Substation Monitoring Device (SMD)

SureSeT™ Active and Active+

User and Commissioning Guide for Substation Monitoring Device (SMD) in SureSeT MV Metal-Clad Switchgear

D3982892
09/2025

Schneider Electric

www.se.com

Legal Information

The information provided in this document contains general descriptions, technical characteristics and/or recommendations related to products/solutions.

This document is not intended as a substitute for a detailed study or operational and site-specific development or schematic plan. It is not to be used for determining suitability or reliability of the products/solutions for specific user applications. It is the duty of any such user to perform or have any professional expert of its choice (integrator, specifier or the like) perform the appropriate and comprehensive risk analysis, evaluation and testing of the products/solutions with respect to the relevant specific application or use thereof.

The Schneider Electric brand and any trademarks of Schneider Electric SE and its subsidiaries referred to in this document are the property of Schneider Electric SE or its subsidiaries. All other brands may be trademarks of their respective owner.

Schneider Electric does not grant any right or license for commercial use of the document or its content, except for a non-exclusive and personal license to consult it on an "as is" basis.

Schneider Electric reserves the right to make changes or updates with respect to or in the content of this document or the format thereof, at any time without notice.

To the extent permitted by applicable law, no responsibility or liability is assumed by Schneider Electric and its subsidiaries for any errors or omissions in the informational content of this document, as well as any non-intended use or misuse of the content thereof.

Table of Contents

Safety Information

Read these instructions carefully and examine the equipment to become familiar with the device before attempting to install, operate, service, or maintain it. The following special messages may appear throughout this user guide or on the equipment to warn of hazards or to call attention to information that clarifies or simplifies a procedure.

The addition of either symbol to a “Danger” or “Warning” safety label indicates that an electrical hazard exists which will result in personal injury if the instructions are not followed.

This is the safety alert symbol. It is used to alert you to personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

⚠⚠ DANGER

DANGER indicates a hazardous situation which, if not avoided, **will result in** death or serious injury.

⚠WARNING

WARNING indicates a hazardous situation which, if not avoided, **could result in** death or serious injury.

⚠CAUTION

CAUTION indicates a hazardous situation which, if not avoided, **could result in** minor or moderate injury.

NOTICE

NOTICE is used to address practices not related to physical injury.

NOTE: Provides additional information to clarify or simplify a procedure.

Please Note

Electrical equipment should be installed, operated, serviced, and maintained only by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material.

A qualified person is one who has skills and knowledge related to the construction, installation, and operation of electrical equipment and has received safety training to recognize and avoid the hazards involved.

Electrical equipment should be transported, stored, installed, and operated only in the environment for which it is designed.

SMD Safety Precautions

⚠⚠DANGER

HAZARD OF ELECTRIC SHOCK, EXPLOSION, OR ARC FLASH

- Apply appropriate personal protective equipment (PPE) and follow safe electrical work practices. See NFPA 70E or CSA Z462.
- This equipment must only be installed and serviced by qualified electrical personnel.
- Turn off all power supplying this equipment before working on or inside equipment.
- Always use a properly rated voltage sensing device to confirm power is off.
- Replace all devices, doors and covers before turning on power to this equipment.
- Perform such work only after reading and understanding all the instructions contained in this guide.
- Before performing visual inspections, tests, or maintenance on this equipment, disconnect all sources of electric power. Assume all circuits are live until they are de-energized, tested, and tagged. Pay particular attention to the design of the power system. Consider all sources of power, including the possibility of backfeeding.
- Handle this equipment carefully and install, operate, and maintain it correctly in order for it to function properly.
- Operate the equipment within the specified electrical and environmental limits.
- Carefully inspect your work area and remove any tools and objects left inside the equipment.
- All instructions in this manual are written with the assumption that the customer has taken these measures.

Failure to follow these instructions will result in death or serious injury.

⚠WARNING

HAZARD OF COMPROMISED SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY

- Change default passwords to help prevent unauthorized access to device settings and information.
- Disable unused ports/services to help minimize pathways for malicious attackers.
- Place networked devices behind multiple layers of cyber defenses (such as firewalls, network segmentation, and network intrusion detection and protection).
- Use cybersecurity best practices (for example. least privilege, separation of duties) to help prevent unauthorized exposure, loss, modification of data and logs, or interruption of services.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

About the Document

Document Scope

This document describes the operation and use of the Substation Monitoring Device (SMD) in SureSeT switchgear.

Please read this manual carefully and follow its recommendations. However, this manual cannot describe every single condition of use or every variant specific to the customer.

Validity Note

This manual applies to the SMD in SureSeT switchgear.

The characteristics of the products described in this document are intended to match the characteristics that are available on www.se.com. As part of our corporate strategy for constant improvement, we may revise the content over time to enhance clarity and accuracy. If you see a difference between the characteristics in this document and the characteristics on www.se.com, consider www.se.com to contain the latest information.

Convention

SMD MV Enhanced is hereafter referred to as SMD or SMD MV Enhanced.

General Cybersecurity Information

In recent years, the growing number of networked machines and production plants has seen a corresponding increase in the potential for cyber threats, such as unauthorized access, data breaches, and operational disruptions. You must, therefore, consider all possible cybersecurity measures to help protect assets and systems against such threats.

To help keep your Schneider Electric products secure and protected, it is in your best interest to implement the cybersecurity best practices as described in the Cybersecurity Best Practices document.

Schneider Electric provides additional information and assistance:

- Subscribe to the Schneider Electric security newsletter.
- Visit the Cybersecurity Support Portal web page to:
  - Find Security Notifications.
  - Report vulnerabilities and incidents.
- Visit the Schneider Electric Cybersecurity and Data Protection Posture web page to:
  - Access the cybersecurity posture.
  - Learn more about cybersecurity in the cybersecurity academy.
  - Explore the cybersecurity services from Schneider Electric.

Product Related Cybersecurity Information

For more information about cybersecurity, refer to Cybersecurity Recommendations, page 43.

Environmental Data

For product compliance and environmental information, refer to the Schneider Electric Environmental Data Program.

Related Documents

Title of Documentation	Reference Number
Substation Monitoring Device (SMD) SMD MV Enhanced User Guide	GEX9033400
SMD MV Enhanced Installation Guide	GEX9033500
Modicon M251 Logic Controller User Guide	EIO0000004273
Harmony P6 Advanced and Standard Box/Model, User Manual	EIO0000004201
Harmony P6 Basic Box/Model User Manual	EIO0000005082
Harmony ST6 User Manual	EIO0000003527
EcoStruxure™ Operation Server Breaker Module 100 User Guide	GEX20482
TH110 Installation and Operation Manual	NVE62740
CL110 Installation and Operation Manual	QGH40088
Ecostruxure Panel Server User Guide	DOCA0172EN
Recommended Cybersecurity Best Practices	7EN52-0390
Cybersecurity Guidelines for EcoStruxure Machine Expert, Modicon and PacDrive Controllers and Associated Equipment - User Guide	EIO0000004242
Harmony HMI/iPC Cybersecurity Guide	EIO0000004948
EvoPacT™ Medium Voltage Vacuum Circuit Breaker (VCB) User Guide	JYT3013100

To find documents online, visit the Schneider Electric download center (www.se.com/ww/en/download/).

Information on Non-Inclusive or Insensitive Terminology

As a responsible, inclusive company, Schneider Electric is constantly updating its communications and products that contain non-inclusive or insensitive

terminology. However, despite these efforts, our content may still contain terms that are deemed inappropriate by some customers.

Trademarks

QR Code is a registered trademark of DENSO WAVE INCORPORATED in Japan and other countries.

General Description

When configured with the Active or Active+ options, SureSeT switchgear includes the Substation Monitoring Device for Medium Voltage Enhanced Switchgear. This system enables monitoring and/or remote control of the switchgear as follows:

Operations	Active Option	Active+ Option
Thermal monitoring	✓	✓
Environmental monitoring	✓	✓
Circuit breaker health monitoring	—	✓
Circuit breaker control	—	✓

Monitoring Features

The homepage of the SMD HMI displays a single-line diagram of the switchgear system. Each switchgear device is color-coded to indicate its status. By tapping on a device, users can access a monitoring screen that shows detailed health data for both the switchgear and the circuit breaker.

Refer to document GEX9033400, Substation Monitoring Device (SMD) SMD MV Enhanced User Guide for details on how to operate the system user interface to retrieve switchgear and circuit breaker health monitoring data. The following monitoring features are provided.

Thermal Monitoring

Thermal sensors sense the bus temperature in proximity of bolted connections. The SMD indicates an alarm condition in case the temperature surpasses the applicable threshold or if the maximum temperature difference between phases in a specific bussing location surpasses the applicable threshold.

Environmental Monitoring

Temperature and humidity in each cable compartment are measured, and the severity of conditions based on frequency of condensation and pollution as defined in IEC standard 62271-30 is determined. The severity of condition is used to assess the recommended inspection date for the switchgear. The SMD indicates an alarm condition if high severity conditions are sensed, if the recommended inspection date has passed, if the air temperature inside the cable compartments surpasses its applicable threshold, and if the relative humidity inside the cable compartments surpasses its applicable threshold.

Circuit Breaker Health Monitoring

The following circuit breaker monitoring functions are provided:

1. **Circuit Breaker mechanism monitoring:**

   The speed of the mechanism during opening and closing operations is measured to detect deviations from the initial factory- calibrated conditions. The SMD indicates an alarm condition in case the speed deviations surpass their applicable alarm thresholds.

   Additionally, circuit breaker total opening and closing times (defined as the time between an activation signal is sent to a coil and the full separation of the breaker contacts in the vacuum interrupters) are measured and displayed on the SMD HMI. The SMD indicates an alarm condition in case slow operations are detected.

2. **Vacuum interupter monitoring**

   The vacuum interrupters' erosion gap (E-Gap) is continuously measured on each of the breaker phases. When the E-Gap of any phase passes the upper or lower threshold, the SMD indicates an alarm condition.

3. **Open and close coils monitoring**

   This function monitors the status and health of electronic coils by measuring and analyzing the coils' activation time and number of operations. When the activation time surpasses its configured threshold, the rated number of operations is passed, or coil experiences an internal event, the SMD indicates an alarm condition.

4. **Spring charge motor monitoring**

   The spring charge motor operating time and current draw are measured. Any excessive current draw, operation overtime, missed motor activation will cause the SMD to indicate an alarm condition.

5. **Contact synchronism monitoring**

   The timing of each phase vacuum interrupter is measured during opening and closing operations. If the asynchronism between phases reaches 2 ms the SMD indicates an alarm condition.

