



VoIP Wall Baffle Combo Speaker with Integrated LED Message Display and Flasher Configuration Guide

NQ-S1810WBC



BOGEN®

© 2024–2026 Bogen Communications LLC
All rights reserved
740-00224D
260507

Contents

- Configuring the Nyquist VoIP Wall Baffle Combo Speakers 1**
 - Using the Dashboard3
 - Updating Firmware5
 - Network Settings Tab Parameters6
 - Configuration Settings Tab Parameters9
 - Setting DSP Parameters12
 - Setting the Channel Level.13
 - Adjusting Volume Levels13
 - Knob Adjustments13
 - Intercom Tuning.14
 - Accessing Log Files16
 - Log Settings17
 - Status Reporting Settings.18
- Appendix A: Bogen Digital Certification Authority 21**
 - Installing Certification Authority on Windows System21
 - Installing Certification Authority on Mac System22
 - Installing Certification Authority on an Android Device23
 - Installing Certification Authority on an iOS Device23
 - Viewing the Certificate23

Configuring the Nyquist VoIP Wall Baffle Combo Speakers

The Nyquist VoIP Wall Baffle Combo Speaker with Integrated LED Message Display and Flasher (NQ-S1810WBC) is a VoIP talkback speaker designed to work with the Nyquist Series IP network-based intercom and paging solution. It features an 8.7" × 2.35" LED display panel and a 0.35" × 3.2" flasher (located below the LED display).

The VoIP wall baffle talkback speaker assembly consists of an 8" cone speaker and VoIP module preassembled into a bright white injection-molded wall baffle speaker enclosure.

The speaker is 802.3af-compliant and designed to facilitate rapid and efficient deployment using existing network Power over Ethernet (PoE) ports. It also has a Form-C relay for controlling third-party devices. These VoIP speakers enable ease of placement wherever needed within a facility.

Messages can be displayed on the LED panel using the same methods used to display messages on a GA10PV display (e.g., via the System Controller dashboard's **Display Message** or the **Display-Msg** routine action). Messages can be up to 64 uppercase characters (lowercase characters will display as uppercase) and will scroll if they are too long to fit on the display.

If enabled, a clock showing the date, hour, minutes, and (optionally) seconds will be displayed on the LED panel whenever a message is not being displayed.

While in discovery mode (i.e., not registered with a server), the IP address and MAC will be displayed on the LED panel. The panel will display "Unregistered" if the device has encountered an error communicating with the server and "Restarting" if the device is restarting due to a configuration change by the server (e.g., an update to WBC parameters, such as LED brightness).

The flasher can be displayed—independently or in conjunction with a message—to attract attention to a message or indicate a specific event, such as activation of a Nyquist- or user-defined event. The flasher's color (Amber, Blue, Green, Orange, Red, Violet, White, or Yellow), pattern (No Change, Off, Slow, Fast, Double, Triple, or Quad), and number of pattern cycles can be configured per event type. By default, the flasher is enabled during Nyquist system events (e.g., All-Call, Emergency-All-Call, Zone-Page, etc.).

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 21.

- 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.

