Entry Door Phone Configuration Guide

NQ-EDP01

BOGEN®

Contents

Configuring Nyquist Entry Door Phone

The Nyquist Entry Door Phone (NQ-EDP01) is a hands-free, two-way, wall-mounted, VoIP speaker phone designed to work with the Nyquist Series IP network-based intercom and paging solution. It is 802.3af-compliant and designed to facilitate rapid and efficient deployment using existing network Power over Ethernet (PoE) ports.

This device can be used to place a VoIP/SIP call to an assigned Admin Phone or Admin Group with the press of a button. The device provides *half-duplex* communication, allowing one party to speak at a time, switching automatically whenever it detects that the Admin Phone party is speaking.

Note: Be aware that the Entry Door Phone does *not* receive pages or participate in check-in processes.

The Nyquist server can automatically discover and configure the Entry Door Phone, but you can also manage the device and manually configure some settings through the web-based user interface (web UI). It can also operate in Standalone mode, allowing it to be used in generic, 3rd-party SIP applications without a Nyquist server.

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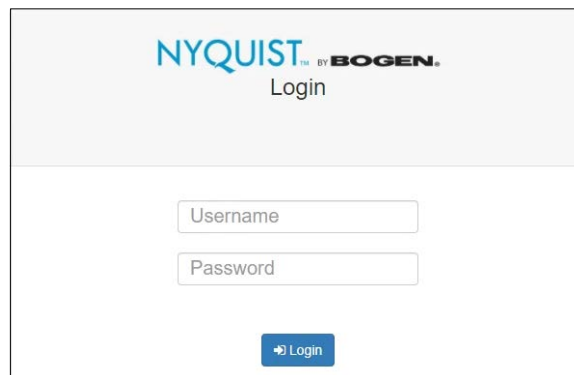
To access the appliance's Web-based user interface (UI):

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 18*.

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.

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 Entry Door Phone 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.
Standalone Operation	Enables or disables Standalone mode.

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.

3

Table 2. Appliance Dashboard Buttons

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 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.

5

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.
	Note: To obtain the firmware file for a specific version, please contact Bogen Technical Support.
Check for Updates	Available only when the appliance is configured for Standalone mode.
	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.
	Note: Ensure your Nyquist appliance has network access to bogen-ssu.bogen.com, port 22.
Restore Factory Settings	Returns the appliance to its original factory configuration.
	Note: 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**.

Figure 4. Network Settings

Network settings are described in the following table:

Table 4. Network Settings

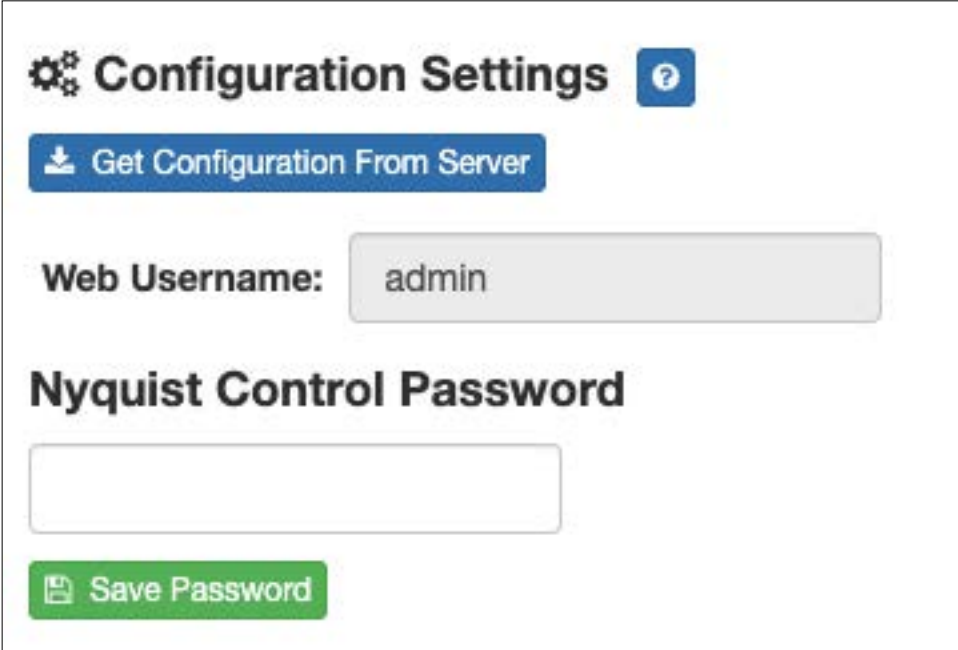|	
IP Address	Identifies the IP address assigned to the appliance.
Netmask	Identifies the subnetwork subdivision of an IP network.
Gateway	Identifies the address, or route, for the default gateway.
VLAN ID	Identifies the Virtual Local Area Network (VLAN) for this appliance. Values range from 0 to 4094.

