



Analog Station Bridge Configuration Guide

NQ-E7030



BOGEN®

© 2018–2026 Bogen Communications LLC

All rights reserved

740-00015K

260507

Contents

- Contents i**
- Configuring the Nyquist Analog Station Bridge 1**
 - Using the Dashboard2
 - Updating Firmware6
 - Network Settings Tab Parameters7
 - Configuration Settings Tab Parameters10
 - Digital Call Switch Management.....11
 - Accessing Log Files13
 - Log Settings15
 - Status Reporting Settings.....16
- Appendix A: Bogen Digital Certification Authority 19**
 - Installing Certification Authority on Windows System19
 - Installing Certification Authority on Mac System20
 - Installing Certification Authority on an Android Device21
 - Installing Certification Authority on an iOS Device21
 - Viewing the Certificate21

Configuring the Nyquist Analog Station Bridge

The Nyquist Analog Station Bridge (ASB) allows the Nyquist solution to use the existing analog call switch and speaker infrastructure when upgrading from Multicom 2000, Quantum Multicom IP, or other compatible third-party intercom systems. When used exclusively as a networked component of the Nyquist paging and intercom solution, the Nyquist ASB permits a hybrid Internet Protocol (IP)/analog system configuration through the use of and connection to analog 25V speakers and associated analog call switches (for example, CA15C type). The ASB has 24 station connections that attach to wired 25V speakers and their associated call switches. While each connection has its own Session Initiation Protocol (SIP)–addressable Station ID, the ASB itself uses a single network IP address.

The Nyquist server can automatically discover and configure the ASB, but you can also manage the device, and manually configure some settings, through the ASB's web-based user interface (web UI).

A two-second press of the appliance's **Reset** button reboots the device. If you press the **Reset** button for 10 seconds, the appliance returns to the factory default configuration settings. Returning to the default configuration settings does not change the appliance's firmware.

The following sections describe the process for manual configuration. For information about using Nyquist's automatic configuration process, refer to the appropriate *Nyquist System Administrator Guide*.

Note: Do not use third-party browser extensions with the Nyquist user interface.

To access the appliance's Web-based user interface (UI):

- 1 Before accessing the web UI for the first time, the Bogen Certification Authority (CA) digital certificate must be installed on the client. This certificate can be downloaded from any Nyquist appliance and enables your browser to recognize the Nyquist web application as a trusted site.

For details on how to download and install the certificate to your client computers, see "*Bogen Digital Certification Authority*" on page 19.

- 2 Access the appliance's web UI by doing one of the following:
 - a) On your web browser, enter the IP address for the appliance as the URL.
 - b) From the Nyquist server's web UI navigation bar, select **Stations**, select **Stations Status** or **Appliance Status**, navigate to the device that you want to configure, and then select the **Link** icon.
 - c) From the Nyquist server's **Appliance Discovery Wizard**, select the **Link** icon for the device that you want to configure.

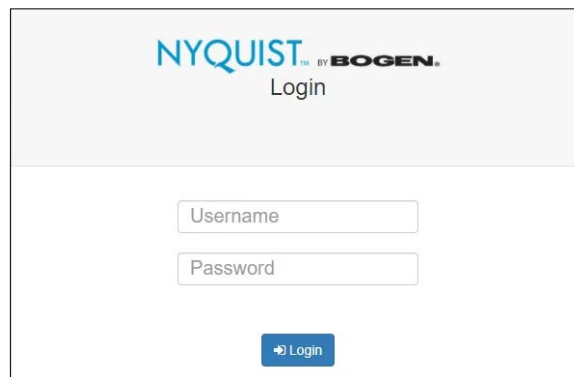
The image shows a web browser window displaying the login page for a Nyquist appliance. The header features the logo "NYQUIST™ BY BOGEN®" in blue and black text, with the word "Login" centered below it. The main content area contains two input fields: "Username" and "Password", both with light gray borders. Below these fields is a blue button with a white right-pointing arrow and the text "Login".

Figure 1. Nyquist Appliance Login

- 3 At the Nyquist appliance's Login page, enter username and password, then press enter or click on the **Login** button.

The default username is `admin`; the default password is `bogen`.

Note: After a successful login, a warning will be displayed if the default password is still in use. We strongly encourage changing the default password as soon as possible.

When you have logged in successfully, you will be presented with the dashboard for the appliance.