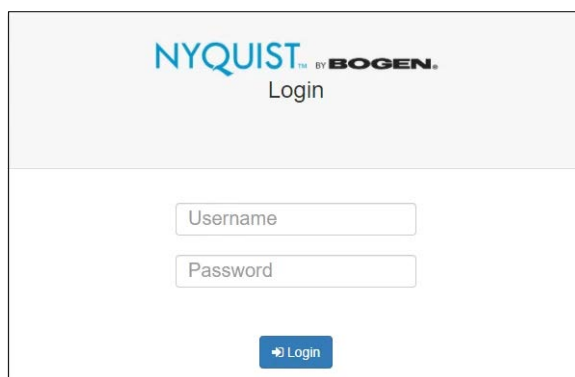


Figure 1. Nyquist Appliance Login

- 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

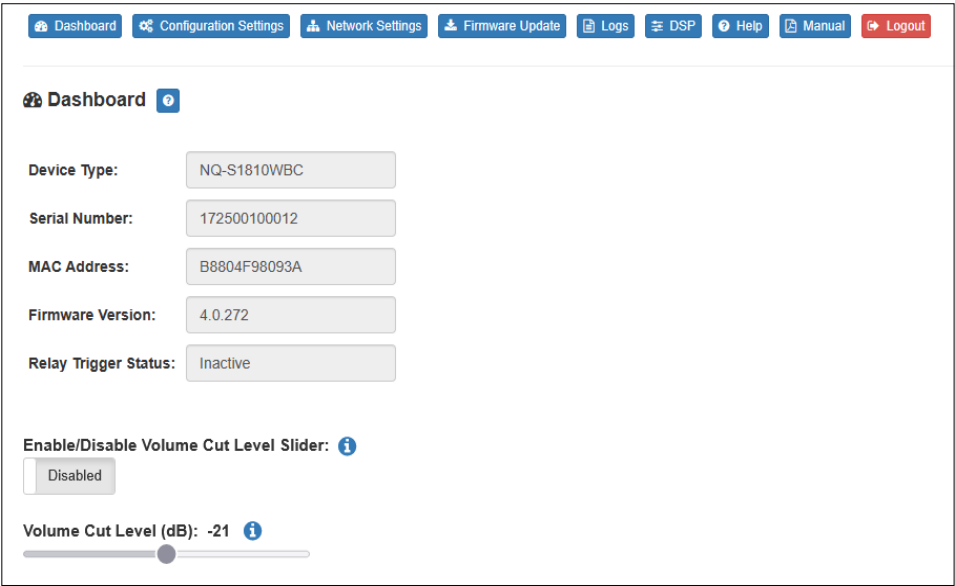


Figure 2. Nyquist VoIP Wall Baffle Combo Speaker Dashboard

The dashboard displays the following fields:

Table 1. Appliance Dashboard Fields

Device Type	Identifies the model of this device.
Serial Number	Identifies the serial number for the device.
MAC Address	Identifies the Media Access Control (MAC) address, which is a unique identifier assigned to network interfaces for communications on the physical network segment.
Firmware Version	Identifies the firmware version installed on the device.
Relay Trigger Status	When enabled in Configuration Settings, this field indicates the status of the NO/NC output relay, which is activated whenever an audio signal is being sent to the VoIP speaker.

Table 1. Appliance Dashboard Fields

Enable/Disable Volume Cut Level Slider	Enables or disables the Volume Cut Level slider.
Volume Cut Level (dB)	Specifies a temporary volume setting for the speaker during the current intercom call or page. <i>Note:</i> This is a temporary adjustment that allows the user to experiment with the loudness of the speaker and will be reset to the normal setting on subsequent calls. To make permanent adjustments, change the station-specific cut level settings on the Nyquist System Controller. The value can be adjusted between -42 and 0 dB.

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

Table 2. Appliance Dashboard Buttons

Dashboard	Displays the dashboard.
Configuration Settings	Accesses the Configuration Settings page where you can view and set various options.
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 defaults, 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.
DSP	Accesses the DSP page where you can view and set parameters for Digital Signal Processing (DSP).
Help	Accesses the appliance's online help.
Manual	Displays this appliance's configuration guide.
Logout	Logs out of the appliance's web UI.

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 3. 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 4. 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 4. 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 5 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:	239.0.1.1	6000	-21	1
All-Call:	239.0.1.2	6004	-21	1
Audio Distribution:	239.0.1.3	6008	-24	1

Nyquist Control Password

Save Password

Device Stations

Port Number	Port Type	Account Id	Local Port	Username
1	Digital-Call-Switch-With-Speaker	sips:0110@172.31.19.202	5060	0110

Digital Call Switches

Volume Control Switches

Figure 5. Appliance Configuration Settings

The following table describes the **Configuration Settings** tab settings:

Table 5. 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 <i>"Network Settings Tab Parameters" on page 6</i>).
Web Username	Displays the username of the current user.
Emergency-All-Call	Identifies the IP address, port number, cut level (volume), and station list used for emergency all-call pages.
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 a specific zone. If this device belongs to more than one zone, then multiple Multicast # entries will be displayed.
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. <i>Note:</i> This password cannot be set unless the Web Password has been changed from the default value.

The **Configuration Settings** tab also displays the following information for each **Device Station** attached to the amplifier:

Port Number	Identifies the port number of the appliance.
Port Type	Identifies the station type to which the port connects.
Account ID	Identifies the SIP account (IP address) associated with the device preceded by the extension of the device associated with this port.
Local Port	Identifies the port used for SIP.
Username	Identifies the username or extension for the station associated with the port.
Digital Call Switches	Identifies the serial numbers of all Nyquist Digital Call Switches (NQ-E7020-G2) connected to this appliance.
Volume Control Switches	Identifies the serial numbers of all Remote Volume Controls (NQ-VCTRL) connected to this appliance.

Setting DSP Parameters

When you select DSP (Digital Signal Processing) from the appliance's web UI, the DSP page appears.

