System Administrator Guide
C4000 Series

Version 11.0

BOGEN

© 2018–2026 Bogen Communications LLC
All rights reserved
740-00064J
260819

All trademarks, logos, and brand names are the property of their respective owners. All company, product, and service names used in this document are for identification purposes only. Use of these names, trademarks, and brands does not imply endorsement.

Contents

Introducing the C4000 System 1
Understanding System Requirements 3
Whitelisted Web Addresses 3
Nyquist System Server Requirements 5
Network Application Services 6
Network Ports 7
Using the Web-Based User Interface 8
Client Requirements 8
Accessing the Dashboard 8
Making UI Selections 13
Configuring the C4000 13
Getting Help 15
Nyquist Training Videos 16

Configuring Your System 17
Security 17
VoIP Security 18
Passwords 19
Understanding System Parameters 20
Viewing System Parameters 20
Exporting a Report 23
Product License 24
Changing the Navigation Bar Order 29
Restarting the Server 29
Station Supervision 30
Email Configuration 31
Performing a System Update 34
Upgrade Debian Operating System Components 38
Configuring Automatic Software Download 41
Shutting Down the Server 43
Check Internet Site Access 44
Check Server Status 44
Custom Configuration 46
DHCP Server 47
Firewall 50
Network Traffic Capture 52
Lightweight Directory Access Protocol (LDAP) 57
DSC01/WBC Flasher Configuration 65

Setting System Parameters 67
Automatic Failover 84
Recoverable Failures 85
Automatic Failover Configuration 86
Automatic Failover Process 93
Failover Routines and Triggers 97
Using CoS Configuration 100
Editing CoS Parameters for a Station 104
Deleting CoS Parameters for a Station 104
Adding CoS Parameters for a Station 104
Managing SIP Trunks 104
How Nyquist Handles Incoming SIP Calls 105
How Nyquist Handles Outgoing SIP Calls 108
Dialing PBX Extensions via Nyquist SIP Trunks 109
Configuring SIP Tie-Trunks Between Nyquist and PBX Systems 110
Adding SIP Trunk Configuration Parameters 111
SIP Trunk Custom Configuration Settings 120
Registering as a Third-Party SIP Endpoint 121
Viewing SIP Trunks 122
Editing a SIP Trunk Configuration 123
Deleting a SIP Trunk Configuration 124
Viewing Outside Line Status 124
Editing Outside Lines 125
Discover Ports 126
Configuring Appliance Firmware 126
Viewing Firmware Stored on the Nyquist System Server 127
Viewing Devices With a Specific Firmware Installed 129
Uploading New Firmware to the Server 129
Checking for Updates 130
Selecting Devices for Firmware Update 130
Setting Default Firmware 131
Downloading Firmware to a Device 132
Editing Firmware 132
Viewing Release Notes for Firmware 132
Viewing Stations Linked to Firmware 132
Deleting Listed Firmware 133
Configuring Facilities 133
Viewing Facilities 134
Editing a Facility 135
Deleting a Facility 136
Adding a Facility 136
Appliance Discovery Wizard 138

Managing Stations, Zones, and Queues 141
Speaker Extension Muting 141

Viewing Station Configuration Settings 142
Editing Station Configuration Settings 155
Viewing I/O Controller Configuration Rules 157
Configuring I/O Controller Input Rules 162
Configuring I/O Controller Output Rules 164
Sample I/O Controller Configuration Rules 167
Viewing an I/O Controller Schedule 169
Adding an I/O Contacts Output Daily Schedule 169
Editing the Daily Schedule for an I/O Contact 171
Deleting an I/O Contacts Output Daily Schedule 171
Configuring Devices for Push-To-Talk 172
Configuring Ambient Noise Sensor 175
Configuring Intercom HDMI Module Display Options 176
Configuring DSC and WBC Display Options 182
Deleting a Station 184
Adding a Station 185
Swapping a Nyquist Device 186
Using a Cisco SPA112 or ATA191/192 Analog Telephone Adapter 187
Using a Grandstream HT813 Adapter 190
Using the Yeastar TA2400 195
Using the Grandstream GXW4224 198
Customizing an NQ-T1100 IP Phone – Color Touch Display 201
Customizing an NQ-ZPMS Zone Paging Microphone Station 204
Routing Intercom Calls to PBX Extensions via SIP Trunk 207
Excluding Stations from Paging 208
Viewing Station Status 210
Viewing Appliance Status 212
Viewing Zone Information 214
Adding a Zone 215
Editing Zone Configuration 219
Cloning a Zone 219
Deleting a Zone 220
Simplified Configuration 220
Displaying Device Status 221
Paging Zones, Time Zones, and Audio Zones 222
Device Discovery 225
Page Queuing 225
Viewing Queues 227
Adding a Queue 228
Editing a Queue 229
Deleting a Queue 229
Sound Masking Zones 229
Viewing Sound Masking Zones 230
Adding and Editing a Sound Masking Zone 232

