7EN12-0259-00
02/2012

PowerLogic ION8600 installation guide and user guide addendum

This document describes the latest product modifications for the PowerLogic™ ION8600 energy and power quality meter.

There is a new 100BaseT Ethernet option, changes to the communications LED indicators and some options have been discontinued. Refer to “New Ethernet option”, “Changes to LED indicators” and “Discontinued order options” on page 4.

Significant improvements have been made to meter security in firmware version 335 (v335) and later. Whether your meter has standard or advanced security enabled, changes to user login methods and behavior have been implemented to help increase security and traceability. Configuration instructions, factory default settings for new meters and recommendations and best practices are described.

- Refer to “Configuring new security features using ION Setup” on page 5 for information on how to configure protocol lockout, session timeout and meter access event logging for meters with standard or advanced security using ION Setup.
- Refer to “Factory access” on page 12 for information on how to configure factory access on your meter.
- Refer to “Security recommendations and best practices” on page 16 for meter security recommendations and best practices.
- Refer to “Default security settings” on page 18 for factory default values for meter security settings.

In order to configure the new features, you need to download the latest version of ION Setup from www.schneider-electric.com.

Schneider Electric
2195 Keating Cross Road
Saanichton, BC
Canada V8M 2A5
Tel: 1-250-652-7100

For technical support:
Global-PMC-Tech-support@schneider-electric.com
(00) + 1 250 544 3010

Contact your local Schneider Electric sales representative for assistance or go to www.schneider-electric.com

Safety information

Important information

Read these instructions carefully and look at the equipment to become familiar with the device before trying to install, operate, service or maintain it. The following special messages may appear throughout this bulletin or on the equipment to warn of potential 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 potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

⚠ DANGER

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

⚠ WARNING

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

⚠ CAUTION

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

NOTICE

NOTICE is used to address practices not related to physical injury. The safety alert symbol shall not be used with this signal word.

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.

Safety precautions

Installation, wiring, testing and service must be performed in accordance with all local and national electrical codes.

⚠ DANGER

HAZARD OF ELECTRIC SHOCK, EXPLOSION OR ARC FLASH

- Apply appropriate personal protective equipment (PPE) and follow safe electrical work practices. See NFPA 70E in the USA or applicable local standards.
- This equipment must only be installed and serviced by qualified electrical personnel.
- Turn off all power supplying this device and the equipment in which it is installed before working on the device or equipment.
- Always use a properly rated voltage sensing device to confirm that all power is off.
- Do not perform Dielectric (Hi-Pot) or Megger testing on this device.
- Replace all devices, doors and covers before turning on power to this equipment.

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

NOTE

Do not perform Dielectric (Hi-Pot) or Megger testing on this device because its internal surge protection circuitry starts functioning at levels below typical Hi-Pot voltages. Contact your local Schneider Electric representative for more information on device specifications and factory testing.

Do not lose your meter's front panel and user password information. If your meter's front panel or user passwords are lost, you must return the meter for factory reconfiguration, which resets your meter to its factory defaults and erases all logged data. Refer to "Password best practices" on page 16 for more information.

NOTICE

LOST DATA

Record your meter's front panel and user password information in a secure location.

Failure to follow this instruction can result in data loss.

New Ethernet option

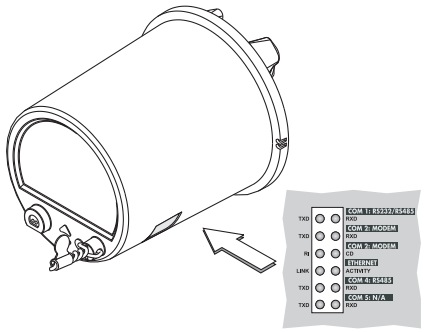
The previous 10Base-T Ethernet communications option has been upgraded to the faster 100Base-T hardware found on other PowerLogic meters. Below are the new option codes to order a meter with the new 100Base-T Ethernet communications card.

Option	Code	Description
Communications M 8 6 0 0 A 0 C 0 H 6 C 7 A 0 A	C7	Front panel infrared optical port, RS-232/RS-485, 10/100Base-T Ethernet, internal modem
	E1	Front panel intrared optical port, RS-232/RS-485, RS-485[1], 10/100Base-T Ethernet

[1] This port is not available on the ION8600C meter.