Health indexes ranging from 0% to 100% are provided to conveniently display the health status of the circuit breaker assembly and its components.

Control Features (Circuit Breaker Control)

The SMD enables control of circuit breakers, within the SureSeT switchgear lineup.

Circuit breakers may be opened or closed, racked into the connected position, or racked out to the test/disconnected position.

Switchgear control may be performed in three different operating modes:

- In **Local** mode by using the pushbuttons provided on the switchgear front panels.
- In **Nearby** mode by using the SMD HMI or by wirelessly connecting a Wi-Fi capable device (smartphone, tablet, or laptop) to the dedicated SMD Wi-Fi network. The wireless connection allows an operator to control the switchgear from outside the arc flash boundary.

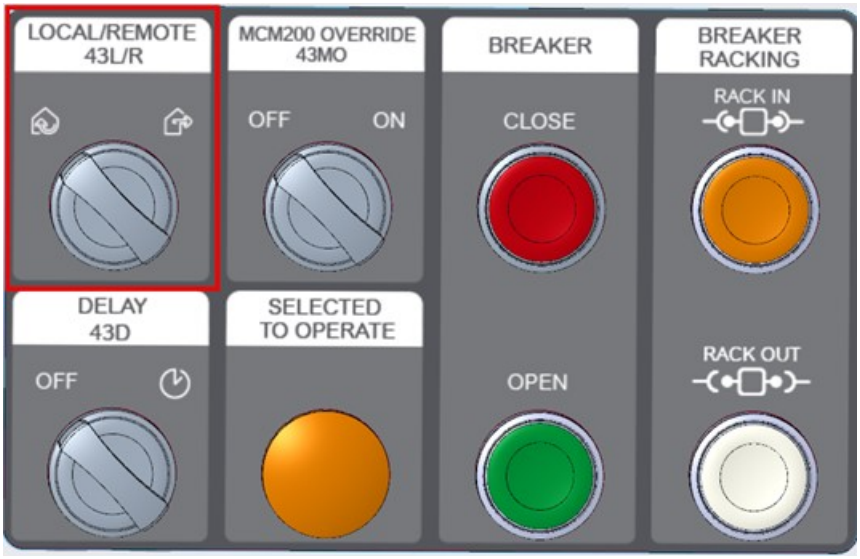
  NOTE: Only one device may be connected to the HMI to operate the switchgear. Multiple device connections will result in a user interface lock. The lock is removed once only one device is connected to the HMI.
- In **Remote** mode by connecting to EcoStruxure Power Monitoring Expert (EPME) or EcoStruxure Power Operation (EPO).

  NOTE: The connection to third party supervisory systems is currently not supported.

Two control points define the SMD operating mode:

- The “Local/Remote” selector switches (one per circuit breaker) located on the swithgear front panels.

Figure 1 - Switchgear front panel with “Local/Remote” switch highlighted



- A digital "Nearby Mode" toggle switch is located in the top-right corner of the SMD HMI homepage. To change the status of this toggle, the user must be logged into the SMD with a profile that has the appropriate permissions. For detailed instructions on how to operate the system interface and manage Nearby Mode, refer to GEX9033400, Substation Monitoring Device (SMD) SMD MV Enhanced User Guide

Figure 2 - HMI with nearby mode on

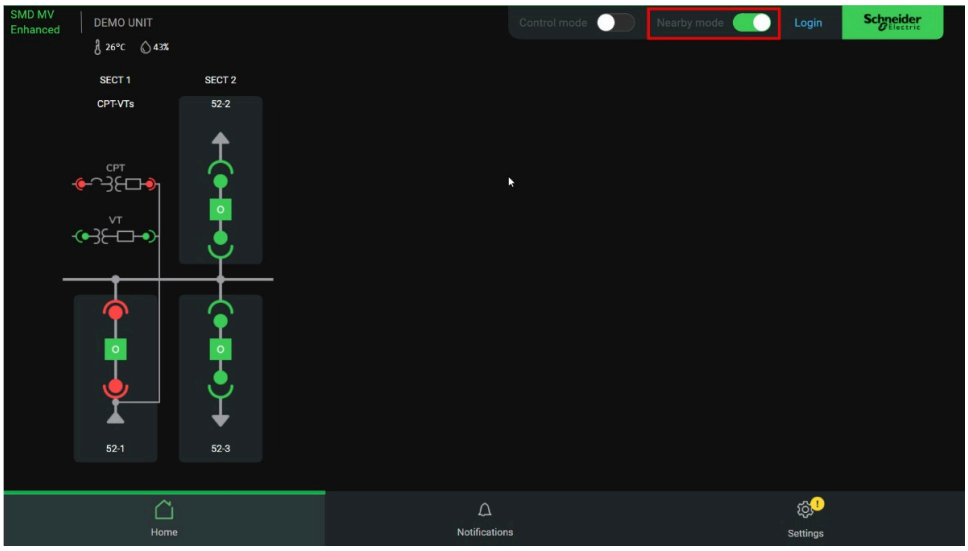
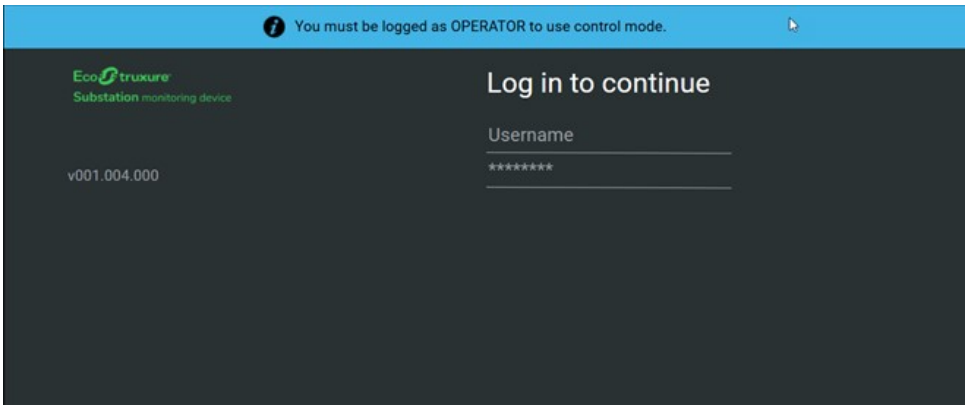


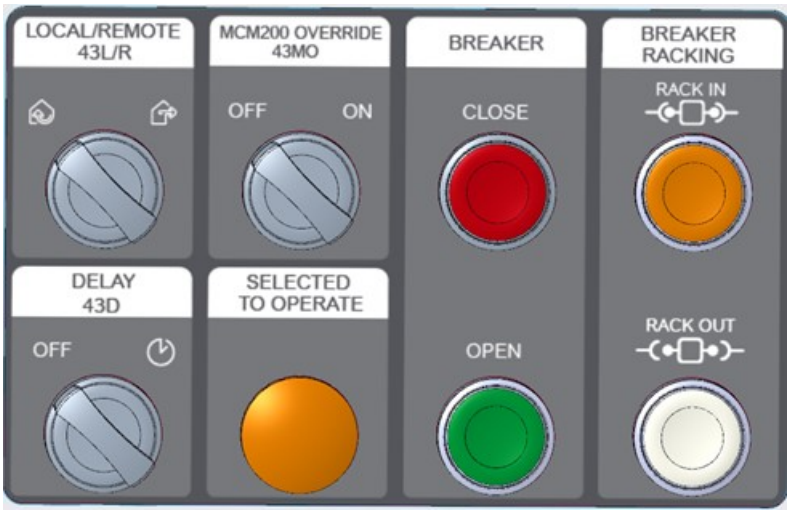
Figure 3 - SMD login popup



Local Mode

When the Local/Remote switch is set to “Local”, the switchgear may only be controlled by using the pushbuttons provided on the switchgear front panels.

Figure 4 - Switchgear front panels pushbuttons and selector switches



Pressing the OPEN, CLOSE, RACK IN, or RACK OUT push buttons initiates circuit breaker operation, provided no interlocking conditions are active.

If the DELAY switch is set to OFF, operations begin immediately when a command is issued. If the switch is ON, a countdown is initiated before the operation is executed. By default, this countdown lasts 10 seconds, but it can be adjusted in the MCM200 configuration using EcoStruxure Power Commission. During the countdown, the "SELECTED TO OPERATE" indicator light blinks to confirm that a delayed operation is in progress. If an interlocking condition arises during the countdown, the countdown continues. However, if the interlocking condition is still active when the countdown ends, the operation will not be executed.

The MCM200 OVERRIDE switch allows the circuit breaker to be electrically opened or closed in local mode when the MCM200 is not operational. When the override is OFF, all control commands are processed through the MCM200, and interlocking contacts are connected to the MCM200 digital inputs. When the override is ON, the panel pushbutton contacts can directly energize the circuit breaker coils. In this mode, interlocking contacts are switched to the close coil circuits, blocking the circuit breaker from closing if any locking conditions are

active. It recommended to ensure the MCM200 OVERRIDE switch is in the “OFF” position prior to switching to nearby or remote mode.

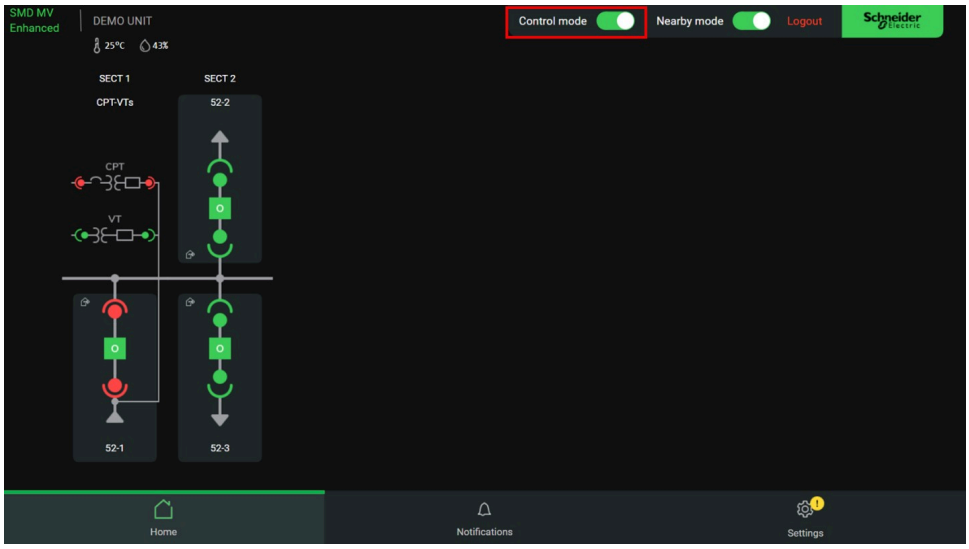
The SELECTED TO OPERATE light provides visual indication of the following conditions:

- A delayed operation countdown is ongoing (blinks once a second).
- An operation is ongoing (blinks twice a second).
- A circuit breaker is selected for operation in Nearby Remote mode (light solidly lit). This light provides indication of the circuit breaker that has been selected for operation on the SMD HMI or EcoStruxure SCADA (Power Operation or Power Monitoring Expert).

