RELEASE NOTES

3-Series Firmware

1.8001.0187 – June 27, 2022

Product or Content Description

Package Update File for the CP3N

Cntrl Eng v1.8001.4925.26115
Cab: 1.8001.0187
Applications: 1.0.8212.18743
Updater: 1.0.33
Bootloader: 1.30.00
IOPVersion: v1.3177.00007
BACnetVersion: 15.1.30
CP3-SetupProgram: 1.003.0024
RouterBootVersion: 4
RouterVersion: 1.004.0017 / 2.001.0006

System Requirements and Dependencies

Software Requirements:

!! Device Database 91.00 or greater

Operational Installation/Upgrade Instructions

When upgrading from 1.007.0019 or later, the recommended upgrade steps are:

- Use FTP client such as FileZilla to upload the file to \FIRMWARE, or using Toolbox FileManager, upload the file to \ROMDISK\USER\SYSTEM
- Using Text Console, use the command: PUF <Filename>

Note regarding credentials when upgrading to PUF 1.601.0050
Upgrading from PUF up to and including 1.504.0040 to PUF 1.601.0050

- No action required, no SSH or Webserver credentials exist.

Upgrading from PUF 1.600.0092 or 1.601.0016 to PUF 1.601.0050

- If Authentication not enabled
  - No action required, no SSH or Webserver credentials exist.
- If Authentication is enabled
  - If Webserver ON (prior to upgrade)
    - No issues, SSH and Webserver credentials both work as expected.
  - If Webserver OFF (prior to upgrade)
    - Webserver accounts will be deleted.
    - New account for Web Server will Need to be created.

There are two methods for creating a webserver account when Authentication is enabled, and Webserver is disabled. Choose whichever one is more convenient.

1. Disable Authentication, then enable Authentication. User will be prompted to create a new user and it will apply to SSH and Webserver.
2. Change the password on the SSH. This will result in user being created for the Webserver. SSH and Webserver will have same credentials.

Important Information

From firmware 1.8001.0176 and up, the following has changed:

- By adding the SETUSERLOCKOUTTIME and SETUSERLOGINATTEMPTS console commands, the default behavior of the existing SETLOCKOUTTIME and SETLOGINATTEMPTS commands has changed:
  - SETLOGINATTEMPTS
    - Default was 3 attempts and has now been changed to 5 attempts.
    - This command now only controls blocking of source IP address.
  - SETLOCKOUTTIME
    - The default was 24 hours and has now been changed to 30 minutes.
    - The command now supports setting the lockout in minutes as well as hours.
    - This command now only controls blocking of source IP address.
  - SETUSERLOGINATTEMPTS
    - Default value is 5 attempts.
    - This command only blocks username.
  - SETUSERLOCKOUTTIME
    - Default value is 30 minutes.
    - The command supports setting the lockout in minutes as well as hours.
    - This command only blocks username.

Version History

Version 1.8001.0187 June 27, 2022

Changes since Last Version

Resolved Bugs:

- Sending a specially formatted BACnet packet could result in a crash of the control system.
- Webserver did not redirect to HTTPS when request contains specific host header values.
- IP connections could drop periodically on router-based systems.

Known Issues:

- Server certificates with RSA key size of 4096 cannot be loaded to the control system.

Version 1.8001.0176 May 11, 2022

Changes since Last Version

New:

- Added SETUSERLOCKOUTTIME and SETUSERLOGINATTEMPTS console commands. Please read the Important Information section on the previous page.

Resolved Bugs:

- MYCRESTRON console command no longer times out.
- Remote Ethernet Processing without SETCSAUTHENTICATION configured on the remote device would not reconnect if the parent device rebooted or program reloaded.

Updates:

- Upgraded IoT SDK to 1.8.0

Version 1.8001.0146 March 8, 2022

Changes since Last Version

Resolved Bugs:

- User Page Authentication no longer gets turned off after a firmware upgrade.
- IP address could get blocked when creating initial user with an invalid username.
- Resolved issue when loading improperly formatted CA signed certificates.