Managing Amplifiers and Gateway Devices 236
Viewing Amplifier and Gateway Devices 236
Adding Amplifier and Gateway Devices 238
Editing Amplifier and Gateway Devices 241
Configuring Push-To-Talk for a Public Address Mixer Amplifier 242
Using Station Management for Amplifiers and Gateway Devices 244
Deleting Amplifier and Gateway Devices 245

Managing Roles and Users 246
Viewing Roles 246
Adding a Role 247
Editing a Role 248
Assigning and Editing Permissions 248
Deleting a Role 250
Viewing Users 251
Adding a User 252
Understanding User Information 254
Deleting a User 255
Editing User Information 256
User Logging 256

Using Admin Groups 258
Viewing Admin Groups 258
Editing an Admin Group 259
Deleting an Admin Group 260
Adding an Admin Group 260

Managing Schedules 262
Understanding the Site Page 262
Using Site Settings 263
Renaming a Site 264
Adding a Schedule 264
Copying a Schedule 265
Replacing a Schedule 266
Reviewing and Editing a Schedule 266
Viewing Events for a Schedule 267
Editing Name and Description for a Schedule 268
Editing an Event 269
Deleting an Event 270
Adding an Event 270
Deleting a Schedule 272
Using the Calendars Feature 273
Schedule Popup Window Parameters 274
Using the Holidays Management Tool 275
Viewing Holidays 275
Adding a Holiday 276

Deleting a Holiday 277
Editing a Holiday 277
Exporting Holidays 277
Importing Holidays 278
Using the Schedule Announcements Feature 278
Adding a Schedule Announcement 280
Deleting a Schedule Announcement 282
Editing a Schedule Announcement 282
Using the Schedule Routines Feature 283
Add a Scheduled Routine 285
Edit a Schedule Routine 287
Schedule Routine Call Details Records 288
Retrieving First and Last Scheduled Events 288

Managing Audio 290
Audio Distribution 290
Managing Line-Input Sources 292
Managing Songs 294
Viewing the Song List 295
Playing Songs Directly from a USB Flash Drive 296
Adding Songs 296
Editing Song Information 298
Deleting a Song 299
Managing Playlists 299
Using Internet Radio Services 304
Creating an Audio Distribution 311
Starting and Stopping Audio Distribution 313
Other Features and Audio Distribution 317
Audio Distribution Status 317
Using the Admin Phone 319
Using Announcements 319
Announcements, Facilities, Zones, and Priorities 320
Recording Announcements 322
Adding an Announcement 322
Using SSML for Text-to-Speech Entries 325
Viewing Announcements 328
Editing Announcements 329
Deleting an Announcement 331
Creating Temporary Announcements from Routines 331
Managing Tones 332
Viewing Available Tones 332
Adding Tones 333
Editing Tones 339
Deleting a Tone 341
Tone Operational Notes and Limitations 341

Managing Recordings 342
Zone Control: Volume and Audio Distribution Panel 344
Initial Setup and Settings 344
Zone View 347
Audio Distribution Window 348

Maintenance and Troubleshooting 349
Backing Up Your Nyquist System and Files 349
Viewing System Backup Files 350
Creating a Backup File 352
Deleting a Backup File 352
Editing System Backup/Restore Information 353
Editing Backup Settings 354
Exporting a Backup File 357
Restoring a Backup File 358
Importing a Backup File 358
Software Components List 359
Using System Log Files 359
Viewing System Log Files 361
Exporting a Log File 362
Using the Call Details Feature 362
Viewing Call Details Records 363
Exporting and Printing a Call Log 363
Deleting All Call Records 364
Tuning Volume with White or Pink Noise 364
Troubleshooting Common Issues 365
Dashboard Messages 367
911 Call Errors 369
Maximum Concurrent Call Error 369
Equipment Errors 369
Facility Error Conditions 370
Automatic Failover Messages 371
Zone Overlap Messages 372
Finding Nyquist System Controller's IP Address 372
Changing a System Controller's IP Address 373

