



VoIP Speaker Configuration Guide

NQ-S1810CT-G2, NQ-S1810WT-G2

Contents

Configuring the Nyquist VoIP Speakers	1
Using the Dashboard	3
Standalone Operation	5
Updating Firmware	5
Network Settings Tab Parameters	7
Configuration Settings Tab Parameters	10
Standalone Operation Configuration Settings	13
Setting DSP Parameters	19
Setting the Channel Level	20
Adjusting Volume Levels	20
Knob Adjustments	20
Intercom Tuning	21
Presets	23
Accessing Log Files	25
Appendix A: Bogen Digital Certification Authority	27
Installing the Bogen Digital Certification Authority	27
Installing Certification Authority on Windows System	27
Installing Certification Authority on Mac System	28
Installing Certification Authority on an Android Device	29
Installing Certification Authority on an iOS Device	29
Viewing the Certificate	29

Configuring the Nyquist VoIP Speakers

The Nyquist VoIP Ceiling Speaker Gen 2 (NQ-S1810CT-G2) and Nyquist VoIP Wall Baffle Speaker Gen 2 (NQ-S1811WT-G2) are VoIP talkback speakers designed to work with the Nyquist Series IP network-based intercom and paging solution.

The ceiling talkback speaker assembly consists of an 8" cone speaker and VoIP module preassembled onto a 13" steel ceiling grille painted with bright white enamel.

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

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

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 Chrome 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 *"Installing the Bogen Digital Certification Authority" on page 27*.

- 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.

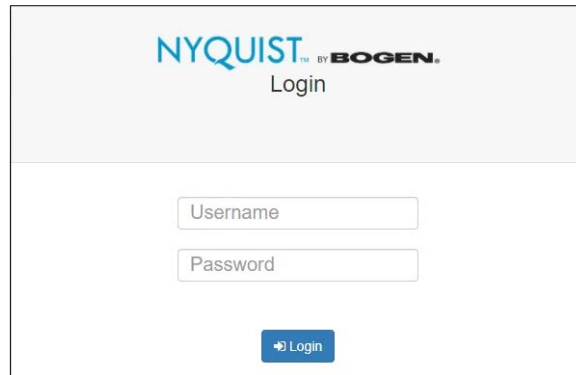
The image shows a login page for a Nyquist appliance. At the top, there is a header with the text "NYQUIST™ BY BOGEN." in blue and black, and "Login" in black below it. Below the header, there are two input fields: "Username" and "Password", both with light gray borders. At the bottom, there is a blue button with a white right-pointing arrow and the text "Login" in white.

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

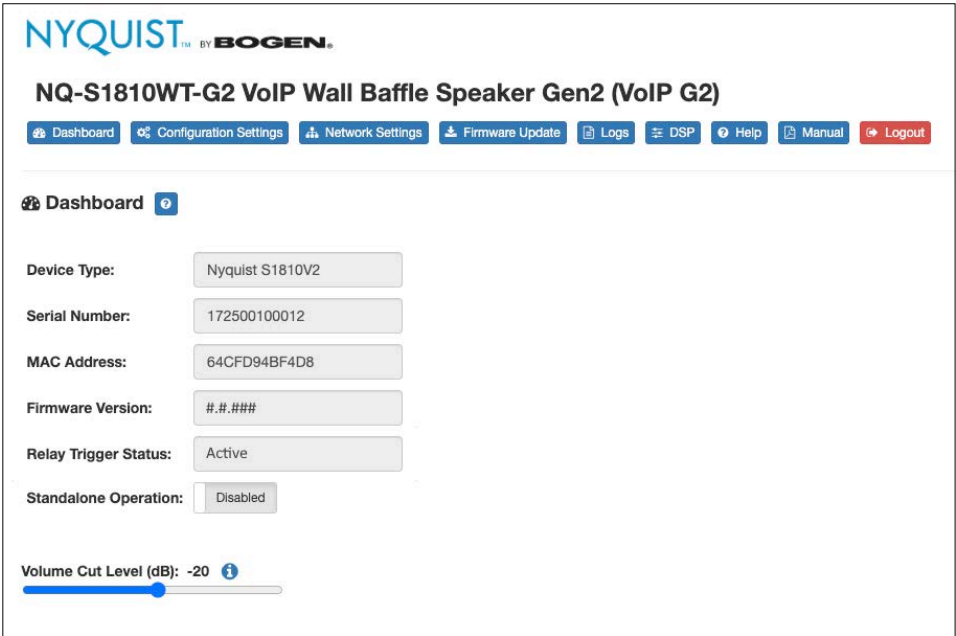


Figure 2. Nyquist Speaker Dashboard

Note: On the Dashboard, the **Device Type** *Nyquist S1810V2* refers to the Nyquist S1810-G2.