Using the Dashboard

The ASB dashboard displays information about the ASB, including LEDs and temperature output that provides status of the ASB. You can also make temporary adjustments to the ASB volume using a volume slider that appears at the bottom of the ASB dashboard. The volume can be adjusted on a scale from -42 dB to 0 dB.

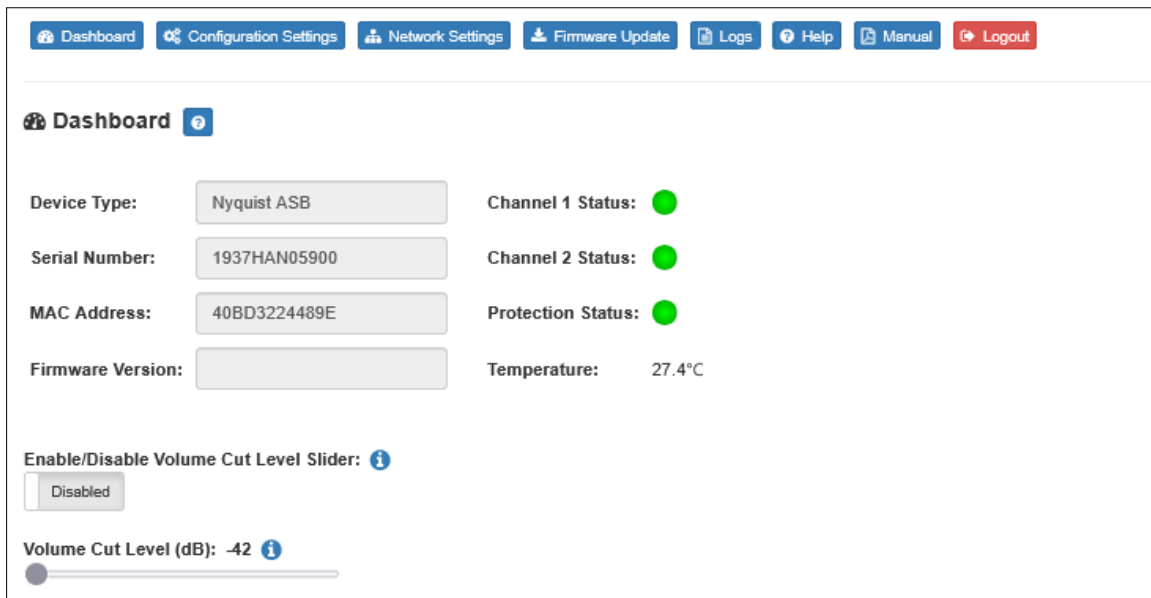


Figure 2. Nyquist Analog Station Bridge Dashboard

The dashboard displays the following fields:

Table 1. Appliance Dashboard Fields

Device Type	Displays the model of this device.
Serial Number	Displays the serial number for the device.
MAC Address	Displays the Media Access Control (MAC) address, which is a unique identifier assigned to network interfaces for communications on the physical network segment.
Firmware Version	Displays the firmware version installed on the station.

Real-time statuses that can be viewed from the dashboard are described in the following table:

Table 2. ASB Status Indicators

Channel 1/2 Status

Provides clipping status for **Channel 1** and **Channel 2**. Clipping is sound distortion that occurs when an amplifier attempts to deliver an output voltage or current that is beyond its maximum capability. If this indicator is green, the channel is not clipping. Red means the channel is clipping. Gray means that the appliance's web UI is not receiving data from the appliance's web server, indicating that the ASB may be offline or rebooting.

Protection Status

Indicates if the ASB is in partial shutdown mode to protect the built-in two-channel amplifier module.

In this case, the appliance itself may remain "on" as indicated by its front panel Status and Power LEDs. However, the ASB's amplifier module senses various faults that can be caused by factors such as incorrect speaker wiring (for example, shorts or too low an impedance). These faults can overload the amplifier output capability (overcurrent/clipping) and/or amplifier thermal conditions (overheating).

If the indicator is green, the amplifier module is operating in a normal capacity. If the indicator is red, the amplifier module is in protection mode and audio will not be passed to any ASB port. If the cause is temporary or intermittent (for example, signal clipping), the amplifier module will quickly return to normal mode.