Version 1.8001.0133 February 10, 2022

Changes since Last Version

New features:

- BACNet port now selectable between port 1024 – 65535 through SIMPL Windows program

Resolved Bugs:

- Unable to authenticate using 802.1x EAP-TLS on non-router based control systems
- Self-signed and CA certs could get removed on firmware upgrade.
- S# SecureTcpClient Fails SSL handshake when using client-side certs.
- HYDROGENPROXY console command password was logged in audit log.
- MYCRESTRON console command password was logged in audit log.
- USERPAGEAUTH command doesn't work when Forced Auth Mode is false.
- Resolved an issue where certain processes could take up more memory.
- Remote Ethernet Processing between 4-Series and 3-Series would intermittently fail when SETCSAUTHENTICATION was set.
- NVRAM writes using S+ nonvolatile string array not persisting past program restarts.
- Security fixed for Secure WebSocket port 49200
- SFTP session remained active after log-off idle time.
- Removed erroneous *HandleIncomingDataPacketsOverUDP* error message for App 0
- Removed erroneous *Schema not resolved* error message.
- CIP crash during longevity run using Crestron One.
- Audit log doesn't show *restore* event happening.
- DNS traffic from LAN side available on router side when isolation mode is enabled.

Known Issues:

- 802.1x only supports TLS1.2

Version 1.8001.0075 October 11, 2021

Changes since Last Version

New features:

- Added support for Fusion HTML5 XPanel.

Resolved Bugs:

- Disable and stop using DES, 3DES, IDEA or RC2 ciphers.
- Unable to serve .svg files from CH5 interface when project was loaded to control system.
- MPC3 unable to come online in XiO Cloud with ancillary devices loaded
- Stop erroneous *pTempSignalTableEntry* error from showing in log when using BACnet.
- Unable to copy current files to backup folder when loading between RM and Internal.

Updates:

- Upgraded Azure IoT TLS Root CA

Known Issues:

- Unable to authenticate using 802.1x EAP-TLS on non-router based control systems.

Version 1.8000.0014 May 20, 2021

Changes since Last Version

New features:

- Added support for XIO Cloud proxy with **HYDROGENPROXYURL** command.

Resolved Bugs:

- Resolved issue where uploading a file as “multipart/formdata” to CWS server would result in an error
- Resolved issue where ancillary devices are not showing up in XiO Cloud after network outage on control processor.

Updates:

- Removed erroneous messaging in error log from Hydrogen Manager.

Version 1.7001.0008 March 16, 2021

Changes since Last Version

New features:

- Added support to report Crestron Driver status to XiO Cloud.

Resolved Bugs:

- Resolved issue where CrestronAuthentication.Authentication.GetGroups wouldn’t return all groups.
- Resolved issue where user could be created without a password.
- Resolved issues with Auto Update cancellations.
- Resolved issue where CWS would return HTTP Code 403 when HTTP OPTIONS was used.
- Resolved issue with SecureTcpClient not accepting all ciphers.
- Resolved issues setting longitude/latitude.

Version 1.7000.0021 December 18, 2020

Changes since Last Version

New features

- Added support for HTML XPanel.

Resolved Bugs:

- Improved reconnection logic for XiO Cloud.
- Resolved issue where the Put method of HttpsClient.DispatchAsync() didn’t return the correct response code.
- Resolved issue generating RVI files.
- Resolved console issue with regard to debugging SIMPL Windows programs.

Version 1.603.0113 October 8, 2020

Changes since Last Version

New features:

- Added ability to enable IP and User blocking when user attempts to log in with invalid credentials multiple times.
- Added command CRESTRONONETPR which reports time remaining on Crestron ONE trial period.

Resolved Bugs:

- Resolved issue with Websocket class implementation, where internal buffer could overflow. This caused interoperability issues with Sonos firmware upgrade.
- Resolved issue where serial joins on SNMP symbol would show part of previous values.
- Resolved issue where control system can end up in a reboot cycle when starting a large program.
- Resolved issue where password rules were not enforced correctly.
- Resolved compatibility issue with Josh.ai modules.