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	Identifies the IP address or the domain name of the Network Time Protocol (NTP) Server. *Note:* This field is only editable when Standalone Operation is enabled.
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. *Note:* 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. *Note:* 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. *Note:* This setting is not available when Standalone Operation is enabled.
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). *Note:* This setting is not available when Standalone Operation is enabled.
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.

8

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 *"Standalone Operation Configuration Settings" 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 10 for normal configuration, or modify the settings as described in *"Standalone Operation Configuration Settings" on page 11* for Standalone Operation configuration.

3   If changes were made (Standalone Operation only), click the **Save Configuration Settings** button to save your changes.

Figure 5. Appliance Configuration Settings (Standalone disabled)

The following table describes the **Configuration Settings** tab settings when Standalone Operation is *not* enabled for this device:

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 "*Network Settings Tab Parameters" on page 6*).
Web Username	Displays the username of the current user.
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. *Note:* This password cannot be set unless the Web Password has been changed from the default value.

Standalone Operation Configuration Settings

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.
SIP Server Address	Specifies the IP address of the SIP Registration Server with which the device will register.

**Table 6. Configuration Settings (Standalone enabled)**

SIP Extension	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:
	sip:<extension>@<local_ip_address>
SIP Network Port	Specifies the IP port on which to communicate with the SIP Registration Server (typically 5060).
SIP Username	Specifies the SIP username used to register with the SIP server.
SIP Password	Specifies the SIP registration password used to register with the SIP server.
Dial Extension	Specifies the extension number to call when the device's call button is pressed.
Intercom Cut Level	Specifies the cut level for the speaker.
	This can be a value from -42 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.

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.
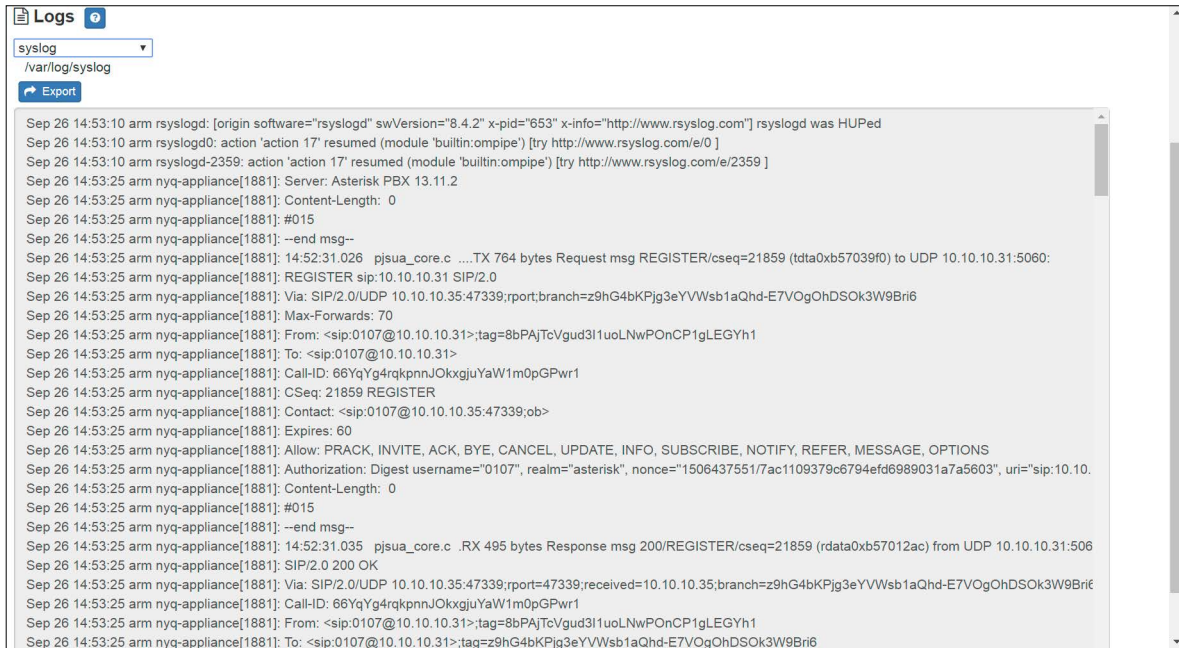
Figure 7. Logs

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 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.
btmp	Contains information about failed login attempts.
daemon.log	Contains information logged by the various back-ground 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.

13

Table 7. Logs (Continued)

Log	Description
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.