Nearby Mode

When the Local/Remote switch is set to “Remote” and the digital “Nearby Mode” toggle switch is activated, the switchgear may only be controlled by using the SMD HMI or by wirelessly connecting a device to the the switchgear. To allow the device control screen to be launched on the SMD HMI, the digital toggle switch “Control Mode” needs to be activated.

Figure 5 - HMI screen with Control Mode Activated



In nearby mode, remote operation commands sent over Modbus TCP/IP by a supervisory system (EPME or EPO) will not be executed.

NOTE: If the system is in nearby mode and the MCM200 override switch is in the "ON" position, open and close commands sent via the HMI will not execute. Ensure the MCM200 override switch is in the "OFF" position when in nearby mode.

Refer to document GEX9033400, Substation Monitoring Device (SMD) SMD MV Enhanced User Guide for details on how to operate the system user interface in order to control circuit breakers in nearby mode.

⚠DANGER

HAZARD OF ELECTRICAL SHOCK, EXPLOSION, OR ARC FLASH

- Apply appropriate personal protective equipment (PPE) and follow safe electrical work practices. See NFPA 70E, NOM-029–STPS. or CSA Z462 or local equivalent.
- This equipment must be only be installed and serviced by qualified electrical personnel.
- Turn off power supplying this equipment before working on or inside equipment.
- Always use a properly rated voltage sensing device to confirm power is off.
- Ensure that personnel are outside of the arc flash boundary when in Nearby mode because operation may be executed remotely.
- Beware of potential hazards, and carefully inspect the work area for tools and objects that may have been left inside the equipment.

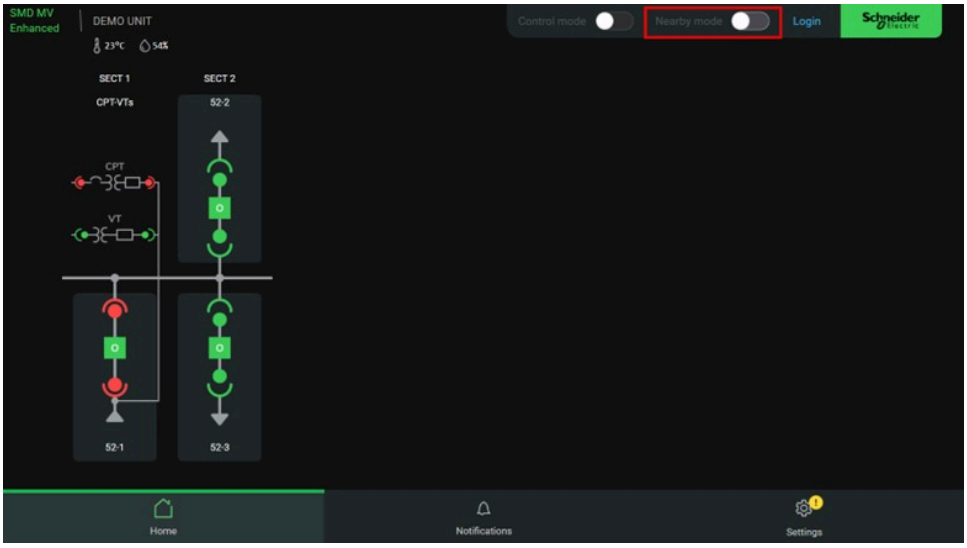
Failure to follow these instructions will result in death or serious injury.

NOTE: Use the SELECTED FOR OPERATION light to confirm the correct breaker has been selected for operation.

Remote Mode

When the Local/Remote switch is set to “Remote” and the digital “Nearby Mode” toggle switch is deactivated, the switchgear may only be controlled by the connected supervisory system (EPME or EPO) or by any external contacts wired to the provisions for Close or Trip Contacts Active in Remote Mode (refer to switchgear factory drawings).

Figure 6 - HMI with Nearby mode deactivated



NOTE: If the system is in remote mode and the MCM200 override switch is in the “ON” position, open and close commands sent via the supervisory system or by any external contacts wired to the provisions for Close or Trip Contacts Active in Remote Mode will not execute. Ensure the MCM200 override switch is in the “OFF” position when in remote mode.

⚠DANGER

HAZARD OF ELECTRICAL SHOCK, EXPLOSION, OR ARC FLASH

- Apply appropriate personal protective equipment (PPE) and follow safe electrical work practices. See NFPA 70E, NOM-029–STPS. or CSA Z462 or local equivalent.
- This equipment must be only be installed and serviced by qualified electrical personnel.
- Turn off power supplying this equipment before working on or inside equipment.
- Always use a properly rated voltage sensing device to confirm power is off.
- Ensure that personnel are outside of the arc flash boundary when in Nearby mode because operation may be executed remotely.
- Beware of potential hazards, and carefully inspect the work area for tools and objects that may have been left inside the equipment.

Failure to follow these instructions will result in death or serious injury.

NOTE: Use the SELECTED FOR OPERATION light to confirm the correct breaker has been selected for operation.

Interlocking

In all operating modes, the following electrical interlocking rules apply to circuit breakers:

Circuit Breaker Close Operation Commands are not allowed if:
The circuit breaker close spring is not charged
An electrical or mechanical open signal is active and engaging the tripping kinematic chain of the circuit breaker mechanism
The circuit breaker is not in the open position. Open position is defined by the status of the auxiliary contacts (52/a contact in open position and 52/b contact in closed position)
The circuit breaker is in the travel position
Other operations are ongoing
Project specific interlocks wired to the MCM200 DI22 are active (refer to factory drawings)

In all operating modes, the following electrical interlocking rules apply to circuit breakers

Circuit breaker rack-in operation commands are not allowed if:	Circuit breaker rack-out operation commands are not allowed if:
The circuit breaker is not in the open position	The circuit breaker is not in the open position
The circuit breaker is not fully racked out in the disconnected position	The circuit breaker is already fully racked out in the disconnected position
The circuit breaker compartment door is open. In case the door is opened during the racking operation, the racking motor will stop	The circuit breaker compartment door is open. In case the door is opened during the racking operation, the racking motor will stop
The racking handle is inserted in the circuit breaker truck's racking port or the red racking/emergency trip push button on the circuit breaker truck is depressed	The racking handle is inserted in the circuit breaker truck's racking port or the red racking/emergency trip push button on the circuit breaker truck is pressed
Padlocks are applied to the red racking/emergency trip push button on the circuit breaker truck	Padlocks are applied to the red racking/emergency trip push button on the circuit breaker truck
Padlocks or key locks are applied to the Lock-Out/Tag-Out provision of the circuit breaker compartment	Padlocks or key locks are applied to the Lock-Out/Tag-Out provision of the circuit breaker compartment
Other operations are ongoing	Other operations are ongoing
The truck locking magnet (optional feature) is deenergized	The truck locking magnet (optional feature) is deenergized
Project specific interlocks wired to the MCM200 DI19 are active (refer to factory drawings)	Project specific interlocks wired to the MCM200 DI19 are active (refer to factory drawings)

NOTE: Protective relay trip contacts are wired directly to the circuit breaker coils, allowing the protective relay functions to remain active regardless of the selected operating mode.

NOTE: Each circuit breaker is provided with a red racking/emergency trip push button. The operation of the red racking/emergency trip push button is independent from the operating mode settings.

⚠ WARNING

DEFEATING SETTING OF THE OPERATING MODE

- Use the provision for External Protection Trip contact in case external protective devices are to be wired to the trip circuit (refer to switchgear factory drawings)
- Use the provision for Trip or Close Contacts Active in Remote Mode in case external control devices are to be wired to the trip or close circuits (refer to switchgear factory drawings)

Failure to follow these instructions can result in death, serious injury, or equipment damage.

NOTE: Hardwiring additional external control contacts directly to the trip or close coils without the interlocking of the Local/Remote switch (43L/R) may provide a second point of control that defeats the setting of the operating mode.

SMD User Interface and Connection to Supervisory Systems

Monitoring and control features of the SMD may be accessed by using the SMD HMI provided with the SureSeT switchgear. Refer to document GEX9033400, Substation Monitoring Device (SMD) SMD MV Enhanced User Guide for details on how to operate the SMD HMI.

Refer to document GEX9033400, Substation Monitoring Device (SMD) SMD MV Enhanced User Guide for details on how to operate the system user interface in order to retrieve switchgear and circuit breaker health monitoring data and remotely operate circuit breakers.

The SMD HMI may be remotely accessed using the wireless network generated by the Wi-Fi access point provided in the SureSeT switchgear. By connecting Wi-Fi enabled devices to that network, it is possible to “mirror” the HMI on your device screen and operate the SMD without the need of being in front of the HMI.

The SMD HMI is available in two configurations:

- Standard Option: Includes a 15" touchscreen that is used as the user interface. This HMI is typically mounted on the door of one of the switchgear compartments.
- Faceless Option: Offers the same computing hardware as the standard version but without the touchscreen. This version is usually installed inside one of the low-voltage control compartments of the switchgear.

When the faceless option is selected, external peripherals (display, keyboard, and mouse) are required to be connected to the HMI to complete the initial setup during the switchgear commissioning phase or in case changes are required to the HMI Microsoft Windows™ settings or SMD user accounts. Once the HMI is configured for operation, no external peripherals are required. The HMI user interface may be viewed and operated on devices connected to the HMI via the provided WLAN access point Wi-Fi network.

The SMD may be connected to the Schneider Electric EcoStruxure supervisory platforms such as EcoStruxure Asset Advisor, EcoStruxure Power Monitoring Expert, and EcoStruxure Power Operation.

Switchgear and circuit breaker monitoring data may be read by third party supervisory systems. Contact your Schneider Electric representative if such access is desired.

For applications requiring switchgear and circuit breaker operations from a supervisory system, only EcoStruxure Power Monitoring Expert and EcoStruxure Power Operation may be used. Connection to third party SCADA for switchgear operation is not supported by the SMD.