Performing Tasks via the Dashboard 375
Viewing Messages 376
Weather Alert messages 376
Starting Pages 377
Single-Zone Paging 378
Record Page 379
Prepend Page 380
All Call Paging 381
Emergency All Call Paging 382
Facility Paging 383

Multi-Site All Call Paging 384
Multi-Site Emergency All Call 385
Backup Paging from an NQ-T1100 Admin Phone 386
Inter-Facility Calling and Paging Passwords 387
Managing Alarms via the Dashboard 388
Managing Tones via the Dashboard 389
Managing Announcements via the Dashboard 390
Facility Announcement 391
Managing Calls via the Dashboard 393
Receiving Calls 393
Placing Calls 394
911 Dashboard Alerts 396
Call Forwarding 398
Requesting a Callback 398
Receiving and Returning a Callback 399
Using Page Exclusion 399
Deleting From Page Exclusion List 401
Viewing the Schedule for the Week 401
Using Audio Distribution 402
Enabling and Disabling Audio 404
Manually Controlling Output Contacts 406

Using the Maps Feature 407
Maps Panel Overview 408
Configuring Parameters for the Maps Feature 409
Assigning Maps Panel Permissions 409
Setting CoS Configurations for the Station 410
Assigning the Default Map 410
Adding a Site Graphic 410
Adding a Defined Action Object 411
Assigning an Image to Defined Action Object 412
Editing a Defined Action Object 413
Starting Pages and Announcements via the Map Feature 417
Page an Individual Zone 417
Page or Play Announcement at Multiple Selected Facilities 418
Start All Call or Emergency All Call Pages 419
Calling an Extension via the Maps Feature 420
Using Maps for Check-In 421
Creating a Map Object for Check-In 422
Monitoring Check-In 422
Using Check-In Routines from Maps View 423
Deleting a Defined Action Object 424
Deleting a Graphic 424

Using Routines 425
Starting and Stopping a Routine from the Admin Web UI 426

Starting and Stopping a Routine from the Admin Phone 426
Using the Routines API 428
Invoking a Routine via the Routines API 428
Viewing Routines 448
Adding a Routine 450
Editing a Routine 451
Cloning a Routine 452
Deleting a Routine 452
Creating and Executing Multi-Site Routines 452
Multi-Site Call Detail Records 453
Triggers 453
Viewing Triggers for a Routine 453
Adding a Trigger 455
Editing a Trigger 455
Deleting a Trigger 456
Understanding Trigger Parameters 456
Actions 456
Viewing Actions for a Routine 457
Adding an Action 458
Editing an Action 458
Cloning an Action 459
Understanding Action Parameters 460
Using Email Action to Send Text Message 460
How Actions Impact Other Actions 462
Zones and Stations Parameters for Deleting Display Messages 466
Using Variables for Dashboard, NQ-GA10PV, NQ-DSC01, and NQ-S1810WBC Text Parameters ..
467
The $weather variable and the OpenWeather API 475
Using Variables in Dashboard and NQ-GA10PV Identifiers 477
Using Variables in Display-Msg Text 478
Reordering Actions 478
Condition Statements 478
Simple Conditions 479
Advanced Conditions 480
Condition Statement Functions 481
Available Condition Variables 487
Routines Log 492
Exporting a Routine 494
Importing a Routine 494
Managing Routine Database Variables 495
Importing and Exporting Database Variables 496

Managing Display Messages 498
Message Priorities and Precedence 499
Message Precedence Rules 499
Creating a Display Message via the Dashboard 501

Using Color in Display Messages 505
Removing Display Messages via the Dashboard 508
Removing an Event Name from a Display 511
Viewing Message Templates 511
Viewing Message Images 513
Creating a Message Template via the Message Templates Page 514
Create or Edit a Message Image 514
Create or Edit a Message Template 515
Displaying a Message from the Message Templates Page 521
Deleting a Saved Message Template 522