Changes to LED indicators

The “Step 9: Verify Meter Operation” section in the installation guide has changed:



LED	Function
TXD / RXD	Flash = signals are being transmitted and received for serial ports
RI	Ring Indicator (flash = modem rings)
CD	Carrier Detect (on = active connection to modem)
LINK	On = Ethernet connection is active Off = Ethernet connection is not active Flash = Ethernet signals are being received
ACTIVITY	Flash = Ethernet signals are being transmitted

Discontinued order options

The following options are no longer available on the ION8600. Disregard any mention of the following in your meter’s technical documentation:

Form Factor

- Form 39S (Form Factor option code “3”)
- Form 76S (Form Factor option code “N”)

Communications

- Internal modem with RJ31 connector (Communications option code “C2”)
- 10Base-FL Ethernet-Fiber (Communications option code “F0”)
- 10Base-T Ethernet RJ45 (Communications option codes “C1” and “E0”)

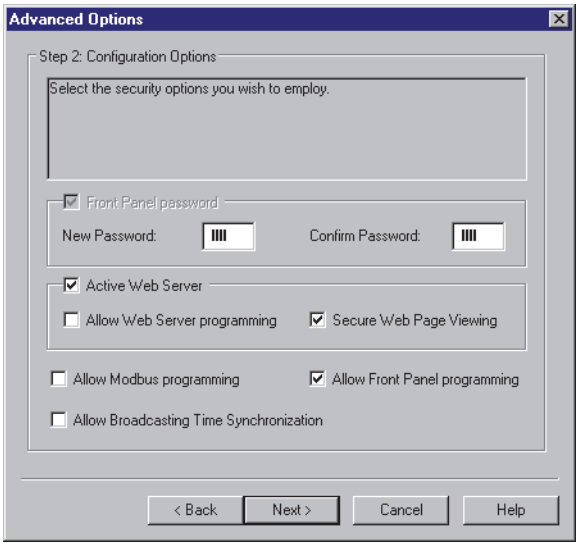
Configuring new security features using ION Setup

The simplest way to configure the new security features is to use the advanced security wizard in the ION Setup Assistant, as described below. These settings will apply regardless of whether standard or advanced security is enabled on your meter. You can also modify security settings using the advanced mode in ION Setup to manually edit individual registers in the Security User and Security Options modules.

You must be logged into ION Setup with supervisor authority in order to configure security on your meter.

Step 1: Set basic security options

1. Open the Setup Assistant for your meter. See the ION Setup Help for instructions.
2. Select the **Security** screen.
3. Select **Security Mode** from the **Security** tab and click **Edit**. The **Open** dialog box appears.
4. Select the Advanced.scf file and click **Open** to edit. The **Advanced Options** dialog box appears.
5. On the **Advanced Options** configuration screen, select the check boxes of the security options you want enabled. Some options may be disabled (grayed out) because of existing security settings.
   - To change the meter's password, type a new meter password, then confirm the new password by typing it again. Refer to "Password best practices" on page 16 for more information.
   - **Allow Web Server programming** is disabled (cleared) by default. Disable web-based meter configuration unless you are actively using this feature.
   - **Allow Modbus programming** is disabled (cleared) by default. Disable Modbus programming unless you are actively using this feature.



Changing communications port settings with the **Allow Front Panel Programming** setting cleared (unchecked) may cause loss of communications with your meter, and render it inoperable. In this case a factory reconfiguration of your meter is required, which resets your meter to its factory defaults and destroys all logged data.

NOTICE
LOST DATA Do not change communications ports settings with the Allow Front Panel Programming setting cleared (unchecked). **Failure to follow this instruction can result in data loss.**

6. Click **Next**. The **Select protocol lockout options** screen appears; see “Step 2: Configure communications protocol lockout options” on page 6.

Step 2: Configure communications protocol lockout options

The communications protocol lockout advanced security feature allows you to set the number of invalid login attempts that each user can make using a particular protocol and communications method before being locked out (a user is defined as a user login and password combination). For protocols that are not session-based (ION and HTTP), you can configure how often the meter registers invalid login attempts. You can also configure the lockout duration for all configurable protocols. By default, all protocols are set to eight invalid attempts and a 24-hour lockout duration.