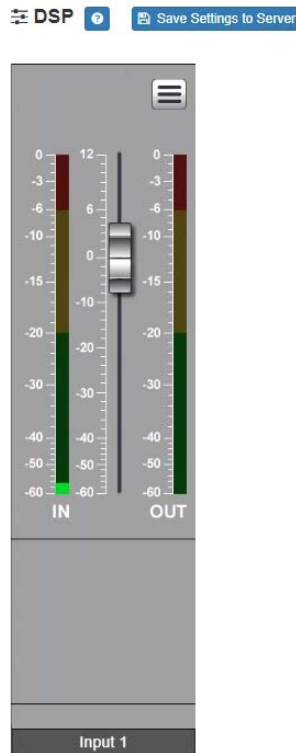


Figure 6. DSP Page

From this page, you can set parameters for DSP, which is a form of processing that uses digital data to simulate characteristics found in analog circuits. With DSP, you can alter analog signals, such as audio signals, that have been converted to a digital format.

You can also select **Save Settings to Server** to back up all configuration settings to the Nyquist server.

The DSP page allows you to adjust the signal level for the Output channel, as well as viewing level indicators for both the input and output signals. Selecting the DSP Features button (hamburger menu above the OUT signal indicator) displays a menu that allows you to access DSP features, as described in the following table.

Tip: You can select **Save Settings to Server** to back up all configuration settings to the Nyquist server.

Note: The slide control controls the input gain of the microphone, not the output level of the speaker. To control the output level of the speaker, use the **Intercom Cut Level** control for this station on the Nyquist server.

Table 6. DSP Features

Intercom Tuning

Allows you to specify settings used in intercom calls and when the intercom switches between send and receive modes.

Setting the Channel Level

The channel level control is a channel fader, which is adjusted in 1-dB increments and controls the microphone volume level for the channel. The channel levels can range from -60 to +12 dB. If you place the mouse over the fader, the numerical value of the level appears.

Adjusting Volume Levels

The channel fader control can be used to adjust the channel's microphone volume level in 1-dB increments between -60 and +12 dB. The overall adjusted microphone volume level of the channel signal can be viewed on the **OUT** VU meter, marked in 2-dB increments between -60 and 0 dB.

To adjust the channel volume level:

- 1 On the appliance Web UI's main page, select **DSP**.
- 2 Use the channel's fader to adjust the volume level.

Knob Adjustments

Many DSP controls use knobs to adjust one or more settings. The value of a knob can be adjusted in one of two ways:

- 1 Click the knob control, hold the mouse button down, and drag the mouse up or down to increase or decrease the value.
- 2 Double-click the knob, type a value into the resulting popup, and click the Save button.

Intercom Tuning

The VoIP Speaker provides *half-duplex* communications, which means that only one party can transmit at a time. Which party can transmit (i.e., this VoIP Speaker or the Admin Phone) is controlled automatically by the Intercom Tuning settings. Whenever a signal from the calling station exceeds a certain level—known as the *switching sensitivity* level—the VoIP Speaker switches to receive mode, allowing the party using the Admin Phone to speak. When the signal is below that level, it switches back to send mode, allowing the party using the VoIP Speaker to speak.

Selecting **Intercom Tuning** from the **Menu** icon on the DSP page displays the Intercom Tuning page. The intercom is designed to turn off the speaker while the intercom user is talking and turn off the microphone while the remote user is talking. This DSP feature defines at what input and output levels the intercom will switch between the microphone and the speaker.

