NX General Security Best Practices

Security Document

General

Honeywell hereby expressly states that its controllers are not inherently protected against cyber attacks from the Internet and that they are therefore intended solely for use in private networks. However, even private networks can still be subject to malicious cyber attacks by skilled and equipped IT individuals and thus require protection. Customers should therefore adopt the installation and security best practices guidelines for CentraLine / Honeywell IP-based products to mitigate the risk posed by such attacks.

The following guidelines describe the General Security Best Practices for CentraLine / Honeywell IP-based products. They are listed in order of increasing mitigation.

The exact requirements of each site should be assessed on a case-by-case basis. The vast majority of installations implementing all of the mitigation levels described here will be far in excess of that required for satisfactory system security. Incorporating the items 1-5 (relating to Local Area Networks) will generally meet the requirements for most automation control network installations.

Local Area Networks (LAN) Incorporating CentraLine Components

Ensure the systems operate on an appropriate password policy for user access to all services. This guideline would include, but is not limited to:

1. **The use of strong passwords.**
2. **A recommended password cycle time.**
3. **Unique user names and passwords for each user of the system.**
4. **Password disclosure rules.**
5. **If remote access to IT-based building control systems is required, use VPN (Virtual Private Network) technology to reduce the risk of data interception and protect the controls devices from being directly placed on the internet.**

Further Considerations

- Prevent unauthorized access to the network equipment that is used in conjunction with systems provided by CentraLine. With any system, preventing physical access to the network and equipment reduces the risk of unauthorized interference. Security best practices with IT installations would ensure that the server rooms, patch panels, and IT equipment are in locked rooms. CentraLine equipment should be installed within locked control cabinets, themselves located in secured plant rooms.
- When completing commissioning, ensure the device is password protected. Ensure appropriate user levels are assigned for the site users.
- Adopt an appropriate update policy for the infrastructure installed at the site as part of a service level agreement. This policy should include, but is not limited to, updating the following system components to the latest release:
  - Devices firmware for controller, I/O modules, HMI, etc.;
  - Supervisor software, such as Arena NX software;
  - PC / Server operating systems;
  - Network infrastructure and any remote access systems.
- Configure separate IT networks for the automation control systems and the customer's corporate IT Network. This may be achieved by configuring VLANs (Virtual LANs) within the customer's IT infrastructure or by installing an air-gapped separate network infrastructure dedicated to the automation control systems.
- Once the system has been commissioned, restrict IP traffic on the automation control network (for example using access lists) to the types of protocols required for normal operation, i.e., C-Bus, BACnet, etc. Further information regarding the communications traffic required for normal operation can be found in the product documentation.
- When interfacing with CentraLine controllers using a centralized system supervisor (e.g., ARENA NX) and where the system does not require direct access to the individual devices web server, the network infrastructure should be configured to restrict web server access.
- Dynamic VLANs using MAC address allocation can protect against the unauthorized connection of a device into the system and can reduce the risk associated with an individual monitoring information on the network.

For more information, see also section "Network Security" of the Product Data of the given controller.

NOTE: It is highly recommended that you include all your CentraLine migration files from earlier versions of NX software to a secure location as defined in *Users home directory*.

Setting up Google 2 Factor Authentication

The Google Authentication Scheme is a two-factor authentication mechanism that requires the user to enter his password as well as a single-use token when logging in to a station. This protects a user's account even if his password is compromised.

This authentication scheme relies on TOTP (Time-based One Time Password) and the Google Authenticator app on the user's mobile device to generate and verify single-use authentication tokens. Google authentication is time-based, so there is no dependency on network communication between the user's mobile device, the Station, or external Servers. Since the authenticator is time-based, the time in the station and time in the phone must stay relatively in sync. The app provides a buffer of plus or minus 1.5 minutes to account for clock skew.

Prerequisites: The user's mobile phone requires the Google Authentication app. You are working in Workbench. The user exists in the station database.

PERFORM THE FOLLOWING STEPS:

1. Open the gauth palette and add **GoogleAuthenticationScheme** to the **Services > Authenticationservice** node in the Nav tree.
2. Right-click **Userservice**, and double-click the user in the table. The Edit view for the user opens.
3. Configure the *Authentication Scheme Name* property to **GoogleAuthenticationScheme** and click **Save**.
4. Click the button next to *secret Key* under the user's authenticator and follow the prompts.
5. To complete the configuration, click **Save**. Depending upon the view you are using, you may have to open the user again or refresh after saving.

Manufactured for and on behalf of the Environmental & Energy Solutions Division of Honeywell Technologies Sàrl, Rolle, Z.A. La Pièce 16, Switzerland by its Authorized Representative:

CentraLine
Honeywell GmbH
Böblinger Strasse 17
71101 Schönaich, Germany
Phone +49 (0) 7031 637 845
Fax +49 (0) 7031 637 740
info@centraline.com
www.centraline.com

Subject to change without notice
EN0Z-1040GE51 R0919

by Honeywell