Once a user is locked out, the meter will not accept login attempts from that user on that protocol and communications method until the lockout duration has passed. Invalid login attempts accumulate until the user has completed a valid login or been locked out. For example, once USER01 has been locked out using ION over Ethernet, USER01 cannot access the meter using ION over Ethernet until the lockout duration has passed, even if USER01 enters the correct password.

However, if the user enters the correct USER/password combination before being locked out, the invalid attempt counter is reset to zero. Even if the user is locked out using ION over Ethernet, that user can still access the meter by entering the correct USER/password combination over a different protocol and communications method (for example, connecting to the meter's front optical port using ION protocol).

You can also configure the event priority for meter access and protocol lockout events, so they can be viewed in the meter's event log. By default, the Invalid login event priority is set to 128 and the lockout event priority is set to 255. The meter access event priorities can be configured by clicking the **Events** on the protocol lockout screen.

Configuring communications protocol lockout

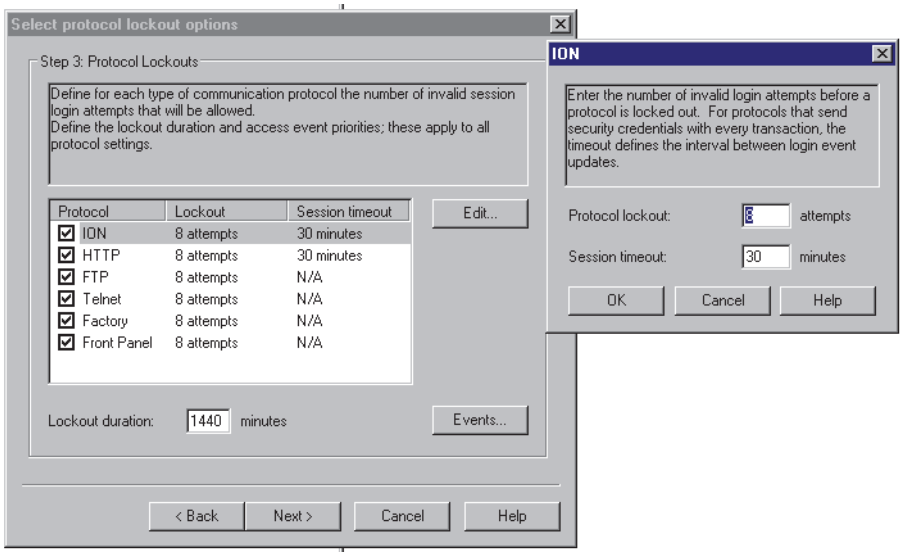
See "Communications protocol lockout examples" on page 8 for examples of how these settings affect login and communications.

1. Select the check boxes beside the protocols for which you want to enable communications protocol lockout. By default, all protocols are selected.
2. Highlight a selected protocol and click **Edit** to modify the lockout values for that protocol.
   - Protocol lockout attempts specifies the number of invalid login attempts allowed per user/password combination before access is denied to that user over that protocol and communications method. This value can range from 0 to 255.

NOTE

If Invalid logins is set to 0, there is no limit to the number of invalid login attempts and that protocol will never be locked out. However, the invalid login attempt events are recorded if the meter access events are configured to record invalid access attempts.

   - Session timeout specifies the active duration for a protocol; during this time, repeated invalid login attempts using the same USER/password combination are not registered (repeated invalid attempts with different combinations are still registered). This only applies to protocols which are not session-based, and send credentials with each packet. Configuring this setting helps prevent accidental lockouts and filling the meter's event log with protocol access events. This value can range from 1 minute to 43200 minutes (30 days).



Click **OK**. Repeat for all protocols on which you want to enable communications protocol lockout.

3. Type the lockout duration, in minutes. The lockout duration specifies how long the meter ignores communication attempts by a user that is locked out. The lockout duration value applies to all lockout-enabled protocols, and has a default value of 24 hours.

   Once a user is locked out, the user cannot access the meter using the same protocol and communications method, regardless of whether or not the user enters the correct USER/password combination.

