Honeywell

Advanced

SECURITY GUIDE

Why Secure Your Advanced Controllers? **5**

System Overview **6**

Internet/intranet/corporate network 7
BAS network 7
BAS firewall 7
Niagara 4 workstation 7
Ethernet Switch 7
Advanced Plant Controller 7
HMI 7
IO Module 7

Network Planning and Security **8**

Ethernet Network 8
Web Server 8
BACnet IP Network 8
MS/TP (NC licences) 8
USB 8
RS485 (including Modbus licences) 8
Modbus IP Network (INT licences) 8

Advanced Controller, HMI, and IO Module Security System **9**

Security when Unconfigured 9
Protection from Unauthorized Devices 9
Account Verification Code 9
System Accounts 9
Engineering System Account 9
Engineering Role 10
Administrator Role 10
Device System Account 10
System Account Creation 10
Synchronized Account Management 10
Changing an Advanced Controller Network Key 11
Local Security 11
Access to Web Pages 11
Initial Access 11
Logged in Users 12
Password Recovery 12

Securing the Niagara Operating System **12**

General Good Practice 12
Firewall Setting 12
Operating System Version 12
Virus Protection 12
Intrusion Protection 13
General Data Protection Regulation (GDPR) 13
Secure communication 14
Client/server relationships 14
Certificates 15
Self-signed certificates 15
Naming convention 15
Certificate stores 16
Encryption 16
Security Dashboard Overview 16
Planning and Installation 17
Recommended installation and configuration 17
BACnet only 17
BACnet and Niagara 18
Local Area Networks (LAN) Recommendation 18
Documentation 19
Document physical devices and configurations, including key security-related information 19
Document external systems, especially interaction between the Advanced Plant Controller and its related systems 19
Access control and physical security 20
Physically secure the Advanced Plant Controller, HMI, and IO Module 20
Sticker over controller access panel or enclosure 20
Segregate and protect networks 20
Securing the Advanced Controller, HMI, and IO Module 21
Admin System Account Credentials Provided to Site User 21
Developing a Security Program 21
Physical and Environmental Consideration 21
Security Updates and Service Packs 21
Users & Passwords 21
Users 21
Passwords 22
Configuring an Advanced Plant Controller 23
Create and maintain a baseline configurations 23

Change default passwords 23
Further Considerations 23
Service Level agreement 23
IT network configuration 23
Configuring the BAS firewall 24
Setting Up Authentication 25
Procedure 25
System Delivery 25
USB Backup and CleanDist file installation 25
System Decommissioning 25
Advanced Niagara Based products Security 26
Installation security checklist 27

Disclaimer

While we have engaged in efforts to assure the accuracy of this document, Honeywell is not responsible for damages of any kind, including without limitations consequential damages arising from the application or use of the information contained herein. Information and specifications published here are current as of the date of this publication and are subject to change without notice. The latest product specifications can be found on our website or by contacting our corporate office in Atlanta, Georgia.

For many industry RS-485-based communication, the default status is being disabled at the time of shipping out of factory to make sure the best security, because those legacy communication buses use legacy technology for the best compatibility and they were designed with weak security protection. So, to maximize the protection of your system, Honeywell has proactively disabled the legacy industrial bus communication ports (by the time of factory shipment), and user has to explicitly enable the networks in Station of each network. If you want to enable these ports, you need to be aware of the risk of any security breaches brought by the use of legacy technology. These includes but not limited to: Panel-bus, C-Bus, BACnet, M-Bus, CP-IO Bus, NovarNet, XCM-LCD protocol, SBC S-Bus and Modbus, etc.

Developing to ISA-62443

Honeywell has relied on the ISA 62443-4-1 standard for many years and applicable companion standards to develop our building technology products securely. For example, Honeywell building products also use ISA/IEC 62443-4-2 as the baseline for technical security requirements within components, and we use ISA/IEC 62443-3-3 for complete systems. So for the integrators and customers selecting building technologies, Honeywell's adherence to the family of ISA/IEC 62443 standards can provide a high level of confidence that our products don't just claim to be cyber resilient – they've been designed, tested, and validated for cyber resilience from the start.

Honeywell develops our products to ISA/IEC 62443-4-1 and we have been assessed by a 3rd party and audited against this standard.

Introduction and Intended Audience

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 Advanced Plant Controller IP-based products to mitigate the risk posed by such attacks.

The following guidelines describe the General Security Best Practices for Advanced Plant ControllerIP-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), See *"Local Area Networks (LAN) Recommendation" on page 18.* will generally meet the requirements for most automation control network installations.

This manual contains information to guide personnel at an Honeywell dealer on how to securely install and configure an Advanced Plant Controller, HMI and IO modules. Security-related information on operation, USB backup and restore, and CleanDist file installation of the controller can be found in the Installation Instruction and Commissioning Guide (31-00584).

NOTE:

Please take the time to read and understand all relevant installation, configuration, and operation manuals and ensure that you regularly obtain the latest versions

.

Table 1 Product Information

Product	Product Number	Description
Plant Controller	N-ADV-134-H	Niagara advanced controller with Four Ethernet ports, Port for HMI, and 4 RS485 port
	N-ADV-133-H	Niagara advanced controller with Four Ethernet ports, Port for HMI, and 3 RS485 port
	N-ADV-112-H	Niagara advanced controller with Two Ethernet ports, Port for HMI, and 2 RS485 port
HMI	HMI-DN	HMI with Din rail mounting
	HMI-WL	Door/Wall mounting
IO Module	IO-16UIO-S-S	16UIO IO Module without HOA, Serial Comms, Screw Terminals
	IOD-16UIO-S-S	16UIO IO Module with HOA Display, Serial Comms, Screw Terminals
	IO-16UI-S-S	16UI IO Module, Serial Comms, Screw Terminals
	IO-16DI-S-S	16DI IO Module, Serial Comms, Screw Terminals
	IO-8DOR-S-S	8DO IO Module without HOA, C/O Relays, Serial Comms, Screw Terminals
	IOD-8DOR-S-S	8DO IO Module with HOA Display, C/O Relays, Serial Comms, Screw Terminals
	IO-16UIO-S-P	16UIO IO Module with HOA Display, Serial Comms, Push Terminals
	IO-16UI-S-P	16UIO IO Module, Serial Comms, Push Terminals
	IO-16DI-S-P	16DI IO Module, Serial Comms, Push Terminals
	IO-8DOR-S-P	8DO IO Module without HOA, C/O Relays, Serial Comms, Push Terminals
	IOD-8DOR-S-P	8DO IO Module with HOA Display, C/O Relays, Serial Comms, Push Terminals

1. WHY SECURE YOUR ADVANCED CONTROLLERS?

- Protect your customer's plant systems from unauthorized changes to operating set-points, overrides and time schedules.
- Prevent access to user account details: e.g. usernames, passwords, email addresses, SMS (mobile) numbers etc.
- Prevent access to commercially-sensitive data: Example- Energy consumption metrics, specialist control strategy solutions etc.
- Prevent unauthorized access to controller, computers and networks hosting BMS software and control devices.
- Maintain data integrity and provide accountability.

