Nyquist System Controller Setup Guide

E7000 Release 10.0
C4000 Release 7.0

eLearning!

BOGEN

740-00206C
250317

Contents

List of Figures

Setup Introduction

This guide is intended for system engineers, system integrators, and IT personnel who are responsible for installing and setting up a Nyquist System Controller (NQ-SYSCTRL). It assumes that users of this guide understand basic networking concepts.

Two options are available for installing and deploying a Nyquist system:

1. Using a Nyquist System Controller, a purpose-built appliance computer with the Nyquist application software preinstalled.
2. Using your own server platform to install the Debian OS and Nyquist server application software.

Option 1 is the quickest and easiest approach, but option 2 may be better suited for situations where high-availability server features like Redundant Array of Independent Disks (RAID) or hot-swappable power supplies are desired.

This guide describes the Nyquist installation and setup process when using the Nyquist System Controller (i.e., option 1). If you are using your own server platform, see the *Nyquist Server Installation and Setup Guide*.

For information about training resources for the Nyquist controller and other Bogen products, visit:

`https://www.bogen.com/eLearningQR`

Nyquist Network Organization

The System Controller is a multi-homed computer with two Ethernet ports, A and B. (See *Figure 1, "Port A-Only Configuration," on page 2* and *Figure 2, "Port A and B Configuration," on page 2*.)

The System Controller always communicates with Nyquist devices on Port A. Port B is optional: It is used to communicate with the Internet when the network connected to Port A is a private "Nyquist" network that is not connected to the Internet.

The System Controller only requires access to the Internet for system activation, software upgrades, and when adding new or additional license activation keys. Normal operation does not require an Internet connection unless one of the available embedded Internet radio or music streaming services is going to be used for audio distribution, or if Routine API invocations from Internet-based systems, Routine Webhook-Post actions to Internet-based systems, weather alerts, or weather conditions will be used.

As shipped from the factory, Port A is configured to use static Internet Protocol (IP) address 192.168.1.10, and Port B is set to obtain an IP address through Dynamic Host Configuration Protocol (DHCP).

If the network to be connected to Port A cannot accommodate the default static IP address 192.168.1.10, the default address must be changed during installation, as described in *"Install the System Controller" on page 8*.

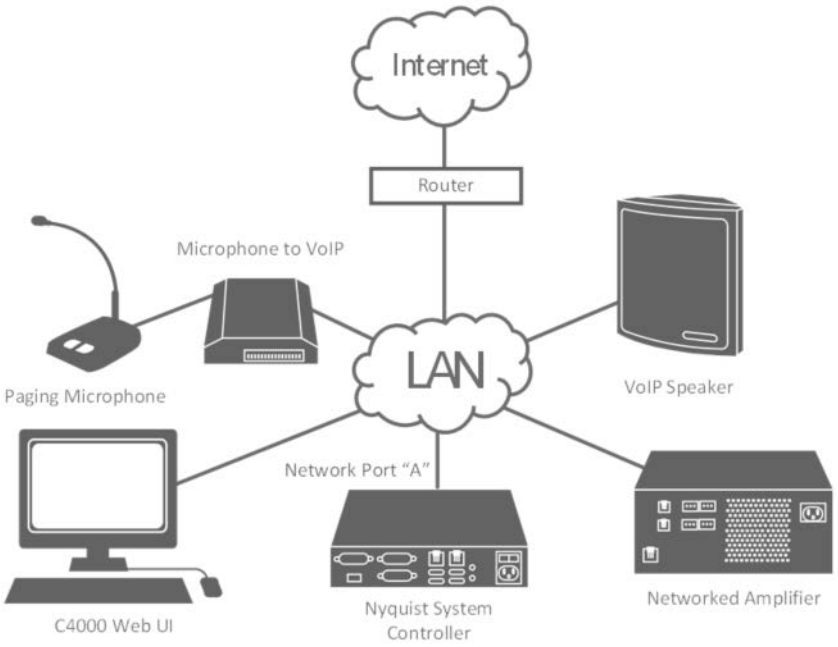


Figure 1. Port A-Only Configuration

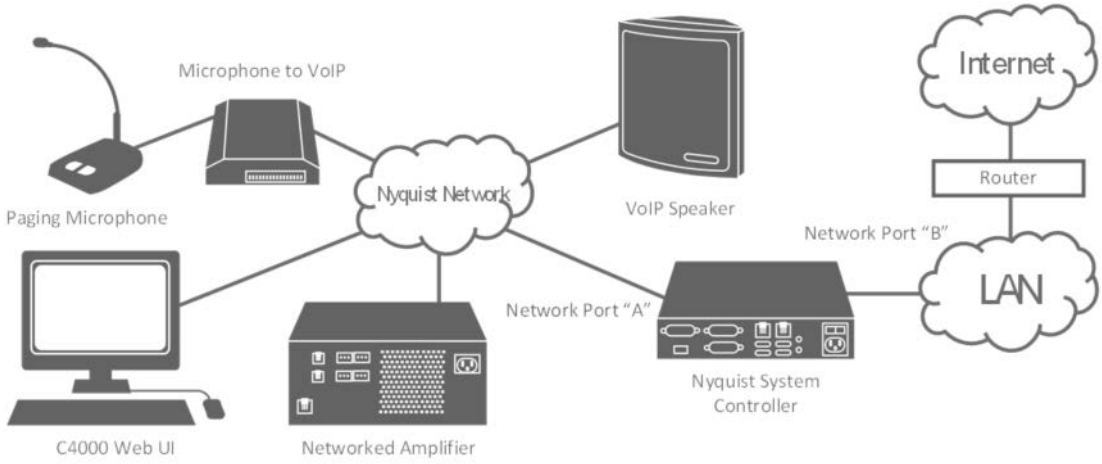


Figure 2. Port A and B Configuration

Understanding System Requirements

The Nyquist controller web-based UI requires a secure Hypertext Transfer Protocol Secure (HTTPS) network connection to the Nyquist controller. Users can log in to the Nyquist controller using the Google Chrome or Microsoft Edge web browser from a computer or tablet running either the Windows 10 (or later) or Mac OS X 10.12.x (or later) operating system (OS), or using the Safari browser from an iPhone or iPad device running iOS 14 (or later). The UI can also be accessed via a Chrome or Edge browser-enabled Android-based tablet or mobile device.

To access the server, type your server's IP address (for example, 10.10.20.12) in your browser's address bar.

Whitelisted Web Addresses

The Nyquist controller requires access to specific Uniform Resource Locators (URLs), commonly referred to as web addresses. Access to many of these web addresses is required during installation; access to other web addresses, such as the address for the Network Time Server (NTS) are required during runtime. The Information Technology (IT) department for the site must whitelist the web addresses so that they can be easily accessed as needed.

Nyquist controller access to these URLs can be checked via the **Check Internet Site Access** feature on the **System Parameters** page or by pressing the **Check Internet Site Access** button on the **Network Wizard** page during product activation.

The following table lists the URLs that must be whitelisted.

Table 1. Whitelisted Web Sites

URL	Description
http://hostedactivation.com (specifically, http://hostedactivation.com/bogen)	Required for Nyquist controller License support
http://downloads.digium.com	Required for downloads from Digium Phone Module for Asterisk (DPMA)
http://downloads.asterisk.org/ (specifically, http://downloads.asterisk.org/pub/telephony/sounds/releases)	Required for sounds download
http://www.pjsip.org/	Required for PJSIP download
http://ftp.us.debian.org (specifically: http://ftp.us.debian.org/debian/)	Required during Linux package installation
http://deb.debian.org/debian/	
https://deb.debian.org/debian/	
http://security.debian.org (specifically: http://security.debian.org/)	Required during Linux package installation
stun01.sipphone.com stun:stun01.sipphone.com	Required for STUN based IP address resolution (This is used by the Nyquist controller Web UI and should be enabled on the computer that runs the web UI.)
https://raw.githubusercontent.com/	Serves unprocessed versions of files stored in the GitHub repositories.
http://2431612419.airable.io https://2431612419.airable.io	The *airable* URL for Internet-based-radio Audio Distributions

Table 1. Whitelisted Web Sites (Continued)

URL	Description
http://api.sound-machine.com https://api.sound-machine.com	The SoundMachine URL for Internet-based-radio Audio Distributions
http://api.bogenedu.com/api/customers	Required for Nyquist controller warranty support
http://bogen-ssu.bogen.com/	Bogen System Software Update server. Required for automatic Nyquist server software and Nyquist firmware software update notifications and downloads.
https://www.weather.gov/alerts	Required for displaying weather alerts.
https://ipapi.co	Required for automatically finding county code for alerts.
https://api.weather.gov	Required for obtaining alerts from the National Weather Service.
http://openweathermap.org http://api.openweathermap.org	Required for obtaining current weather conditions.
ns1.google.com resolver1.opendns.com	Required for obtaining the Nyquist server's public IP address for Audio Distribution streams and for automatically finding the county code for alerts.
dl-ssl.google.com	Required for Nyquist installation and updates to download and install Google Chrome browser.

URLs that are entered on the Nyquist **System Parameters** page are used during runtime and include the URLs for the NTS, the Session Traversal Utilities for Network Address Translation (NAT) (STUN) server, and the Traversal Using Relays around NAT (TURN) server.

The default URLs for the STUN and TURN servers are not set. The default URL for NTS is pool.ntp.org.

Network Application Services

Required application services will be installed automatically on the Nyquist controller as part of the Nyquist software installation. All other network services must be already present or installed manually on the associated network. The following table lists the services and their locations:

Table 2. Network Application Services

Service	Description	Required	Location
Apache	Used as the web server to drive the Nyquist controller web interface.	Mandatory	Nyquist controller
DHCP	Supplies dynamic IP addresses to the Nyquist controller system server and associated devices. (DHCP is the acronym for Dynamic Host Configuration Protocol.) It also supplies the Trivial File Transfer Protocol (TFTP) server IP address or host name to devices on the network via option_66.	Optional	Network and/or Nyquist controller
DNS	Resolves host names to IP addresses. DNS is an acronym for Domain Name System, a hierarchical naming system for computers, servers, or other resources connected to either the Internet or to a private network.	Mandatory[a]	Network
ICE STUN TURN	Resolves IP addresses behind Network Address Translation (NAT)/firewall. • Interactive Connectivity Establishment • Session Traversal Utilities for NAT • Traversal Using Relays around NAT	Optional	Nyquist controller Network
LDAP	LDAP is used by the Nyquist controller to import users into the Nyquist system.	Optional	Network
NTP	Network Time Protocol provides date/time synchronization for the Nyquist controller and the associated devices (IP Phones, appliances).	Mandatory	Network
SNMP	Provides the Nyquist controller Linux server statistics via Simple Network Management Protocol (SNMP) v1 through Port 161.	Optional	Nyquist controller
TFTP	TFTP is used by IP phone and Nyquist controller device provisioning. A TFTP server runs on the Nyquist controller on port 69 (the standard TFTP port #). Device provisioning files are stored on the Nyquist controller in directory: `/srv/tftp`. This is the only directory exposed by the TFTP server.	Mandatory	Nyquist controller

a. Required for Nyquist software upgrades, updating license keys, adding new feature license keys, using Internet-based features, e.g., Internet Radio service, weather alerts, weather conditions, Routines API, Routine Webhook-Post action.

Network Ports

The following table lists the network ports required by the Nyquist System Controller and the associated devices.