4. Click **Events** to enter the event priority for valid login attempts, invalid login attempts and protocol lockouts. The event priorities apply to all lockout-enabled protocols. Enter “0” (zero) to disable event logging for a particular type of login attempt. By default, valid login events are zero, invalid login events are 128 and lockout events are 255.

5. Click **Next**. The **Define individual users/passwords** screen appears. Refer to “Step 3: Configure users” on page 10 for the next step in configuring Advanced security, and “Communications protocol lockout examples” on page 8 for scenarios describing protocol lockout behavior.

Communications protocol lockout examples

In the following examples:

- The configured users and their valid passwords are:
  - USER01/password 11
  - USER02/password 22
- For the ION protocol:
  - Protocol Lockout is configured to allow 3 invalid login attempts by a particular user/password combination before locking the user out.
  - Session timeout is set to 30 minutes.

- For all protocols that can be locked out:
  - Lockout duration is set to 1440 minutes (one day).
  - The meter is configured to log invalid event entries and lockouts.

Scenario 1

This example illustrates what happens when a user repeatedly enters the same incorrect password when attempting to access the meter.

1. An access attempt is made using ION over Ethernet by USER01 but with a password of 0.

   The user is informed of the invalid attempt and cannot access the meter. The invalid attempt is logged in the event log and the counter of invalid attempts is incremented to 1.

2. The user attempts to access the meter again 10 minutes later with USER01/password 0.

   The user cannot access the meter but the event is not logged and the counter of invalid attempts is not incremented, because the session timeout has not elapsed.

3. The user attempts to access the meter again with the invalid USER01/password 0 combination 30 minutes after the initial attempt.

   Because the session timeout has elapsed, the event is logged and the counter of invalid login attempts is incremented to 2.

   - If the user attempts to login again after 30 minutes has elapsed with the same invalid USER01/password 0 combination, the event is logged and the counter of invalid attempts is incremented to 3. USER01 is locked out for the duration of the lockout time (1440 minutes), and cannot connect to the meter using ION over Ethernet, regardless of whether or not they subsequently try to login with the correct user/password combination. The lockout event is logged by the meter. USER01 can access the meter through another communications method (for example, ION over serial) if the user enters the correct USER/password combination.
   - If the user attempts to login with USER01/password 11, the access is allowed and the invalid login counter is reset to 0.

Regardless of the invalid attempts of USER01, USER02 can access the meter using ION over Ethernet if they enter the correct password; they are not affected by the lockout.

Scenario 2

This example illustrates what happens when different invalid combinations of user and password are entered.

1. An access attempt is made using ION over Ethernet by USER01 but with a password of 0.

   The user is informed of the invalid attempt and cannot access the meter. The invalid attempt is logged in the event log and the counter of invalid attempts is incremented to 1.

2. The user attempts to access the meter again with USER01/password 3.

The user is informed of the invalid attempt and cannot access the meter. In this case, this is considered a new invalid attempt because it is a different combination of user and password. It is logged in the event log and the counter of invalid attempts is incremented to 2.

3. The user attempts to access the meter again with USER01/password 4.

   The user is informed of the invalid attempt and cannot access the meter. Once again, this is considered a new invalid attempt and it is logged in the event log and the counter of invalid attempts is incremented to 3. The meter logs a lockout event.

   USER01 is locked out for the duration of the lockout time (1440 minutes), and cannot connect to the meter using ION over Ethernet, regardless of whether or not they subsequently try to login with the correct user/password combination. USER01 can access the meter through another communications method (for example, ION over serial) if they enter the correct USER/password combination.

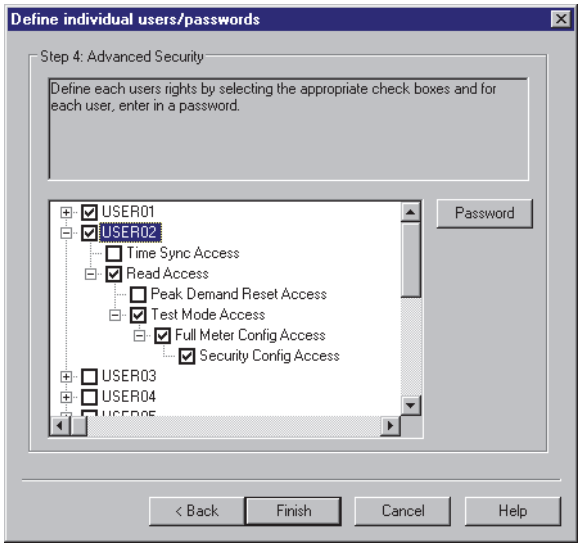
Regardless of the invalid attempts of USER01, USER02 can access the meter using ION over Ethernet if they enter the correct password; they are not affected by the lockout.

