText Transfer Protocol over Secure Sockets Layer (HTTPS) is enabled as the default for access to the device. HTTPS is a Web protocol that uses Transport Layer Security (TLS) to encrypt and decrypt page requests from the user and pages that are returned by the Web server to the user. The Monitor supports TLS versions 1.1 and 1.2.

NOTE: HTTPS cannot be disabled. When TLS is enabled, your Web browser displays a small lock icon.

TLS uses a digital certificate to enable the browser to authenticate the server (in this case, the Monitor). 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 (CA). Each major browser manufacturer distributes CA root certificates of the commercial Certificate Authorities in the certificate store (cache) of its browser so that the browser 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. If you do not want to use an existing Certificate Authority, you can also create a root certificate to upload to the certificate store (cache) of the browser. You can also use OpenSSL to create a server certificate to upload to the device.

NOTE: See Creating and Installing Digital Certificates, page 9 for a summary of how these certificates are used. To create certificates and certificate requests, see

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

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, page 10
- Method 2: Use a Certificate Generator to Create a CA Certificate and a Server Certificate , page 11
- 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 , page 12**NOTE:** You can also use a certificate generator if your company or agency operates its own Certificate Authority. Use the certificate generator in the same way, but use your own Certificate Authority in place of a commercial Certificate Authority.

Method 1: Use the Default Certificate

If you remove the current certificate, you must reboot the monitor. If no server certificate exists during the reboot process, the Monitor generates a default server certificate that is self-signed but is not configurable. Method 1 has 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 Monitor takes up to 1 minute to create this 256-bit (ECC key) certificate, and the Web UI 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 Monitor in place of a valid *Common Name* or *Subject Alt Name* (the DNS name or the IP address of the Monitor). Therefore, although the Monitor can control access to its Web UI by user name, password, and account type (Super User, Administrator, or Read-only User), the browser cannot authenticate which device is sending or receiving data.

Method 2: Use a Certificate Generator to Create a CA Certificate and a Server Certificate

Use a certificate generator to create two digital certificates:

- *A CA 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 Monitor.
- *A server certificate* that you upload to the Monitor. 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 Monitor, 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 Web 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 advantages and disadvantages.

Advantages: Before they are transmitted, the user name and password and all data to and from the Monitor 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 Monitor 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.

Disadvantages: 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 Web 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.

Method 3 has advantages and disadvantages.

Advantages: Before they are transmitted, the user name and password and all data to and from the Monitor 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 Monitor.
- 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 Monitor 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 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.

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.

Using an OpenSSL Certificate Generator

You can use OpenSSL to create the 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. You can download OpenSSL from www.openssl.org/source.

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 such as TLS.

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

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. Download OpenSSL from www.openssl.org/source Extract the necessary files and install OpenSSL according to the OpenSSL documentation.

   NOTE: You may have to perform the file extraction more than once.
2. Open a command prompt and navigate to the folder containing the extracted OpenSSL files.
3. Enter the following commands and complete the fields to create the **CA Key File** and **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_names>"`

Load the CA Root Certificate to your Browser

For each user who needs to access the Monitor, load the **.crt** file to the certificate store (cache) of the user's preferred Web browser. The following procedure is for Internet Explorer. For other Web browsers, check the browser documentation for instructions to load the **.crt** file to the certificate store.

1. Inthe menu bar, Select **Tools > Internet Options**.
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. Enter the following commands and complete the fields to create the **SSL Server Key File** and the **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.

Create a Server Certificate and Signing Request

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.

First you must create Certificate Signing Request (CSR). The CSR contains all the information for a server certificate except the digital signature. This process creates two output files:

- The file with the **.key** suffix contains the private key of the device.
- 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, you must load the server certificate onto the device.

Repeat the steps to create and load the server certificate for each Monitor that requires a 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. Enter the following commands 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 either a commercial Certificate Authority or a Certificate Authority managed by your company.

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

Load the Server Certificate to the Monitor

1. In the Monitor Web UI, select **Configuration > Network > Web > Configure Certificate**.
2. Select **Choose File**, and browse to the server certificate, the **server.crt** and **server.key** files you created in the procedure to Create an SSL/TLS Server Certificate, page 14.
3. Click **Apply**. The Web server reboots automatically for the changes to take effect.

Web UI Access and Security Protocols (HTTP/HTTPS)

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. HTTPS cannot be disabled.

NOTE: See Creating and Installing Digital Certificates, page 9 for information on the methods for using digital certificates.