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

Standalone Operation	Enables or disables Standalone mode.
Volume Cut Level (dB)	<p>Specifies a temporary volume setting for the speaker during the current intercom call or page.</p> <p><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.</p> <p>The value can be adjusted between –42 and 0 dB.</p>

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. If Standalone Operation is not enabled, you can also 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 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.

Standalone Operation

This device can also run in Standalone Operation mode, where it will not interact with a Nyquist server (e.g., E7000 or C4000). This means the device will not:

- Fetch device configuration from Nyquist server
- Register with Nyquist server (via SIP)
- Store backup information to Nyquist server
- Allow access to Nyquist server-based NTP

Standalone Operation allows this device to be used without a Nyquist server as a generic SIP endpoint when integrated with a 3rd-party VoIP telephone system or other SIP server-based solutions, such as a unified communications (UC) platform. In a non-SIP environment, these devices are capable of receiving audio through one or more prioritized multicast channels.

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 the device is in Standalone mode, the **Check for Updates** button will be shown. Selecting it checks the Bogen website for the latest firmware version available. If a version newer than the one currently installed is found, it is downloaded to the appliance and the **Update Firmware** button will be shown.
 - 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	<p>Available only when a new firmware version has been loaded onto the appliance (as specified in New Nyquist Version).</p> <p>Installs the loaded firmware. A reboot may be required after installation.</p>
Upload Firmware	<p>Prompts the user to specify a firmware file, which will then be loaded (though not installed) onto the appliance.</p> <p><i>Note:</i> To obtain the firmware file for a specific version, please contact Bogen Technical Support.</p>
Check for Updates	<p>Available only when the appliance is configured for Standalone mode.</p> <p>Checks the Bogen website for the latest firmware version available and, if it finds a version newer than what is currently installed, downloads it to the appliance.</p> <p><i>Note:</i> Ensure your Nyquist appliance has network access to bogen-ssu.bogen.com, port 22.</p>
Restore Factory Settings	<p>Returns the appliance to its original factory configuration.</p> <p><i>Note:</i> This does not install the original appliance firmware. The firmware will not be changed.</p>
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 ⓘ

IP Address: 172.31.19.220

Netmask: 255.255.255.0

Gateway: 172.31.19.254

VLAN ID: 9

VLAN Priority: 0 - Best Effort ▼

NTP Server: 172.31.19.203

TFTP Server: 172.31.19.203

TFTP Server from DHCP: No ▼

DHCP Enabled: Yes ▼

Reboot Appliance: No ▼

Save

Figure 4. Network Settings

Network settings are described in the following table:

Table 4. Network Settings

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.
VLAN ID	Identifies the Virtual Local Area Network (VLAN) for this appliance. Values range from 0 to 4094.

Table 4. Network Settings (Continued)

VLAN Priority	Identifies the priority of the network traffic on the VLAN. Priority can range from 0 through 7.
NTP Server	<p>Identifies the IP address or the domain name of the Network Time Protocol (NTP) Server.</p> <p><i>Note:</i> This field is only editable when Standalone Operation is enabled.</p>
TFTP Server	<p>Identifies the host name or IP address of the Trivial File Transfer Protocol (TFTP) server.</p> <p>The specified TFTP server can be used to automatically set this device's Configuration settings via the Get Configuration from Server button.</p> <p>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.</p> <p><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.</p> <p><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.</p> <p><i>Note:</i> This setting is not available when Standalone Operation is enabled.</p>
TFTP Server from DHCP	<p>"Yes" means the device will use the DHCP option 66 value to retrieve an address for the TFTP Server from DHCP.</p> <p>"No" means the device will ignore the DHCP option 66 value and use the manually configured value of the TFTP Server (see above).</p> <p><i>Note:</i> This setting is not available when Standalone Operation is enabled.</p>
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**. However, you can manually configure an appliance through the appliance’s Web UI when Standalone Operation is enabled (see *"Configuration Settings (Standalone disabled)" on page 11*).

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 11 for normal configuration, or modify the settings as described in *"Configuration Settings (Standalone disabled)" on page 11* for Standalone Operation configuration.
- 3 If changes were made (Standalone Operation only), click the **Save Configuration Settings** and/or **Save Multicast Addresses** buttons to save your changes.

