Configuring security in ION devices using ION Setup

This document instructs you on how to configure PowerLogic™ ION devices to help minimize security vulnerabilities, using ION Setup configuration software.

This instruction bulletin applies to ION Setup versions up to and including ION Setup version 2.2.

This instruction bulletin applies to the following devices:

- ION8300, ION8400, ION8500, ION8600, ION8650
- ION7500, ION7600, ION7500 RTU
- ION7550, ION7650, ION7550 RTU
- ION8800

In this document

Additional information

Additional information is available for download at www.schneider-electric.com.

- ION Setup online help
- ION device documentation
- ION device template reference

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

Schneider Electric

Hazard categories and special symbols

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 manual 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.

CAUTION

CAUTION used without the safety alert symbol indicates a potentially hazardous situation which, if not avoided, can result in equipment damage.

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.

Overview

This document describes best practices and recommendations for ION device security. It also instructs you on how to appropriately configure your default advanced security configuration file (Advanced.scf), default standard security configuration file (Standard.scf) and any other security configuration files used to store and transfer these settings to ION devices using ION Setup configuration software.

NOTE

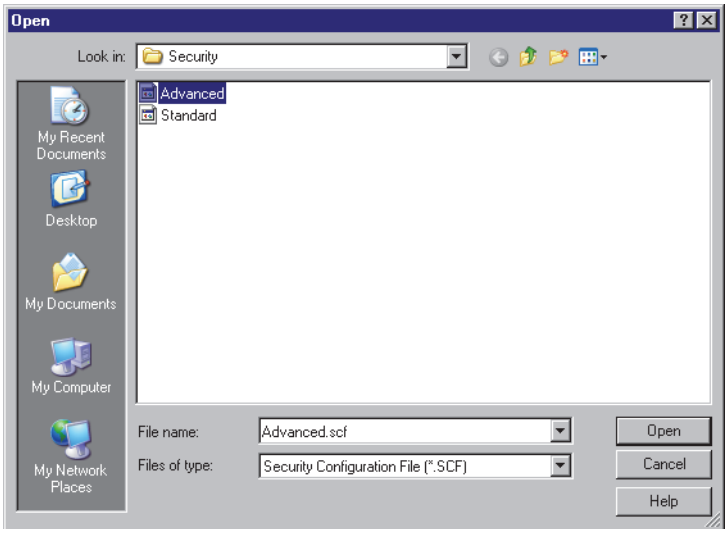
ION Setup is available as a free download from www.schneider-electric.com.

Configuring your device's advanced security settings using ION Setup

Perform these steps even if you are only using standard security on your device as it will help ensure that the appropriate default settings are used if advanced security is applied at a later date.

These are recommended settings, and should be reviewed and implemented based on the specifics of your device's installation.

1. Open the Setup Assistant for your device. See the ION Setup help for instructions
2. Select **Security**.
3. Select **Security Mode** and click **Edit** (or double-click to edit). You may be prompted for a device password. The **Open File** dialog box appears.



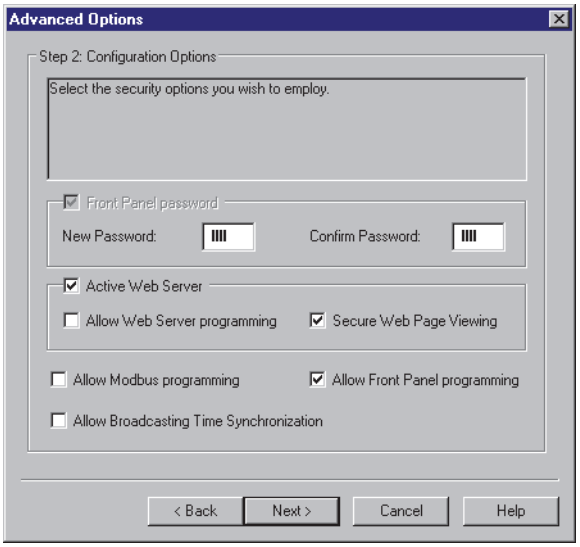
NOTE

.By default, security configuration files are stored in ...\Schneider Electric\ION Setup\Security

4. Select the Advanced.scf file and click **Open**.

   The Advanced Security wizard leads you through the configuration procedure.
5. Modify the settings on the **Configuration Options** screen as follows:
   - New Password: Ensure that your device is not using the default front panel password of "0" (zero). Refer to "Password recommendations" on page 9 for more information.
   - Web Server: Uncheck **Allow Web Server programming** unless you are actively using this feature on your device.
   - Allow Modbus programming: Uncheck **Allow Modbus programming** unless you are actively using this feature on your device.