Setting DSP Parameters

When you select DSP from the appliance's web UI, the DSP page appears.
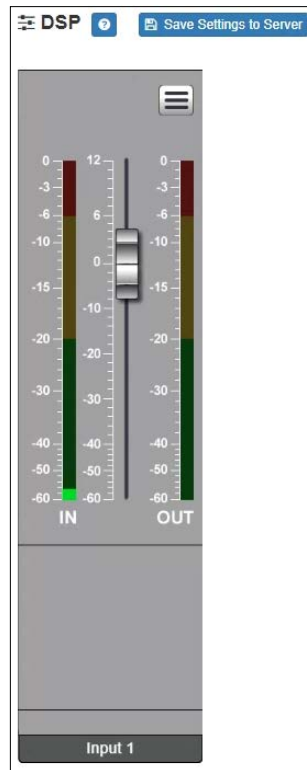
Figure 8. DSP Page

From this page, you can configure the device's Digital Signal Processing (DSP) features, 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.

The DSP page allows you to adjust the microphone input gain, as well as viewing level indicators for both the input and output signals. Selecting the DSP Features button (i.e., the 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 channel fader 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

15

level can be controlled using the **Intercom Cut Level** control on the Configuration Settings page.


Table 8. DSP Features

Intercom Tuning	Allows you to specify when the intercom switches between send and receive modes.

Intercom Tuning

The Entry Door Phone provides *half-duplex* communications, which means that only one party can transmit at a time. Which party can transmit (i.e., this Entry Door Phone 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 Entry Door Phone 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 Entry Door Phone to speak.

Selecting **Intercom Tuning** from the **Menu** icon on the DSP page displays the Intercom Tuning page.
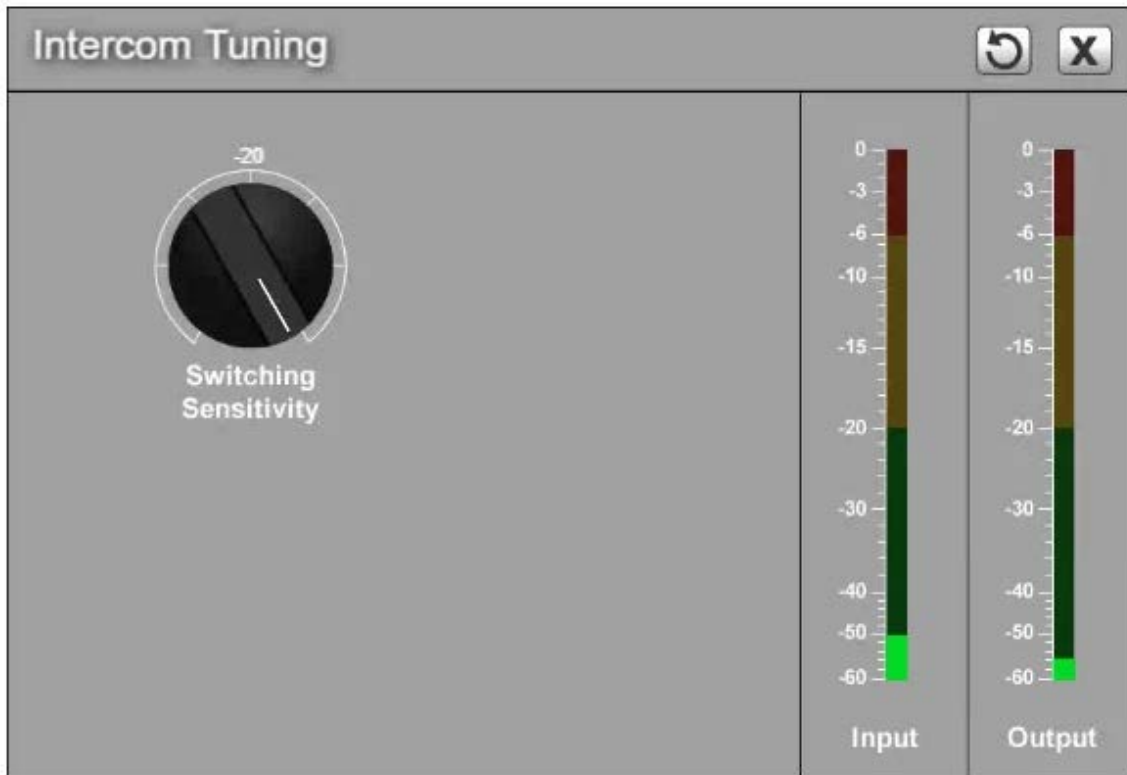
Figure 9. Intercom Tuning Settings

The Intercom Tuning page has LEDs for input and output signals and contains the following settings (see *Table 9*).

Table 9. Intercom Tuning Settings

Switching Sensitivity	Specifies the input level above which the Admin Phone transmits, below which the Entry Door Phone transmits.
	The range is -90 to -20 dB.

17

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 -Argu-
  mentList "$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