Configuration Settings

Get Configuration From Server

Web Username: admin

	IP Address	Port Number	Cut Level	Station List
Emergency-All-Call:	239.0.1.1	61001	-21	1
All-Call:	239.0.1.2	61002	-21	1
Audio Distribution:	239.0.1.3	61003	-24	1
Multicast 1:	239.0.2.12	62012	-6	1

Nyquist Control Password

Save Password

Device Stations

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

Figure 5. Appliance Configuration Settings (Standalone disabled)

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

Table 5. Configuration Settings (Standalone disabled)

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</i> " on page 7).
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	<p>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.</p> <p>The specified password must be exactly 20 characters long and include uppercase, lowercase, and numeric characters.</p> <p><i>Note:</i> This password cannot be set unless the Web Password has been changed from the default value.</p>

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.

Standalone Operation Configuration Settings

Configuring this device consists of specifying one or more of the following:

- The SIP server addresses, ports, and SIP extensions at which to register for incoming SIP calls.
- The input multicast (Receive) addresses (and ports) from which the device will receive encoded signals, which will then be converted to analog and played to the speaker.

To receive networked audio, configure one or more **Multicast Addresses (Receive)** entries with the multicast addresses, ports, and codecs from which to receive the encoded streams. Specify the cut level for the speaker output channel.

Configuration Settings

Device Type:

NQ-S1810-E7020 VoIP Speaker

Device Name:

Nyquist S810V2

Web Username:

admin

Web Password:

Web Confirm Password:

Time Zone:

Select a time zone

Output Power (Watts):

1/2

Enable SIP Calls:

Yes

External Relay Trigger:

Disabled

SIP Server Address:

SIP Network Port:

SIP Codecs:

G722 ulaw alaw

SIP Extension:

SIP Username:

SIP Password:

Type:

Digital Call Switch & Speaker

Dial Extension:

Intercom Cut Level: -6 dB

Save Configuration Settings

Multicast Addresses (Receive)

Sorting:

Disabled

		Multicast IP Address	Multicast Port Number	Codec	Channels	Cut Level (dB)	Description
		239.1.1.1	6000	G711 u-law	Speaker	-30	Empty
		239.1.1.1	6002	G711 u-law	Speaker	-20	Empty

Figure 6. Appliance Configuration Settings (Standalone enabled)

The following table describes the **Configuration Settings** tab settings when Standalone Operation is enabled for this device:

Table 6. Configuration Settings (Standalone enabled)

Device Type	Displays the type of this device.
Device Name	Provides a name for this device.
Web Username	Specifies a web username for this appliance.
Web Password	Specifies a web password for logging into the appliance.
Web Confirm Password	Re-enter the password used to log into the appliance.
Time Zone	Specifies the time zone in which the device resides.
Output Power (Watts)	Specifies the output power for the amplifier in Watts. Valid values are: 1/8, 1/4, 1/2, 1, 2, 4, and 8.
Enable SIP Calls	Enables this device to receive one-way SIP calls, wherein only the caller can be heard (such as announcements). If enabled, a number of SIP-related configuration settings are displayed.
External Relay Trigger	Enables/disables the activation of the NO/NC output relay to notify an external device that an audio signal is being sent to the VoIP speaker.
SIP Server Address^a	Specifies the IP address of the SIP Registration Server with which the device will register.
SIP Codecs^a	Displays a read-only list of codecs allowed on SIP sessions.
SIP Extension^a	Specifies the SIP extension for this device. The extension, along with the IP address, is used to specify the URI used to place a SIP call to this extension: <code>sip:<extension>@<local_ip_address></code>
SIP Network Port^a	Specifies the IP port on which to communicate with the SIP Registration Server (typically 5060).
SIP User Name^a	Specifies the SIP user name used to register with the SIP server.
SIP Password^a	Specifies the SIP registration password used to register with the SIP server.
Type^a	Specifies how the device will be used. Options are: <ul style="list-style-type: none">• VoIP Speaker Only• Digital Call Switch & Speaker

Table 6. Configuration Settings (Standalone enabled)

Dial Extension^a	Only available when Type is set to Digital Call Switch & Speaker , this indicates which extension will be called when the call button is activated.
Intercom Cut Level^a	<p>Specifies the output level of the speaker.</p> <p>This can be a value from –42 and 0 dB.</p> <p>The default value is –6 dB.</p> <p><i>Note:</i> To modify, click on the value, adjust the slider on the popup using the cursor keys or mouse, and click the check box button.</p>

a. Available only when **Enable SIP Calls** has a value of **Yes**.

The following parameters appear for each Multicast Address configured for this device.