Click **Next** to continue.

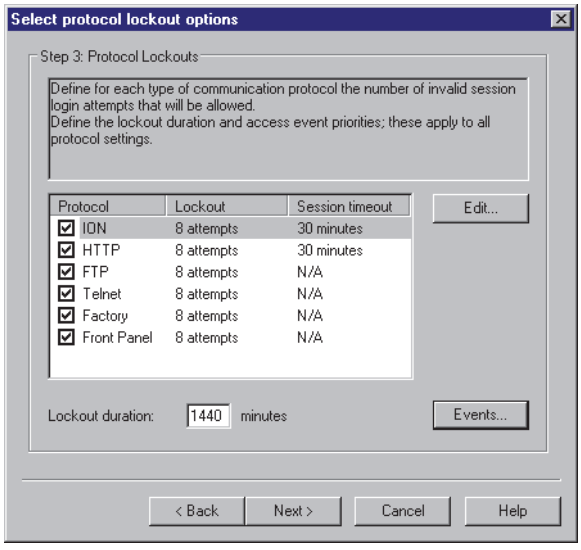


On devices with the protocol lockout and device access logging features, the Protocol Lockout screen appears.

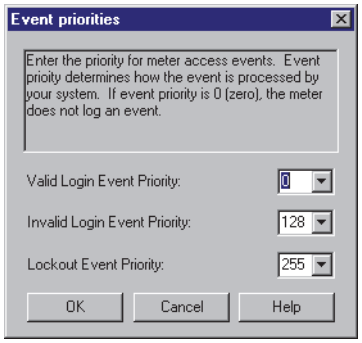
NOTE

For more information about these features, refer to the *ION8650 user guide*, available from www.schneider-electric.com

6. Configure the Protocol Lockout screen as follows:
   - Select the checkboxes beside all the protocols to enable the protocol lockout feature.
   - Configure the protocol lockout attempts (recommended eight invalid attempts) and default lockout duration (recommended 24 hours) to reflect your system's security settings. Refer to the *ION8650 user guide* for more information.



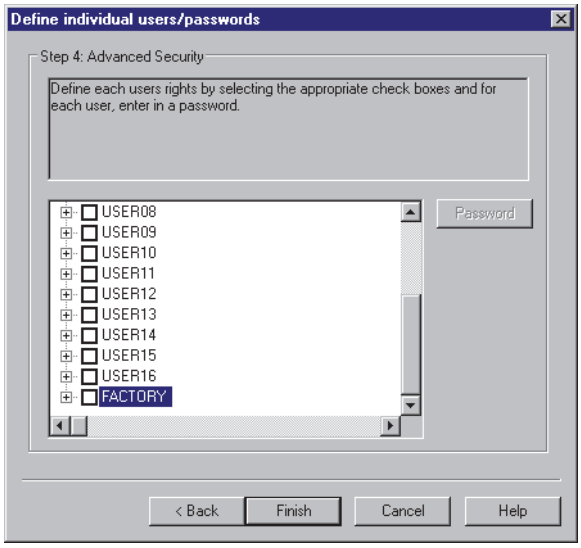
- Click **Events** to configure device access event priorities for valid login attempts (recommended priority 0), invalid login attempts (recommended priority 128) and lockout events (recommended priority 255). These values will help enable event logging of invalid access attempts and lockouts.



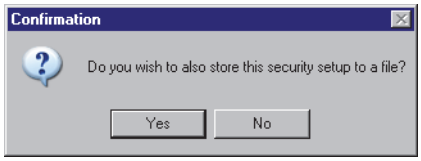
- Click **Next** to proceed.

The User configuration screen appears.

7. In the User configuration screen, scroll down to the bottom of the user list, and clear the box beside the Factory user in order to disable the default Factory user. Edit the access levels of existing users, add new users and assign user passwords as desired. Click **Finish**.



8. An advanced security confirmation screen may appear, where you must enter a valid user ID and password before continuing.
9. A file save dialog box appears. Click **Yes** to store your advanced security configuration to a file.