To configure HTTP and HTTPS:

1. In the Web UI, go to **Configuration > Network > Web**.
2. Enable or disable HTTP and configure the ports used by HTTP/HTTPS. Then click **Apply**. You must restart the Monitor for changes to take effect. When TLS is activated, your browser displays a small lock icon (or a warning symbol if the CA that signed the certificate is not recognized by the browser).

   NOTE: If you have created a certificate other than the default, upload the certificate and the key file to the Monitor. See Load the Server Certificate to the Monitor, page 15 for details.

Many common Web browsers allow you to view certificate details: select the lock icon or warning sign in the URL address bar, then select the option to view certificate details. See your browser documentation for more detailed instructions. The following certificate details are typically available:

- Subject / Issuer (typically the Common Name (CN) of the the device the certificate was issued to / the CN of the certificate issuer)
- Validity (the date the certificate was issued and the date the certificate expires)
- Algorithms used for authentication and encryption
- Fingerprints (unique identifiers to further authenticate the server)

Secure Disposal Guidelines

To securely dispose of the Monitor, first perform a reset to defaults, then dispose of the device in accordance with the guidelines in the *Statement of Volatility* document on www.apc.com.

Hold down the **Reset** button on the Monitor for ten seconds. Release the Reset button to allow the format function to complete and for the Monitor to reboot. This will reset the Monitor to its default values and remove all information.

To find the *Statement of Volatility*, go to www.apc.com and enter the model number for your MDC in the search bar to find its product page.. On the MDC product page, select **Documentation**. You can find the *Statement of Volatility* under .

Appendix A: Security Deployment Guide

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 Monitor of the Easy Micro Data Center is implemented to provide users with as much flexibility as possible. Industry standard security implementation, coupled with the flexibility of the Monitor, enables this product line to exist in different user environments.

This document provides general security guidance to help you decide on an appropriate secure deployment based on your specific security requirements. To maintain security throughout the deployment lifecycle, Schneider Electric recommends reviewing the following considerations

- Physical Security
- Device Security
- Network Security

NOTE: Different deployments may require different security considerations.

Physical Security

Attackers with physical access to covered equipment can access the device without authorization. Physical security must be in place to control physical access to restricted areas and facilities containing the Micro Data Center. Schneider Electric strongly recommends that you follow the following recommendations to improve the security of your location and access control for the Easy Micro Data Center:

- **Location security:**
  - The cabinet should remain locked to protect the equipment inside from unauthorized access or removal.
  - Access to areas containing the Easy Micro Data Center and other restricted equipment should only be granted to personnel who require access based on their job function.
  - 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.
- **Access control:**
  - 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

Software Patch Updates

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

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

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

Privileged Accounts

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

Certificates

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

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 MDC supports TLS 1.1 and 1.2.

Network Security

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.

When deploying an Easy Micro Data Center to a production environment, Schneider Electric strongly recommends that the following key configuration changes are made:

- **Network Segmentation:** Network traffic to the Monitor’s management should be 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. 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.
- **Security Detection and Monitoring Tools:** The network environment should be protected and monitored by appropriate physical, technical and administrative tools for network intrusion and monitoring such as IDS/IPS and appropriate SIEM solutions.

Appendix B: Security Hardening Checklist

_ **Upgrade to the latest firmware version**

Visit the appropriate product page on www.apc.com or www.se.com to verify you are running the latest firmware for your Micro Data Center. This will help ensure security vulnerabilities and features are up-to-date for your protection.

_ **Disable HTTP and enable HTTPS**

Disable HTTP for a more secure and encrypted channel for Web communication. See the *User Guide* on www.apc.com for detailed instructions.

_ **Upload a custom HTTPS certificate**

The Monitor creates an internally-generated HTTPS certificate. It is recommended that you create a custom certificate to help strengthen authenticity. See Creating and Installing Digital Certificates, page 9 for detailed instructions.

_ **Disable SNMPv1, SNMPv2c, and enable SNMPv3**

If enabled and configured, the Monitor can be accessed via SNMP. It is recommended to use SNMPv3, which 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. See the *User Guide* on www.apc.com for detailed instructions.

_ **Use custom network ports where applicable**

By using a non-standard port, your Monitor can mislead scans looking only at standard ports. These ports apply to protocols such as HTTPS, SNMP, etc.

_ **Change the Super User account password**

During the initial configuration of the Monitor, you must change the default Super User account password. It is recommended that you use a strong password which conforms to your company's password requirements.

_ **Delete Administrator and Read-only User accounts (if applicable)**

Delete all unused accounts for Administrator and Read-only users to manage access control.

Schneider Electric
70 Mechanic Street
02035 Foxboro, MA
USA

www.apc.com

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

990-91544