Step 3: Configure users

Advanced security allows configuration of up to 16 users, each with unique access rights to the meter.

1. Select the check boxes of the users you want to configure (USER01 through USER16). Select the appropriate access for each user:
   - **Timesync:** set time on the meter.
   - **Read:** view any parameter except the security configuration.
   - **Peak Demand Reset:** perform a reset of peak demand values (for example, sliding window demand for kW, kVAR, kVA etc.).
   - **TEST Mode:** put the meter into Test mode.
   - **Full Meter Configuration:** configure any programmable register on the meter except for registers related to the security setup, registers that result in a demand reset, or actions that place the meter in Test mode.

- **Security Configuration:** configure advanced security for the meter; full meter configuration must also be set to YES.



When configuring users, in most cases, you must set Read access to YES. However, you can set up a user without read access; for example, you can create a user who can only timesync the meter. In some cases (such as Advanced security configuration access), you must set multiple access options to YES. When you are configuring advanced security, the software rejects unacceptable user configurations.

2. Select a user, then click **Password** to set a password for that user. Refer to “Password best practices” on page 16 for more information. Type the password in the **New Password** and **Confirm new password** fields and click **OK**.

   If your meter’s front panel or user passwords are lost, you must return the meter for factory reconfiguration, which resets your meter to its factory defaults and destroys all logged data.

NOTICE
LOST DATA Record your meter’s front panel and user password information in a secure location. **Failure to follow this instruction can result in data loss.**

3. Click **Finish** when you are done configuring users to apply the security settings to the meter. A prompt appears asking if you want to save your security settings in a file.
   - Click **Yes** to save your security settings in a file.
   - Click **No** if you do not want to save your security settings in a file.

TIP

Save your meter’s security settings file under a descriptive name in a secure location, along with your meter and user password information. Your meter’s security settings file can be used to configure additional meters with the same settings, and can also assist with meter troubleshooting.

Factory access

Factory access is restricted to Schneider Electric Technical Support, and should only be enabled when requested by Schneider Electric authorized personnel.

The factory access security feature interacts with standard and advanced security to enable factory-level access to the device for the specific period of time entered in the *Factory Access Minutes* setup register, located in the Security Options module. The *Factory Access Minutes* register value can range from one minute to 19 years, and is set to 0 (zero) by default, which disables all factory access. The *Factory Access Minutes* setup register is new to firmware version v335 and later.

If the meter uses standard security, when you press any of the meter's front panel buttons, power cycle the meter, or edit the *Factory Access Minutes* setup register, factory-level access is enabled on the meter for the duration specified in the *Factory Access Minutes* setup register. If the meter has advanced security enabled, the Factory user must also be enabled. The meter will only permit factory-level access, with the correct login credentials, for the period specified in the *Factory Access Minutes* setup register.

Configuring the Factory Access Minutes setup register

You must use ION Setup in advanced mode or the Designer component of ION Enterprise to configure the *Factory Access Minutes* setup register, located in the Security Options module.

Using ION Setup:

1. Connect to your meter in advanced mode.
2. Navigate to the Security Options Modules folder and double-click on the module in the right-hand pane.
3. Select the **Setup Registers** tab.
4. Select *Factory Access Minutes* and click **Edit**. A dialog box appears.
5. Enter the desired duration (in minutes) for factory access to be enabled.

TIP

Select *Elapsed Interval Format* from the dropdown list to enter day, hour and minute values.

Factory access and standard security

If a user tries to login to factory-level access (using Telnet or Hyperterminal), on a meter with standard security, both of the following conditions must be met before the meter can proceed with subsequent checks:

1. *Factory Access Minutes* setup register is not 0 (zero).
2. The user and password information for factory-level access has been entered correctly.