2. SYSTEM OVERVIEW

The overview of the typical system installation..

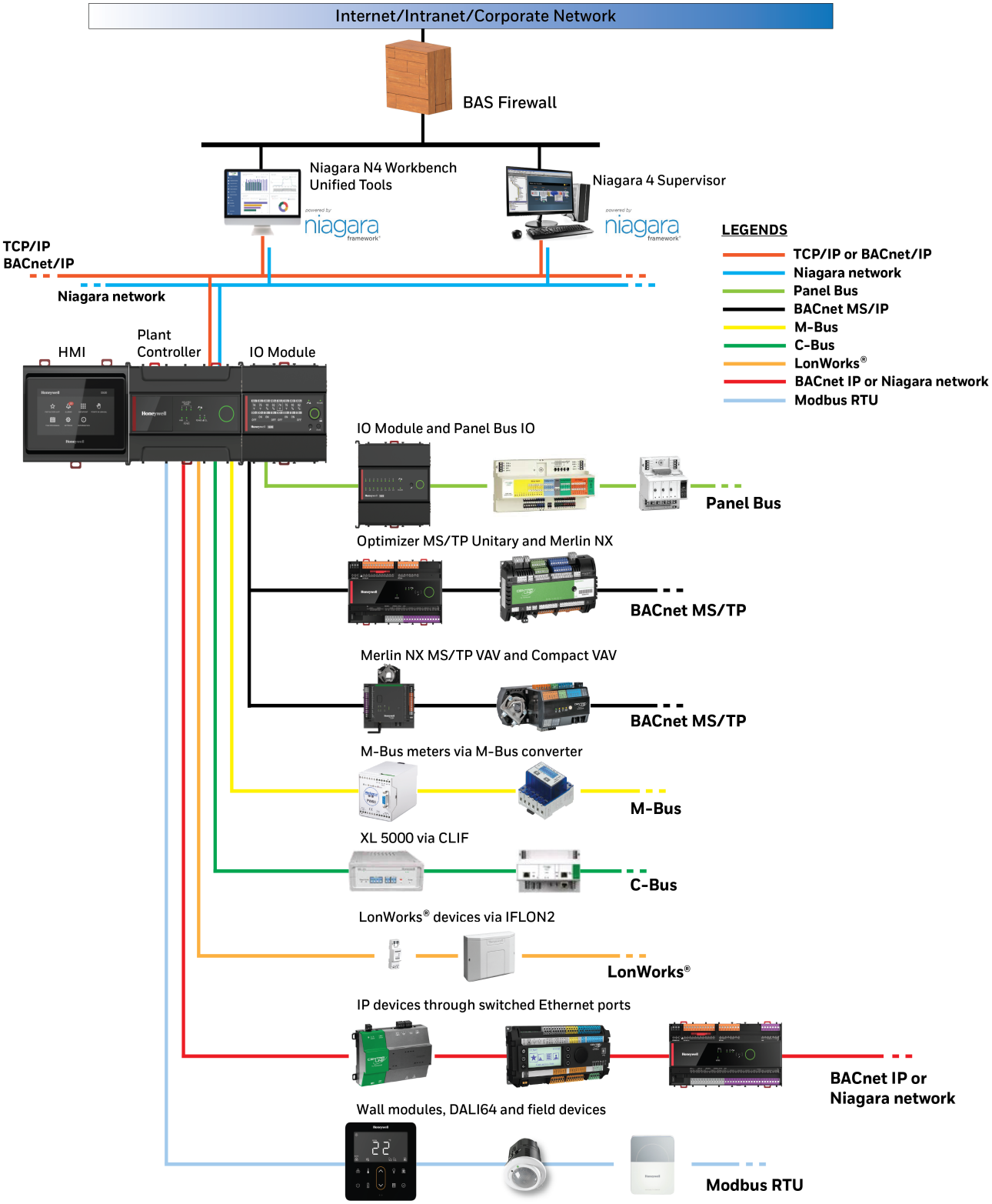

Fig. 1 System Overview

2. 1 Internet/intranet/corporate network

This is a simplified, logical network representation of all networks outside of the building automation system (BAS) scope. It may provide access to the BAS management interfaces (e.g. the Niagara primary workstation web user interface) but must provide access to the Internet so that Niagara computers can check for and download operating system and virus scanner updates unless another means to do this is provided.

2. 2 BAS network

This network is used solely for BAS protocols, which consists of BACnet/IP, BACnet/ Ethernet, and any protocols that Niagara Integration Services on an Advanced Plant Controller might use. This network must not be the same network as the Internet/intranet/corporate network.

2. 3 BAS firewall

To provide additional separation and protection to the BAS, a firewall must be used between the Internet/intranet/ corporate network and any BAS device that connects to it, such as the Niagara primary workstation, Niagara workstations, and Advanced Plant Controller. This firewall limits access to the BAS to only computers that are authorized and may help reduce the risk of attacks, such as a denial-of-service attack.

2. 4 Niagara 4 workstation

The Niagara primary workstation is a computer running Niagara software. It requires two network connections – one for connecting to the management web user interface through a web browser (usually on the Internet/intranet/corporate network) and another for connecting to the BAS network.

2. 5 Ethernet Switch

An Ethernet switch creates networks and uses multiple ports to communicate between devices in the LAN. Ethernet switches differ from routers, which connect networks and use only a single LAN and WAN port. A full wired and corporate wireless infrastructure provides wired connectivity and Wi-Fi for wireless connectivity.

2. 6 Advanced Plant Controller

The Advanced Plant Controller is a global controller that connect to an Ethernet network, BACnet IP and host MS/TP network segments. MS/TP is a low bandwidth connection that is used to connect controllers and sensors.

2. 7 HMI

HMI is connected and receives power from Advanced Niagara plant controllers. These devices are built with a capacitive touch-screen display that supports a selection by bare finger and provides the operator with functions to view, access, and troubleshoot the controller points, IO modules, and other connected equipment.