Manage Check-In 523
Managing Check-In Status 523
View Check-In Status on NQ-GA10PV display 525
Starting Check-In 525
Ending the Check-In Process 527
Resetting the Check-In Process 527
Using Spy Mode 528
Configuring Check-In 528
Managing Exclusion and Vacancy Lists 530
Check-In Routine Actions and Triggers 532
Creating and Using Multiple Check-In Routines 532
Check-In Log and Call Detail Records 533

Managing Weather Alerts 535
Alert Filters Configuration 535
NWS Alert Routines 539
View NWS Alert Routines 539
Add or Edit an NWS Alert Routine 540
Display NWS Alerts Using a Routine 547
Setting Variables for the Display Message 548
$auto_resize Parameters 549
$alerts Parameters 549
Viewing National Weather Service Alerts 560
Viewing NWS Alerts on NQ-ZPMS Admin Phone 560
Viewing NWS Alerts on NQ-T1100 Admin Phone 562

Appendix A: Bogen Digital Certification Authority 565
Installing Certification Authority on Windows System 565
Installing Certification Authority on Mac System 566
Installing Certification Authority on an Android Device 567
Installing Certification Authority on an iOS Device 567
Viewing the Certificate 567

Appendix B: Acronyms and Abbreviations 569

Appendix C: Nyquist DTMF Feature Dialing Codes 574
Alarm/Tone Activation 575
Announcements 576
Calling 577
Call Parking/Call Pickup 578
Call Forwarding 578
Conferencing 579
Call Transfer 579
Monitoring/Recording 580
Paging 581
Voicemail 582
Walking CoS 583
Dial Codes Used for Simulating Calls to Admin Station from Station Call Switches 583
Audio Distribution 584
Routines 584
Miscellaneous Dial Codes 585
Alternate Dialing Codes 586

Appendix D: Routine Action Types 587
Routine Action Parameter Descriptions 587
Overriding Routine Action Parameters via Routines API v2 611

Appendix E: Routine Trigger Types and Parameters 615

Appendix F: C4000 Software Licenses 622
Nodelocked License Activation Key 622
Product License Activation Key (NQ-C4000-B1, B2, B3, B4) 622
Feature License Activation Keys 622
Concurrent Call License Expansion Package (NQ-C4000CCLX) 623
System Software Update Subscriptions (NQ-C4SWUP3YRB1, B2, B3, B4) 623
Intercom Call License (NQ-C4000ICL) 624
Map-Based Paging License (NQ-C4000MBP) 624
Paging Zone License Expansion Package (NQ-C4000PZX) 624
Queued Paging/Page Stacking License (NQ-C4000QPL) 624
Text-To-Speech License (NQ-C4000TTS) 625
Automatic Failover License (NQ-C4000AFL) 625
Sound Masking License (NQ-C4000SML) 625
System Software License Bundle Upgrades 625
NQ-C4000-B12UP Nyquist C4000 Series System Software License Bundle Upgrade - B1-B2 ..625
NQ-C4000-B23UP Nyquist C4000 Series System Software License Bundle Upgrade - B2-B3 ..626
Nyquist C4000 Series System Software License Bundle Upgrade - B3-B4 626

Introducing the C4000 System

The Nyquist C4000 is a TCP/IP-based solution for commercial paging and audio distribution applications. It addresses the unique communication needs of various types of businesses, including industrial facilities, transportation hubs, retailers, offices, restaurants, and bars.

Note: This guide describes the tasks, including configuration tasks, that you can perform if you are assigned an **Admin** role with proper permissions and if your **Station Type** is an **Admin Web Interface**. If you are assigned a **User** role, refer to the *C4000 User Guide* and to *"Performing Tasks via the Dashboard" on page 375* of this manual. For information about station types, see *"Viewing Station Configuration Settings" on page 142*. For information about roles, see *"Managing Roles and Users" on page 246*.

The heart of the C4000 system is a robust, state-of-the-art System Controller (NQ-SYSCTRL) that comes preinstalled with the Nyquist application software. The System Controller features an easy-to-use web-based graphical user interface (GUI) accessible through almost any personal computer (PC), tablet, or mobile device from any location in the connected world.

Note: See *"Network Application Services" on page 6* if you elect to *not* use the Nyquist System Controller (NQ-SYSCTRL).