Moving Circuit Breakers Between Switchgear Compartments

When SureSeT switchgear is provided with the Active+ option, it is required to manually update the BM100 Modbus Address and the circuit breaker BM100 Modbus address label in order to move circuit breakers from a lower compartment to an upper compartment or vice versa. Follow the instructions listed in section “Circuit Breaker Position Change in SureSeT Switchgear” of JYT3013100 EvoPacT™ Medium Voltage Vacuum Circuit Breaker (VCB) User Guide.

Such procedure is not required when moving a circuit breaker from an upper compartment to another upper compartment within the SureSeT switchgear lineup or when moving a circuit breaker from a lower compartment to another lower compartment within the SureSeT switchgear lineup.

NOTICE

INACCURATE CIRCUIT BREAKER HEALTH DATA

Follow all setup and operations to maintain the integrity of the circuit breaker health monitoring system.

Failure to follow these instructions can result in equipment damage.

NOTICE

DAMAGED CIRCUIT BREAKER CODE PLATE

Verify that the circuit breaker rating is suitable for the circuit breaker compartment prior to moving a circuit breaker into a compartment.

Failure to follow these instructions can result in equipment damage.

Rating code plates are provided in the breaker compartment to block accidental insertion of circuit breakers with incorrect current, voltage, or interrupting ratings into the compartment.

Setup and First Use

Instructions on how to set up the SureSeT switchgear digital control and monitoring system including the SMD for operation after receival are listed below.

The following label is provided on the SureSeT switchgear to assist and speed up the commissioning process.

Figure 7 - Setup Instruction Label

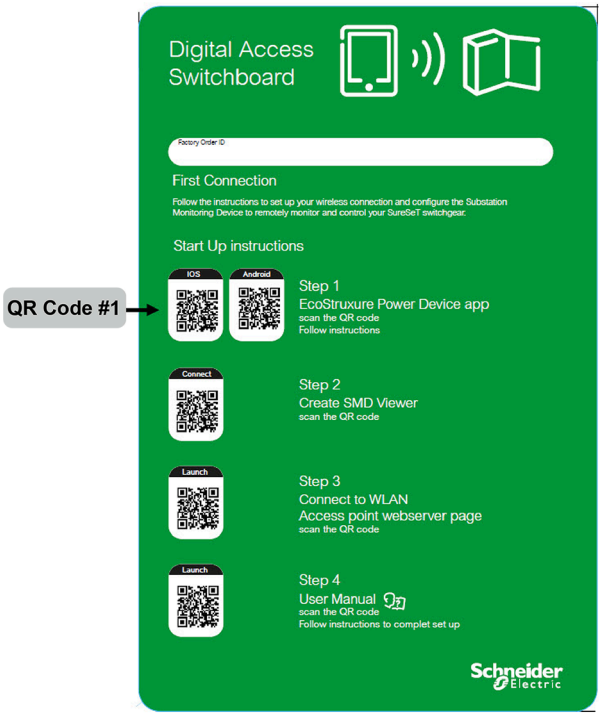
The instructions below provide alternative procedures that may be used in case access to such label is not available or practical, or if you are not able to access the INTERNET from the installed location of the switchgear.

EcoStruxure™ Power Device (EPD) App Download and Setup

1. **Download the EcoStruxure Power Device App**

   Scan QR code #1 that matches the software (IOS, Android) of your device. If you do not have the QR code, you can search for “EcoStruxure Power Device” on your devices app store to download it.

Figure 8 - QR code #1 on Setup Instruction Label

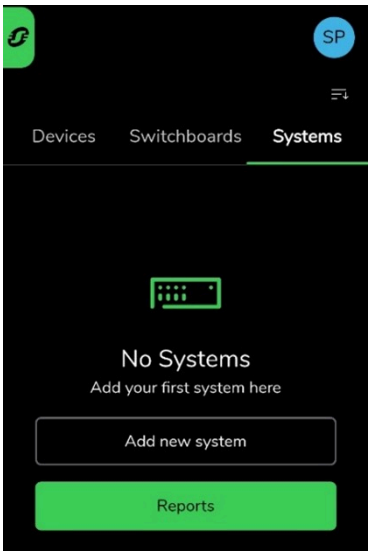


2. **Log in into your Schneider Electric account**

   If you do not have a Schneider Electric account, you will need to create one.

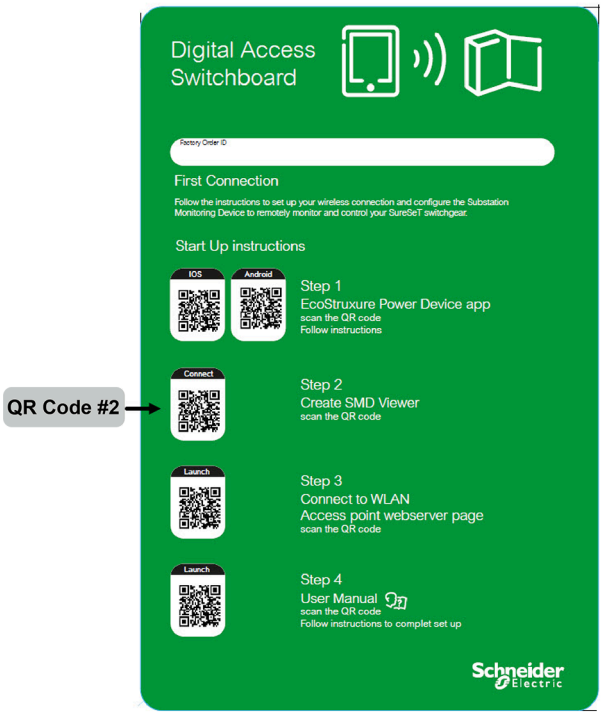
3. **Create the SMD System Viewer**
   Go to the Systems tab and tap on "Add new system". If previous systems have been created, tap on "Add system".

Figure 9 - EcoStruxure Power Device App's and new system screen



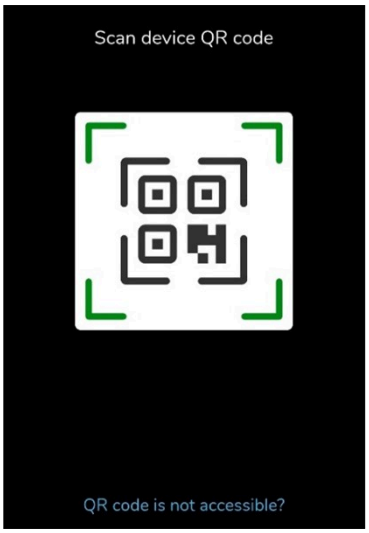
Launch the in-app QR scanner by tapping on the screen and scan QR code #2 to create the SMD WebViewer.

Figure 10 - QR code #2 on Setup Instruction Label



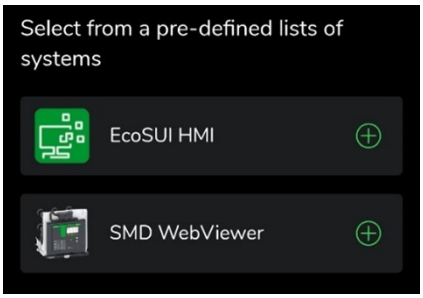
- In case QR code #2 is not available, tap "QR code not accesible".

Figure 11 - EPD app QR scanner screen



- Select “SMD WebViewer”.

Figure 12 - EPD app’s QR code not accessible screen

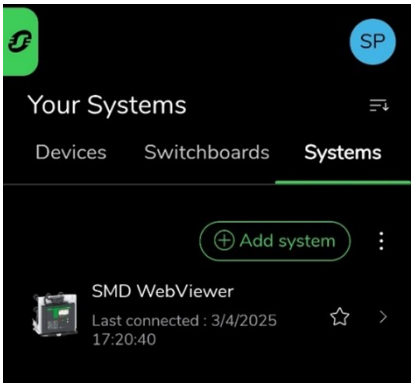


- Enter in the URL field: http://192.168.4.105:8082/webviewer/index.html, populate the “Asset Name” as needed, and tap on the return arrow to complete the creation of the SMD WebViewer.

  NOTE: The same SMD viewer may be used for multiple SMD systems. Generating multiple SMD WebViewers is not required in case multiple SureSeT lineups are part of the same installation.

Whether the system is created with the QR code or manually, make sure the SMD WebViewer is now listed in your “Systems” tab.

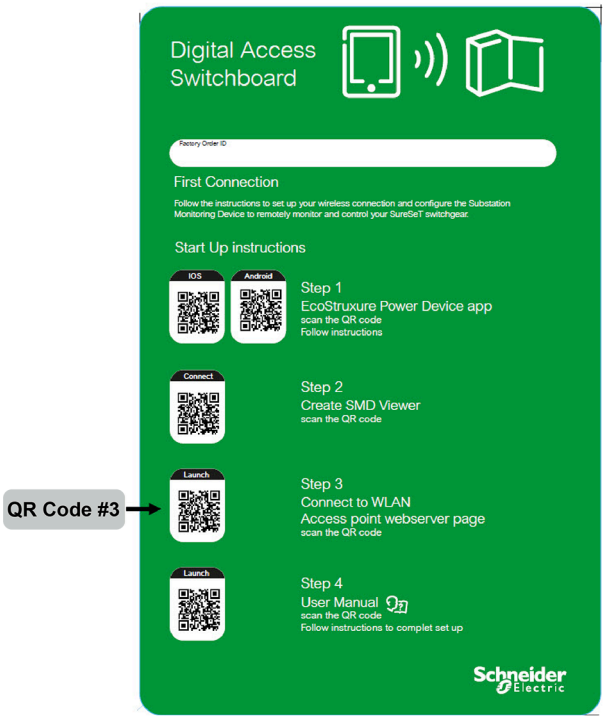
Figure 13 - EPD app’s your systems tab



WLAN Access Point Setup

1. **Connect to the Wi-Fi network and launch the device webserver page**
   Scan QR code #3 to automatically connect to WLAN device.