2. 8 IO Module

The IO modules can connect to the controller using the touch flake connections (power and communications) or the IO modules can connect to a wiring adapter which will be supplied with power and connected to one of the RS485 interfaces on the controller. The IO modules are programmable using the existing engineering tool such as ComfortPoint Open Studio tool and Niagara 4 Workbench.

3. NETWORK PLANNING AND SECURITY

3. 1 Ethernet Network

It is recommended that the Ethernet network used by the BMS system is separated from the normal office network.

Example:

Using an air gap, or virtual private network. Physical access to the Ethernet network infrastructure must be restricted. You must also ensure that the installation complies with your company's IT policy.

Advanced Controllers must not be connected directly to the internet.

3. 2 Web Server

The Advanced Controller provides both HTTP and HTTPS web servers. If a web server is not required, it is recommended that both web servers are disabled.

3. 3 BACnet IP Network

Due to the insecure nature of the BACnet protocol the Advanced Controller, HMI, and IO modules that use BACnet must not be connected to the internet under any circumstance. The Advanced Controller security system does not protect against BACnet writes. Physical access to the BACnet IP network infrastructure must be restricted. If BACnet IP communications are not required, the Advanced Controllers (BACnet IP) Network Module must be disabled by setting the 'Disable Module' parameter to '1'.

If BACnet communications are required it is strongly recommended that the BACnet Backup/Restore, Reinitialize Device and BACnet Writable services are not enabled. However, this will mean that the strategy created is not BTL compliant - See *"Local Security" on page 11.*

3. 4 MS/TP (NC licences)

Physical access to the MS/TP network infrastructure must be restricted. If the MS/TP network is not required, the Advanced Controller (BACnet MSTP) Network Module must be disabled by setting the 'Disable Module' parameter to '1'.

IO Bus (CAN licences)
Physical access to the IO Bus must be restricted.

3. 5 USB

Physical access to the Advanced Controller USB Local Engineering Port must be restricted.

3. 6 RS485 (including Modbus licences)

Physical access to the Controller's RS485 port must be restricted. If not required any Network Modules connected to the port should not be included in the strategy.

3. 7 Modbus IP Network (INT licences)

Due to the insecure nature of the Modbus protocol Advanced Controller's that support Modbus IP must not be connected to the internet under any circumstance. Physical access to the Modbus IP network infrastructure must be restricted. If Modbus IP communications are not required, the Advanced Controller's (Modbus IP) Network Module should not be included in the strategy.

4. ADVANCED CONTROLLER, HMI, AND IO MODULE SECURITY SYSTEM

The Advanced controllers security complies with ISA 62433-3-3 SL 3 and provides secure boot, an authenticated and encrypted network, at rest encryption, and synchronized account management.

To gain access to the Advanced Controller products or perform any of the above tasks a valid username and password for an Engineering System Account or Device System Account must be provided.

4. 1 Security when Unconfigured

To interact with an Advanced controller, HMI and IO Modules, valid credentials must be provided. The controller is supplied from the factory without any credentials (System Accounts or User modules) which ensures that when first powered up it is protected against unauthorized access. The first time an attempt is made to connect to a vCNC in one of the Advanced products on the Niagara network an Engineering System Account with Administrator Role must be created.

4. 2 Protection from Unauthorized Devices

A unique key (Network Key) is used to ensure that only authorized devices can join the Niagara network. All the controllers that are to form a Niagara network must have the same Network Key and UDP port. These are configured using IP Tool during the initial configuration process.

Example:

If four Advanced Plant Controllers have the same Network Key (112233), and a fifth has a different Network Key (222). When they are connected to the same Ethernet network the four controllers with the same Network Key join together to form a single network, but the fifth Controller will not be able to join the network because it has a different Network Key i.e (222).

Similarly, if the fifth controller is new (as shipped from the factory) and is added to the Ethernet network it will not be able to connect to the Niagara network because it does not have a Network Key.

4. 2. 1 Account Verification Code

When an Admin System Account is added to one of the controllers on the network an Account Verification Code is automatically generated by the controller to which the System Account was added. This code is synchronized to all the other controllers with the same Network Key and UDP port on the Ethernet network.

Once an Account Verification Code has been generated ALL controllers on the network MUST have the same Account Verification Code as well as the same Network Key and UDP port.

Example:

If there are five controllers, all the Advanced controllers have the same Network Key. Four have the same Account Verification Code (AVC) and therefore form a network. The fifth has a different Account Verification Code and even though it has the same Network Key it is unable to join together with the other controllers.

4. 3 System Accounts

System accounts enable people and devices to interact with the Advanced Controller. The access given is dependent on the type of account and role.

There are two types of System Accounts:

1. Engineering System Account
2. Device System Account

4. 3. 1 Engineering System Account

Engineering System Accounts are intended for use by engineers. Each engineering System Account has an account name and password that must be supplied when requested by the controller. If a valid username and password are provided the controller will grant access.

A separate engineering System Account must be created for each person. Engineering System Accounts can be set to one of two roles:

- Engineering Role
- Administrator Role

Engineering Role
The Engineering role provides the necessary access for engineering the Advanced system, creating/managing Device System Accounts and to manage the user's own account details (email address, password etc).

Administrator Role
The Administrator role provides the same access as the Engineering role plus the ability to manage all Engineering and Device System Accounts.

4. 3. 2 Device System Account

Device System Accounts are intended to allow devices such as Niagara to connect to the network to obtain the required information and make changes. It is recommended that a separate Device System Account is created for each device that is to access the network. They have a role of 'Supervisor'.

IMPORTANT:
Important: The supervisor's own security system must be configured to restrict the access rights of each supervisor user.

4. 3. 3 System Account Creation

An Engineering System Account with Administrator Role must be created the first time an attempt is made to connect to a vCNC on the Niagara network. This account is then synchronized to the other controllers on the Niagara network

- See *"Synchronized Account Management" on page 10.* Additional accounts can be created as necessary using Niagara workbench.

NOTE:
The first time an Engineering System Account is created in a controller an Account Verification Code is automatically generated and synchronized with the other controllers on the Ethernet network with the same Network Key and UDP port. When a controller has an Account Verification Code it can only join a network with controllers that have the same Account Verification Code - See *"Account Verification Code" on page 9.*

4. 4 Synchronized Account Management

Synchronized account management easily and securely synchronizes System Accounts, including the Account Verification Code, with all the Advanced Controllers on the same Niagara network. This enables:

- Single log on for the network
- Reduced overhead of configuring and maintaining access across the site without reducing security

All Advanced Controllers on the same network will have the same System Accounts.

When an Advanced Controller without any System Accounts is connected to the Ethernet network and configured with the Network Key and UDP port for the Niagara network it will join the network and automatically obtain its System Accounts from the other controllers on the Niagara network.