Multicast IP Address	Specifies the multicast IP address on which to receive audio streams.
Multicast Port Number	Specifies the multicast port on which to receive audio streams.

Codec

Specifies the codec to be used when decoding audio.
Select one of the following values:

- G711 u-law
 - Intercom call quality
 - A narrowband audio codec that provides toll-quality audio at 64 kbps. The u-law version is primarily used in North America and Japan.
- G711 a-law
 - Intercom call quality
 - A narrowband audio codec that provides toll-quality audio at 64 kbps. The a-law version is primarily used in most countries outside of North America and Japan.
- G722
 - Tone and paging quality
 - A wideband audio codec operating at 48, 56, and 64 kbps.
- OPUS
 - Music quality
 - An audio codec format designed for speech and general audio, supporting low latency, constant and variable bitrate encoding (6 to 510 kbps), and five sampling rates (from 8 to 48 kHz).

Channels

Channel(s) on which the audio streams will be output.

One or more of the following values:

- Speaker

Tip: Fine tuning of levels per output channel can be adjusted using DSP settings.

Cut Level (dB)

Specifies the cut level for the audio stream. This can be a value from -70 to 0 dB.

The default value is -20 dB.

Note: To modify, click on the value, adjust the slider on the popup using the cursor keys or mouse, and click the check box button.

Description

User-specified description of this multicast address.

This setting can contain a maximum of 30 characters and should not contain any of the following:

[] { } < > , | :

Note: A maximum of 24 multicast entries is supported.

Multicast Addresses should be ordered by priority, highest priority first. If multiple streams are active on the same channel simultaneously, the one with the highest priority will be played. Set the **Sorting** switch to Enabled and drag entries using the 4-way arrow symbols to drag entries up and down to rearrange the priorities.

Setting DSP Parameters

When you select DSP from the appliance's web UI, the DSP page appears.

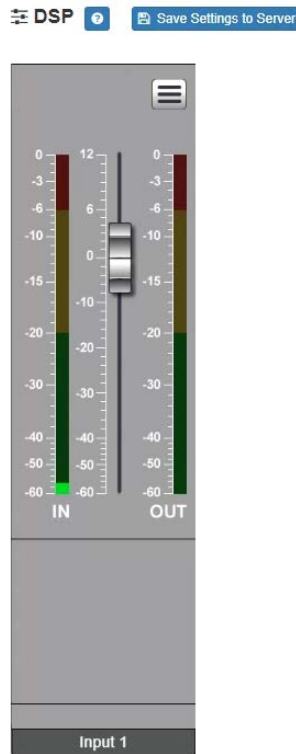


Figure 7. DSP Page

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. If this device is in Standalone mode, the output level can be controlled using the **Intercom Cut Level** control on the Configuration Settings page.

Table 7. DSP Features

Intercom Tuning	Allows you to specify settings used in intercom calls and when the intercom switches between send and receive modes.
Presets	Allows you to use preset DSP settings for the selected speaker type.

Note: Selecting the Speaker Type to match the installed speaker will help eliminate feedback and noise from the device's microphone.

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 Admin Phone 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 8. Intercom Tuning Settings

The Intercom Tuning page has level indicators for input and output signals and contains the following settings (see *Table 8*).

Table 8. Intercom Tuning Settings

Switching Sensitivity	<p>Specifies the minimum level of the received (i.e., speaker) signal at which the microphone will be muted and the speaker will be enabled.</p> <p>The range is -144 to $+24$ dB.</p>
Talkback Threshold	<p>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.</p> <p>The range is -144 to $+24$ dB.</p>
Talkback Decay	<p>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.</p> <hr/> <p><i>Tip:</i> If the microphone audio sounds choppy, set this to a smaller value.</p> <hr/> <p>The range is 0 to $+1000$ dB/sec.</p>

Presets

There are a number of DSP effects that are used to enhance the quality of the audio signal being played on the VoIP speaker device (though not all of these effects are visible and available for customization). Due to design differences between the VoIP speaker models (e.g., microphone placement), these DSP settings must be customized for each model.

Bogen has created predefined sets of model-specific DSP configurations to customize the signal for each device. These configurations are available via **Presets**.

Note: It is important that the preset corresponding to the speaker model be specified.

Selecting **Presets** from the **Menu** icon on the DSP page displays the Presets page.