Table 3. Network Ports Used by Nyquist

Service	Description	Port
Automatic Failover	Local ports used for Automatic Failover support. These only need to be available between the two servers.	5405,2224,3121
DHCP	Dynamic Host Configuration Protocol (Optional)	67, 68
DNS	Domain Name System (Optional)	53
HTTP	Hypertext Transfer Protocol Used for phone provisioning.	8088
HTTP	Provide access to Bogen product information.	80
HTTPS	Secure HTTP	8089
HTTPS	Secure HTTP (HTTP over TLS/SSL) Provides access to Bogen product information.	443
IAX	Inter-Asterisk eXchange Used for inter-facility communications.	4569
LDAP	Lightweight Directory Access Protocol	389
LDAP over TLS	Lightweight Directory Access Protocol over Transport Layer Security	389 (configurable)
NTP	Network Time Protocol	123
ODBC	Open Database Connectivity Provides database connectivity.	3306
RLM	Reprise License Manager Provides Nyquist license activation via hostedactivation.com.	5053
RSYNC	Remote sync utility Used to synchronize files (Automatic Failover Only).	873
RTP	Real-time Transport Protocol Used for distribution of audio streams.	10000–20000 (configurable)
secure-mqtt	Nyquist control messages between Nyquist server and Nyquist appliances	8883
Server Management	Local port used for server management **DO NOT** allow outside access to this port. During system controller installation, an IP filter rule is installed to block outside access to this port.	5038
SFTP	Provide access to Bogen product information.	22

Table 3. Network Ports Used by Nyquist

Service	Description	Port
SIP	Session Initiation Protocol (SIP) Transfer Control Protocol (TCP)/ User Datagram Protocol (UDP) connections	5060, 5061
SIP over Web Services	SIP WS/WSS connections	8088
SNMP	Simple Network Management Protocol (Optional)	161
SRTP	Secure Real-time Transport Protocol	(same as RTP)
TFTP	TFTP connections	69

Installing and Configuring the Nyquist System Controller

The System Controller always uses Port A to communicate with Nyquist devices and, optionally, to communicate with Internet-based services. See *Figure 1, "Port A-Only Configuration," on page 2* and *Figure 2, "Port A and B Configuration," on page 2*.

The System Controller must have a known IP address on the Port A network so that its Web-based UI can be accessed via a supported browser. The System Controller ships with Port A configured with static IP address 192.168.1.10. Before proceeding with the installation, verify that your Port A network can accommodate this static address.

Be sure to check the following:

- IP address 192.168.1.10 must be compatible with your network number. (Usually, this requires a 192.168.1.x/24 or 192.168.1 class C network.)
- IP address 192.168.1.10 must not already be in use on your network.
- If your network has a DHCP server, it must be prevented from assigning IP address 192.168.1.10.

If your Port A network cannot accommodate IP address 192.168.1.10, determine an IP address to use for the System Controller. During installation and setup, you will reconfigure Port A to use that address. This will require temporarily connecting Port B to a network with a DHCP server.

Alternatively, you can connect Port A directly to a computer that has an adapter temporarily configured with a subnet mask of 255.255.255.0 and an IP address in the 192.168.1.0/24 subnet, such as 192.168.1.1, and begin the System Controller installation process. During the Network Wizard, configure the System Controller to use an IP address appropriate for your Nyquist network. When the wizard prompts you to change cables, connect the Port A network cable to the Nyquist network and continue the wizards using a computer on the Nyquist network (or a DHCP address from Port B).

Install the System Controller

Before installing your System Controller, ensure that you have your Nyquist License Activation Key(s).

To install the System Controller:

1. Unpack the System Controller and power cord.
2. Obtain an Ethernet cable (customer-supplied). If your network can accommodate IP address 192.168.1.10, use the cable to connect Port A to your network. If you cannot accommodate 192.168.1.10, use the cable to temporarily connect Port B to a network with a DHCP server. (This could be your *Port A* network if it has a DHCP server.) If you are connecting Port B to your office network, ensure that your DHCP server is *not* assigning IP addresses on the 192.168.1.x subnet.
3. Connect the power cord to the back of the System Controller.
4. Toggle the power switch, located above the power cord, to the on (—) position. A green light displays next to **POWER** at the front of the device. Allow the System Controller to boot (3–5 minutes).
5. Obtain the System Controller's IP address. The following suggestions may help:
   - If you connected to Port A in step 2 and are able to use the default static IP address, the IP address is 192.168.1.10.
   - Attach an HDMI monitor to the controller's HDMI port; the IP configuration should be displayed on the screen. The IP address (`xxx.xxx.xxx.xxx`) and subnet mask (`yy`) for each network adapter can be found within the displayed text as:

     ```
     inet xxx.xxx.xxx.xxx/yy
     ```
   - If you connected to Port B in step 2, determine the IP address that was assigned to the System Controller by your DHCP server.

     This can usually be determined by interrogating your DHCP server. Look for a DHCP client name of **debian** or **nq-sysctrl-003018xxxxxx** or for the System Controller's MAC address, which is available on the chassis of the System Controller and begins with `00:30:18`.
   - Execute the following PowerShell command, replacing `00-30-18-xx-xx-xx` with your System Controller's MAC address, which is available on the chassis of the System Controller:

     ```
     Get-NetNeighbor -LinkLayerAddress 00-30-18-xx-xx-xx
     ```
   - If you don't have access to the network switch or the facility DHCP server, it might be necessary to download and install an IP scanner (e.g., Advanced IP Scanner or nmap) on your client computer to scan the network and identify the IP address that was assigned to Port B. Look for the MAC address associated with Port B or a host name of "JET" in the scan results.
6. Using a browser, access the System Controller's IP address. Proceed to *"Using the Setup Assistant" on page 9*.

Using the Setup Assistant

Navigate to the System Controller's IP address in the browser:

http://<server>

The following *Welcome to the Setup Assistant* screen appears (*Figure 3*). If this screen does not display, check your network cables and IP addresses and try again.

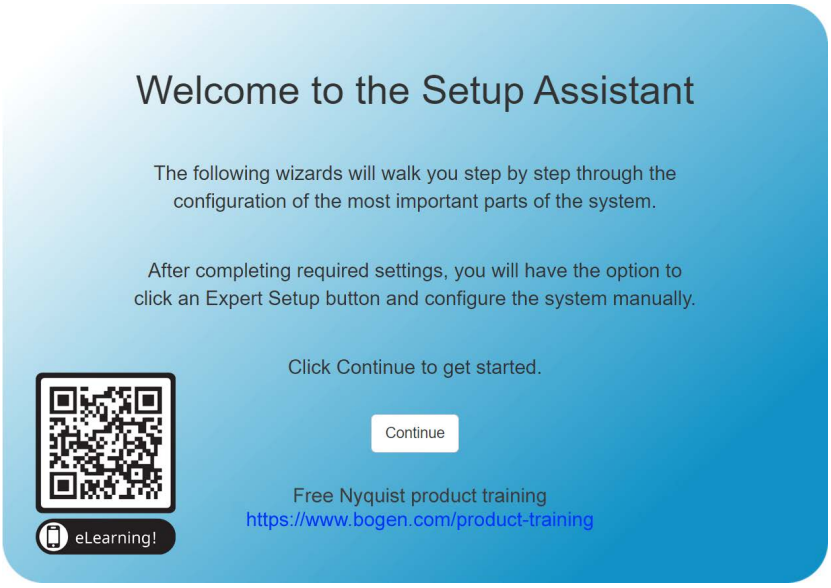


Figure 3. Setup Assistant

The Setup Assistant presents a series of wizards to guide you through the setup process.

Click **Continue** on the *Welcome to the Setup Assistant* screen to launch the *Network Wizard* screen.

Network Wizard

1 The Network Wizard, as shown in *Figure 4, "Network Wizard"*, allows you to configure the IP address settings on Ethernet ports A and B.

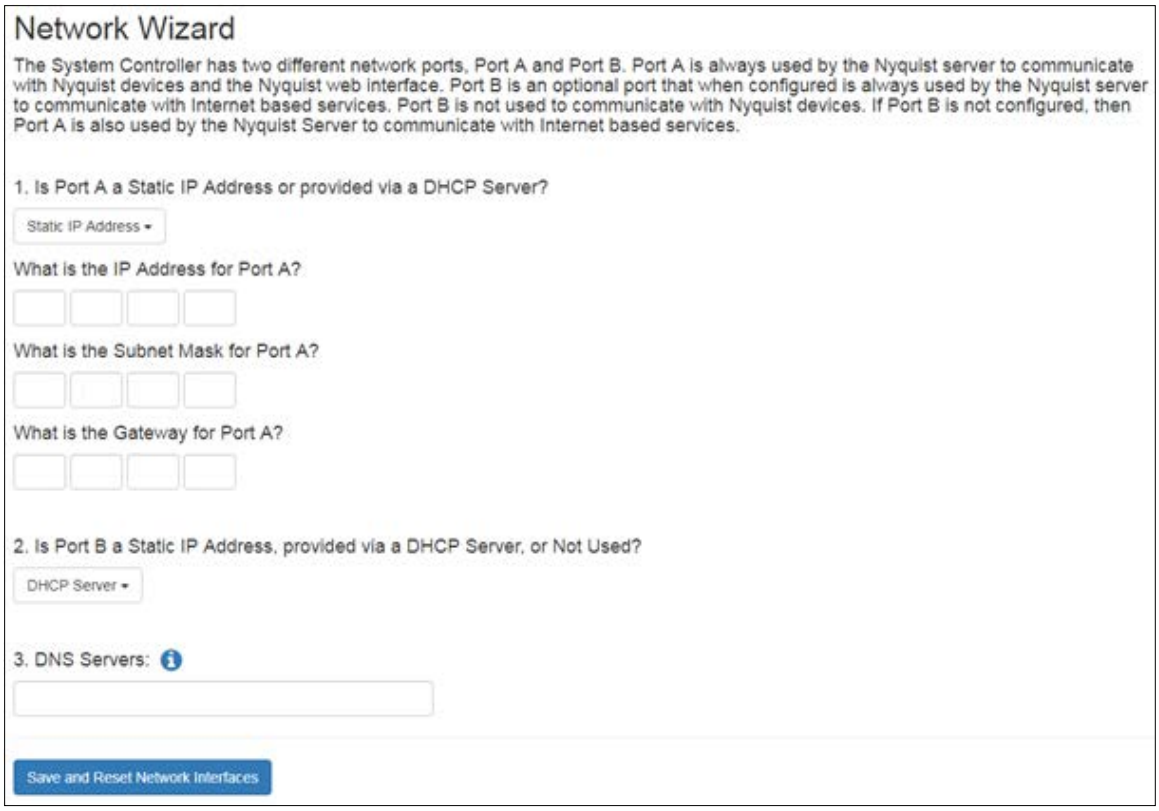


Figure 4. Network Wizard

2 In the **Is Port A a Static IP Address or provided via a DHCP Server?** field, select **Static IP Address**.[1]

3 In the **What is the IP Address for Port A?** field, type **192.168.1.10** if you are using the default static IP address for Port A; otherwise, type the static IP address that you want to use for the System Controller on the Port A network.

4 In the **What is the Subnet Mask for Port A?** field, type the subnet mask, typically 255.255.255.0.

5 In the **What is the Gateway for Port A?** field, type the gateway address of your Port A network.

6 Port B can provide access to the Internet if the Internet is not available through the Port A network. If Port B will *not* be used, select **DHCP Server** from the **Is Port B a Static IP Address, provided via a DHCP Server, or Not Used?** drop-down field and go to step 8. This provides a fallback mechanism to access the Nyquist System Controller in the event that access via Port A fails. Otherwise, continue with step 7.