Figure 14 - QR code #3 on Setup Instruction Label



If the QR code is not available or if it is preferred to use a laptop to set the WLAN access point configuration, go into your device Wi-Fi settings and search for the SureSeT switchgear Wi-Fi network. The network SSID follows the naming convention listed below:

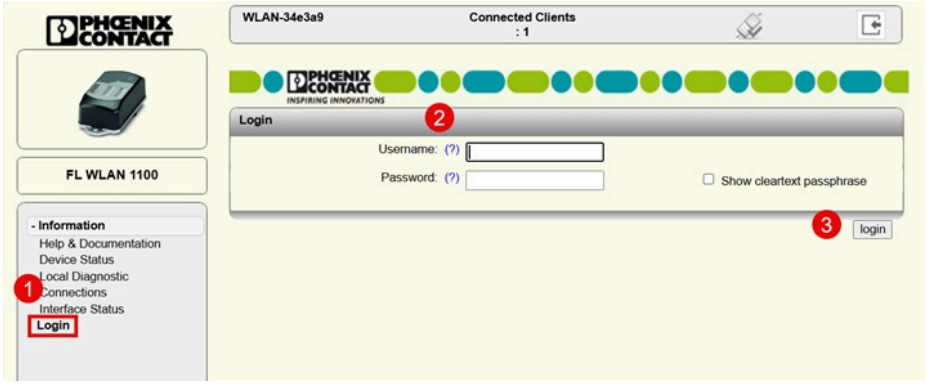
SSID: SureSeT_Factory order # XXXXXXXXXX-YYYYYY

> **NOTE:** XXXXXXXXXX-YYYYYY is the factory order number displayed on the SureSet switchgear nameplate. For example, if the Factory order number is 0042664369-000529 the Wi-Fi network SSID will be "SureSeT_0042664369-000529".

Connect to the Wi-Fi network using its default password “Digital1” and open a web browser. Type “https://192.186.4.100” into the web browser address bar to access the WLAN settings page.

2. **Log in** to WLAN access point using the “customer” user account. The Username is “customer” and the Password is “customer”.

Figure 15 - WLAN’s web browser login steps



3. **Change the Wi-Fi network password**

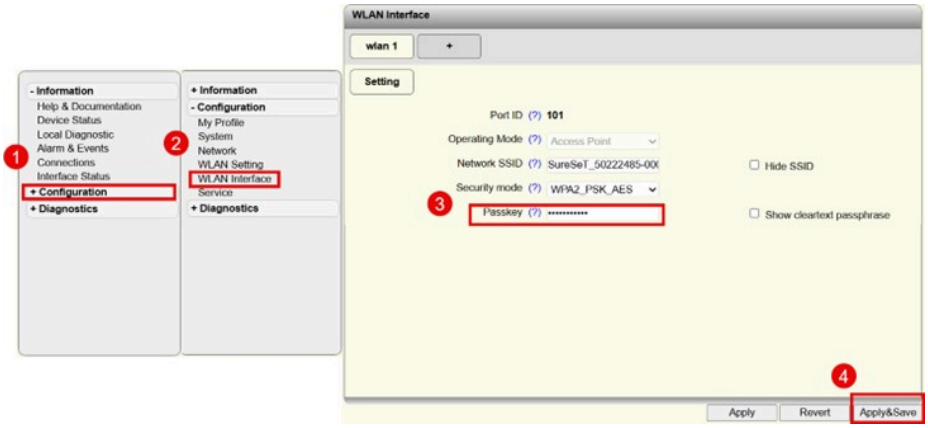
   All the WLAN access points provided with SureSeT switchgear are shipped from the factory with the same factory default password for their Wi-Fi networks (default password = Digital1). To comply with cybersecurity recommended practices, it is recommended to change such password during the switchgear commissioning.

   To change the Wi-Fi Password:

Change the Wi-Fi Password	
Step 1	Select “Configuration”
Step 2	Select “WLAN Interface”
Step 3	Change “Passkey” field as needed. Record and store the password
Step 4	Select on “Apply and Save” to complete the password change

   NOTE: Do not modify the Wi-Fi network SSID. If changed, some of the QR codes printed on the provided instruction labels may no longer work.

Figure 16 - Changing the WLAN’s password steps



4. **Disconnect, reconnect, and log in**

   Disconnect from the Wi-Fi network, then reconnect to the Wi-Fi network using the newly set password. Refer to step 1 and 2 to reconnect and log in to make changes to your “customer” user account.

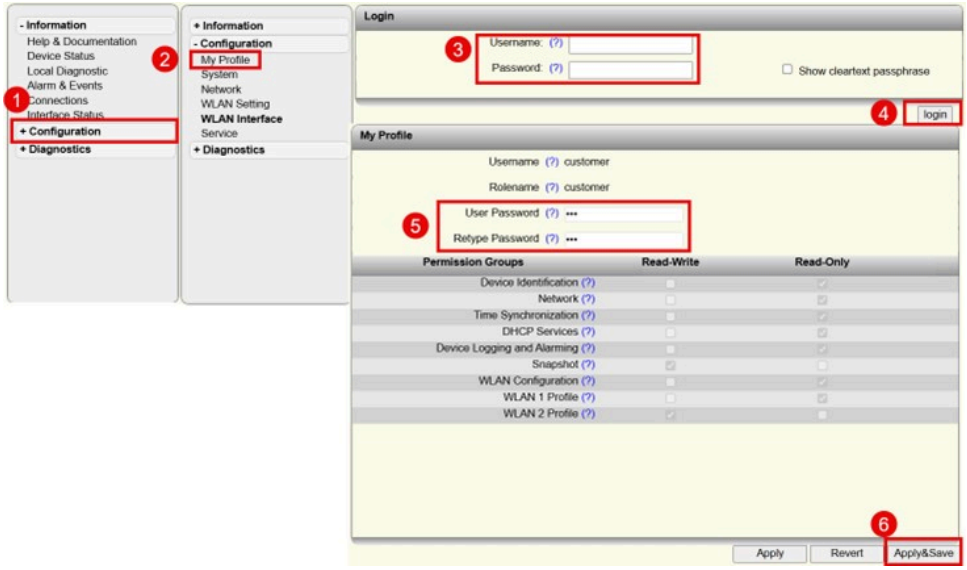
5. **Change “customer” user account password**

   All the WLAN access points provided with SureSeT switchgear are shipped from factory default username and password for the device “customer” user account. To comply with cybersecurity recommended practices, it is recommended to change such password during the switchgear commissioning. These log in credentials are required to modify the Wi-Fi network password, refer to steps 1, 2, 3. For instructions on how to modify the Wi-Fi network password.

To change the “customer” user account password:

Change the user account Password	
Step 1	Select “Configuration”
Step 2	Next select “My Profile”
Step 3	Enter Username as “customer” and Password as “customer”
Step 4	Log in
Step 5	Type the new password in the “User Password” and “Retype Password” fields. Record and store the new password
Step 6	Select “Apply and Save” to complete the password change

Figure 17 - Changing WLAN’s User account password steps



The WLAN access point is now ready for operation.

Microsoft Windows Login

The SMD HMI provided with SureSeT switchgear is a Microsoft Windows based industrial computer. EcoStruxure Operator Terminal Expert Runtime is used to launch the SMD HMI interface; such software automatically launches when Microsoft Windows starts, and it may be started anytime by using the shortcut available on the Microsoft Windows desktop.

It is required to log into Microsoft Windows to set up the SMD HMI interface. Follow the instructions below.

1. **Microsoft Windows login**

   Power on the SMD HMI and log in Microsoft Windows. The username is “SureSeT” and the Password is “SMD_Digital_1”. This log in features administrator rights. In case modifications to the Microsoft Windows account are needed, it may be required to enter answers to security questions. As factory default, 3 randomized questions are going to selected and the answer to all of them will be "SureSeT". To comply with cybersecurity recommended practices, it is recommended to change such questions and answers in the MS Windows account settings.

2. **Modify factory provided Microsoft Windows credentials**

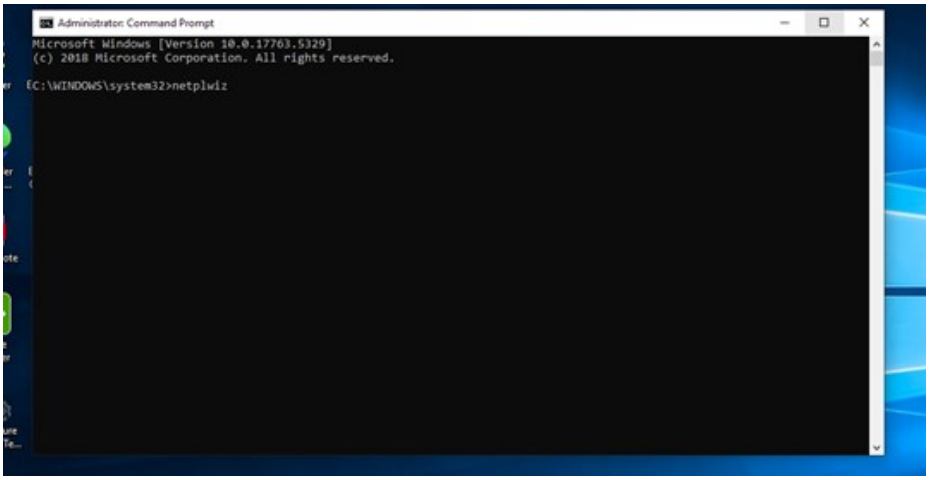
   All the SMD HMI provided with SureSeT switchgear are shipped from the factory with the same factory default Microsoft Windows username and password (the Username is "SureSeT" and the Password is "SMD_Digital_1").

   To comply with cybersecurity recommended practices, it is recommended to change such password during the switchgear commissioning. This change may be done in the Microsoft Windows account settings after log in. Record and store the username and password.

If the HMI power supply is lost and restored, it is necessary to enter the Microsoft Windows username and password in order to launch the SMD HMI interface. In case an automatic restart is desired after the power supply is restored, it is possible to configure Microsoft Windows to avoid asking for username and password. The automatic restart setup is strongly recommended in case of "faceless" HMI applications because local user interfaces are not available with such options, and the connection of external peripherals (keyboard, mouse, and display) would be required to enter Microsoft Windows credentials. The procedure for such configuration is detailed on the following page.