The **Save As** screen appears

10. In the **Save As** screen, select Advanced.scf and click **Save** to overwrite the default advanced security configuration file.

NOTE

The default security configuration files are set to read-only by default. To overwrite, right-click on the file in the **Save As** screen and select **Properties**. In the General tab, remove the checkmark beside the Read-only attribute and click **OK**. You should now be able to overwrite the default security configuration file.

You have now saved your default advanced security configuration file. Repeat these steps to configure any custom advanced security files in your system.

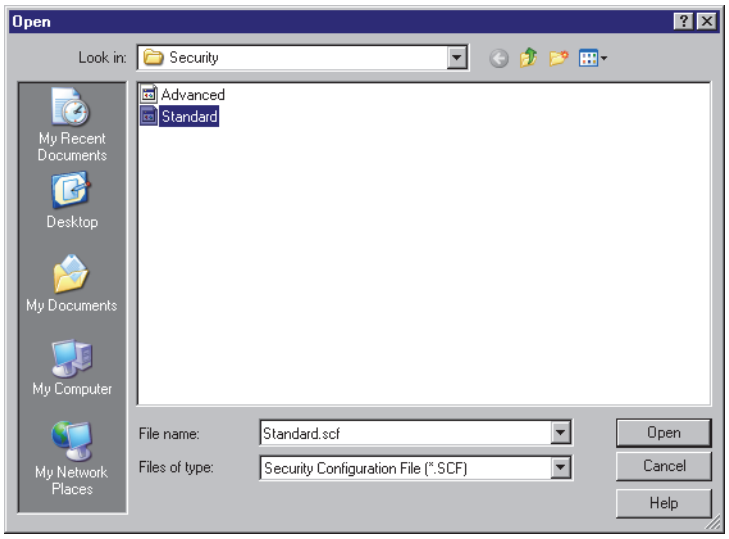
Additional device security recommendations

Configuring standard security on your device using ION Setup

If you have already enabled advanced security on your device, do not use standard security.

These are recommended settings, and should be reviewed and implemented based on the specifics of your device's installation.

1. Open the Setup Assistant for your device. See the ION Setup help for instructions
2. Select **Security**.
3. Select **Security Mode** and click **Edit** (or double-click to edit). You may be prompted for a password. The **Open File** dialog box appears.

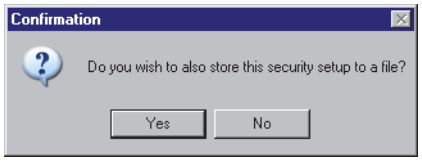


4. Select Standard and click **Open**.
5. Modify the settings on the **Configuration Options** screen as follows:
   - New Password: Ensure that your device is not using the default front panel password of "0" (zero). Refer to "Password recommendations" on page 9 for more information.
   - Web Server: Uncheck **Allow Web Server programming** unless you are actively using this feature on your device.

   Click **Finish**.

   A file save dialog box appears.

6. In the file save dialog box, click **Yes** to store your standard security configuration to a file.



   The **Save As** screen appears.

7. In the **Save As** screen, select Standard.scf and click **Save** to overwrite the default standard security configuration file, or enter a new file name and click **Save**.

NOTE

The default security configuration files are set to read-only by default. To overwrite, right-click on the file in the **Save As** screen and select **Properties**. In the General tab, remove the checkmark beside the Read-only attribute and click **OK**. You should now be able to overwrite the default security configuration file.

Password recommendations

Perform the following actions to help ensure device password-protected security:

- Enable front panel security on your device.
- Ensure the front panel password is not at the default factory value of “0” (zero).
- Make the all device’s passwords, especially the front panel password, as complex as possible, using the full number of characters available.
- Schedule regular changes to the device’s passwords, especially the front panel password.
- Ensure that your device’s password information is maintained in a secure location. Password information is required in order to configure your device.

Telnet access

All devices that can be accessed using Ethernet must be protected by a properly configured firewall that prevents Telnet access over port 23.

Modbus access

Use standard security for read-only Modbus access. Use advanced security if you need to read and write Modbus registers.

Device protocols

Device communication ports must be set to the Factory protocol only when necessary to permit access to Schneider Electric Technical Support and returned to their original settings as soon as possible.