Figure 1. Nyquist System Controller

The solution features a built-in streaming Internet radio service, *airable*, and optional custom-tailored music selections from *SoundMachine*, the premier music subscription service for business. Both services are perfect for a wide variety of background music applications. SoundMachine gives large and small retailers, restaurants, bars, or any other company looking to enhance their customer experience the ability to craft a seamless, engaging, and on-brand music experience using commercially licensed content.

Available feature-rich IP phones and purpose-built networked appliances provide convenient communication, control, and interoperability with third-party devices and systems such as access control, fire alarm, clock, and PBX systems.

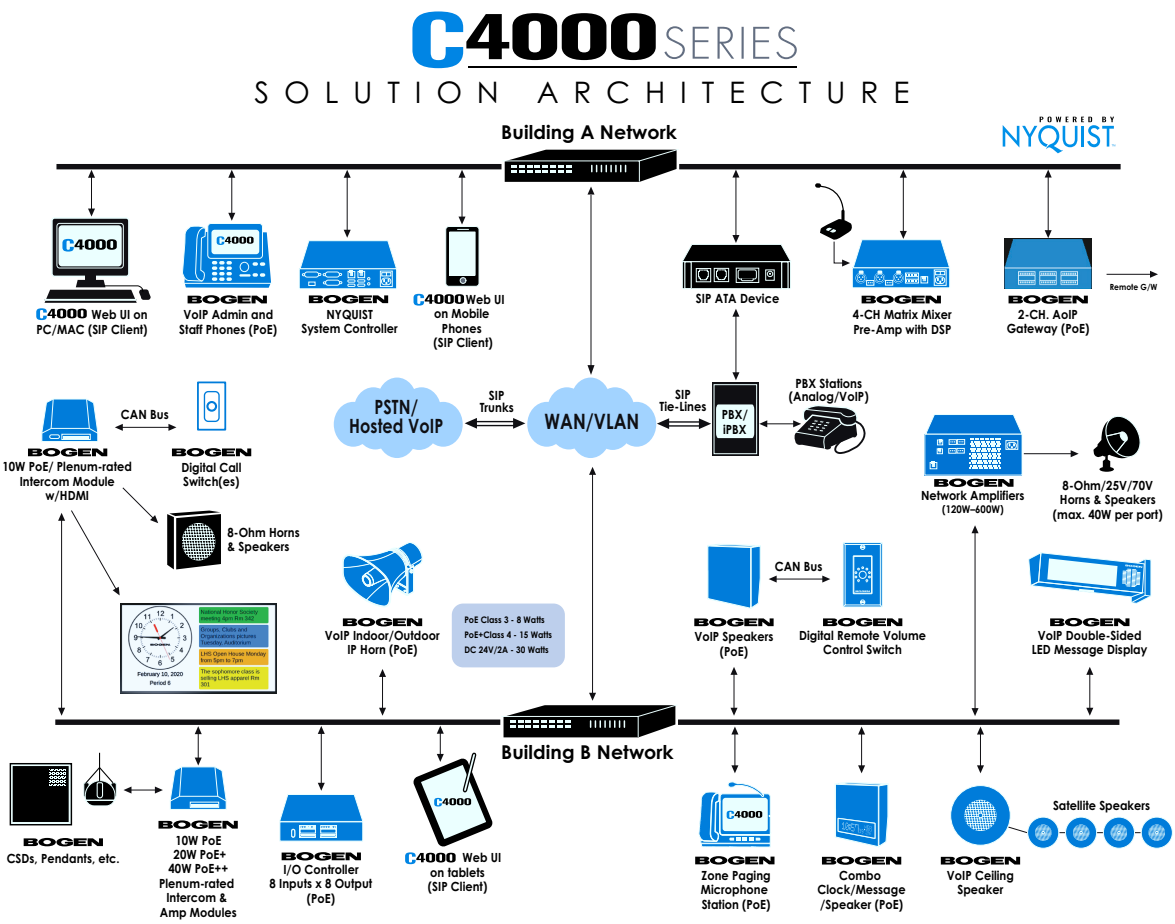


Figure 2. Example of C4000 Network

The C4000 system supports the following hardware:

- Desktops, laptops, tablets, and mobile phones (Android, Apple, and Windows) that support the full Google Chrome or Microsoft Edge web browser—or an Apple iPhone or iPad device running iOS 14 forward using the Safari browser—to access the C4000 Admin Web user interface (UI)
- C4000-certified Voice-over-IP (VoIP) phones
- Nyquist appliances