Version 1.603.0076 August 13, 2020

Changes since Last Version

New features:

- System will require authentication upon a restore.
- Added support for Mobile Room Control via Crestron ONE™ app. Crestron ONE app allows you to connect and control a Crestron programmed smart room from a personal mobile device.
    - Supported System Requirements
        - 60-Series Firmware (minimum version tsw-xx60_3.000.0014.001)
            - Models: versions that include Bluetooth, excludes the models with "-NC" in the product name as these do not include Bluetooth
        - 3-Series Control Processors (minimum version 1.603.0076)
            - Models: AV3, CP3, CP3N, DIN-AP3, FT600, MPC3 Family, PRO3, RMC3, TSCW
        - After the free 60-day trial period expires on control processor, a Mobility License is required and applied to the control processor to enable Mobile Room Control functionality.
            - **Trial period is included within firmware, no trial license is required.** To activate the 60-day trial period, follow the instructions within the "Programming Guide: Crestron ONE™ App" under the Resources section of the Crestron ONE Product Page

Updates:

- Added Autoupdate puf support for DIN-CENCN-2, DIN-CENCN-2-POE and CAEN-BLOCK-CENCN-2-POE
- Added support for a password protected private key.
- Added ability to define subject alternative name(s) in certificate requests.
- Improved security for Autodiscovery.
- Improved EISC communications for large updates.

Resolved Bugs:

- Fix issue with inability to upload file via CWS
- Update behavior of "ssl ca" command when processing "rootCA_cert.cer" file to allow for multiple certificates, including intermediates in the file
- Fix issue with MPC3-102 where a button pressed remains latched high if button held and then disabled.
- Fix issue where BACnetRemoteCOVList may not display device online status, IP and subscription information correctly.

Version 1.601.0050 October 11, 2019

Changes since Last Version

Updates:

- Minor updates made to BACNet stack to ensure BTL compliance.

Version 1.601.0048 October 10, 2019

Changes since Last Version

Resolved Bugs:

- Fix issue where S# using SQLite class resulted in error in initializing system.
- Fix issue where project not getting removed from device when project name contains .(dot)
- Fix issue where ARPing on Default Gateway could result in gateway IP in ARP being truncated (router-based systems only).
- Fix issue where upgrading from PUF prior to 1.600.xxx to PUF 1.600.0092 or 1.601.0016 with Authentication enabled results in credentials not working.
- Fix issue where SIMPL Console Symbol interferes with SIMPL debugger.

Version 1.601.0016 July 25, 2019

Changes since Last Version

New features:

- Added support for Apple HomeKit.

Updates:

- SSP Secure sockets security enhancements.

Resolved Bugs:

- Fix issue with SSP Authentication class method AddGroupToSystem not properly setting access level.
- Fix issue with attempting to import private key failing.

Known Issues:

- SSLVERIFY is OFF in CA mode, it should be enabled.

Version 1.600.0092 May 10, 2019

Changes since Last Version

New features:

- Upgraded cryptography libraries, used for TLS and SSH

Updates:

- General security enhancements
- General and stability enhancements for XiO Cloud
- General and stability enhancement for SNMP
- Enhancement for Certificate utilities
- Enhancements for AuditLog
- Enhancements for AutoUpdate
- Stability enhancements for RemoteSyslog
- Stability enhancements for Secure Sockets
- Stability enhancements for FITC connections
- Stability enhancements for Crestron Web Sockets
- Stability enhancements for BACNet
- Stability enhancements for 802.1x
- Remove unnecessary messages from logs

Resolved Bugs:

- Fix issue where closing instance of UDP socket in S+ code results in other instance not able to receive data.
- Fix for MPC3-10x wakeup issue.

Known Issues:

- SSLVERIFY is OFF in CA mode, it should be enabled.

Version 1.504.0040.0004 February 14, 2019

Changes since Last Version

New features:

- Added support for loading programs via XiO Cloud.

Updates:

- XiO Cloud enhancements.
- Update webserver to use TLS1.2.
- Improve Secure Socket robustness.

Resolved Bugs:

- Fix issues with LEDs in MPC3.

Version 1.503.0070.0001 November 16, 2018

Changes since Last Version

New features:

- CTP and Telnet are disabled by default.
- Add a default SSH Banner which prints a warning recommending securing the device.

Updates:

- Updated support for XiO Cloud.
- Updated support for Dynamic BACNet.
- Updated support for BACNet stack.
- Updated support for Auto Update.
- Updated support for SNMP walks.
- Stability update for Secure Client connections.
- Stability update for Web Sockets.
- Stability update for TimerEngine.