7 If Port B will be used, indicate whether it will have a static or DHCP-assigned IP address. If it will be static, specify the gateway address and network mask, as was done previously for Port A.

1. Note that DHCP *may* be used to configure Port A, provided that the dynamically assigned IP address is reserved by the DHCP server.

Note: If Port B is set to DHCP to facilitate Internet connectivity, do not specify DNS or a Gateway for Port A.

8 If either Port A or Port B uses a static IP address, enter one or more space-separated IP address(es) of the Domain Name System (DNS) server(s) to be used.

Note: When using DHCP servers to assign IP addresses to both Port A and Port B, you do not need to enter a DNS Server. Doing so could result in an invalid network configuration that causes the Setup Assistant, the Network Wizard, or both, to become unresponsive during the Reset Network Interfaces action described later.

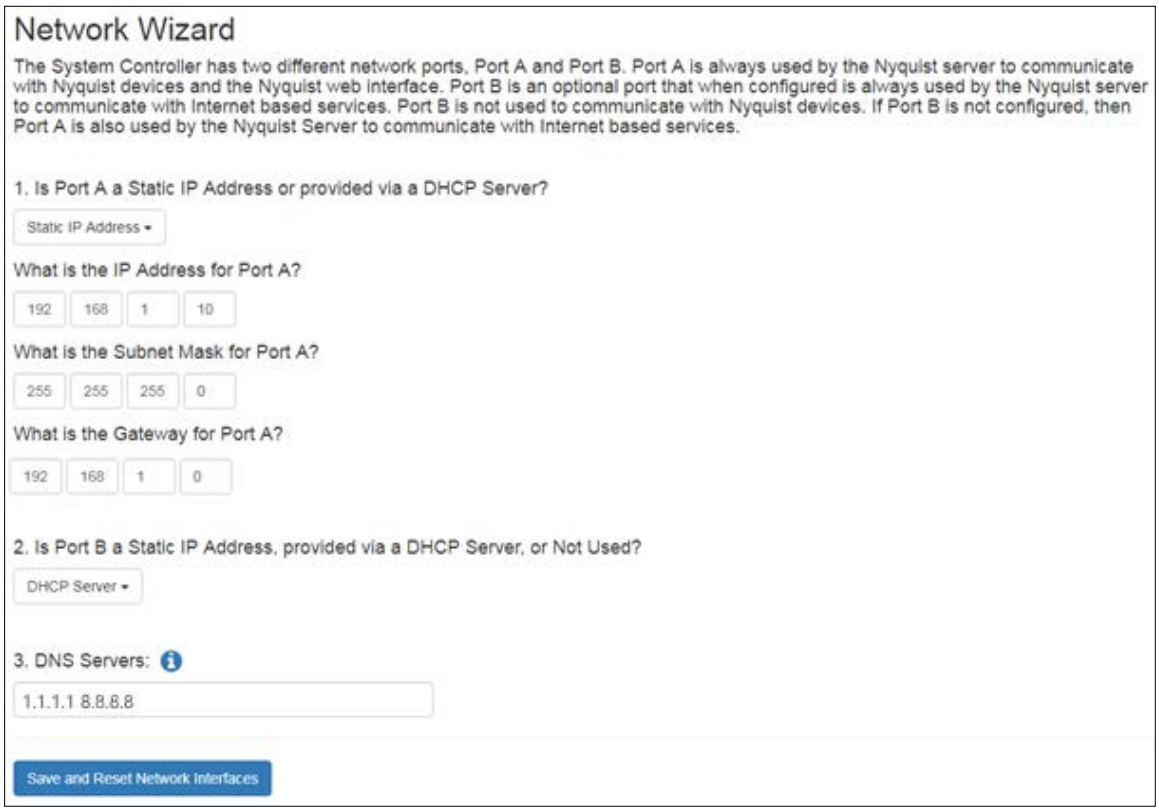


Figure 5. Example of Completed Network Wizard

9 Before continuing, be prepared to make any necessary changes to the network cables, as you will only have two minutes to make these changes (e.g., if you were unable to use 192.168.1.10 on Port A and were temporarily using Port B to reconfigure Port A, you would need to connect Port A).

When you are ready, click **Save and Reset Network Interfaces** to display the Reset Network Interfaces screen. If prompted, enter the Nyquist System Controller's serial number, which can be found

on the bottom of the System Controller (see *Figure 6, "Enter Serial Number," on page 12*), then make any required cable changes, as needed.

Figure 6. Enter Serial Number

Reset Network Interfaces

The Network Wizard displays two countdown timers, as shown in Figure 7, Reset Network Interfaces. The first timer represents the two minutes provided to make any required network cable changes. The second timer represents the total time needed by the Network Wizard's reset operation.

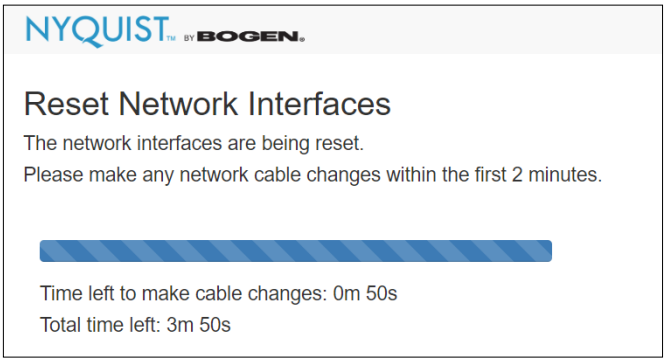


Figure 7. Reset Network Interfaces

Note the **Total time left** and wait at least that long for the reset operation to complete and display the configurations, as shown in Figure 8, Configured Network Interfaces.

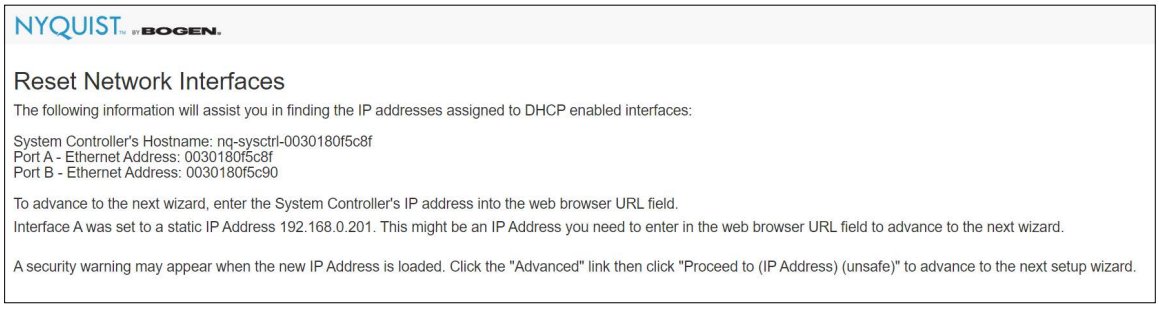


Figure 8. Configured Network Interfaces

10 Once the reset finishes, use the browser to visit the IP address assigned to the System Controller from the Port A network.

Tip: To revisit the Network Wizard at a later time (e.g., when changing the Nyquist server's IP address), navigate to:

http://<server>/setup/network

License Wizard

11 The Nyquist system launches the *License Wizard* screen, which shows the network configuration for Port A and (if used) Port B. See *Figure 9, "License Wizard," on page 13*.

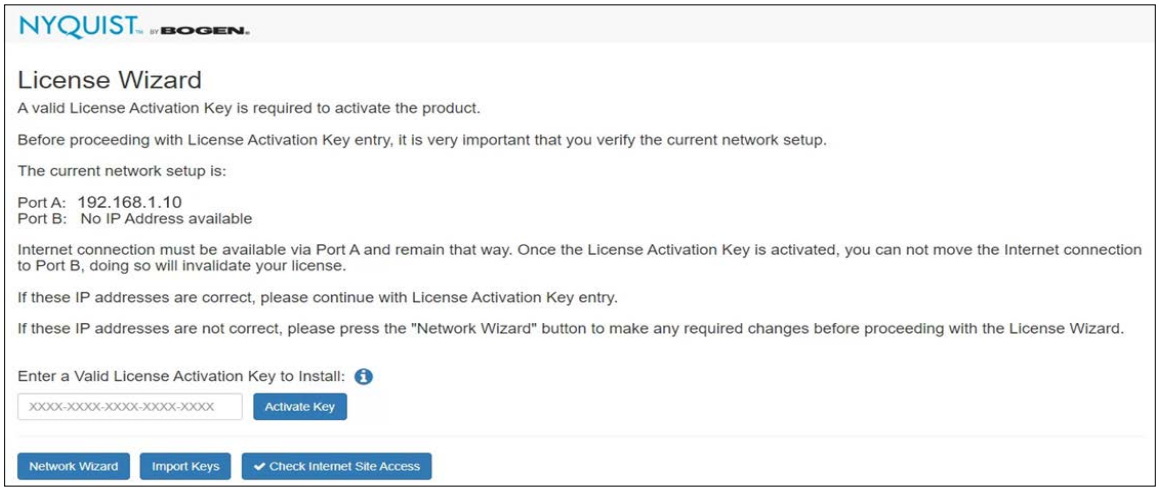
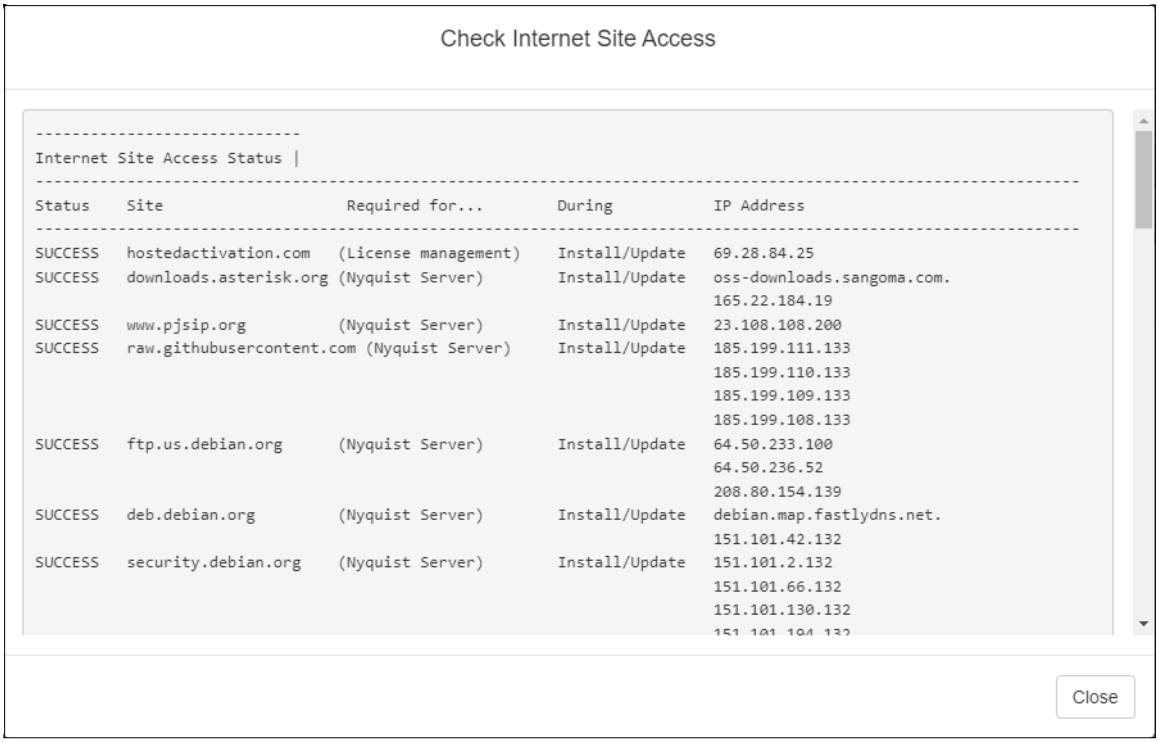


Figure 9. License Wizard

Verify that the network setup is correct before continuing. If the displayed IP addresses are incorrect, click **Network Wizard** at the bottom of the page to go back and make any required changes before proceeding with the License Wizard.