Example:

if an Advanced Controller without any System Accounts is added to the system above and given the Network Key for the Niagara network (112233) and UDP port it will join the network and obtain its System Accounts (User 1, User 2, User 3) from the other Advanced Controllers on the Niagara network.

Once the synchronization has completed it will be possible to connect to any vCNCs, display web pages and log in to any Advanced controller on the Niagara network using any of the System Accounts.

If changes are made to the System Accounts i.e. an account is added, deleted or edited these changes will automatically be synchronized across all Advanced Controllers on the Niagara network.

Example:

if there are five Advanced Controllers, The System Accounts in Controller (1) are edited to remove User 2, rename User 3 to User 3a and User 4 is added the changes will be synchronized to Controller (2), Controller (3), Controller (4) and Controller (5).

NOTE:
If during synchronization a conflict is discovered the latest change takes priority.

4. 5 Changing an Advanced Controller Network Key

When an Advanced Controller Network Key is changed, all its System Accounts will be deleted and it will be removed from its current Niagara network. The change to the Network Key must be authorized by a valid Engineer or Administrator System Account.

Once the change has been made it will join a Niagara network using the new Network Key, if one exists, and obtain System Accounts from the Advanced Controller on the new Niagara network providing it has the same UDP port.

4. 6 Local Security

Local security uses local users (User Modules) to allow access to the Advanced Controllers web pages or a locally connected display and to control the information that is visible or values that can be adjusted.

To gain access and make changes a valid username and password for a local user must be provided. The user's PIN level determines what parameters a user can see and adjust.

NOTE:
Local users are NOT synchronized with other Advanced Controllers on the Niagara network.

4. 7 Access to Web Pages

Access to the controller's web pages is protected by the Advanced Controller security system. When the controller's web server is accessed a web page is displayed that provides some basic information and enables a user to login - See *"Initial Access" on page 11.*

Users that login will be treated as logged in users - See *"Logged in Users" on page 12.* and users that access the web pages without logging in will be given access as described in *"Initial Access" on page 11*.

4. 7. 1 Initial Access

When the controller's web server is first accessed the Welcome page displayed and access given depends on the controller's current security configuration:

- No Engineering System Accounts and no User modules (factory default)
  The 'Welcome' page is displayed and full access to the controller's web pages and the ability to make changes will be given.

NOTE:
Because there are no Engineering System Accounts or user modules it will not be possible to login.

- Engineering System Accounts and no User modules
  The 'Welcome' page is displayed, and the controller will only give access to Sensor, Digital Input, Knob, Switch, Driver, Schedule, Time Schedule, Time, Plot modules, the Alarm Log, and Graphics and will not allow changes.

NOTE:
It will be possible to login using the Engineering System Accounts.

- Engineering System Accounts and User modules
  The initial display and access is controlled by the User modules. If there is a User module called 'Guest' without a password when the Advanced Controller web pages are accessed without logging in the controller will give the access rights (user level, home page, and view defaults) specified by the 'Guest' User module.

  By default the 'Guest' User module only provides access to the Advanced 'Welcome' page and has a user level of '0'. This means that a user accessing the controller without logging in will only be able to view the 'Welcome' page. In order to give more access the 'Guest' user can be configured in the same way as any other Type 0 User Module.

NOTE:
The Niagara workbench prevents the 'Guest' user being given a password, PIN, or user level higher than '0'. It does allow a home page and view defaults to be configured.

It is strongly recommended that the Guest user is left with the default configuration (user level of '0' and no view rights).

If there is not a User module called 'Guest' or it has been configured with a password the 'Welcome' page is displayed, and the controller will only give access to Sensor, Digital Input, Knob, Switch, Driver, Schedule, Time Schedule, Time, Plot modules, the Alarm Log, and Graphics and will not allow changes.

NOTE:
It will be possible to login using the Engineering System Accounts and any User modules that exist.

4. 7. 2 Logged in Users

To log in to an Advanced Controller web pages a user name and password that is a match for one of the Advanced Controller Engineering System Accounts or Type 0 User Modules must be entered.

4. 8 Password Recovery

If a user has forgotten their password it can be recovered by using the Niagara workbench. For details of recovering a forgotten password using Niagara see the Niagara workbench User guide.

5. SECURING THE NIAGARA OPERATING SYSTEM

5. 0. 1 General Good Practice

Follow general good practice for securing the operating system such as:

- Password protected screen saver
- Drive encryption software

5. 0. 2 Firewall Setting

The operating system must be configured to use a firewall which is automatically updated. The configuration must prevent access (IN/OUT) for all ports except those for which access is required, DO NOT leave any unused ports open.

5. 0. 3 Operating System Version

You MUST ensure that any device running Niagara applications or connected to the same IP network has the latest operating system updates installed. It is good practice to ensure that Windows Updates are left on automatic and that they are installed in a timely manner.

5. 0. 4 Virus Protection

You MUST ensure that any computers running the Niagara applications or connected to the same IP network are running virus protection software, and the virus definitions are kept up-to-date.

5. 0. 5 Intrusion Protection

The use of an Intrusion Detection System (IDS) from a reputable provider of security products on any computer running the Niagara application is recommended. Follow best practice for the products chosen as well as any corporate IT policy where the installation is made.

Many IDS and firewall products offer a complete solution for recording all the traffic coming in and out of the computer, providing users with the ability to record all activity at the lowest level.

6. GENERAL DATA PROTECTION REGULATION (GDPR)

The General Data Protection Regulation (EU)2016/679 (GDPR) is a regulation in EU law on data protection and privacy for all individual citizens of the European Union (EU) and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas. The GDPR contains provisions and requirements related to the processing of personal data of individuals (data subjects) inside the EEA and applies to any enterprise established in the EEA (regardless of its location and the data subjects' citizenship) or that is processing the personal information of data subjects inside the EEA.

Under the terms of the GDPR personal data includes any information that may be used to identify an individual. This includes (but is not limited to):

- user names,
- passwords,
- phone numbers,
- email addresses,
- work or residential addresses.

Any such information entered into the Advanced Controller, HMI, and IO Module is encrypted and stored on the Advanced products on a customer's premises. Honeywell don't have any involvement with the storage and/or processing of personal data within Advanced Honeywell products.

Responsibility for compliance with the requirements of the GDPR lies fully with the system integrator or system administrator and, as such, they must ensure that adequate technical and organizational systems are in place to:

- obtain explicit consent from each data subject for personal data to be stored, used and/or processed,
- allow individuals to have access to their personal data in order to verify accuracy,
- allow individuals to withdraw their consent at any time and to have their personal data to be permanently erased,
- maintain the security and integrity of data storage and access at all times,
- report any breaches of data security (that may affect user privacy) to the relevant authority within 72 hours of the breach occurring.