For information about the Nyquist appliances that work with the C4000 system, visit:

https://www.bogen.com

For information about training resources for the C4000 and other Bogen products, visit:

https://www.bogen.com/BogenUniversity

Understanding System Requirements

Whitelisted Web Addresses

The C4000 requires access to specific Uniform Resource Locators (URLs), commonly referred to as web addresses. Access to many of these web addresses is required during installation; access to other web addresses, such as the address for the Network Time Server (NTS), are required during runtime. The Information Technology (IT) department for the site may need to whitelist the web addresses so that they can be accessed as needed.

C4000 access to these URLs can be checked via the **Check Internet Site Access** feature on the **System Parameters** page or by pressing the **Check Internet Site Access** button on the **Network Wizard** page during product activation.

The following table lists the URLs that should be whitelisted.

Table 1. Whitelisted URLs

URL	Description
http://hostedactivation.com (specifically, http://hostedactivation.com/bogen)	Required for C4000 License support
http://downloads.digium.com	Required for downloads from Digium Phone Module for Asterisk (DPMA)
http://downloads.asterisk.org/ (specifically, http://downloads.asterisk.org/pub/telephony/sounds/releases)	Required for sounds download
http://www.pjsip.org/	Required for PJSIP download
http://ftp.us.debian.org (specifically: http://ftp.us.debian.org/debian/)	Required during Linux package installation
http://deb.debian.org/debian/	
https://deb.debian.org/debian/	
http://security.debian.org (specifically: http://security.debian.org/)	Required during Linux package installation
stun01.sipphone.com	Required for STUN-based IP address resolution
stun:stun01.sipphone.com	(This is used by the C4000 Web UI and should be enabled on the computer that runs the web UI.)
https://raw.githubusercontent.com/	Serves unprocessed versions of files stored in the GitHub repositories.
http://2431612419.airable.io	The *airable* URL for Internet-based-radio Audio Distributions
https://2431612419.airable.io	

Table 1. Whitelisted URLs

URL	Description
http://api.sound-machine.com https://api.sound-machine.com	The SoundMachine URL for Internet-based-radio Audio Distributions
http://api.bogenedu.com/api/customers	Required for C4000 warranty support
http://bogen-ssu.bogen.com/	Bogen System Software Update server. Required for automatic Nyquist server software and Nyquist firmware software update notifications and downloads.
https://www.weather.gov/alerts	Required for displaying weather alerts.
https://ipapi.co	Required for automatically finding county code for alerts.
https://api.weather.gov	Required for obtaining alerts from the National Weather Service.
http://openweathermap.org http://api.openweathermap.org	Required for obtaining current weather conditions.
ns1.google.com resolver1.opendns.com	Required for obtaining the Nyquist server's public IP address for Audio Distribution streams and for automatically finding the county code for alerts.
dl-ssl.google.com	Required for Nyquist installation and updates to download and install Google Chrome browser.

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

The default URLs for the STUN and TURN servers are not set.

The default URL for NTS is time.google.com.

Nyquist System Server Requirements

The following are the minimum requirements for the C4000 if you elect not to use the Nyquist System Controller (NQ-SYSCTRL):

Table 2. Nyquist System Server Minimum Requirements

OS	Debian Linux OS (AMD 64-bit version) release 12.13 or a higher minor revision of release 12. *Note:* Refer to the most up to date Release Notes on the www.bogen.com web site for details about which Linux OS versions have been tested for use with the C4000.
CPU	Quad-core Intel-based processor running at 3.0 GHz or higher
Memory	8 GB Error Correcting Code (ECC) RAM is recommended for increased performance and reliability.
Disk Storage	One 250 GB disk drive Some form of hardware-based Redundant Array of Independent Disks (RAID) is recommended for redundancy and high availability. Consider using a larger drive if large amounts of audio (for example, voice mail, announcements, recordings, and music) are being stored on the system. Note that music, tones, and announcements created or stored as WAV files will be larger than if created or stored as MP3 files. Other factors that should be considered are: • How often will backups be performed? • Will the system be backed up locally or remotely on a detachable drive, Storage Area Network (SAN)/Network Attached Storage (NAS), or Network File System (NFS)? • How many users will have voicemail ability? • How long will voicemail messages be stored? • Will voicemail messages be part of the local system backups?
Network Interface Card (NIC)	Minimum 1000 MB Ethernet port
PCI Expansion Slots	One or more Peripheral Component Interconnect (PCI)/PCI Express (PCIe) slot if telephony network connectivity other than, or in addition to, SIP trunking is required; contact your Bogen Dealer for assistance in determining these telephony hardware needs.
Telephony Interfaces	One or more PCI/PCIe type third-party telephony interface cards (for example, Foreign Exchange Office [FXO], Foreign Exchange Subscriber [FXS], etc.) if telephony network connectivity other than, or in addition to, SIP trunking is required; contact your Bogen Dealer for assistance in determining these telephony hardware needs.