If the system remains in protection mode for an extended period of time, this likely indicates some sort of wiring fault or low-impedance condition is present that must be rectified.

When the indicator is gray, the ASB's web UI is not receiving protection status information from the appliance's web server. This usually indicates that the network connection has been interrupted or dropped or that the device is rebooting.

Table 2. ASB Status Indicators (Continued)

Temperature	Provides a snapshot of the amplifier module's temperature in degrees Celsius during any transition (that is, change state) on the Channel 1, Channel 2, or Protection Status indicators. <i>Note:</i> The ASB's UI displays the temperature reading from the latest update; it does not receive or display continuous real-time amplifier module temperature readings.
Enable/Disable Volume Cut Level Slider	Enables or disables the Volume Cut Level slider.
Volume Cut Level	Sets the volume for the speaker during an intercom call or page. This is a temporary adjustment that allows the user to experiment with the loudness of the speaker. To make permanent adjustments, change the various cut level settings on the Nyquist server. The value can be adjusted between -42 dB and 0 dB.

The following buttons are available at the top of all pages in the application.

Table 3. Appliance Dashboard Buttons

Dashboard	Displays the dashboard.
Configuration Settings	Accesses the Configuration Settings page where you can view and set various options or select to receive configuration settings from a Nyquist server.
Network Settings	Accesses the Network Settings page where you can view and set network settings, such as the static IP address.
Firmware Update	Accesses the Firmware Update page where you can view the current Nyquist version, update firmware to a new version, restore the configuration to factory settings, and reboot the appliance.
Logs	Accesses log files, which record either events or messages that occur when software runs and are used when troubleshooting the appliance.
Help	Accesses the appliance's online help.
Manual	Displays the appliance's configuration manual.
Logout	Logs out of the appliance's dashboard.

Updating Firmware

When you select **Firmware Update** from the appliance's web UI, the Firmware Update page appears. From this page you can determine which Nyquist firmware version the appliance is using and if an update is available. You can also load a firmware release, install the loaded firmware, restore the configuration to factory defaults, and reboot the appliance.

Note: A Nyquist appliance connected to the Nyquist network receives a configuration file from the Nyquist server that includes the latest firmware available from the server. If the firmware is different from the one installed on the appliance, an automatic firmware update occurs unless the **Firmware** parameter for the station is left blank. Refer to the *Nyquist System Administrator Guide* for more information.



Note: Some buttons only appear on this page when applicable.

Figure 3. Firmware Update Page

To use the Firmware Update page:

- 1 On the appliance web UI's main page, select **Firmware Update** to view or update the firmware version.
 - If you already have a firmware file you would like to install to the appliance, select **Upload Firmware** to upload the firmware file from your computer to the appliance. A popup screen appears that allows you to select the file that you want to

upload. You can navigate to the file's location. After you select the file, select **Upload**.

The page displays the uploaded firmware version ("New Nyquist Version") and an **Update Firmware** button appears. Select this button if you want to update the appliance's firmware to the uploaded version.

- If you want to return your appliance to its original factory configuration, select **Restore Factory Settings**.
- Select **Reboot Appliance** to restart your appliance.

Table 4. Firmware Update settings

Current Nyquist Version	Shows the version of the appliance's currently installed firmware.
New Nyquist Version	Shows the version of the firmware that has been loaded, though not installed, onto the appliance.
Update Firmware	Available only when a new firmware version has been loaded onto the appliance (as specified in New Nyquist Version). Installs the loaded firmware. A reboot may be required after installation.
Upload Firmware	Prompts the user to specify a firmware file, which will then be loaded (though not installed) onto the appliance. <i>Note:</i> To obtain the firmware file for a specific version, please contact Bogen Technical Support.
Restore Factory Settings	Returns the appliance to its original factory configuration. <i>Note:</i> This does not install the original appliance firmware. The firmware will not be changed.
Reboot Appliance	Restarts the appliance.

Network Settings Tab Parameters

Network settings can be configured dynamically by the Nyquist server or manually by using the appliance's web UI.

To manually configure network settings:

- 1 On the appliance web UI's main page, select **Network Settings**.

- 2 Select your desired network settings.
- 3 Select **Save**.