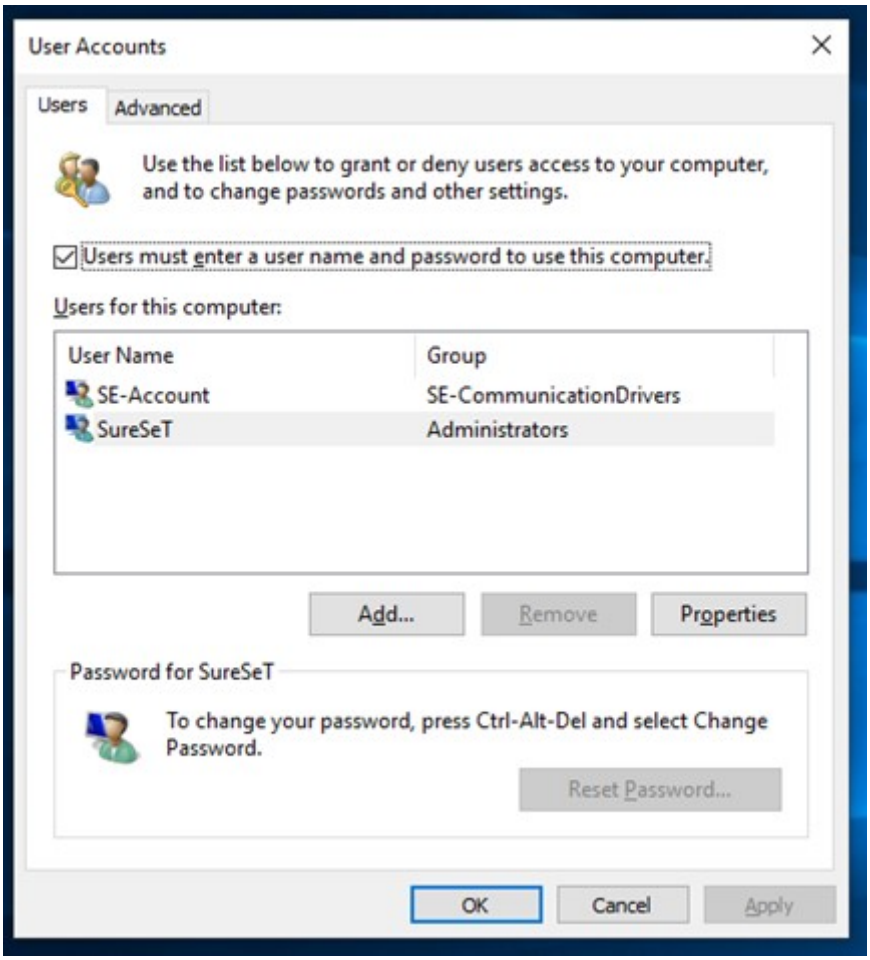
1. Open the Microsoft windows command prompt and run the “netplwiz” command:

Figure 18 - Administrators command prompt running the “netplwiz” command



Uncheck the “Users must enter a username and password to use this computer” box in the User Accounts dialog box and tap on “OK” to confirm,

Figure 19 - Windows User accounts screen



2. Enter the Microsoft Windows account password twice to confirm and conclude the procedure.

Microsoft Windows will not ask for username and password entry at start up from now on.

The Eth2 port is not intended to be connected to any other local systems and shall only be connected to the Wi-Fi access point. IP readdressing will not be necessary.

NOTE: Do not change the ethernet adapter settings of the HMI ethernet port Eth2. If changed, it will be impossible to “mirror” the HMI screen on a wirelessly connected device

In case the IP addressing of the HMI (and the other SMD devices like the main controller and the EcoStruxure Panel Servers) is required per customer corporate policies, it is possible to modify the Eth1 port ethernet adapter settings.If this change is required, end users may change the SMD HMI IP address and the EcoStruxure Panel Servers’ IP addresses, but they may not modify the SMD main controller IP address. Contact your local Schneider Electric representative in case such modification is needed. It is recommended to provide the required IP addressing, subnet masking, and gateway addressing as specifications for the switchgear factory order to allow the required configuration to be completed prior to switchgear shipping from the factory.

System Time Synchronization

As a factory default, all the components of the digital monitoring and control system SureSeT switchgear are synchronized to the SMD HMI time via NTP (Network Time Protocol). The SMD HMI is configured as the NTP server of the system. In case the SMD provided with the SureSeT switchgear is required to be synchronized to an external NTP server, the HMI may be set to be an NTP client to receive time synchronization requests from an external NTP server. Instructions on how to set the HMI for such purpose are listed below:

1. Start from the SMD HMI Microsoft Windows desktop (if EcoStruxure Operator Terminal Expert Runtime is in full screen mode, swipe from the outer left edge of the screen towards the center of the screen and create a new desktop).
2. Open command prompt by running the application as an administrator.
3. Type “C:\windows\system32>w32tm /config /manualpeerlist:“XXX.XXX.XXX.XXX” /syncfromflags:manual /update” (where XXX.XXX.XXX.XXX is the IP address of the external NTP Server) and press Enter.

   NOTE: The NTP server and the HMI shall be on the same subnetwork.

To verify proper time synchronization the following steps may be followed:

1. Open command prompt by running the application as an administrator
2. Type “C:\windows\system32>w32tm /query /source” and press Enter.
3. The return message shows the NTP server’s IP address that the HMI Microsoft Windows Time service is synchronizing with. The IP address should match the one previously entered.
4. The “C:\windows\system32>w32tm /resync” and press Enter to force a time synchronization command. The SMD HMI date and time should now match the NTP server date and time.

SMD Login

Before being able to access the SMD HMI interface, it is required to modify the SMD factory default credentials and log into the SMD. Follow the instructions below.

1. **Launch EcoStruxure Operator Terminal Expert User Management Tool**

   Launch EcoStruxure Operator Terminal Expert User Management Tool on the HMI using the shortcut provided on the Microsoft Windows Desktop.

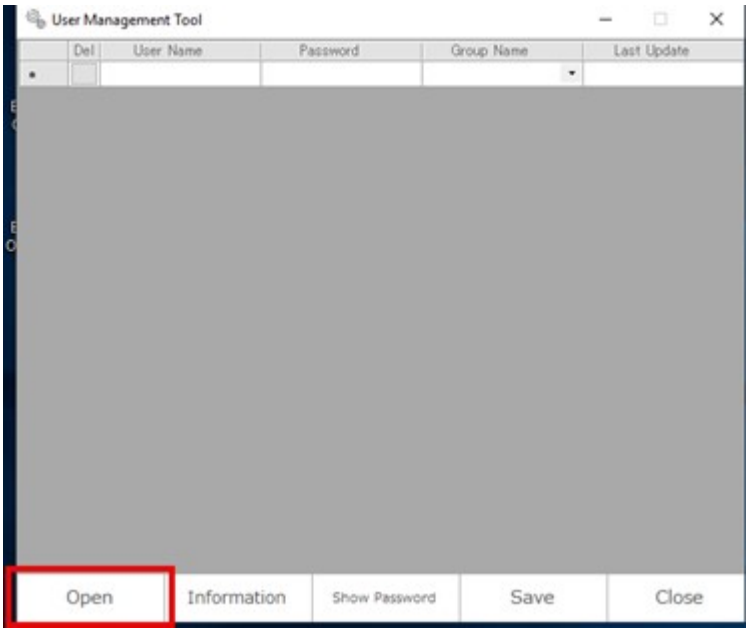
   Figure 20 - Icon for EcoStruxure Operator Terminal Expert User Management Tool

   NOTE: It is recommended to connect a USB keyboard to the HMI to make data entering easier.

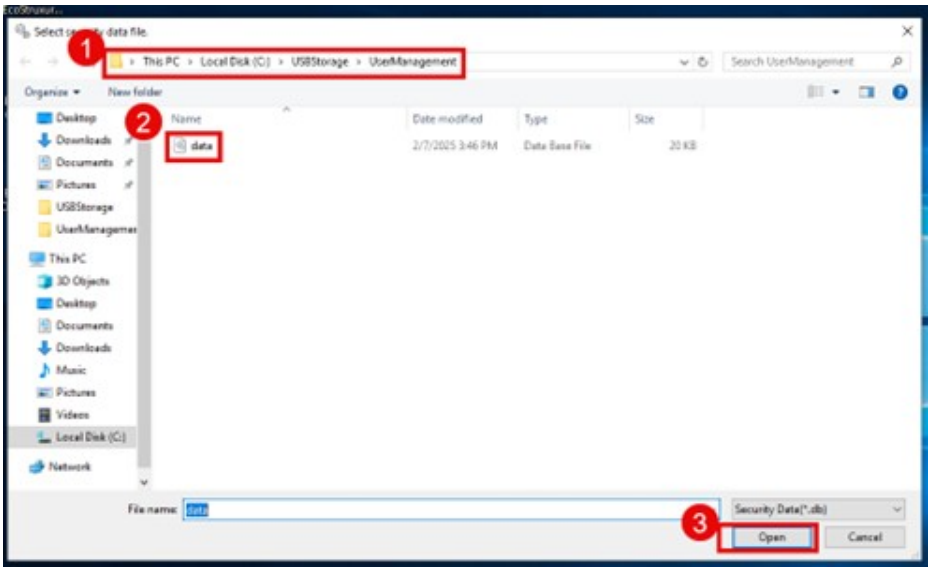
2. **Open the User Database**
   Tap on “Open”

Figure 21 - User management tool home page



Select the User data file (C:\USBStorage\UserManagement\data.db)

Figure 22 - Steps to load user data file



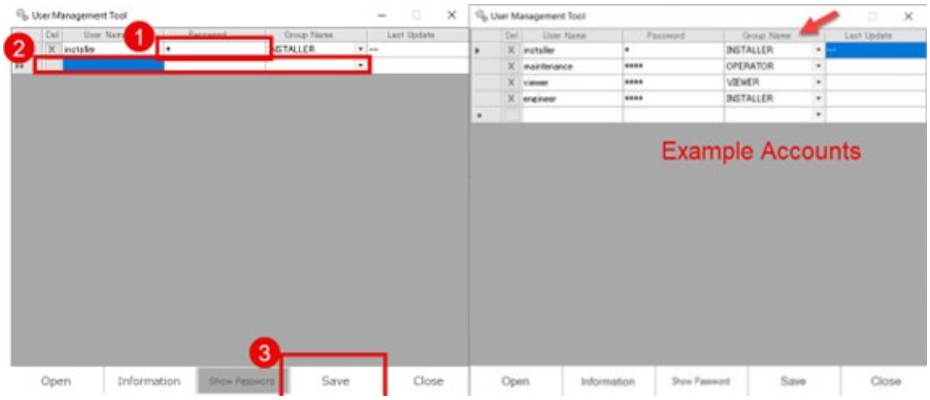
Enter the database default password “1234”.

3. **Modify the factory default credentials and add user accounts as needed**

   As factory default, a single user account is provided (Username: “installer”, Password: “1234”).

1. Modify the password of the user profile
2. Create as many User profiles as needed
3. Record and store the usernames and passwords

Figure 23 - Steps to change “installer” password and create new account



Refer to document GEX9033400, Substation Monitoring Device (SMD) SMD MV Enhanced User Guide for more details on the user types defined by the “Group Name” field. A summary table is provided below for reference.