Network Application Services

Required application services will be installed automatically on the C4000 as part of the Nyquist software installation. All other network services must be already present or installed manually on the associated network. The following table lists the services and their locations:

Table 3. Network Application Services

Service	Description	Required	Location
Apache	Used as the web server to drive the C4000 web interface.	Mandatory	C4000
DHCP	Supplies dynamic IP addresses to the C4000 system server and associated devices. (DHCP is the acronym for Dynamic Host Configuration Protocol.) It also supplies the Trivial File Transfer Protocol (TFTP) server IP address or host name to devices on the network via option_66.	Optional	Network and/or C4000
DNS	Resolves host names to IP addresses. DNS is an acronym for Domain Name System, a hierarchical naming system for computers, servers, or other resources connected to either the Internet or to a private network.	Mandatory[a]	Network
ICE STUN TURN	Resolves IP addresses behind Network Address Translation (NAT)/firewall. • Interactive Connectivity Establishment • Session Traversal Utilities for NAT • Traversal Using Relays around NAT	Optional	C4000 Network
LDAP	LDAP is used by the C4000 to import users into the Nyquist system.	Optional	Network
NTP	Network Time Protocol provides date/time synchronization for the C4000 and the associated devices (IP Phones, appliances).	Mandatory	Network
SNMP	Provides the C4000 Linux server statistics via Simple Network Management Protocol (SNMP) v1 through Port 161.	Optional	C4000
TFTP	TFTP is used by IP phone and C4000 device provisioning. A TFTP server runs on the C4000 on port 69 (the standard TFTP port #). Device provisioning files are stored on the C4000 in directory: `/srv/tftp`. This is the only directory exposed by the TFTP server.	Mandatory	C4000

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

Network Ports

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

Table 4. Network Ports Used by Nyquist

Service	Description	Port
Automatic Failover	Local ports used for Automatic Failover support. These only need to be available between the two servers.	5405,2224,3121
DHCP	Dynamic Host Configuration Protocol (Optional)	67, 68
DNS	Domain Name System (Optional)	53
HTTP	Hypertext Transfer Protocol Used for phone provisioning.	8088
HTTP	Provide access to Bogen product information.	80
HTTPS	Secure HTTP	8089
HTTPS	Secure HTTP (HTTP over TLS/SSL) Provides access to Bogen product information.	443
IAX	Inter-Asterisk eXchange Used for inter-facility communications.	4569
LDAP	Lightweight Directory Access Protocol	389
LDAP over TLS	Lightweight Directory Access Protocol over Transport Layer Security	389 (configurable)
NTP	Network Time Protocol	123
ODBC	Open Database Connectivity Provides database connectivity.	3306
RLM	Reprise License Manager Provides Nyquist license activation via hostedactivation.com.	80
RSYNC	Remote sync utility Used to synchronize files (Automatic Failover Only).	873
RTP	Real-time Transport Protocol Used for distribution of audio streams.	10000–20000 (configurable)
secure-mqtt	Nyquist control messages between Nyquist server and Nyquist appliances	8883
Server Management	Local port used for server management **DO NOT** allow outside access to this port. During system controller installation, an IP filter rule is installed to block outside access to this port.	5038
SFTP	Provide access to Bogen product information.	22
SIP	Session Initiation Protocol (SIP) Transfer Control Protocol (TCP)/User Datagram Protocol (UDP) connections	5060, 5061
SIP over Web Services	SIP WS/WSS connections	8088
SNMP	Simple Network Management Protocol (Optional)	161

Table 4. Network Ports Used by Nyquist

Service	Description	Port
SRTP	Secure Real-time Transport Protocol	(same as RTP)
TFTP	TFTP connections	69

Using the Web-Based User Interface

The web-based UI is an interactive dashboard that presents system information and parameters in an easy to read and use format. The view of the dashboard varies depending upon the permissions (i.e., role) assigned to the user (see *"Viewing Roles" on page 246*).