7. SECURE COMMUNICATION

A Public Key Infrastructure (PKI) supports the distribution and identification of public encryption keys used to protect the exchange of data over networks, such as the Internet. PKI verifies the identity of the other party and encodes the actual data transmission. Identity verification provides non-repudiated assurance of the identity of the server. Encryption provides confidentiality during network transmission. Requiring signed code modules ensures that only expected code runs in the system.

To provide secure networks using PKI, Niagara supports the TLS (Transport Layer Security) protocol, versions 1.0, 1.1 and 1.2. TLS replaces its predecessor, SSL (Secure Sockets Layer).

Each Niagara installation automatically creates a default certificate, which allows the connection to be encrypted immediately. However, these certificates generate warnings in the browser and Workbench and are generally not suitable for end users. Creating and signing custom digital certificates allows a seamless use of TLS in the browser, and provides both encryption as well as server authentication.

Beyond communication security, each module of computer code that runs in the system is protected with a digital signature. Added program objects require this signature or they do not run.

Verifying the server, encrypting the transmission and ensuring that only signed code runs do not secure data stored on a storage device. You still need to restrict physical access to the computers and controllers that manage your building model, set up user authentication with strong passwords, and secure components by controlling permissions.

Niagara supports and uses secure communication and signed code by default. You do not need to purchase an additional license.

Security is an ongoing concern. While you will find much valuable information in the secure communication topics, expect future updates and changes.

Below are the secure communications. For more details refer the Niagara Station Security guide.

- Client/server relationships
- Certificates
- Certificate stores
- CSR folder structure
- Certificate set up
- Certificate Wizard
- Signing multiple certificates
- Configuring secure platform communication
- Configuring secure station communication
- Enabling clients and configuring them for the correct port
- Installing a station copy on another platform
- Securing email
- Secure communication troubleshooting

7. 1 Client/server relationships

Client/server relationships identify the connections that require protection.Workbench client/server relationships vary depending on how you configure and use a system. Workbench is always a client. A platform is always a server. A station may be a client and a server.

The system protocols that manage communications are:

- Platform connections from Workbench (client) to controller or Supervisor PC platform daemon (server) use Niagarad. A secure platform connection is sometimes referred to as platformtls. You enable platformtls using the Platform Administration view.
- Local station connections (Supervisor and platform) use Foxs. You enable these connections in a station's FoxService (Config > Services > FoxService).
- Browser connections use Https, as well as Foxs if you are using Web Launcher with a WbWebProfile. You enable these connections using the station's WebService (Config > Services > WebService).
- Client connections to the station's email server, if applicable. You enable secure email using the station's EmailService (Config > Services > EmailService).

8. CERTIFICATES

A certificate is an electronic document that uses a digital signature to bind a public key with a person or organization. Certificates may serve a variety of purposes depending on how you configure the certificate's Key Usage property. Their primary purpose in this system is to verify the identity of a server so that communication can be trusted. For more details please refer the Niagara Station Security Guide - Certificate.

Niagara supports these types of certificates:

- A **CA** (Certificate Authority) certificate is a self-signed certificate that belongs to a CA. This could be a third party or a company serving as its own CA.
- A **root CA certificate** is a self-signed CA certificate whose private key is used to sign other certificates creating a trusted certificate tree. With its private key, a root CA certificate may be exported, stored on a USB thumb drive in a vault, and brought out only when certificates need to be signed. A root CA certificate's private key requires the creation of a password on export and the provision of the same password when you use it to sign other certificates.
- An **Intermediate certificate** is a CA certificate signed by a root CA certificate that is used to sign server certificates or other intermediate CA certificates. Using intermediate certificates isolates a group of server certificates.
- A **Server certificate** represents the server-side of a secure connection. While you may set up a separate certificate for each protocol (Foxs, Https, Webs). While you may configure a platform and station (as server) with separate server certificates, for simplicity most systems usually use the same server certificate.
- A **code-signing certificate** is a certificate used to sign program objects and modules. Systems integrators use this certificate to prevent the introduction of malicious code when they customize the framework.

8. 1 Self-signed certificates

A self-signed certificate is one that is signed by default using its own private key rather than by the private key of a root CA (Certificate Authority) certificate.

The system supports two types of self-signed certificates:

- A **root CA certificate** is implicitly trusted because there is no higher authority than the CA (Certificate Authority) that owns this certificate. For this reason, CAs, whose business it is to endorse other people's certificates, closely guard their root CA certificate(s) and private keys. Likewise, if your company is serving as its own CA, you should closely guard the root CA certificate you use to sign other certificates.
- A **default**, **self-signed certificate**: The first time you start an instance of Workbench, a platform or a station after installation (commissioning), the system creates a default, self-signed server certificate with the alias of tridium.

NOTE:

Do not export this certificate and import it into any store of another platform or station. Although possible, doing so decreases security and increases vulnerability.

To minimize the risk of a man-in-the-middle attack when using self-signed certificates, all your platforms should be contained in a secure private network, off line, and without public access from the Internet.

CAUTION

To use self-signed certificates, before you access the platform or station from Workbench for the first time, make sure that your computer and the platform are not on any corporate network or the Internet. Once disconnected, connect the computer directly to the platform, open the platform from Workbench, and approve its self-signed certificate. Only then should you reconnect the platform to a corporate network.

8. 2 Naming convention

The **User Key Store**, **User Trust Store**, and **System Trust Store** form the heart of the configuration. Certificates look a lot alike, and the various default self-signed certificates are named identically.

8. 3 Certificate stores

Certificate management uses four stores to manage certificates: a **User Key Store**, **System Trust Store**, **User Trust Store** and **Allowed Hosts** list.

The **User Key Store** is associated with the server side of the client-server relationship. This store holds certificates, each with its public and private keys. In addition, this store contains the self-signed certificate initially created when you launched Workbench or booted the platform for the first time.

The **User** and **System Trust Stores** are associated with the client side of the client-server relationship. The System Trust Store comes pre-populated with standard public certificates: root CA certificates from wellknown Certificate Authorities, such as VeriSign, Thawte and Digicert. The **User Trust Store** holds root CA and intermediate certificates for companies who serve as their own certificate authority.

The **Allowed Hosts** list contains server certificate(s) for which no trusted root CA certificate exists in the client's **System** or **User Trust Stores**, but the server certificates have been approved for use anyway. This includes servers for which the host name of the server is not the same as the Common Name in the server certificate. You approve the use of these certificates on an individual basis. While communication is secure, it is better to use signed server certificates.