 **Network Settings**

  Network Traffic Capture

IP Address:

192.168.90.18

Netmask:

255.255.255.0

Gateway:

192.168.90.1

VLAN ID:

VLAN Priority:

0 - Best Effort ▾

NTP Server:

192.168.90.10

TFTP Server:

192.168.90.10

TFTP Server from DHCP:

Yes ▾

DHCP Enabled:

Yes ▾

Reboot Appliance:

No ▾

 Save

Figure 4. Network Settings

Network settings are described in the following table:

Table 5. Network Settings

Network Traffic Capture	Captures network traffic on this appliance and saves it to a PCAP file that can be downloaded to the user’s computer. For details, see <i>Network Traffic Capture</i> in the Nyquist System Administrator Guide.
IP Address	Identifies the IP address assigned to the appliance.
Netmask	Identifies the subnetwork subdivision of an IP network.
Gateway	Identifies the address, or route, for the default gateway.

Table 5. Network Settings (Continued)

VLAN ID	Identifies the Virtual Local Area Network (VLAN) for this appliance. Values range from 0 to 4094.
VLAN Priority	Identifies the priority of the network traffic on the VLAN. Priority can range from 0 through 7.
NTP Server	Identifies the IP address or the domain name of the Network Time Protocol (NTP) Server.
TFTP Server	Identifies the host name or IP address of the Trivial File Transfer Protocol (TFTP) server. The specified TFTP server can be used to automatically set this device's Configuration settings via the Get Configuration from Server button. If TFTP Server from DHCP (see below) is set to "Yes", this value will be auto-configured via DHCP option 66, assuming the DHCP server has been configured to provide option 66. For details, see the documentation for your DHCP server. <i>Note:</i> A TFTP server runs on the Nyquist server on port 69 (the standard TFTP port) and the optional Nyquist DHCP service automatically provides this TFTP address via option 66. <i>Note:</i> If this value is unspecified, the TFTP Server from DHCP will automatically be set to "Yes", this field will become read-only, and DHCP will be used to configure this setting. To change this value, the TFTP Server from DHCP setting must be set to No, which makes the field editable.
TFTP Server from DHCP	Yes means the device will use the DHCP option 66 value to retrieve an address for the TFTP Server from DHCP. No means the device will ignore the DHCP option 66 value and use the manually configured value of the TFTP Server (see above).
DHCP Enabled	Indicates if the device is enabled to use DHCP to retrieve its IP configuration.
Reboot Appliance	Indicates that this appliance should reboot when the Save button is clicked.

Configuration Settings Tab Parameters

The easiest way to configure Nyquist appliances is to obtain configuration settings from the Nyquist server by selecting **Get Configuration From Server**.

To view the Nyquist appliance configuration:

- 1 On the appliance Web UI's main page, select **Configuration Settings**.
- 2 View the settings as described in Table 6, "Configuration Settings," on page 10 for normal configuration

Configuration Settings

Get Configuration From Server

Web Username:

admin

	IP Address	Port Number	Cut Level	Station List
Emergency-All-Call:	239.1.1.1	6000	-35	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23
All-Call:	239.1.1.3	6004	-33	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23
Audio Distribution:	239.1.1.2	6008	-31	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23
Multicast 1:	239.1.1.10	6100	-25	1

Nyquist Control Password

Save Password

Device Stations

Port Number	Port Type	Account Id	Local Port	Username	Intercom Cut Level (dB)	Digital Call Switches
1	Digital-Call-Switch-With-Speaker	sip:0301@172.31.19.202	5060	0301	-6	
2	Digital-Call-Switch-With-Speaker	sip:0302@172.31.19.202	5060	0302	-6	
3	Digital-Call-Switch-With-Speaker	sip:0303@172.31.19.202	5060	0303	-6	
4	Digital-Call-Switch-With-Speaker	sip:0304@172.31.19.202	5060	0304	-6	
5	Digital-Call-Switch-With-Speaker	sip:0305@172.31.19.202	5060	0305	-6	
6	Digital-Call-Switch-With-Speaker	sip:0306@172.31.19.202	5060	0306	-6	

Figure 5. Configuration Settings for ASB

Table 6. Configuration Settings

Get Configuration from Server	Retrieves configuration settings (i.e., web username, server, and local port) from the TFTP server specified in the Network Settings (see "Network Settings Tab Parameters" on page 7).
Web Username	Displays the web username for this appliance.
Emergency-All-Call	Identifies the IP address, port number, cut level (volume), and station list used for emergency all-call pages.