Table 1 - User account types and their corresponding permissions

Operations	User Type			
	Viewer	Operator	Installer	Secadm
View monitoring data	✓	✓	✓	✓
WebViewer operation	—	✓	✓	—
Switchgear operation	—	✓	✓	—
System debug	—	—	✓	—
Hardware configuration	—	—	✓	✓
User management	—	—	✓	✓
Security log access	—	—	✓	✓

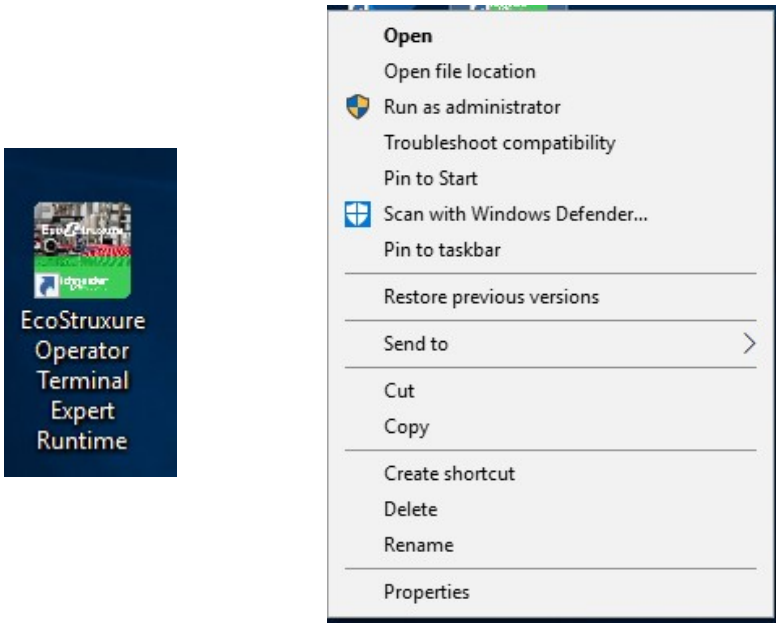
Tap on “Save” and “Close” to complete the user database modifications.

NOTE: User profiles may be modified at any time during the operation of the SMD. Refer to section Managing the SMD User Database, page 41.

4. **Start the SMD HMI interface, user database load, and log in**

   In case the EcoStruxure Operator Terminal Expert Runtime is already launched, terminate it and launch it using the shortcut provided on the Microsoft Windows Desktop. Run EcoStruxure Operator Terminal Expert Runtime with administrator rights by long-tapping (or right clicking, in case a mouse is used) on the shortcut icon and choose the “Run as administrator” option.

Figure 24 - Icon for EcoStruxure Operator Terminal Expert Runtime and shortcut launch menu



Tap on “Login” and log in using the factory default credentials. (Username: “installer”, Password: “1234”).

Figure 25 - Steps for logging into EcoStruxure Operator Terminal Expert Runtime for the first time

Tap on “Load user database” to load the User data file modified during step 3. Enter the User database file password “1234”, and tap on “OK” to confirm.

Figure 26 - Steps for loading user database into EcoStruxure Operator Terminal Expert Runtime

5. **Confirm date and time**

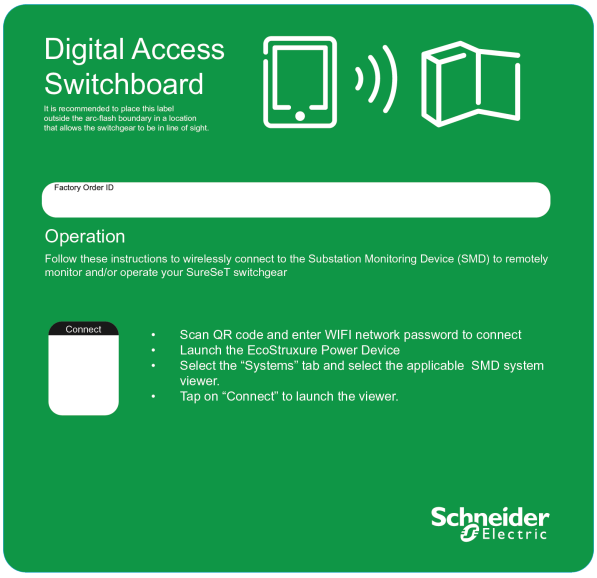
   Tap on “Next” and confirm the date and time automatically read by the application from the Microsoft Windows settings. The SMD HMI interface will now start with the user profiles defined during step 3 loaded. Such profiles are to be used for the logins required to operate the SMD.

   NOTE: After this step, it will not be necessary to log in when EcoStruxure Operator Terminal Expert Runtime is launched. The application will start at the SMD HMI home page after the booting process.

Nearby Mode Operation

A label is included with SureSeT switchgear spare parts to help speed up the connection to the SMD HMI during operation. It is recommended to place this label in a location outside the arc flash boundary, where the switchgear front panels and the status of the pilot lights are clearly visible.

Figure 27 - Label for Nearby Mode Operation

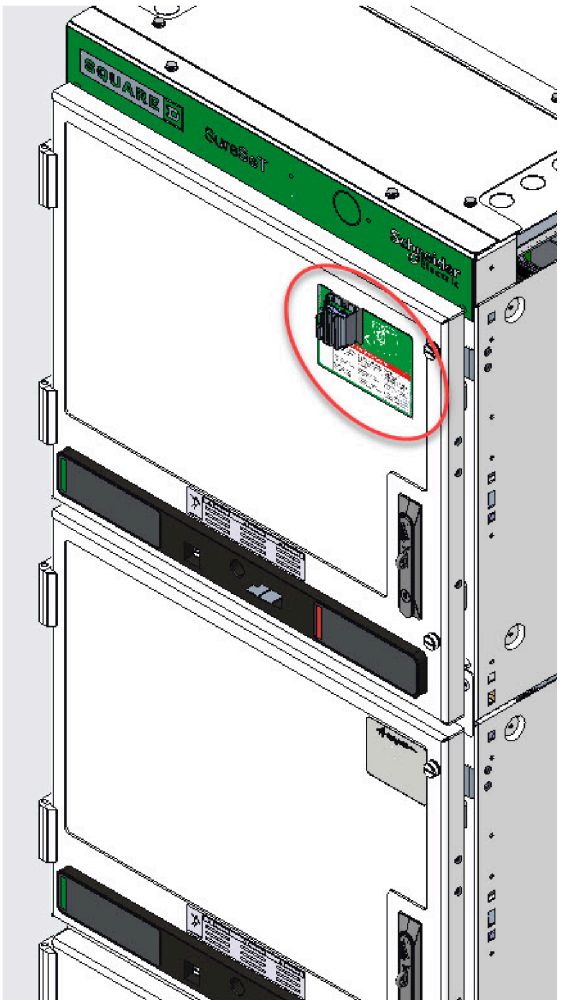


The instructions below provide alternative procedures that may be used in case access to such label is not available or practical.

For proper operation, make sure the following actions are completed;

- All circuit breakers are properly inserted in their compartments. Verify their position matches the information listed on the BM100 Modbus address setting label of the circuit breaker.
- The CL110 labeled "AMB" is correctly positioned in the designated opening on its placement guide label, located in the top-right corner of the upper front door of one of the switchgear compartments.

Figure 28 - “AMB” CL110 sensor on SureSeT switchgear

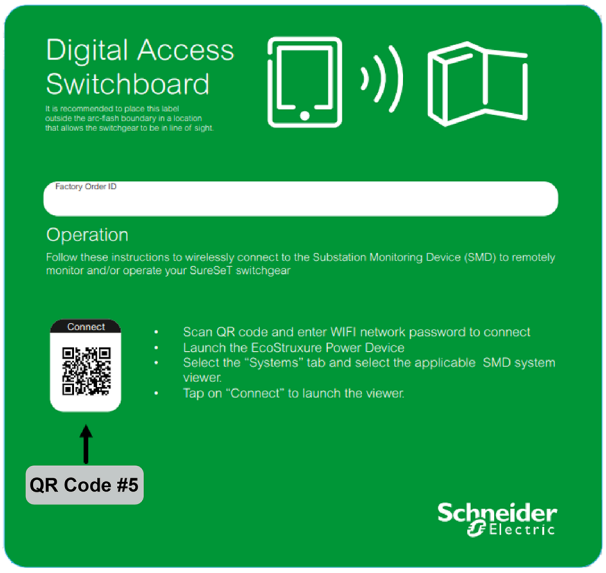


NOTE: TH110 sensors are self-powered wireless sensors that will power on when a sufficient current flows through the switchgear bus. The sensors will not respond if sufficient current is not flowing through the conductor to which they are mounted on.

Nearby Mode with Smartphones or Tablets

1. Connect the switchgear Wi-Fi network by scanning QR code #5 on the provided label and entering the Wi-Fi network password.

Figure 29 - QR code #5 on Label for Nearby Mode Operation



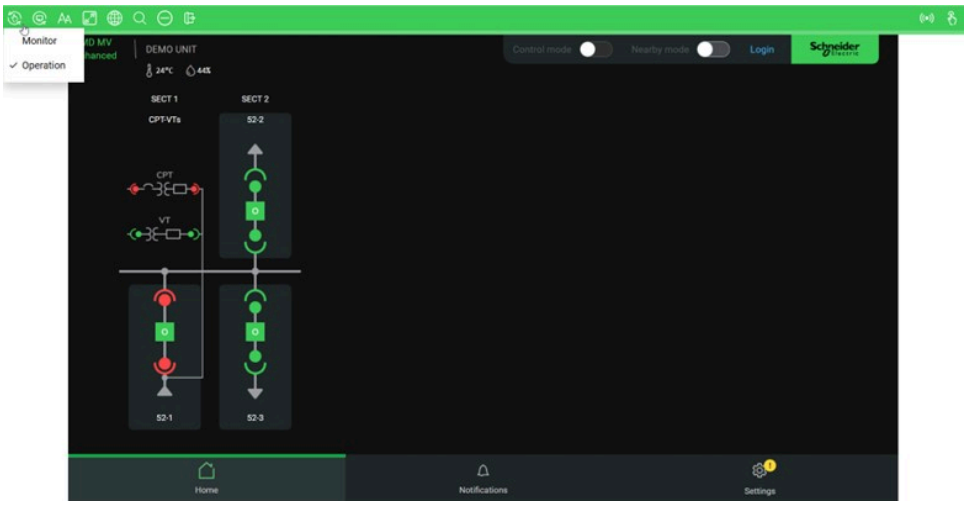
If the QR code is unavailable, you can manually connect to the Wi-Fi network through your device's Wi-Fi settings. If multiple networks are in range, make sure you connect to the correct one by verifying the switchgear factory order number on the switchgear rating nameplate.