12 Click the **Check Internet Site Access** button and verify that all listed sites have a status of SUCCESS. If one or more sites failed, work with your IT department to verify that the Nyquist system has an

Internet connection; there are no firewall, DNS, or gateway settings preventing connectivity; and all white-listed web addresses are accessible from the Nyquist system's network port.



13 Enter the product **License Activation Key** (LAK) for your system into the **Enter a Valid License Activation Key to Install** field and press **Activate Key**.

For the E7000, the key format is xxxx-xxxx-xxxx-xxxx. For the C4000, the key format is **PC**xx-xxxx-xxxx-xxxx-xxxx. Letters must be entered in uppercase. (All "0" characters in the license string are the digit, zero.)

Important: If the LAK is already in use on a System Controller that is being replaced, the LAK must first be released from the previous System Controller. If the LAK was not released, contact Bogen Technical Support to request that the LAK be released before using it on the replacement System Controller.

---

14 If you are replacing an existing System Controller running Nyquist C4000 software with a new one, you can use the **Import Keys** button to import any license keys that were exported from the previously configured System Controller.

15 For the C4000, repeat the previous step(s) to install any additional feature or option License Activation Keys (format **FC**xx-xxxx-xxxx-xxxx-xxxx) that you may have purchased. You can add as many

feature or option License Activation Keys as needed. Each one appears in the installed window following its activation (*Figure 10*).

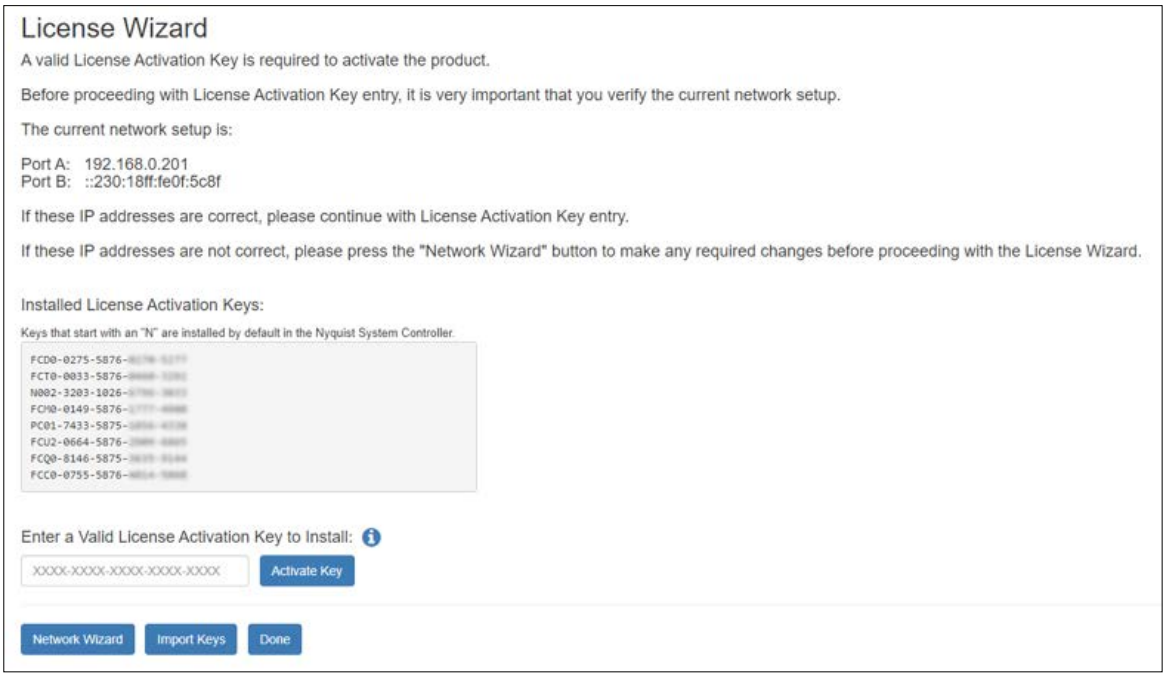


Figure 10. C4000 Feature/Option License Activation Keys

You can also enter C4000 License Activation Keys for features or options through the Admin Web UI after the initial installation. For more information about entering keys through the Admin Web UI at any time after the initial system setup process is complete and for feature License Activation Keys descriptions, see the C4000 *Nyquist System Administrator Guide*.

Important: For each License Activation Key, do not close the browser or the *License Wizard* screen until the activation process completes. .

---

16 Once all licenses have been imported and/or activated, press the **Done** button to proceed.

17 The End User License Agreement (EULA) appears next in a pop-up window (*Figure 11, "End User License Agreement," on page 16*).

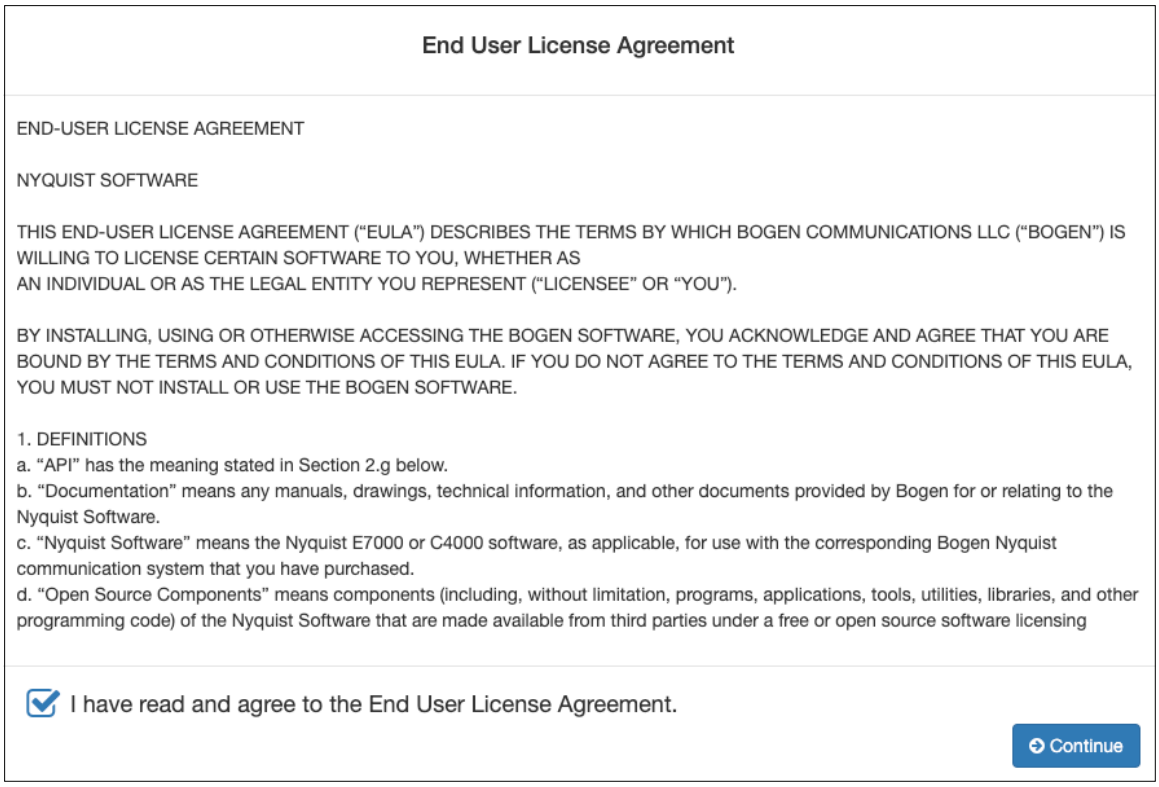


Figure 11. End User License Agreement

After reading the EULA, check the box to indicate that you have read and agree to the license, then click **Continue** to complete the License Wizard.

The product key(s) are now listed under Installed License Activation Keys. For the C4000, this includes a Node-Locked License Activation Key, which is preinstalled at the factory on all C4000 System Controllers.

18 After entering all License Activation Keys, select **Done**. The *Product Activation* screen appears (*Figure 12, "Product Activation (C4000 and E7000)"*).