8. 4 Encryption

Encryption is the process of encoding data transmission so that it cannot be read by untrusted third parties. TLS uses encryption to transmit data between the client and server. While it is possible to make an unencrypted connection using only the fox or http protocols, you are strongly encouraged not to pursue this option. Without encryption, your communications are potentially subject to an attack. Always accept the default Foxs or Https connections.

9. SECURITY DASHBOARD OVERVIEW

In Niagara 4.u5 and later, the Security Dashboard feature provides (for admin and other authorized users) a bird's eye view of the security configuration of your station. This allows you to easily monitor the security configuration in many station services, and identify any security configuration weaknesses on the station.

⚠ CAUTION

The Security Dashboard View may not display every possible security setting, and should not be considered as a guarantee that everything is configured securely. In particular, third party modules may have security settings that do not register to the dashboard.

The Security Dashboard view is the main view on the station's SecurityService. The view alerts you to security weaknesses such as poor password strength settings; expired, self-signed or invalid certificates; unencrypted transport protocols, etc., indicating areas where the configuration should be more secure. Other reported data includes: system health, number of active accounts, inactive accounts, number of accounts with super-user permissions, etc. Optionally, the "system" attribute on the "securityDashboard" license feature can be set to "true" to enable the System View of the station which provides security details for each subordinate station in the NiagaraNetwork.

The Security Dashboard is the main view for the Security Services. For complete details on the view, Refer to "nss-SecurityDashboardView" in Niagara Station Security Guide.

10. PLANNING AND INSTALLATION

This section includes information for planning and performing an Advanced Plant Controller installation.

10. 1 Recommended installation and configuration

The following section illustrates two recommended installation configurations.

- BACnet only
- BACnet and Niagara

10. 1. 1 BACnet only

When the Advanced Plant Controller is only used for BACnet communications, connect only Ethernet 1 to the BAS network where BACnet (BACnet/IP or BACnet/Ethernet) will be running.

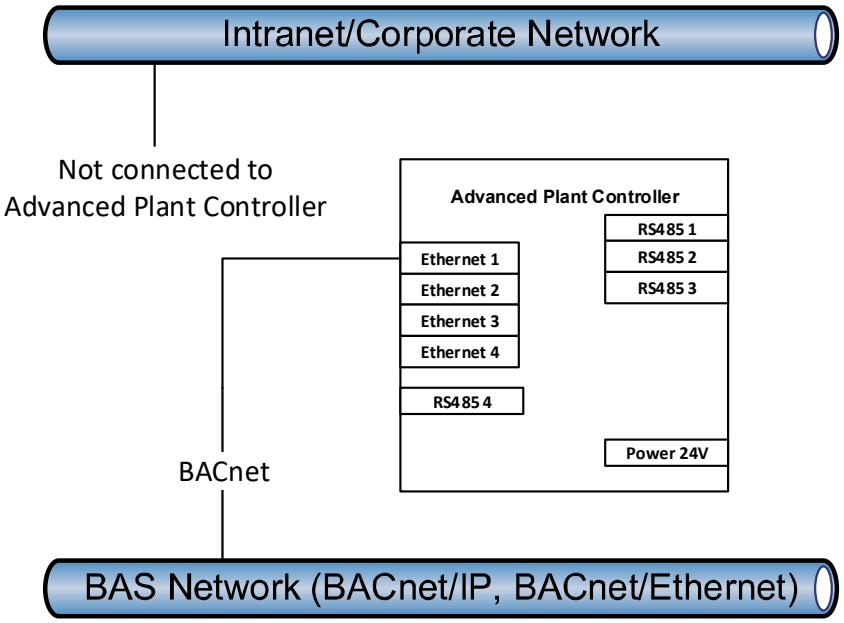

Fig. 2 BACnet Connection

10. 1. 2 BACnet and Niagara

When Niagara is used on the Advanced Plant Controller, it may be configured to provide services, such as web services or Niagara FOXS, to the Internet/intranet/corporate network. If this is the case, connect Ethernet 2 to the Internet/ intranet/corporate network through the BAS firewall to provide services to that network.

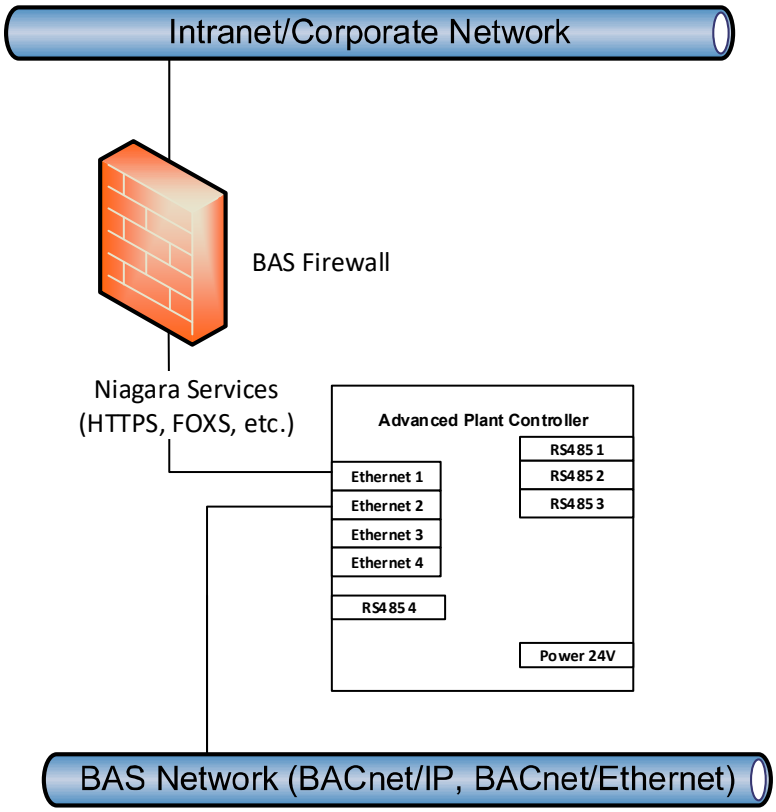

Fig. 3 BACnet and Niagara Connections

10. 2 Local Area Networks (LAN) Recommendation

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.

11. DOCUMENTATION

Documentation is essential in capturing design and configuration information required to maintain a secure system.

11. 1 Document physical devices and configurations, including key security-related information

All documentation on devices and configurations must include security-related information to establish and maintain the intended security controls. For example, if changes to default services or ports are made on the Advanced Plant Controller, then clearly document these so that the settings can be restored at some point in the future.

