Release Notes Com'X 210/Com'X 510 - v6.0.7 firmware

Firmware upgrade compatibility

If your Com'X 210/510 device is currently running a firmware version earlier than v2.1, you will first need to upgrade to v2.1 before upgrading to later versions.

If your Com'X 210/510 device is currently connected to Digital Services Platform (DSP) in support of a cloud application such as EcoStruxure™ Facility Expert, it must be upgraded to firmware version v5.6.9 or greater by August 1, 2019 to avoid interruption of service. After August 1, 2019 firmware versions v5.6.9 or later are required to connect to cloud applications via DSP.

Publication platforms

Com'X v6.0.7 supports the following publication platforms:

- Energy Operation
- Digital Services Platform (DSP)
- Comma Separated Values (CSV)

Release scope

- Security updates to the previous Com'X v6.0.4 release.

Enhancements

- Implemented the Account Lockout feature.

Com'X 510

- Limited the file types accepted when creating a custom web page. The accepted file types include HTML, SHTML, HTM, JS, JPG, JPEG, PNG, GIF, and CSS.

- Limited the file types accepted when uploading files through the Documentation Links feature. Only PDF files can be uploaded through the Documentation Links feature.

Fixed defects

- Issue with custom contactor model which prevented support for custom events based on the contactor state is now resolved.

Known Issues

The Account Lockout feature is currently not documented in the Com'X User's Manuals and is displayed only in English only the HMI. Please refer to the next section for information regarding the Account Lockout feature.

Account Lockout Policy

Account lockout feature disables a user account when the number of failed login attempts exceeds the set limit within a predetermined time interval. This feature is enabled by default.

You can configure the following:

- Enable account lockout – Account lockout policy is enabled by default. Select **No** to disable this feature.

  NOTE: It is recommended to keep the Account Lockout enabled to better secure the device from unauthorized access.

- Reset account lockout counter (number of attempts) - determines the number invalid login attempts allowed before user account gets disabled. The default is set to 10 attempts.

- Account lockout duration (minutes) - determines amount of time user account remains disabled. The default is set to 15 minutes.

To configure the Account Lockout policy:

1. Navigate to **Settings > Firewall Management**.
2. Click **Account Lockout Policy**.
3. Enter **Reset account lockout counter**.
4. Enter **Account lockout duration**.
5. Click **Save changes**.

To disable the Account Lockout policy:

1. Click **Settings > Firewall Management**.
2. Click **Account Lockout Policy**.
3. Click **No** to disable the account lockout policy.
4. Click **Save changes**.