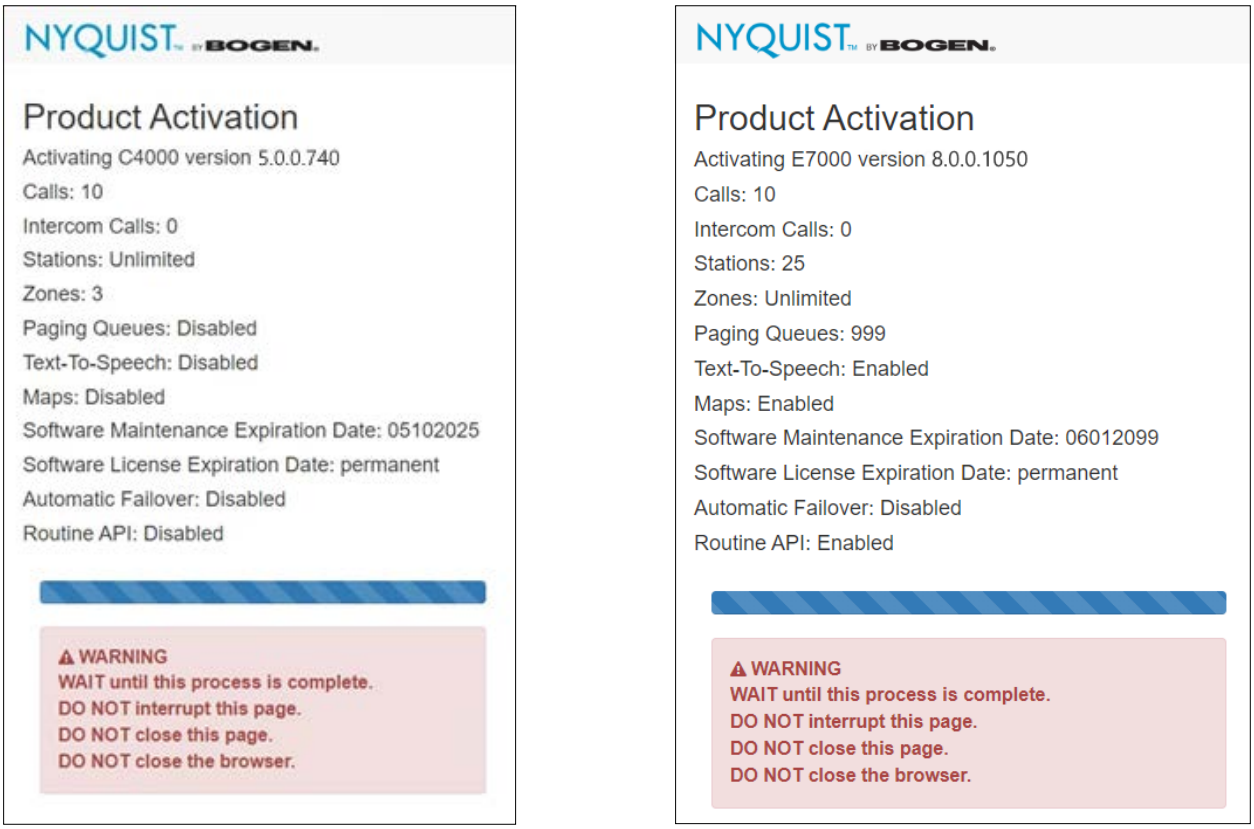


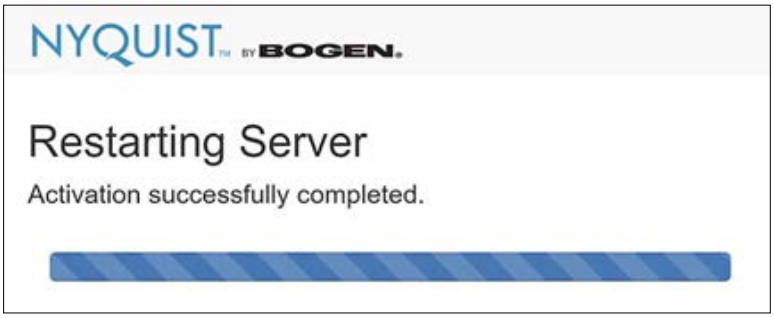
Figure 12. Product Activation (C4000 and E7000)

This screen provides information about the software and features that are being activated.

Note: Do not interrupt or close the *Product Activation* screen.

Restarting the Server

After activation has been completed, the System Controller will restart.



Customer Information Wizard

1 The *Customer Information Wizard* screen launches to collect product registration information for warranty purposes and to activate the system's Software Update Subscription (SUS). (See *Figure 1, "Customer Information Wizard," on page 18*.)

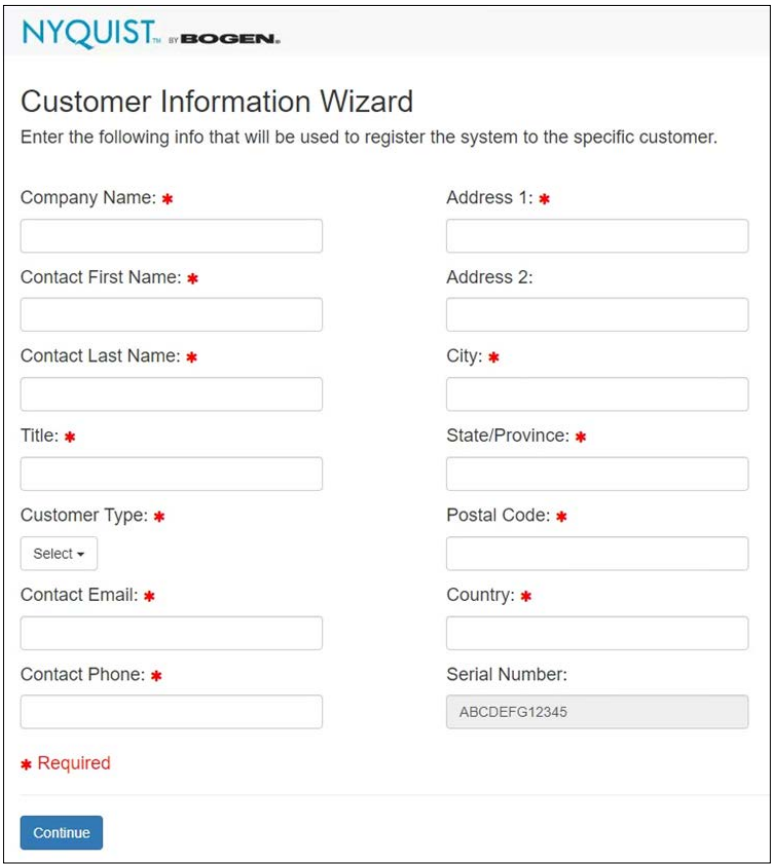


Figure 1. Customer Information Wizard

Complete the form and click **Continue**.

Dialing Length Wizard

If you already know how to configure a Nyquist system and want to skip the wizards, click **Expert Setup**, which takes you directly to the Nyquist system's Login screen and will not redirect you back to any of the wizards.

Note: If you select **Expert Setup** and have not set a new password, you will need to enter the default username, **admin**, and the default password, **bogen**, to log into the system. Login credentials are case sensitive.

After completing Expert Setup, you must manually complete system configuration using the Admin Web UI (see the *Nyquist System Administrator Guide*).

2 On the *Dialing Length Wizard* screen, set the dialing length (number of digits) used by stations in your system.

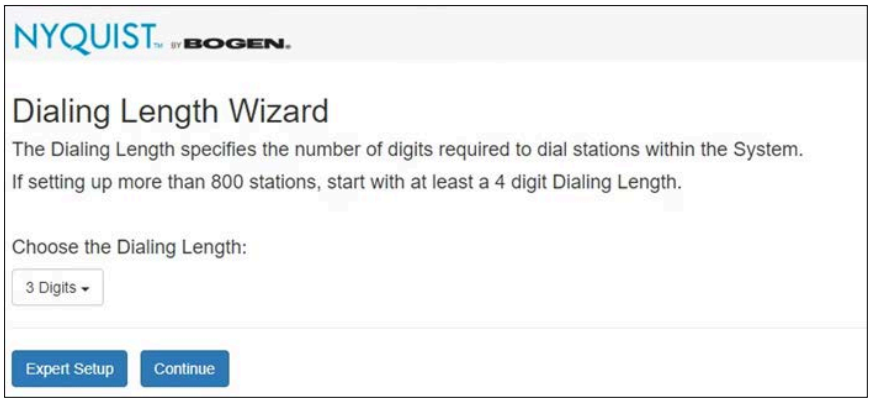


Figure 2. Dialing Length Wizard

Click **Continue** to advance to the next wizard.

Station Wizard

3 On the *Station Wizard* screen, create the Admin Web UI station by entering the Extension and Name for this station. You can enter any value that does not start with a nine (9).

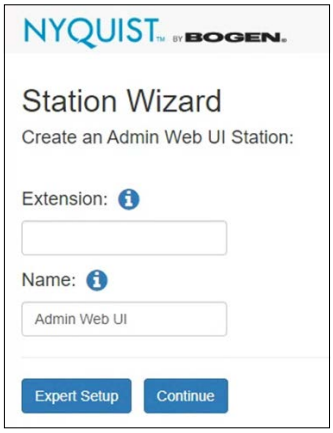


Figure 3. Station Wizard

Click **Continue** to advance to the next wizard.

User Wizard

Important: The User Wizard specifies the administrative password for the System Controller. We recommend that you create a strong password, click **Show** to verify the entered password, and store the password in a secure location (e.g., a trusted password manager application).

4 On the *User Wizard* screen, type an updated password for the Admin Web user.

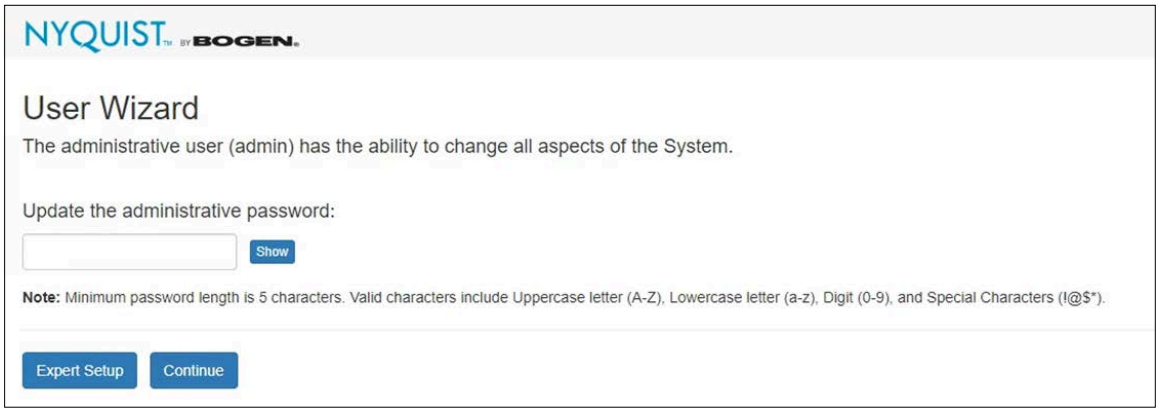


Figure 4. User Wizard

Click **Continue** to advance to the next wizard.

Time Zone Wizard

5 On the *Time Zone Wizard* screen, set the time zone to be used by your system.

Figure 5. Time Zone Wizard

Click **Continue** to advance to the next wizard.

Network Time Server Wizard

6 On the *Network Time Server Wizard* screen, specify the Network Time Server—also known as a Network Time Protocol (NTP) server—to be used by the Nyquist server.

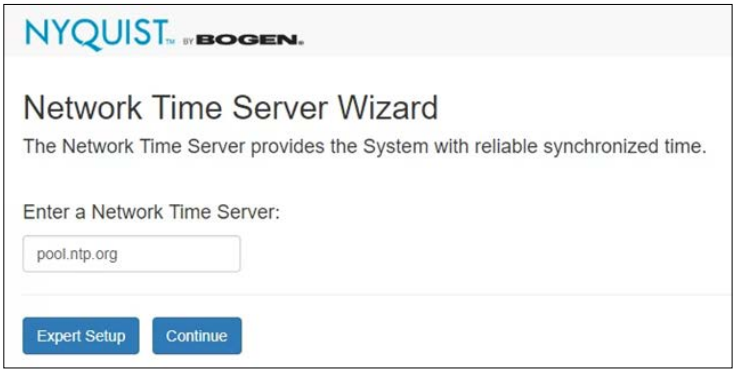


Figure 6. Network Time Server Wizard

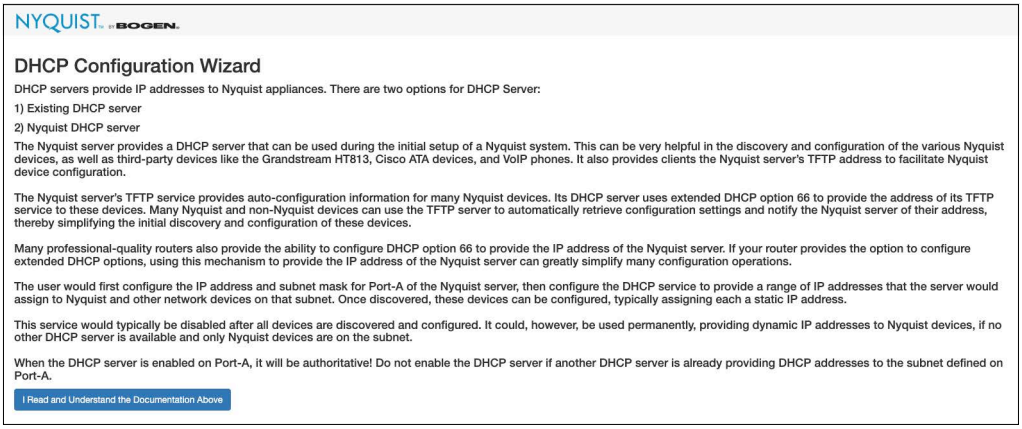
Click **Continue** to advance to the next wizard.