11. 2 Document external systems, especially interaction between the Advanced Plant Controller and its related systems

The BAS commonly requires or utilizes external systems for functionally, such as existing network infrastructure, VPN access, virtual machine hosts, and firewalls. If the BAS requires those systems be configured in a certain way for security, such as a firewall allowing or denying certain ports or a network allowing access to certain systems, then you must document this information. If these systems need to be restored at some point in the future, **Example:** due to equipment failure, or changes need to be made to the external systems, **Example:** upgrading a firewall, having documented this information will help you restore to the previous security level.

12. ACCESS CONTROL AND PHYSICAL SECURITY

Access control involves specifying and limiting access to devices or functions to authorized users only.

12. 1 Physically secure the Advanced Plant Controller, HMI, and IO Module

Prevent unauthorized access to the network equipment that is used in conjunction with systems provided by Honeywell. 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. Honeywell equipment should be installed within locked control cabinets, themselves located in secured plant rooms.

12. 2 Sticker over controller access panel or enclosure

Apply a tamper-evident sticker over the Advanced Plant Controller, HMI, and IO Module access panel or enclosure

If a customer needs additional assurance that the physical access protecting an Advanced Plant Controller, HMI, and IO Module has not been entered, then install a tamper-evident seal or sticker over the access point.

12. 3 Segregate and protect networks

1. Use a firewall between the Internet/intranet/corporate network and the BAS.
2. Use a separate dedicated physical network (separate wires) or virtual network (VLANs) for BACnet communication. This must be a separate network from the Internet/ intranet/corporate network.
3. Do not connect EN2 on the Advanced Plant Controller to any network unless you need Niagara services (Platform, Station, and/or Webserver). If you do need to connect EN2 to the Internet/ intranet/corporate network, then you must use an external BAS firewall between the Advanced Plant Controller and Internet/intranet/corporate network.

13. SECURING THE ADVANCED CONTROLLER, HMI, AND IO MODULE

13. 1 Admin System Account Credentials Provided to Site User

The credentials of the 'Admin' System Account must be provided to the site owner to allow them to manage the System Accounts.

13. 2 Developing a Security Program

Refer to the 'General Security Best Practice'

13. 3 Physical and Environmental Consideration

The Advanced Controller, HMI, and IO Module must be installed within a locked environment e.g. located in a secured plant room, or a locked cabinet.

NOTE:
Ensure adequate ventilation.

13. 4 Security Updates and Service Packs

Ensure the Advanced Controller, HMI, and IO Module is running the latest release of firmware.

14. USERS & PASSWORDS

14. 1 Users

Ensure the number of users and access levels provided are appropriate for the activities they need to perform.

- **At the controller device level configure system accounts or users in controllers for Web client, Supervisor and Peer-to-peer access.**

  Configuring User modules in the Advanced controllers, this means a user will have to log into a device with valid credentials before adjustments can be made. Ensure appropriate access rights are assigned for the system accounts and users.

- **Use a Different Account for Each User**

  Use unique names and passwords for each user/account on the system, rather than generic access. Different people should never share the same account. For example, rather than a general 'managers' account that many managers could use, each manager should have their own, separate account.

There are many reasons for each user to have their own individual account:

- If each person has their own account, audit logs will be more informative. It will be easy to determine exactly which user did what. This can help detect if an account has been compromised.

NOTE:
Not all products have an audit log facility, but where available it should not be disabled.

- If an account is removed or modified, it does not inconvenience many people. For example, if a person should no longer have access, deleting their individual access is simple. If it is a shared account, the only options are to change the password and notify everyone, or to delete the account and notify everyone. Leaving the account as-is is not an option – the goal is to revoke the access.
- If each person has their own account, it is much easier to tailor permissions to precisely meet their needs. A shared account could result in people having more permissions than they should.

  - A shared account means a shared password. It is an extremely bad security practice to share passwords. It makes it much more likely for the password to be leaked, and makes it more difficult to implement certain password best practices, such as password expiration.

- **Use of Unique Engineering Users for Projects**

  It is a common practice that some companies use the same account details on every project. Once this is known if one system is compromised, the attacker could potentially have credentials for access to many other projects installed by the same company.

- **Disable Known Accounts When Possible**

  Some products have default accounts. These should be configured so that the password is no longer the default.

- **Assign the Minimum Required Permissions for users**

  Ensure only required accounts are set up on the system with the minimum security levels required rather than full access. When creating a new account, think about what the person needs to do in the system, and then assign the minimum permissions required to do that job. For example, a someone who only needs to see alarms does not need administrator access. Giving permissions which are not required increases the chance of a security breach. The user might inadvertently (or purposefully) change settings that they should not change.

- **Use the Minimum Possible Number of System Administrator accounts**

  Only assign System Administrators permissions when absolutely necessary. This type of account is an extremely powerful account – it allows complete access to everything. Only the system administrator should have access to the account. Also think about providing the System Administrator two accounts, one for daily access to manage day to day activities, and a second high level access account which is only required when administration type changes are required.

14. 2 Passwords

The Trend system and operating systems used Trend products use passwords to authenticate ‘users’ into a Supervisor, Display, Tool or Operating systems. It is particularly important to handle passwords correctly. Not employing this most initial level of security will mean anyone accessing the system via a display, web client or supervisor will have access to make adjustments. Ensure the Niagara system operates an appropriate password policy for user access this guideline would include, but not limited to:

- **The use of strong passwords** - Strong passwords shold be used. Refer to the latest security standards for details of what makes a strong password.
- **A recommended password cycle time** - Some Niagara products allow the system administrator to specify a period after which a password must be changed. Although not all products currently enforce this password change period a site policy can recommend this.
- **Password disclosure rules** - The user MUST ensure that they do not disclose details of their user name and password, to others and to not write them down.

15. CONFIGURING AN ADVANCED PLANT CONTROLLER

For configuration of an advanced plant controller, Refer Installation Instruction and Commissioning Guide (31-00584). Refer HMI Driver guide (31-00590) for HMI, and Panel Bus Driver Guide (31-00591) for IO module.

15. 1 Create and maintain a baseline configurations

Create and maintain a baseline of Advanced Plant Controller configurations that have been properly configured for security. Ensure that this baseline also includes DCF files and Niagara components. Do not commit insecure configurations to the baseline to prevent inadvertently applying them in the future. Update any relevant documentation when configurations change.

15. 2 Change default passwords

Change all default passwords: Console Configuration password, the backup/Restore/Restart/Control password, and the Niagara Platform password. When completing commissioning, ensure the device is password protected. Ensure appropriate user levels are assigned for the site users.