2. Launch the EcoStruxure Power Device app.
3. Tap on the "Systems" tab and select the applicable SMD viewer.
4. Tap on "Connect".
5. Log in the SMD by entering the applicable username and password.

The device should display the SMD HMI home page.

If the device screen appears unresponsive, check that "Operation" mode is selected in the top-left corner of the screen.

Figure 30 - Nearby screen mirroring with "Operation" mode selected

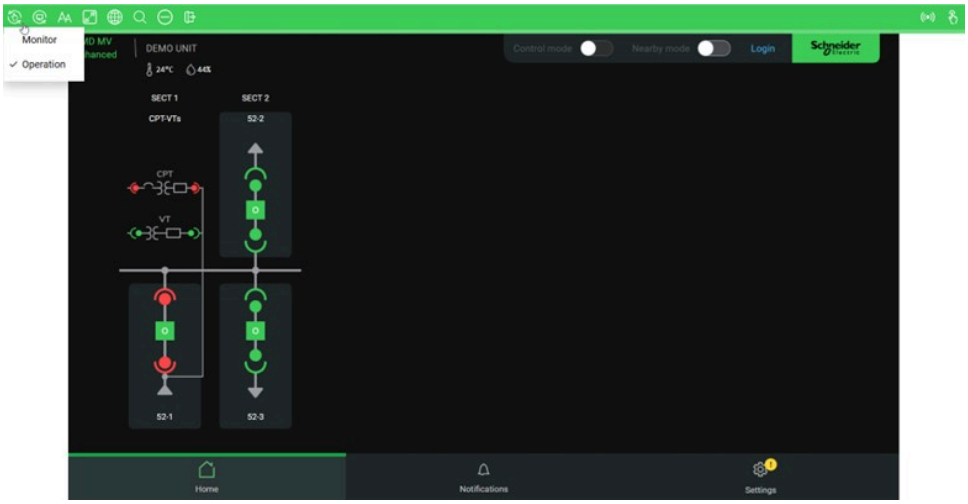


Nearby Mode with Laptops

1. Connect to the switchgear Wi-Fi network by entering the applicable Wi-Fi network SSID and password. If multiple Wi-Fi networks are in range, connect to the proper Wi-Fi network by verifying the switchgear factory order number on the switchgear rating nameplate.
2. Change the laptop Wi-Fi network Internet Protocol Version 4 (TCP/IPv4) settings as follows:
   - Select “Use the following IP address”.
   - Set the Address as “192.168.4.200”.
   - Set Subnet Mask as “255.255.255.0”.
   - Set Default gateway as “192.168.4.100”.
   - Click on “OK” to confirm.
3. Open your web browser (the use of Google Chrome is recommended) and enter “http://192.168.4.105:8082/webviewer/index.html” into the web browser bar.
4. Log in to the SMD by entering the applicable username and password.

   If your device screen appears unresponsive, make sure that "Operation" mode is selected in the top-left corner of the screen.

Figure 31 - Nearby laptop screen mirroring with “Operation” mode selected



Managing the SMD User Database

The user credentials of the SMD may be managed by exporting, modifying, and importing the SMD user database file on the SMD HMI. If you need to update usernames or passwords, or add or remove user profiles, follow the steps outlined below.

1. Starting from the SMD HMI interface's home page (running on EcoStruxure Operator Terminal Expert Runtime), tap on the settings icon.
2. Tap on the "Advanced" tab, log in with a user profile featuring "INSTALLER" or "SECADMIN" as Group Name,and tap on User database:"Export".
3. Enter "C:\USBStorage\UserManagement\data.db" as export destination file.
4. Enter the database password. Record it and store the database password.
5. Minimize the EcoStruxure Operator Terminal Expert Runtime window (swipe from the outer left edge of the screen towards the center of the screen if in full screen mode) and open EcoStruxure Operator Terminal Expert User Management Tool by using the shortcut provided on the SMD HMI desktop.

Figure 32 - Icon for EcoStruxure Operator Terminal Expert User Management Tool

6. Tap on "Open", select the newly exported user data file (C:\USBStorage \UserManagement\data.db), and enter the password assigned during step 4.
7. Modify the user database file as needed and click on "Save" and "Close" to complete the modification.
8. Return to the SMD HMI interface's home page (running on EcoStruxure Operator Terminal Expert Runtime) and tap on the settings icon.
9. Tap on the "Advanced" tab and tap on User database:"Import".
10. Enter "C:\USBStorage\UserManagement\data.db" as import destination file.
11. Enter the password assigned during step 4 when prompted.

The new SMD user accounts are now loaded into the SMD and are to be used for future logins. Refer to document GEX9033400, Substation Monitoring Device (SMD) SMD MV Enhanced User Guide for a visual representation of the Advanced Setting screen.

Summary of User Accounts

The following user accounts are required to operate and maintain the SureSeT digital monitoring and control system of SureSeT switchgear including the SMD. The table below lists the factory default credentials that are provided when the switchgear is received. Track and record username and password changes.

Table 2 - User Accounts

Account Type	Factory Default Credentials	Comments
Schneider Electric customer account	N/A	This account is needed to log in the EcoStruxure Power Device app to “mirror” the SMD HMI screen.
SMD HMI Windows	Username: **SureSeT** Password: **SMD_Digital_1**	Credentials needed to log in Microsoft Windows and make changes that require administrator rights. Users are strongly recommended to update these credentials during the startup procedure. Refer to Windows Login.
WLAN Access Point	Username: **customer** Password: **customer**	Credentials needed to log in the WLAN access point to modify the Wi-Fi network password.Users are strongly recommended to update these credentials during the startup procedure. Refer to WLAN Access Point Setup.
Wi-Fi Network	Network SSID:**SureSeT_Factory order #** Password: **Digital1**	Credentials needed to connect to the Wi-Fi network that enables the “screen mirroring” of the SMD HMI.It is recommended not to change the Wi-Fi network SSID.Users are strongly recommended to update the WiFi network password during the startup procedure. Refer to WLAN Access Point Setup.
SMD User Management Data File	Password: **1234**	Password needed to open and modify the user database file and to load user database files into the SMD. This password may be modified when a user database is exported for modifying SMD user credentials. Refer to Managing the SMD User Database.
SMD user account/s	Username: **installer** Password: **1234**	Credentials needed to start he SMD during commissioning (SMD first use after shipment), remotely control devices and make advanced setting changes. One user profile is provided as factory default. The password of this account shall modified to load the user database and allow the SMD to run during the startup procedure. Refer to SMD Login. Additional user profiles may be created as needed; refer to Managing the SMD User Database, page 41.

Cybersecurity Recommendations

General Cybersecurity Recommendations

⚠WARNING

HAZARD OF COMPROMISED SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY

- Change default passwords to help prevent unauthorized access to device settings and information.
- Disable unused ports/services to help minimize pathways for malicious attackers.
- Place networked devices behind multiple layers of cyber defenses (such as firewalls, network segmentation, and network intrusion detection and protection).
- Use cybersecurity best practices (for example, least privilege, separation of duties) to help prevent unauthorized exposure, loss, modification of data and logs, or interruption of services.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

For detailed information about cybersecurity for the SMD, refer to:

- HMIST6700 Hardening Guide
- Cybersecurity Guidelines for EcoStruxure Machine Expert, Modicon and PacDrive Controllers and Associated Equipment, User Guide

For a general introduction to cybersecurity threats and how to address them, refer to How can I Reduce Vulnerability to Cyber Attacks?.

For more information about cybersecurity, visit the Schneider Electric Cybersecurity Support Portal.

Security Features

Security features have been built into the SMD to help the device to operate correctly and behave according to its intended purpose.

The key features are:

- Authentication when accessing product resources from the HMI.
- Configurable security services and settings, using the User Management Tool for HMI user definition.

These features provide security capabilities which help to protect the product from potential security threats, which could disrupt the product operation (availability), modify information (integrity) or disclose confidential information (confidentiality).

The security capability features are intended to mitigate the inherent threats which are linked with the use of the SMD in an Operational Technology environment.

However, the effectiveness of these capabilities depends on the adoption and application of the following recommendations:

- Recommendations provided in this chapter to cover the commissioning, operation, maintenance, and decommissioning of the product.
- Recommendations Cybersecurity Best Practices.

Potential Risks and Compensation Controls

Area	Issue	Risk	Compensating controls
Unsecure protocols	Modbus and some IT protocols (NTP, DHCP, DNS, and DPWS) are unsecure. The device does not have the capability to transmit data encrypted using these protocols.	If a malicious user gained access to your network, they could intercept communications.	If transmitting data over an internal network, physically or logically segment the network. If transmitting data over an external network, encrypt protocol transmissions over all external connections using a VPN or a similar solution.
Wireless radio communication	During the pairing window, unauthorized radio devices may try to join the network.	If a rogue device gained access to your network, they could eavesdrop on the communication of your wireless network, create an integrity data breach (for example, by sending fake data), or create a Denial of Service (DoS).	Reduce commissioning window to limit exposure. Once the pairing is performed, consult the list of paired devices in SMD configuration using EcoStruxure Power Commission software and make sure that the list of devices contains no unexpected or rogue devices.

Security Recommendations for Commissioning

Refer to Cybersecurity Recommendations, page 43.

Security Recommendations for Operation

Refer to Cybersecurity Recommendations, page 43.

Security Recommendations for Decommissioning

Refer to Cybersecurity Recommendations, page 43.

Glossary

Acronym	Full name
BMS	Building Management System
CB	Circuit Breaker
CT	Current Transformer
HMI	Human Machine Interface
IED	Intelligent Electronic Device
LV	Low Voltage
MCM	Motor Control Monitoring
MV	Medium Voltage
PLC	Programmable Logic Controller
RFID	Radio Frequency Identification
SCADA	Supervision Control And Data Acquisition
SLD	Single Line Diagram
SMD	Substation Monitoring Device
EPME	EcoStruxure Power Monitoring Expert
EPO	EcoStruxure Power Monitoring Operation

Printed in:
Schneider Electric
800 Federal Street
Andover, MA 01810 - USA
888–778–2733

Schneider Electric
800 Federal Street
01810 Andover, MA
USA

888–778–2733

www.se.com

D3982892