If both conditions are met, the meter checks the following to determine if access will be granted:

- Front panel button: if the time since one of the meter's front panel buttons was pushed is less than the *Factory Access Minutes* register value, the user is given access.
- Power cycle: if the time since the meter was powered up is less than the *Factory Access Minutes* register value, the user is given access.
- Factory Access Minutes edit: if the time since the *Factory Access Minutes* register value was edited is less than the *Factory Access Minutes* value, the user is given access.

If any one of these conditions are met, the user is given access. If none of these conditions are met, the user is not given factory-level access on meters with standard security even if they have entered appropriate user and password information.

Factory access and advanced security

If a user tries to login to factory-level access (using Telnet or Hyperterminal) on a meter with advanced security, all three of the following conditions must be met before the meter can proceed with subsequent checks:

1. *Factory Access Minutes* setup register is not 0 (zero).
2. The user and password information for factory-level access has been entered correctly.
3. The ION Factory user has been enabled.

NOTE

The Factory user can be enabled and disabled in the ION Setup advanced security wizard, user configuration screen.

If all three of these conditions are met, the meter checks the following to determine if access will be granted:

- Front panel button: if the time since one of the meter's front panel buttons was pushed is less than the *Factory Access Minutes* register value, the user is given access.
- Power cycle: if the time since the meter was powered up is less than the *Factory Access Minutes* register value, the user is given access.
- Factory Access Minutes edit: if the time since the *Factory Access Minutes* register value was edited is less than the *Factory Access Minutes* value, the user is given access.

If any one of these conditions are met, the user is given access. If none of these conditions are met, the user is not given factory-level access on meters with advanced security even if they have entered appropriate user and password information.

Factory access examples

Scenario 1

This example illustrates how factory access functions on a meter using standard security, with a *Factory Access Minutes* setup register value of 10, over a protocol that is not session-based.

NOTE

A protocol that is not session-based actively communicates login credentials while you are connected to the meter (for example, ION and HTTP).

1. The user pushes a front panel button on the meter (T=0). This starts the factory access duration of ten minutes.
2. Two minutes after the button press (T=2), Schneider Electric Technical Support requests factory-level access to the meter, with the correct login credentials, over HTTP. Factory-level access is granted.
3. Ten minutes after the button press (T=10), factory-level access expires, and the user is automatically logged out.

Any attempt to connect to the meter using factory-level access is now denied.

NOTE

With protocols that are not session-based (for example, ION and HTTP), the access expires when the time since the factory access was activated equals the duration specified in the *Factory Access Minutes* setup register.

Scenario 2

This example illustrates how factory access functions on a meter using advanced security, with a *Factory Access Minutes* setup register value of 5, over a serial port (a session-based protocol).

1. The user connects to the meter using ION Setup with Supervisor-level access.
   - In the advanced security wizard, he enables the ION Factory user.
   - In the Communications tab, he sets the appropriate serial port protocol to Factory.
2. The user power cycles the meter (T=0). This starts the factory access duration of five minutes.
3. Two minutes after the power cycle (T=2), Schneider Electric Technical Support requests factory-level access to the meter, with the correct login credentials, over the serial port. Factory-level access is granted.
4. An hour after the power cycle (T=60), Schneider Electric Technical Support logs off factory-level access.

NOTE

With session based protocols, once factory-level access has been granted, it does not matter if the logged-in time exceeds the value of the *Factory Access Minutes* setup register.

The factory-level access period has expired, and must be restarted by pushing one of the meter's front panel buttons, power cycling the meter, or modifying the *Factory Access Minutes* setup register.

5. The user connects to the meter using ION Setup with Supervisor-level access.
   - In the advanced security wizard, he disables the ION Factory user.
   - In the Communications tab, he changes the serial port protocol from Factory back to its original setting.

Scenario 3

This example illustrates how remote factory access functions on a meter using advanced security, over a protocol that is not session-based.

NOTE

A protocol that is not session-based actively communicates login credentials while you are connected to the meter (for example, ION and HTTP).