Note: Keep in mind that your Nyquist server must be able to reach the Network Time Server that you specify. If you specify an Internet-based server (e.g., pool.ntp.org, time.google.com), you may need to update your network routers' whitelist tables to allow the network traffic.

If you are not keeping your Nyquist system connected to the Internet, you should attempt to use a Network Time Server that is available on your private network; your network router may provide a Network Time Service. Consult your local Information Technology (IT) team for advice.

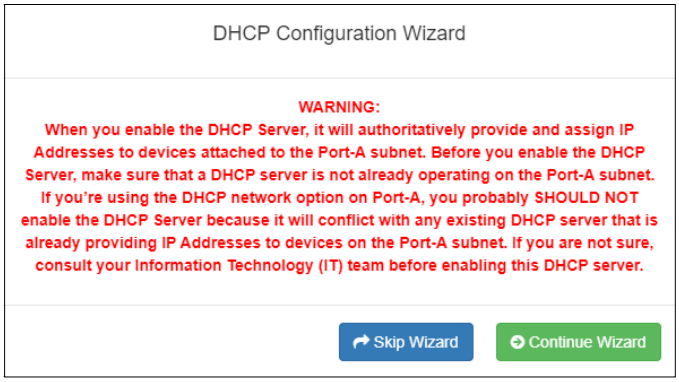
DHCP Wizard

7 The first page of the *DHCP Configuration Wizard* screen describes how to best use DHCP, DHCP option 66, and the Nyquist TFTP server for discovery and configuration of Nyquist appliances. It also explains that the Nyquist server's DHCP service should not be used if there is already an existing DHCP server on the Nyquist server's Port-A subnet.



Click **I Read and Understand the Documentation Above** to continue.

8 A warning message will be displayed explaining the risks of enabling the Nyquist DHCP Server when there is another DHCP server operating on the local subnet.



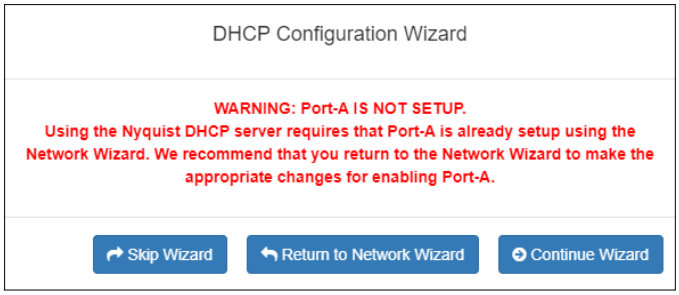
If you do *not* already have a DHCP server on your subnet and would like to use the Nyquist DHCP feature, select **Continue Wizard** and proceed to configure Nyquist's DHCP server. If you already have a DHCP server, select **Skip Wizard** and advance to the next wizard.

Tip: The Nyquist server's TFTP service provides autoconfiguration information for many Nyquist devices. Many Nyquist and non-Nyquist devices can use the TFTP service to automatically retrieve configuration settings and notify the Nyquist controller of their address, thereby simplifying the initial discovery and configuration of these devices.

If you choose to use a different DHCP server during the device discovery process, many professional-grade routers allow you to configure extended DHCP option 66 to provide the IP address of the Nyquist server. This mechanism can greatly simplify many configuration operations.

Caution Configuring any address *other* than the Nyquist server for DHCP option 66 will cause problems with device discovery and autoconfiguration.

If Port-A has not been properly setup, you will be warned and asked whether you want to skip the *DHCP Configuration Wizard*, continue it, or return to the *Network Wizard* to configure Port-A. If you skip the DHCP wizard, DHCP will *not* be activated on the Nyquist server.



Caution Only execute the *Network Wizard* if your system is using the Nyquist System Controller (NQ-SYSCTRL) device. Executing it on a custom server can result in unpredictable behavior.

9 On the *DHCP Configuration Wizard* screen, configure the Nyquist DHCP server settings, as described in *Table 1, "DHCP Wizard settings," on page 23*.

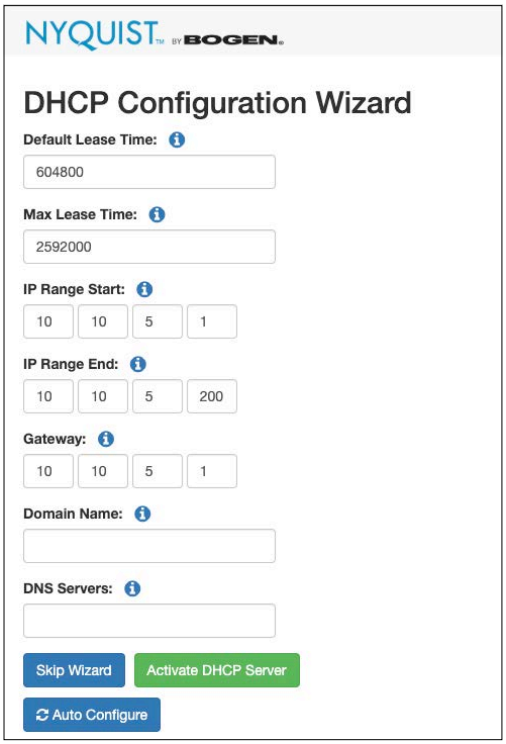


Figure 7. DHCP Wizard

Table 1. DHCP Wizard settings

Default Lease Time	Length in seconds that will be assigned to a lease if the client does not request a specific expiration time. Decrease this value if you are only using the DHCP server to stage Nyquist devices.
Max Lease Time	Maximum length in seconds that will be assigned to a lease. Decrease this value if you are only using the DHCP server to stage Nyquist devices.
IP Range Start	Start of the IP address range from which to allocate addresses to devices on the Port-A subnet. After performing Auto Configure, you can increase this value to reserve a range of IP addresses on the subnet for fixed address assignments.
IP Range End	End of the IP address range from which to allocate addresses to devices on the Port-A subnet. After performing Auto Configure, you can decrease this value to reserve a range of IP addresses on the subnet for fixed address assignments.
Gateway	Gateway address sent to DHCP clients used for routing packets outside of the Port-A subnet. Auto Configure will set this value based on the current Port-A setup; you can still change it if needed. *Note:* If you are setting up the Nyquist DHCP server to provide IP Addresses and TFTP Server IP Address to Nyquist appliances, the Gateway IP address must be set to the Nyquist server's IP address; if you leave it blank, paging and audio distribution will not function. If you're using the Automatic Failover feature, the Gateway address must be set to the Master IP Address.

Table 1. DHCP Wizard settings (Continued)

Domain Name	Domain name for devices operating on the subnet, excluding hostname. Leave this parameter blank if the Port-A subnet is private and not included in DNS managed domain. If the server has a domain name set, Auto Configure will use the server value. This is typically left blank.
DNS Servers	Comma-delimited list of DNS servers that devices on the subnet can use to resolve hostnames. Auto Configure will set this value; you can change it if needed.
Skip Wizard	Skip the DHCP Wizard and do not active the Nyquist DHCP service.
Activate DHCP Server	Saves the specified DHCP configuration and activate the Nyquist DHCP server.
Auto Configure	This button selects appropriate DHCP configuration values based on the existing server configuration. These values can be modified by the user before saving the settings. *Note:* These values will not be saved until the user clicks the **Activate DHCP Server** button.

10 Select **Auto Configure** to generate appropriate DHCP configuration values, then customize the generated values as needed.

11 After all DHCP settings have been configured, select **Activate DHCP Server** to activate the DHCP service and advance to the *Zone Wizard*.

Appliance Discovery Wizard

12 The Nyquist Appliance Discovery and Network Settings Configuration Wizard first displays a popup that asks if discovered Nyquist appliances will receive their IP addresses from a network DHCP server, whether from this System Controller or a network DHCP server.

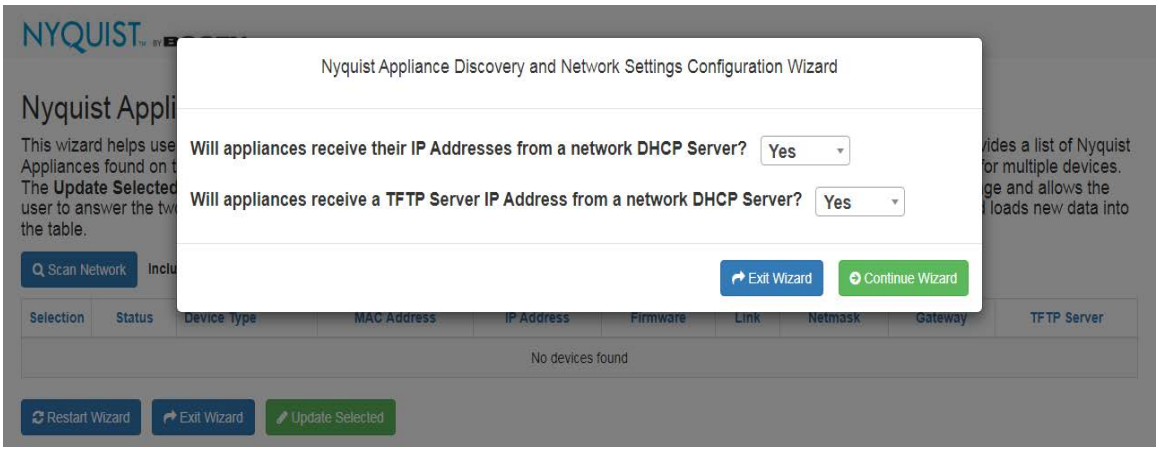


Figure 8. Network Appliance Discovery and Network Settings Configuration Wizard (start)

If so, select **Yes** and indicate if they will also receive the TFTP server address from the DHCP server, otherwise select **No**. Select **Yes** if the DHCP server will publish the System Controller's IP address via DHCP option 66, otherwise select **No**.

13 The Nyquist Appliance Discovery and Network Settings Configuration Wizard page automatically scans the Port-A network and displays all Nyquist appliances discovered.