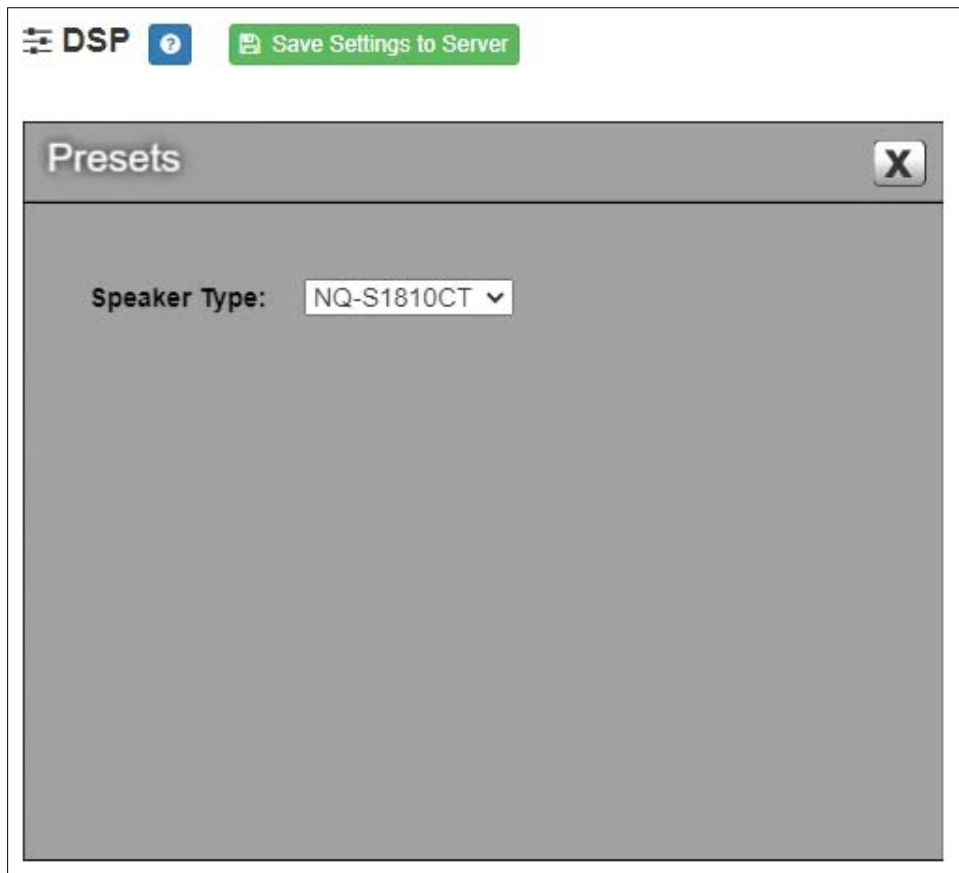


Figure 9. Presets Settings

The Presets page allows you to select the **Speaker Type**.

Table 9. Preset Settings

Speaker Type

Select a predefined Preset configuration from the list of speaker models. Available options are:

- NQ-S1810CT (ceiling-mounted speaker)
- NQ-S1810WT (wall-mounted speaker)

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 of the same log, and zipped copies of the log, may be available.
- 3 To export the file, select **Export**.
A link to a .txt file appears in the browser's lower left corner.



Figure 10. Logs

Available logs are described in the following table. If a log file is empty, however, it will not appear in the drop-down list of available logs.

Table 10. 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.
btmpt	Contains information about failed login attempts.
daemon.log	Contains information logged by the various background daemons that run on the system.
debug	Contains errors and debug information.
dpkg.log	Contains information that is logged when a package is installed or removed using dpkg command.
faillog	Contains user failed login attempts.
kern.log	Contains information logged by the kernel and recent login information for all users.
lastlog	Contains information on the last login of each user.
messages	Contains messages generated by Nyquist.
php5-fpm.log	Contains errors generated by the PHP script.
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.

Appendix A: Bogen Digital Certification Authority

Installing the Bogen Digital Certification Authority

When your 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 you do not install the Bogen CA certificate, 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 when you attempt to access the Bogen device.

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.

You can also 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
```

If you wish to validate the certificate before importing it, execute the following command after retrieving the CRT file:

```
(New-Object -TypeName Security.Cryptography.X509Certificates.X509Certificate2 -ArgumentList "$env:temp\bogenCA.crt").GetCertHashString()
```

The output will be the hash value (i.e., thumbprint) of the downloaded certificate, which should match the following (as of the current release):

```
0A8248F69D970F8DD855D0E0592972DA64B1A845
```

To install the certificate for the current user, execute the following command:

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

That command installs the CA certificate into the CurrentUser certificate store, which only applies to the current user. 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 also 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 Chrome or Edge 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