1. The customer contacts Schneider Electric Technical Support to request that they connect to a meter using factory-level access using the following information:
   - the username and password of an advanced security user that has meter security configuration access, and the front panel password of the meter.
   - the meter's Ethernet connection information.
2. Technical Support connects to the meter using ION Setup, entering the advanced security username and password provided.
   - In the advanced security wizard, he enables the ION Factory user.
   - Using the advanced mode of ION Setup, he changes the *Factory Access Minutes* setup register from 0 (default) to 30 (T=0).
3. Two minutes after editing the *Factory Access Minutes* setup register (T=2), Schneider Electric Technical Support requests factory-level access to the meter, with the correct login credentials, over HTTP. Factory-level access is granted.
4. Twenty minutes after editing the *Factory Access Minutes* setup register (T=20), Schneider Electric Technical Support finishes working on the meter and logs off factory-level access.
5. Technical Support connects to the meter using ION Setup, entering the advanced security username and password provided.
   - In the advanced security wizard, he disables the ION Factory user.
   - Using the advanced mode of ION Setup, he changes the *Factory Access Minutes* setup register back to its default value of 0.

Schneider Electric Technical Support contacts the customer to indicate they are finished working on the meter and have restored the security settings, and recommends that the customer update their advanced user password information and store their password information and meter security configuration file in a secure location.

Security recommendations and best practices

Recommended meter configuration

1. Enable front panel security on your meter.
2. Enable advanced security on your meter.
   - Disable web server programming to help prevent configuration access to your meter over the web.
   - Disable Modbus programming to help prevent configuration access to your meter using Modbus.
   - Configure protocol lockouts to help minimize access to your meter.
   - Disable the Factory user.
   - Configure users and passwords to help minimize access to your meter.

   If your meter's front panel or user passwords are lost, you must return the meter for factory reconfiguration, which resets your meter to its factory defaults and destroys all logged data.

NOTICE
LOST DATA Record your meter's front panel and user password information in a secure location. **Failure to follow this instruction can result in data loss.**

   - Save a copy of your meter's security configuration (.scf) file in a secure location for future reference or troubleshooting. Your meter's security configuration file can be loaded onto other meters to configure their security settings.

Password best practices

1. Change your meter's front panel password from the default factory value of 0 (zero).
2. Make all meter passwords as complex as possible.
3. Record the meter's front panel and user passwords in a secure location.

   If your meter's front panel or user passwords are lost, you must return the meter for factory reconfiguration, which resets your meter to its factory defaults and destroys all logged data.

NOTICE
LOST DATA Record your meter's front panel and user password information in a secure location. **Failure to follow this instruction can result in data loss.**

4. Schedule regular changes to your meter's front panel and user passwords.

Additional recommendations

1. Protect all Ethernet meters with a properly configured firewall that prevents Telnet access over port 23.
2. Set device communication ports to the Factory protocol only when necessary to permit access to Schneider Electric Technical Support, and return the ports to their original settings as soon as possible.
3. Save a copy of your meter's security configuration (.scf) file in a secure location in addition to the password and user information.
4. Set the meter's time synchronization source to a secure communications port, and disable time synchronization on all other ports. Refer to the *ION8650 user guide* for more information.

For the highest level of security, use a hardware-locked, sealed meter with advanced security enabled and configured.

Default security settings

Meters ship from the factory with standard security enabled and a default password of zero (0). New meter security values are defined in the following table; if you are upgrading your meter to use this firmware, the existing security values are not affected.

Security setting	Value
Allow Web Server programming	Disabled (not allowed), applies to standard security only.
Allow Modbus programming	Disabled (not allowed), applies to standard security only.
Protocol lockout attempts	Eight (for all protocols)
Session timeout	30 minutes
Lockout duration	1440 minutes (24 hours)
Valid login event priority	0
Invalid login event priority	128
Lockout event priority	255
Protocols selected for security	All protocols (ION, HTTP, FTP, Telnet, Factory, Front panel)
ION Factory user	Disabled
Factory Access Minutes	0

Unless otherwise noted, these security settings apply regardless of whether the meter has standard or advanced security enabled; for example, if you change the lockout duration to 720 minutes (12 hours), that is the lockout duration for the meter in standard security or in advanced security.