Table 6. Configuration Settings (Continued)

All-Call	Identifies the IP address, port number, cut level (volume), and station list used for all-call pages.
Audio Distribution	Identifies the IP address, port number, cut level (volume), and station list used for audio distribution.
Multicast #	Identifies the IP address, port number, cut level (volume), and station list used for the multicast audio stream of one (or more) zones.
Nyquist Control Password	Specifies a password used to secure Nyquist control messages between this device and the Nyquist server. This value must match the password specified on the Nyquist server to support certain Nyquist features, such as sound masking, amp protection mode, and station check-in. The specified password must be exactly 20 characters long and include uppercase, lowercase, and numeric characters. This password cannot be set unless the Web Password has been changed from the default value.

The following parameters appear for each of the 24 ports associated with the Analog Station Bridge.

Port Number	Shows the port number of the Analog Station Bridge.
Port Type	Shows the station type to which the port connects (speaker only, analog call switch and speaker, or digital call switch and speaker).
Account ID	Shows the SIP account (IP address) associated with the device preceded by the extension of the device associated with this port.
Local Port	Shows the port used for SIP.
Username	Shows the username or extension for the station associated with the port.
Digital Call Switches	Shows the serial numbers of the Digital Call Switch assigned to the ASB port.

Digital Call Switch Management

You can assign digital call switches to ports on an ASB via the appliance's **Configuration Settings** tab. If an analog switch was configured as a station with a type of **Digital Call**

Switch & Speaker, it will also appear on the Configuration Settings/Digital Call Switch Management page. (Refer to the *Managing Stations, Zones, and Queues* chapter of the *Nyquist System Administrator Guide*.)

⚙️ Configuration Settings / Digital Call Switch Management ⓘ

Manage ports:

Available Digital Call Switches

✚ 1730HAN00526

✚ 1730HAN00534

✚ 1730HAN00559

✚ 1730HAN00574

✚ 1730HAN00579

✚ 1730HAN00600

✚ 1730HAN00610

✚ 1730HAN00611

✚ 1730HAN00612

✚ 1730HAN00620

✚ 1730HAN00626

✚ 1730HAN00806

✚ 1730HAN00823

✚ 1730HAN00850

✚ 1730HAN00853

Port1 (0225)

✚ 1730HAN00513

Port2 (0226)

✚ 1730HAN00514

Port3 (0227)

✚ 1730HAN00518

Port4 (0228)

✚ 1730HAN00521

Port9 (0233)

✚ 1730HAN00830

Port10 (0234)

✚ 1730HAN00855

Port11 (0235)

✚ 1730HAN00866

Port12 (0236)

✚ 1730HAN00733

Port13 (0237)

✚ 1730HAN00847

✚ 1730HAN00860

✚ 1730HAN00865

Figure 6. Manage Ports

To assign a digital call switch to a port:

- 1 On the appliance Web UI's main page, select **Configuration Settings**.

- 2 Select the **Manage** button next to the Digital Call Switches column.
- 3 On the Configuration Settings/Digital Call Switch Management page that appears, drag each **Available Digital Call Switch** to its port.

You can assign multiple digital call switches to the same port. If an analog call switch was configured as a station with the type of **Digital Call Switch & Speaker**. (Refer to the Managing Stations and Zones section of the *E7000 Series System Administrator Manual*.)

- 4 When done, select **Save All Changes**.

Accessing Log Files

A log file records events and messages that occur when software runs, to be used when troubleshooting the appliance. From the appliance's web-based UI, log files can be viewed directly or exported via download to your PC, Mac, or Android device, where they can be copied to removable media or attached to an email for technical support.

To view a log file:

- 1 On the appliance Web UI's main page, select **Logs**.
- 2 From the drop-down menu, select the log that you want to view.
Multiple versions and zipped copies of a log may be available.

- 3 To export the file, select **Export**.
The log file will be downloaded to your browser.

View Logs

sw_versions.log

/var/log/sw_versions.log

Export

Debian 8.6 - Linux kernel version:

4.9.0-rc7-bone3 #5 Fri Dec 2 09:26:11 EST 2016 armv7l GNU/Linux

Software Components:

Log Settings

Logging Level:

ERROR

Logging Categories

Log Registration:

No

Log Intercom:

No

Log Check-In:

No

Log Multicast:

No

Log PTT:

No

Log Sound Masking:

No

Save

Status Reporting Settings

Enable Status Reporting:

No

Network IP Address:

Network Port:

0

Status Reporting Categories

Intercom:

No

Paging:

No

Check-In:

No

Save

Figure 7. Logs

Available logs are described in the following table.

