California State Legislation Security Updates for Network-Enabled Devices

INTRODUCTION

With the introduction of new California State legislation (SB-327), which comes into effect from January 1st, 2020, any manufacturer of a device that connects "directly or indirectly" to the internet must equip it with "reasonable" security features, designed to prevent unauthorized access, modification, or information disclosure.

APC™ by Schneider Electric (APC) network-enabled devices are being updated in compliance with this legislation. This document provides information on specific changes and the impact on our customers.

You can upgrade the firmware of network-enabled devices via a USB flash drive, the Firmware Upgrade Utility, or via SCP/FTP. For specific instructions for your device, refer to your product documentation on the APC website.

Overview of Changes

- At first logon, a device with default credentials (`apc / apc`) will require you to change the password.
- The user accounts shipped on the device are disabled by default, and cannot be enabled until the password for each user account is changed. **NOTE:** The Super User account is not disabled by default.
- When creating a new user account, a password is required during account creation in the Command Line Interface (CLI), and a password is required to enable the account in the Web UI.
- To access the Web UI in a web browser, you must add "https://" to the beginning of the URL in the address bar. For example, "https://10.201.188.10"
- Communication protocol changes. See Communication Protocol Changes.
- New Protocol Status Overview screen in the Web UI, and banner in the CLI. See Protocol Status Overview.
- PowerChute Network Shutdown changes. See PowerChute Network Shutdown Changes.

CHANGES

Communication Protocol Changes

All communication protocols are now disabled by default except Secure Shell (SSH), Hypertext Transfer Protocol Secure (HTTPS), and console access to the CLI (serial/USB).

NOTES:

- BACnet is disabled by default and cannot be enabled until the **Device Communication Control** Password is set.
- SNMPv1 is disabled by default, and the **Community Name** must be set before SNMPv1 communications can be established. The previous default Community Names have been removed (`public`, `private`, `public2`, and `private2`).
- SNMPv3 is disabled by default, and a valid user profile must be configured with passphrases (**Authentication Passphrase**, **Privacy Passphrase**) set before SNMPv3 communications can be established. The previous default passphrases have been removed (`apc auth passphrase` / `apc crypt passphrase`).
- Secure Copy Protocol (SCP) will not allow a file transfer until the default password (`apc`) is changed.

Schneider Electric

Protocol Status Overview

The new **Protocol Status Overview** screen in the Web UI displays all system protocols and their value, enabled or disabled. The screen also includes a hyperlink for each protocol to configure its settings. At first log in to the Web UI, you are directed to this new screen, which can be accessed at any time thereafter by following the menu navigation path: **Configuration > Network > Summary**.

The existing banner in the CLI is modified to include all system protocols and their value. This is visible at every log in to the CLI.

PowerChute Network Shutdown Changes

By default, PowerChute Network Shutdown uses HTTP to connect to your network-enabled device. As HTTP is now disabled by default, PowerChute cannot connect to your device unless you enable HTTP or change the communication protocol. The **PowerChute Network Shutdown Configuration** screen in the Web UI has a drop-down box which allows you to choose the protocol used to communicate with PowerChute: HTTP, HTTPS, or none. **NOTE:** The chosen protocol must be enabled on your device before PowerChute communications can be established.

The PowerChute user name is no longer mapped to your device, and the default authentication phrase has been removed (`admin user phrase`). You must specify a user name and authentication phrase before PowerChute can be enabled.

IMPACT OF CHANGES

These changes will not affect existing customers upgrading their firmware to version x*. However, these changes will be the default settings for new customers, and existing customer running version x* who reset their device to its default values.

***** NMC 2: v6.8.2, NMC 3: v1.1.0.16, NMC 4: v4.28. **NOTE:** NMC 3 is scheduled for release in October 2019.

Firmware Upgrade Utility

File Transfer Protocol (FTP) is required to successfully upgrade your device's firmware via the Firmware Upgrade Utility. FTP is now disabled by default.

- Enable FTP on your device before attempting to upgrade its firmware via the Firmware Upgrade Utility.
- If FTP is disabled on your device, the firmware upgrade will not successfully complete and you must manually transfer any missing files to your device via SCP, XMODEM, or USB flash drive. Refer to your device documentation for more information.

NOTE: The Firmware Upgrade Utility is bundled with the firmware download for supported network-enabled devices.

Device IP Configuration Wizard

The Device IP Configuration Wizard relies on SNMPv1 to locate already configured devices. As SNMPv1 is now disabled by default, the wizard cannot discover assigned devices unless SNMPv1 is enabled on your device and the **Community Name** is set to "`public`".

NOTE: When your device's IP address settings are configured, to access the device in a Web browser via the wizard, update the URL from "`http`" to "`https`".

EcoStruxure™ IT and StruxureWare Data Center Expert

EcoStruxure IT and StruxureWare Data Center Expert rely on SNMPv1, SNMPv3 or Modbus to communicate with network-enabled devices. As these protocols are now disabled by default, ensure that the chosen protocol is enabled on your device before attempting device discovery in the EcoStruxure IT Gateway/StruxureWare. It is recommended you use the most secure option, SNMPv3.

FURTHER INCREASE SECURITY

To further increase device security, Schneider Electric recommends you enable the strong passwords and force password change features on your network-enabled device. These features are available via the web user interface by following the **Configuration > Security > Local Users > Default Settings** navigation path.

- **Strong Passwords:** This feature ensures that all device passwords must be a minimum length of 8 characters, comprised of upper-case and lower-case letters, a number, and a special character, to make passwords harder to guess.
- **Force Password Change:** This feature forces all device passwords to be changed after a user-specified number of days.

https://www.apc.com

990-6221A-001
10-2019