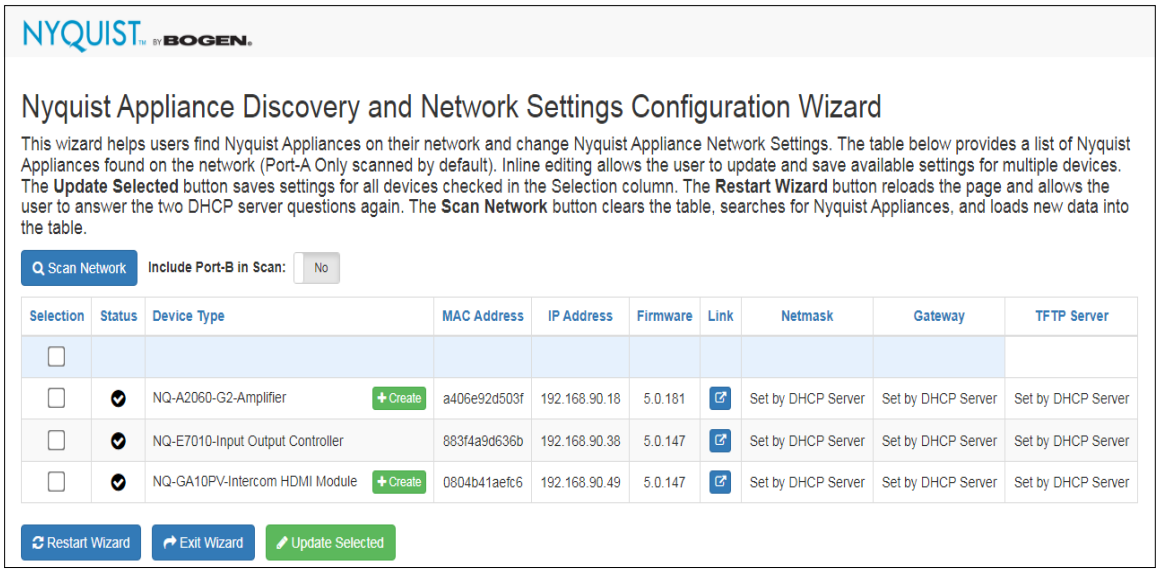


Figure 9. Network Appliance Discovery and Network Settings Configuration Wizard (appliances)

14 If you would like to search the Port-B network in addition to the Port-A network, set **Include Port-B in Scan** to **Yes** and select **Scan Network** to reinitiate the network scan. All Nyquist appliances found will be displayed.

15 If you would like to login to an appliance's web interface, select the **Link** button for that appliance.

16 Select any appliances to be reconfigured and select **Update Selected**.

Note: Updating an appliance changes its network configuration; it does not add a corresponding station for the appliance. If available, a **Create** button will be displayed next to the appliance's **Device Type** which opens the **Add Station** screen for the appliance.

---

17 When ready, select **Skip Wizard** to continue to the next wizard.

Tip: The Appliance Discovery Wizard can be initiated at any time to discover and configure new appliances by browsing to:

https://<server>/setup/discovery

Zone Wizard

The number of zones that you can create for a C4000 depends upon your product license. Regardless of what size system license was purchased, however, the Zone Wizard will only assist in creating a maximum of 20 zones. (Additional zones, if desired and licensed, can be added via the Admin Web UI after

the initial setup is complete.) If you have purchased 20 or fewer zones, the system will automatically generate the zones.

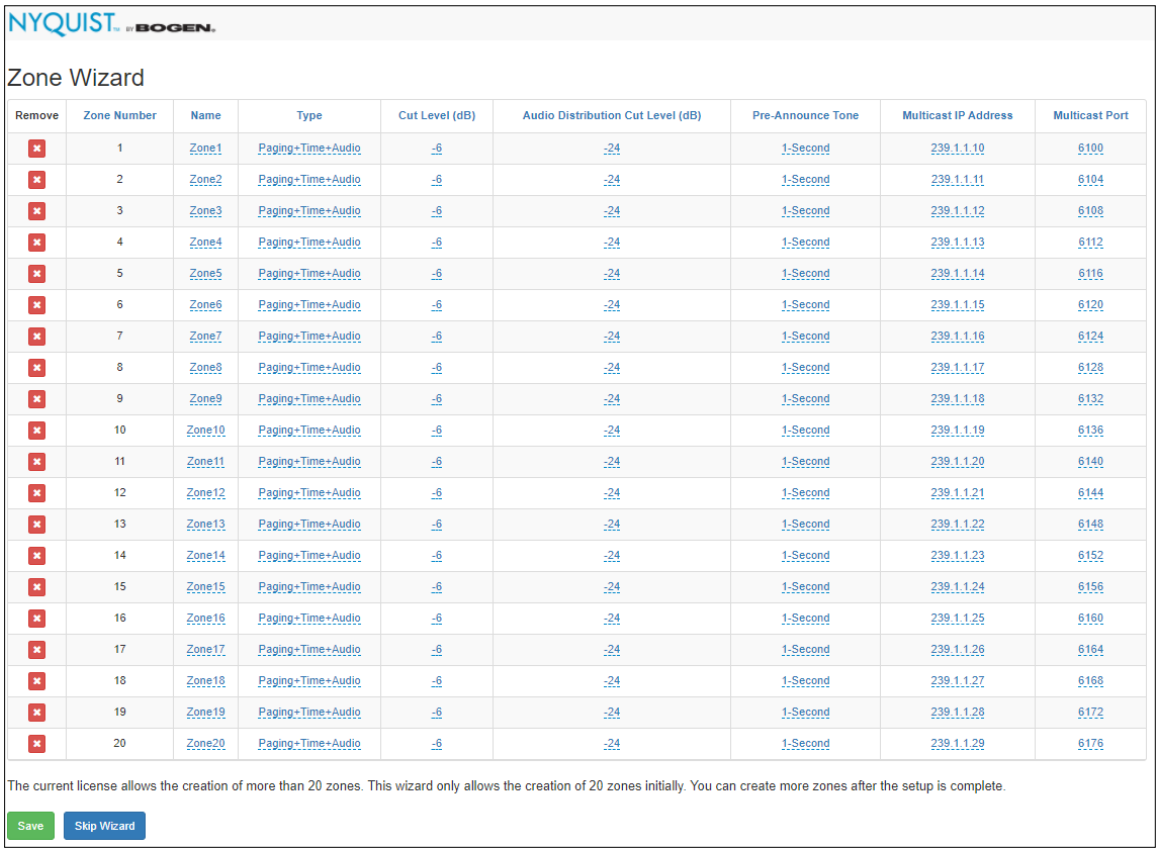


Figure 10. Zone Wizard

18 You can delete an automatically generated zone by selecting the red X next to the zone you want to delete.

You can make edits to a zone by selecting the hyperlink of any zone parameter (except for the Zone Number).

Table 2. Zone Wizard settings

Name	Identifies the zone by the user-created name. The name can be alphanumeric (such as "Bldg 1") and contain up to 30 characters.
Type	Identifies the zone as being able to receive paging, time, audio, or a combination of paging, time, or audio.
Cut Level (dB)	Sets the volume cut level for announcements. The volume cut level can range from 0 to −42 dB. The default level is −6 dB.
Audio Distribution Cut Level (dB)	Sets the volume cut level for audio distribution playing to stations in the zone. The cut level can range from 0 to −42 dB. The default value is −24 dB.
Pre-Announce Tone	Identifies what, if any, tone should play before an announcement.
Multicast IP Address	Identifies the IP address for multicast calls to the zone.
Multicast Port Number	Identifies the port number for multicast calls to the zone.

For some parameters (Type and Pre-Announce Tone), you can select from the drop-down menu that appears; for others, select the value, enter a new value, and select the check box when done.

Or, you can select **Skip Wizard** and create your zones later through the Admin Web UI.

19 After all zones are created, click **Save** to advance to the *Setup Wizards Complete* screen.

Setup Wizards Complete

20 With all setup wizards completed, click **Continue** to go to the *Nyquist Login* screen.

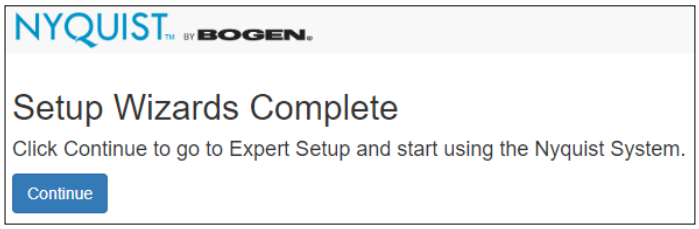


Figure 11. Setup Wizards Complete

Adjusting Final Network Configuration Settings

If you used a temporary network configuration for the setup of the Nyquist server, you should now configure the server to use the permanent configuration.

Open the Network Wizard by entering the following URL in the browser's address bar:

http://<server>/setup/network

Configure the permanent DHCP server, IP address, network ports, DNS setting, and/or other settings.

To modify the Nyquist DHCP settings, open the DHCP Configuration Wizard by entering the following URL in the browser's address bar:

http://<server>/setup/dhcp

Note: You may need to re-enter a new IP address into your browser's address bar to reconnect to the Nyquist server once the settings have been applied.

The Appliance Discovery Wizard can be initiated at any time to discover and configure new appliances by browsing to:

https://<server>/setup/discovery

Logging into the Nyquist Server

Before you can log into the Nyquist server, you must first install the Bogen Certificate Authority (CA), which will allow your browser to recognize the Nyquist server as a trusted server.

For details on how to install the Bogen CA, see *"Bogen Digital Certification Authority" on page 33*.

Once the Bogen CA has been installed, navigate to:

https://<server>

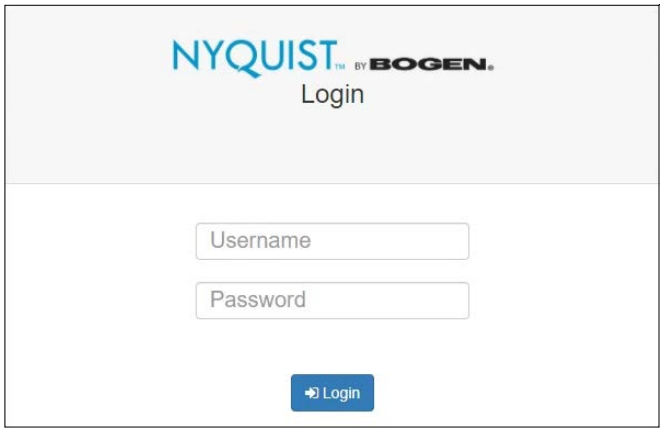


Figure 12. Nyquist System Controller Login

The first time you log in to the server, enter a username of `admin` and the administrative password specified in the User Wizard. If you skipped the User Wizard, the default password is `bogen`.

Update Server Software

Although not required, it is strongly recommended to check for software updates for the Nyquist server.

To check the current version number of the Nyquist server, select **About** from the hamburger menu in the top-right corner of the admin page. The version will be shown at the top of the page.

Note: Updating Nyquist server software will also install the latest firmware for the Nyquist appliances.

Best Practices

This section details recommendations and best practices to use when:

- Updating the Nyquist system server software to a new software release
- Updating Nyquist appliance firmware (software stored on the appliance)
- Using System Backups

Tip: Whenever configuration changes are made, we recommend performing a System Backup and using Export to save a copy of the backup on your local computer.

Note: Before configuring or using any Nyquist appliances, you must ensure that the appliance firmware is updated to the latest release. The latest Nyquist firmware release can also be downloaded directly (as a .tar.gz file) from the appropriate Bogen website:

E7000: https://www.bogen.com/dealers

C4000: https://www.bogen.com/c4000-resources

Updating Nyquist Software

Note: Before beginning the install process, make sure that your Nyquist system server can access the required URLs or web sites (see *"Whitelisted Web Addresses" on page 1*) from a supported browser.

New Nyquist server software may include patches to address known issues or new releases that provide additional features.

When updating to a new Nyquist server software release, use the Admin Web UI to perform a system update unless directed by technical support. Performing a system update ensures that all configuration data, call detail records, recordings, voice mail, and all upload announcements, alarms, tones, and songs are retained and are available after the system software update.

To check the current version number of the Nyquist server, select **About** from the hamburger menu in the top-right corner of the admin page. The version will be shown at the top of the page.