Version 1.503.0026 June 1, 2018

Changes since Last Version

New features:

- Updated IR support file with latest set of standard commands for Crestron Studio.
- Support for new EISC's for communicating with Virtual Control.

Resolved Bugs:

- Resolved issue with data not being sent to extenders of GWEXER on update request.
- Resolved issue with XiO Cloud connectivity.

Version 1.503.0016 February 28, 2018

Changes since Last Version

New features:

- Add support for XiO Cloud.

Resolved Bugs:

- Resolved router port forwarding issues at system boot.
- Resolved BACNet COV issue.

Version 1.502.0039 August 15, 2017

Changes since Last Version

Resolved Bugs:

- Resolve issues with exceptions when a 3 series is slaved to another 3 series controller.
- Updated the range of valid ports allowed for BACnet.

Known issues:

- When a system is configured with one of the time zones listed below, performing this firmware upgrade will set the time zone back to the default time zone of Pacific Standard Time

```
Time Zone: 120  UTC-11
Time Zone: 121  Venezuela Standard Time
Time Zone: 122  Russia TZ 9 Standard Time
Time Zone: 123  W. Australia Standard Time
Time Zone: 124  W. Central Africa Standard Time
Time Zone: 125  W. Europe Standard Time
Time Zone: 126  W. Mongolia Standard Time
Time Zone: 127  West Asia Standard Time
Time Zone: 128  West Bank Gaza Standard Time
Time Zone: 129  West Pacific Standard Time
Time Zone: 130  Russia TZ 8 Standard Time
```

  The time zone should be set back to its correct configuration after upgrading the firmware.
- When Telnet and standard Web services are disabled, and a firmware upgrade is performed the services will be re-enabled. After upgrading it will be necessary to disable them.

Version 1.502.0029 June 7, 2017

Changes since Last Version

Updates:

- Resolve issues with the rf subsystem being out of sync causing a loss in functionality unless the unit was rebooted.
- Resolve issues with the AutoUpdate engine.
- Resolve issues with the BACNet Stack for Invoke Id optimizations.
- Resolve issues with the printing of the username in the **WHOAMI** command.

Version 1.502.0026 May 17, 2017

Changes since Last Version

Updates:

- Initial release for the ZUM-FLOOR-HUB.

Version 1.502.0020 April 6, 2017

Changes since Last Version

Updates:

- Add support for the IGMPProxy command.
- Resolve issues with Websockets connectivity.

Version 1.501.0106 January 31, 2017

Changes since Last Version

Updates:

- Reduced extraneous messages in log.

Version 1.501.0008 December 15, 2016

Changes since Last Version

Updates:

- Initial release for the DMPS3-4K-200-C / DMPS3-4K-300-C.

Version 1.501.0105 November 7, 2016

Changes since Last Version

Updates:

- Reduced extraneous messages in log for Websocket connections.

Version 1.501.0104 October 26, 2016

Changes since Last Version

Updates:

- Improve network resilience for Websocket connections.
- Resolve issue with BACnet where network outage could cause devices to go offline.

Version 1.501.0041 October 14, 2016

Changes since Last Version

Updates:

- Resolved AV Framework and Fusion interoperability issues.

Version 1.501.0103 October 4, 2016

Changes since Last Version

Updates:

- SIMPL Debugger fix
- Resolved issue where gratuitous ARPs would cause devices to lose IP address assignments.
- Added support for SHA256 Certificates.
- Added support for Crestron Web Scripting, allowing SIMPL# to tie into the built-in webserver.
- Optional parameters added to the CreateCSR command.
- Auto Update changes needed for the new tool.
- Resolved issues with TSW Panels not connecting over SSL.
- Resolved issues with 802.1X where we incorrectly advertised support for PEAPv1.
- BACnet fixes:
    - Foreign Device registration is now saved across reboots.
    - Added new console command to disable a Read following a write.
    - Memory leak fixes when NumberOfStates join was not being used for the Multi state.
    - Initiate Foreign device registration before sending out a WHO-IS or I-AM.
    - Resolve memory corruption issues.
    - Handle broadcast unconfirmed COV notifications.

Licensing and Copyright Information