15. 3 Further Considerations

15. 3. 1 Service Level agreement

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, IO modules, HMI, etc.;
- Supervisor software, such as Arena NX software;
- Computer / Server operating systems;
- Network infrastructure and any remote access systems.

15. 3. 2 IT network configuration

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.

When interfacing with controllers using a centralized system supervisor (Example: Niagara) 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.

16. CONFIGURING THE BAS FIREWALL

The following table describes the network ports used in an Advanced Plant Controller. See the See *"System Overview" on page 6.* for an example installation architecture. The table has the following columns:

- Default Port and the Protocol (TCP or UDP)
- Purpose of the port
- Whether or not the default port needs to be changed
- Whether or not incoming connections or traffic should be allowed through the BAS Firewall
- Additional notes are listed below the table

Table 2 Configuring the BAS firewall

Default Port/Protocol	Purpose	Change F Default?	Allow Through BAS Firewall?	Notes
80/TCP	HTTP	No	No	
443/TCP	HTTPs	No	Possibly, if web access from the Internet/intranet/corporate network is required.	1
1911/TCP	Fox (non-secure version of Niagara application protocol)	Yes	No	
4911/TCP	Fox + SSL (secure version of Niagara application protocol)	Yes	No	
3011/TCP	NiagaraD (non-secure version of Niagara platform protocol)	Yes	No	
5011/TCP	NiagaraD + SSL (secure version of Niagara platform protocol)	Yes	No	
2601/TCP	Zebra console port	No	No	2
2602/TCP	RIP console port			2
47808/UDP	BACnet/IP network connection	Yes	No	3

NOTE:

1. If direct remote web user interface is supported, then this port must be allowed through the BAS firewall.
2. Port is automatically opened by this daemon and this functionality cannot be disabled. The daemon is configured to not allow any logins through this port.
3. Follow the network configuration guidelines stated in this manual so the Advanced Plant Controller will never need to pass UDP traffic through the BAS firewall.

17. SETTING UP 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 OneTime 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.

17. 1 Procedure

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.

18. SYSTEM DELIVERY

This section contains information that you must provide when the BAS is delivered to the system owner.

- Documentation that includes security information, configuration settings, administration usernames and passwords, disaster and recovery plans, and backup and restore procedures.
- End-user training on security maintenance tasks.

19. USB BACKUP AND CLEANDIST FILE INSTALLATION

USB backup and CleanDist file installation information can be found in the Installation Instruction and Commissioning Guide - 31-00584.

20. SYSTEM DECOMMISSIONING

Sensitive data should be erased from units that are being taken out of service and this can be done by performing a factory reset. Refer Service Button/Service Alarm LED and Cleandist file installation from Installation Instruction and Commissioning Guide - 31-00584.

NOTE:
The Cleandist file procedure can perform factory set by installing the clean4 file.

21. ADVANCED NIAGARA BASED PRODUCTS SECURITY

For Advanced Honeywell products which are based on the Niagara N4 and Niagara AX frameworks (e.g. Advanced Plant Controller, HMI, and IO Module), you must follow the Tridium's advice on securing the Niagara framework.

There are a number of configuration changes that can be made to Niagara that can be done to maximize the security of the Advanced Honeywell products.

- Use the Password Strength Feature
- Enable the Account Lockout Feature
- Expire Passwords
- Use the Password History
- Use the Password Reset Feature
- Leave the "Remember These Credentials" Box Unchecked
- Change the Default System Passphrase
- Use TLS To Set the System Passphrase
- Choose a Strong System Passphrase
- Protect the System Passphrase
- Ensure Platform Owner Knows the System Passphrase
- Use a Different Account for Each Platform User
- Use Unique Account Names for Each Project
- Ensure Platform Owner Knows the Platform Credentials
- Use a Different Account for Each Station User
- Use Unique Service Type Accounts for Each Project
- Disable Known Accounts When Possible
- Set Up Temporary Accounts to Expire Automatically
- Change System Type Account Credentials
- Disallow Concurrent Sessions When Appropriate
- Configure Roles with Minimum Required Permissions
- Assign Minimum Required Roles to Users
- Use the Minimum Possible Number of Super Users
- Require Super User Permissions for Program Objects
- Use the Minimum Required Permissions for External Accounts
- Use an Authentication Scheme Appropriate for the Account Type
- Remove Unnecessary Authentication Schemes
- TLS & Certificate Management
- Module Installation
- Require Signed Program Objects and Robots
- Disable SSH and SFTP
- Disable Unnecessary Services
- Configure Necessary Services Securely
- Update Niagara 4 to the Latest Release
- Install Product in a Secure Location
- Make Sure that Stations Are Behind a VPN

Specific technical publications are available which must be followed to ensure the system is locked down as securely as possible. Many options exist such as SSL encryption and additional steps to protect elements such as program modules, for more details refer to the Tridium website for the Niagara 4 Hardening Guide (for Niagara N4 based products) and the Niagara Hardening Guide (Niagara AX based products).

Honeywell Building Technologies

715 Peachtree St NE
Atlanta, Georgia 30308
customer.honeywell.com
buildings.honeywell.com

® U.S. Registered Trademark
©2023 Honeywell International Inc.
31-00594-01 Rev. 06-23

Honeywell

22. INSTALLATION SECURITY CHECKLIST

Advanced Plant Controller Device Instance: _____

Advanced Plant Controller Description: _____

Advanced Plant Controller Location: _____

Installer:_____ Date: _____

Complete the following security tasks for each installed Advanced Plant Controller

- ☐ Install a firewall between the Advanced Plant Controller and external network(s). See *"BACnet and Niagara" on page 18.*
- ☐ Physically secure the Advanced Plant Controller. See *"Physically secure the Advanced Plant Controller, HMI, and IO Module" on page 20.*
- ☐ Change the default password to a unique password for each of the following: Console Configuration, Backup/Restore/Restart/Control, and the Niagara Platform. See Installation Instruction and Commissioning Guide - 31-00584
- ☐ If a web server is needed, then configure it to operate in HTTPS mode only. See Installation Instruction and Commissioning Guide - 31-00584

Web Server Status: Disabled / Enabled.

If web service is enabled, complete the following:

- ☐ Set Http Enabled = false.
- ☐ Set Https Enabled = true.
- ☐ Set Https Only = true.
- ☐ Configure the BAS firewall. See *"Configuring the BAS firewall" on page 24.*
- ☐ Provide all required data to the BAS system owner at delivery. See *"Setting Up Authentication" on page 25.*