To perform a system update:

1. On the navigation bar, select **System Backup/Restore**.
2. Select **Create Backup** to perform a **System** backup and use the **Export** feature to save a copy of the system backup to your local computer. You may also want to create backups of **Recordings** and **Voicemail** and export them.
3. From the navigation bar, select **System Parameters**.
4. From the **System Parameters** page, select **System Update.**
5. If the System Controller is connected to the Internet, click the **Check for System Updates** button to

search for and download the latest system update. (This may take some time, depending on your internet connection speed.)

> Some Nyquist system updates are only available by downloading them directly from a Bogen website:
>
> **E7000:** https://www.bogen.com/dealers
>
> **C4000:** https://www.bogen.com/c4000-resources.
>
> The system update file will typically be named `nyquist-c4000-<version>.tar.gz` or `nyquist-e7000-<version>.tar.gz`. After downloading the file to your local computer via a browser, the file can be uploaded to the Nyquist server via the **Upload** button of the **System Update** page.

6 It is *very important* to read the Release Notes, which can be displayed by clicking the blue button. They often contain critical information regarding the upgrade process.

Tip: Copying the notes to a word processor allows you to view the notes during the installation process and may be easier to read.

7 Install the latest version available for the Nyquist server, carefully following relevant instructions from the Release Notes.

Warning Be aware that a system update can sometimes take several minutes, during which time the device should *never* be powered down or interrupted.

8 Once the update has completed, we recommend regenerating the System Controller's server certificate. From the **System Parameters** page, select the **Edit** button, then select the **Generate Server Certificate** button.

For a more detailed explanation, see *Performing a System Update* in the *Nyquist System Administrator Guide*.

Perform the server system update process before updating Nyquist appliance software.

Assigning Permissions for New Features

After you have finished updating the Nyquist software, permissions for features introduced by this new release must be set for the roles that will use these features.

To assign permissions for these new features:

1 On the navigation bar, select **Roles**.

2 On the **Roles** page, select the **Permissions** icon next to the role for which you want to edit permissions.

3 On the **Edit Permissions** page, make desired changes.

4 Select **Save**.

For more information, refer to the *Nyquist System Administrator Guide*.

Updating Appliance Firmware

Note: Before beginning the install process, make sure that your Nyquist system server can access the required URLs or web sites (see *"Whitelisted Web Addresses" on page 1*) using the Nyquist Admin Web UI.

The firmware for all devices used with the Nyquist system must be compatible with the software installed on the Nyquist System Controller, and all Nyquist appliances in a given installation should be configured to run the same firmware version.

The latest Nyquist appliance firmware release can also be downloaded directly (as a `.tar.gz` file) from the appropriate Bogen website:

E7000: https://www.bogen.com/dealers

C4000: https://www.bogen.com/c4000-resources.

The Nyquist appliance firmware will be named `NyqUpdate-<version>.tar.gz`.

Firmware can be updated for Nyquist appliances and Analog Station Bridge (ASB) devices through the Admin Web UI or through the appliance's web UI. For information about the appliance's web UI, refer to the device's configuration guide.

Using the Nyquist Admin Web UI via the **Firmware** page, you can upload a firmware file to the Nyquist system server, download firmware to an appliance or ASB, view a list of appliances and stations and ASBs that are linked to a firmware name, set default firmware for any stations and bridge devices to be added, and delete firmware entries.

To perform an appliance firmware update:

1. On the navigation bar, select **Firmware**.
2. Click the Check for Updates button to search for and download the latest device firmware update.

> Some Nyquist firmware updates are only available by downloading them directly from a Bogen website:
>
> **E7000:** https://www.bogen.com/dealers
>
> **C4000:** https://www.bogen.com/c4000-resources.
>
> The firmware update file will typically be named `NyqUpdate-<version>.tar.gz`. After downloading the file to your local computer via a browser, the file can be uploaded to the Nyquist server via the **Upload** button of the **Firmware** page.

3. It is *very important* to read the Release Notes, which can be displayed by clicking the blue button. They often contain critical information regarding the upgrade process.

Tip: Copying the notes to a word processor allows you to view the notes during the installation process and may be easier to read.

4. To define this update as the default for all Nyquist appliances, select the **Set as Default Firmware** button for this update.

5 To add or edit a custom note for this update, select the **Edit** button for this update, modify the Notes field, and click **Save**.

6 To apply the update to one or more appliances, select the **Device Selection** button, select one or more devices, and select the **Update** button.

Warning Be aware that a firmware update can sometimes take several minutes, during which time the device should *never* be powered down or interrupted.

For a more detailed explanation, see *Configuring Appliance Firmware* in the *Nyquist System Administrator Guide*.

Appendix A: Bogen Digital Certification Authority

When a client (e.g., a web browser) connects to the Bogen device's web application, the device's digital certificate is sent to the client to authenticate the identity of the device's web application. The client uses the Bogen Certification Authority (CA) certificate to authenticate the device's digital certificate, which verifies that the client is connecting to a valid server. If the Bogen CA certificate is not installed on the client, the browser will display a warning that it was unable to authenticate the server, displaying a red *Not secure* warning immediately to the left of the browser's address bar (or a similar warning, depending on the browser) after it attempts to access the Bogen device.

The following sections provide instructions for downloading and installing the Bogen CA in various environments.

Tip: The Bogen CA can be downloaded using the cURL command instead of via the browser. If you prefer that method, issue the following command in lieu of step 1 of the subsequent installation instructions:

```
curl.exe --insecure https://<device>/ssl/bogenCA.crt > bogenCA.crt
```

Installing Certification Authority on Windows System

To download and install the Certification Authority on a Windows device:

1. From your Chrome or Edge browser, type `http://<device>/ssl/bogenCA.crt` in the address bar, where `<device>` is the Nyquist device's IP address or DNS name (for example, `http://192.168.1.0/ssl/bogenCA.crt`).
2. Select the downloaded file and select **Open**.
3. Select Open when prompted with "Do you want to open this file?"
4. Select the **Install Certificate...** button. The Certificate Import Wizard starts.
5. Select **Current User**, and then select **Next**.

Note: To allow *all* users on this Windows client to access the Nyquist device, select **Local Machine** instead of **Current User**. You may be prompted for administrator credentials.

---

6. Select "Place all certificates in the following store", then select **Browse**.
7. Select **Trusted Root Certification Authorities**, and then select **OK**.
8. Select **Next**.
9. Select **Finish**.
10. Restart the browser and log in to the device's web application.

Install Certificate Authority using PowerShell (optional)

You can optionally download and install the Certification Authority using a PowerShell command prompt or script, which involves fewer steps.

To download the certificate to a CRT file, execute the following PowerShell command, replacing `<device>` with the IP address or DNS name of the Nyquist device:

```
Invoke-WebRequest -Uri http://<device>/ssl/bogenCA.crt -OutFile $env:TEMP\bogenCA.crt
```

To optionally validate the certificate before importing it, execute the following command:

```
[Security.Cryptography.X509Certificates.X509Certificate2]::new(
 "$env:TEMP\bogenCA.crt").GetCertHashString() -eq '0A8248F69D970F8DD855D0E0592972DA64B1A845'
```

If the command returns True, the certificate is valid.

To install the CA certificate into the CurrentUser certificate store, which only applies to the current user, execute the following command:

```
Import-Certificate -CertStoreLocation cert:\CurrentUser\Root -FilePath $env:TEMP\bogenCA.crt
```

To install the certificate for all users on this machine, which requires administrator privileges to execute, execute the following command:

```
Import-Certificate -CertStoreLocation cert:\LocalMachine\Root -FilePath $env:TEMP\bogenCA.crt
```

Note: These commands can be executed remotely using PowerShell Remoting, which may be helpful if the certificate needs to be installed on many client machines.

Installing Certification Authority on Mac System

To download and install the Certification Authority on a Mac:

1. From your Safari browser, type `http://<device>/ssl/bogenCA.crt` in the address bar, where <device> is the Nyquist system device's IP address or DNS name (for example, `http://192.168.1.0/ssl/bogenCA.crt`).
2. Save the downloaded bogenCA.crt file to the desktop.
3. Double-click the certificate file on the desktop.
   The Keychain Access App opens.
4. Double-click the certificate to reveal the trust settings.
5. Change the top trust setting to **Always Trust**.
6. Close the Trust Setting window and enter the computer administrative password to save.
7. Restart the browser and log in to the Nyquist web application.

Installing Certification Authority on an Android Device

Note: The Android device WiFi must be connected to the same network as the Nyquist Server.

To download and install the Certification Authority on an Android device:

1. From your Chrome or Edge browser, type `http://<device>/ssl/bogenCA.crt` in the address bar, where <device> is the Nyquist device's IP address or DNS name (for example, `http://192.168.1.0/ssl/bogenCA.crt`).
2. If prompted, verify your identity (e.g., enter your PIN or fingerprint).
3. Type a certificate name (e.g., "Bogen CA"), specify "VPN and apps" under "Used for", and select **OK** to install the certificate.

Installing Certification Authority on an iOS Device

Note: The iOS device WiFi must be connected to the same network as the Nyquist Server.

To download and install the Certification Authority on an iPhone Operating System (iOS) device:

1. From your Safari browser, type `http://<device>/ssl/bogenCA.crt` in the address bar, where <device> is the Nyquist device's IP address (for example, `http://192.168.1.0/ssl/bogenCA.crt`).
2. Select **Go**.
3. Select **Allow** when prompted to allow the download.
4. Select **Close** after the notification that a profile was downloaded.
5. Select **Settings > General > VPN & Device Management**.
6. Select the **Bogen CA** certificate under **DOWNLOADED PROFILE**.
7. Select **Install**.
8. If prompted, enter your passcode.
9. On the **Warning** page, select **Install**.
10. Select **Done**.
11. Select **Settings > General > About > Certificate Trust Settings**.
12. Under **ENABLE FULL TRUST FOR ROOT CERTIFICATES**, enable the switch next to **Bogen CA**.

Viewing the Certificate

The following steps outline how to view and verify the TLS/SSL certificate that was provided by the Nyquist device.

Important: The user interfaces for browsers change not infrequently, so the exact details may vary from what is described in the following instructions. Some security packages can also affect the information available, such as antivirus software that injects its own CA certificate in lieu of the website's actual certificate, which has the effect of hiding the actual certificate from the user.

1. Browse to the Bogen device's web application in your browser (using Safari on iOS, Chrome or Edge on all other platforms).

2 Select the lock icon on the address bar of the browser (to the left of the URL).

3 Display the CA certificate by following one of the following steps:

   a) On the Chrome or Edge browser, select **Connection is secure**, then select either **Certificate is valid**, the certificate icon, or **Certificate information** to display the Certificate Viewer dialog. Select the Details tab, then Bogen CA in the Certificate Hierarchy section.

   b) On the Safari browser *[MacOS or iOS only]*, select **Show Certificate** in the window that appears.

   c) As an alternative on Android devices, select the Android system's **Settings > Biometrics and security > Other security settings >View security certificates**, select the **USER** tab, and select the Bogen certificate.

4 Verify that the Bogen CA certificate is selected and not the server certificate (the server certificate's name will be an IP address). To verify that the certificate is valid, verify that the displayed fingerprint values match the following:

SHA-1: 0A 82 48 F6 9D 97 0F 8D D8 55 D0 E0 59 29 72 DA 64 B1 A8 45
SHA-256: 6B D0 D5 8D C8 F7 E8 03 9E A3 F1 52 32 1D 9C 5C 58 8B 4E FA DF 03 43 64 34 C2 6C 63 C5 4A AC 46