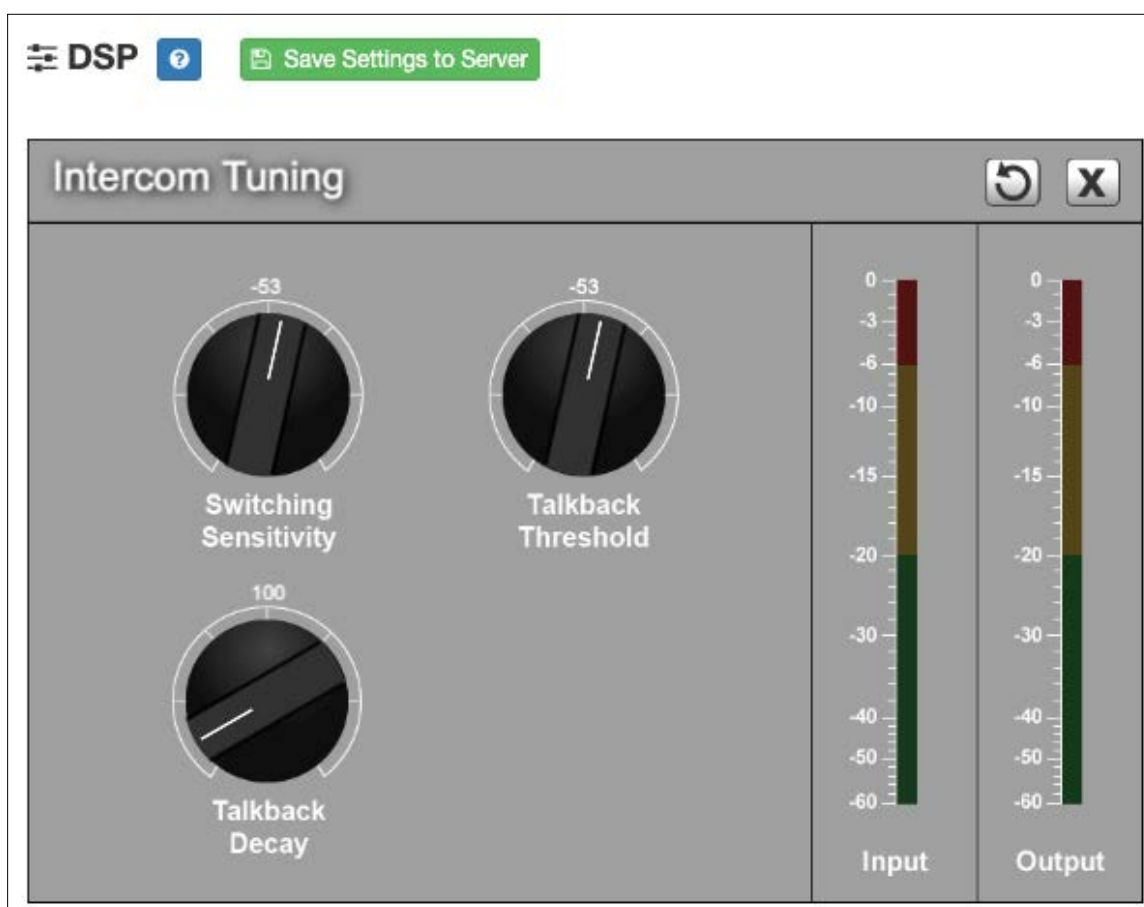


Figure 7. Intercom Tuning Settings

The Intercom Tuning page has level indicators for input and output signals and contains the following settings (see *Table 7*).

Table 7. Intercom Tuning Settings

Switching Sensitivity	Specifies the minimum level of the received (i.e., speaker) signal at which the microphone will be muted and the speaker will be enabled. The range is -144 to $+24$ dB.
Talkback Threshold	Specifies the minimum talkback (i.e., microphone) signal level at which the microphone will be enabled. The lower the level, the more sensitive the microphone is to activating. The range is -144 to $+24$ dB.
Talkback Decay	Specifies the rate (in dB/second) at which the noise gate that enables the talkback (i.e., microphone) signal will close once opened. A larger value will disable the microphone sooner; a smaller value will keep it enabled longer. <i>Tip:</i> If the microphone audio sounds choppy, set this to a smaller value.
	The range is 0 to $+1000$ dB/sec.

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.

The screenshot displays the 'View Logs' section at the top, featuring a dropdown menu currently set to 'sw_versions.log' and an 'Export' button. Below this, a log entry is shown with the text: 'Debian 8.6 - Linux kernel version: 4.9.0-rc7-bone3 #5 Fri Dec 2 09:26:11 EST 2016 armv7l GNU/Linux' and a section for 'Software Components:'. The bottom half of the image shows two settings panels. The 'Log Settings' panel on the left includes a 'Logging Level' dropdown set to 'ERROR', a 'Logging Categories' section, and several toggle switches for 'Log Registration', 'Log Intercom', 'Log Check-In', 'Log Multicast', 'Log PTT', and 'Log Sound Masking', all of which are currently set to 'No'. A green 'Save' button is at the bottom left. The 'Status Reporting Settings' panel on the right includes an 'Enable Status Reporting' dropdown set to 'No', input fields for 'Network IP Address' and 'Network Port' (set to '0'), a 'Status Reporting Categories' section with 'Intercom' and 'Paging' toggles set to 'No', and a green 'Save' button at the bottom right.

Figure 8. Logs

Available logs are described in the following table.

Table 8. 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.
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 9. 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 information. The JSON will be formatted in the following format (the fields are described in *Table 10, "Status Event JSON elements," on page 19*):

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

Table 10. 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
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 11*.

Table 11. 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.

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