Table 7. Logs

Log	Description
ampws.log	Contains information about protection status and logs protection events with temperature information at the time of event.
auth.log	Contains system authorization information, including user logins and authentication methods that were used.
daemon.log	Contains information logged by the various background daemons that run on the system.
debug	Contains errors and debug information.
dmesg	Contains information about hardware, device driver initialization, and kernel module messages that take place during system startup.
dpkg.log	Contains information that is logged when a package is installed or removed using dpkg command.

14

Table 7. Logs (Continued)

Log	Description
kern.log	Contains information logged by the kernel and recent login information for all users.
messages	Contains messages generated by Nyquist.
sw_versions.log	Contains the names and version numbers of key software components used by the Nyquist appliance.
syslog	Contains list of errors that occur when the server is running and server start and stop records
user.log	Contains information about all user level logs.

Log Settings

Log Settings provides the ability to specify the level of detail to be logged at run time (in the *syslog* and *daemon.log* files) for each of several categories.

Note: These settings do not filter the display of events that have already occurred; they indicate which subsequent events will be logged.

Table 8. Log Settings

Logging Level	Indicates the level of detail to be logged at runtime. Valid values are: NONE: No Nyquist logging will be performed. ERROR: Only error conditions will be logged. These are conditions that prevent the appliance from operating correctly. WARNING: Warning and error conditions will be logged. INFO: All information will be logged, including informational, warning, and error conditions. The default value is ERROR.
Logging Categories	Indicates which event categories will be logged for this device. Any number of categories can be enabled. By default, all categories are disabled.
Log Registration	Log detailed information related to station registration.
Log Intercom	Log detailed information related to intercom calls to and from the appliance, as well as talkback parameters.
Log Check-In	Log detailed information related to station check-ins.
Log Multicast	Log detailed information related to incoming multicast pages or audio distribution.
Log PTT	Log detailed information related to Push-to-Talk features.
Log Sound Masking	Log detailed information related to amplifier sound masking, such as spectrum preset applied, slow and fast ramping, and scheduled ramping.

Status Reporting Settings

The **Status Reporting Settings** section provides the ability to configure network-based status reporting for this device.

When an event of any of the specified **Status Reporting Categories** occurs, a JSON packet will be sent to the specified IP address and UDP port containing the event infor-

mation. The JSON will be formatted in the following format (the fields are described in *Table 9, "Status Event JSON elements," on page 17*):

```
{"device":"<string>","port":<int>,"event":"<string>","state":"<string>"}
```

Table 9. Status Event JSON elements

JSON key	Value Description
device	MAC address of the reporting station, with hexadecimal bytes separated by colons (:).
port	The port on the Nyquist appliance to which the reporting station is connected. Valid integer values range from 1 (for most appliances) to 24.
event	The type of event that occurred. Valid values are: • INTERCOM • PAGE • CHECK-IN (Analog Station Bridge only)
state	The status of the event. Valid values are: • PENDING • IN_PROGRESS • TERMINATED

To configure the Status Reporting for this appliance, set **Enable Status Reporting** to **Yes**, configure the **Network IP Address** and **Network Port** (a UDP port) to which status

events will be sent, and specify which **Status Reporting Categories** to send, as described in *Table 10*.

Table 10. Status Reporting Settings

Enable Status Reporting	Enables network-based status reporting whenever a call changes state on a given port. PENDING: Call setup in progress, but not yet connected. IN_PROGRESS: Call or page established. TERMINATED: Call or page ended. This setting is disabled by default.
Network IP Address	The network IP address to which status messages will be sent.
Network Port	The network UDP port to which status messages will be sent.
Status Reporting Categories	Status event types to be sent to the event logging server.
Intercom	Report intercom-related events.
Paging	Report paging-related events.
Check-In	Report check-in-related events.

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
```

Tip: Some browsers do not recognize newly installed CAs until after the browser has restarted. Browse to <chrome://restart> in a Chromium-based browser or <edge://restart> in the Edge browser to restart all open browser windows.

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 multiple 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