Client Requirements

The Nyquist web-based UI is accessed through a client, which can run on PCs, Macs, and Android tablets and mobile devices that support the full Google Chrome or Microsoft Edge web browser, as well as the Safari browser from an iPhone or iPad device running iOS 14 (or later). In addition to supporting Chrome, Edge, or Safari, the client must have a sound card and a microphone.

The Bogen Certification Authority (CA) digital certificate must be installed on the client. This certificate is created by, and downloaded from, the Nyquist C4000 server 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 588*.

Important: If one or more system updates have been installed since the last time the server's certificate was generated, or if you receive an HTTP error or redirection when downloading the certificate file (e.g., 302 Found), you may need to generate a new server certificate before proceeding (see *"Generate Server Certificate" on page 80* for details).

Accessing the Dashboard

Caution Do not use third-party browser extensions with the Nyquist user interface as they may interfere with functionality. If you have browser extensions that you want to use for non-Nyquist browsing, you may want to consider creating a Nyquist-specific browser profile for which all extensions are uninstalled or disabled. See your browser documentation for details regarding profiles.

To access your dashboard:

1 From your Chrome, Edge, or Safari browser, type the C4000 System Controller's IP address or DNS name into the address bar (for example, `https://192.168.1.0`) and press **Enter.**

Tip: If you do not know the C4000's IP address but you have physical access to the Nyquist System Controller, see *"Finding Nyquist System Controller's IP Address" on page 372*.

2 On the *Login* page, type your username and password. (See *Figure 3, "Login Page"*.)

The name of the C4000 system, as defined on the *System Parameters* page (see *Table 23, "Edit System Parameters Page," on page 69*), is displayed on the login page. This can be helpful when managing multiple Nyquist systems.

Tip: To change your password, enable the **Change Password on Next Login** option on the C4000 *Login* page. The *next* time you log in, you will be redirected to a page that prompts you for a new password (https://<server>/reset_password).

If you have forgotten your password, an Admin can change the password via the **Change Password** field of the *Edit User* page (see *"Editing User Information" on page 256*).

---

3 Select **Login**.

4 If your account is already logged in, either on another machine or in another browser session, you will be prompted to log out of the other session and continue. Selecting **No** will return you to the *Login* page.

5 Once logged in, if the current user account is still configured with Bogen's default password, a warning will be displayed reminding you to change the password. Select **OK** to continue.

Warning It is strongly recommended that you do *not* use the default Nyquist password, as it is publicly available and, therefore, not secure. There are also some features that cannot be accessed, such as changing the Nyquist Control Password (see *"Nyquist Control Password" on page 81*), until the current user's password has been changed.

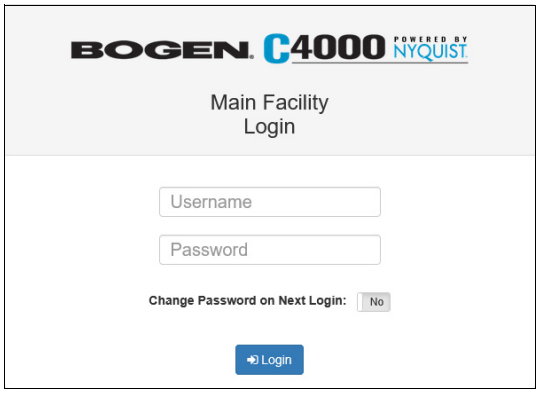


Figure 3. Login Page

Note: The Nyquist system does not support opening multiple sessions of the Nyquist Web UI. Logging into a second session will log off the first session (after user confirmation).

The dashboard that appears depends on whether your station is an *Admin Web Interface* or a non-administrator *Web Interface*.

If you are using the Admin Web Interface and have permissions for configuration tasks, your dashboard will be displayed as shown in *Figure 4, "C4000 Dashboard for Admin Web Interface," on page 10*.

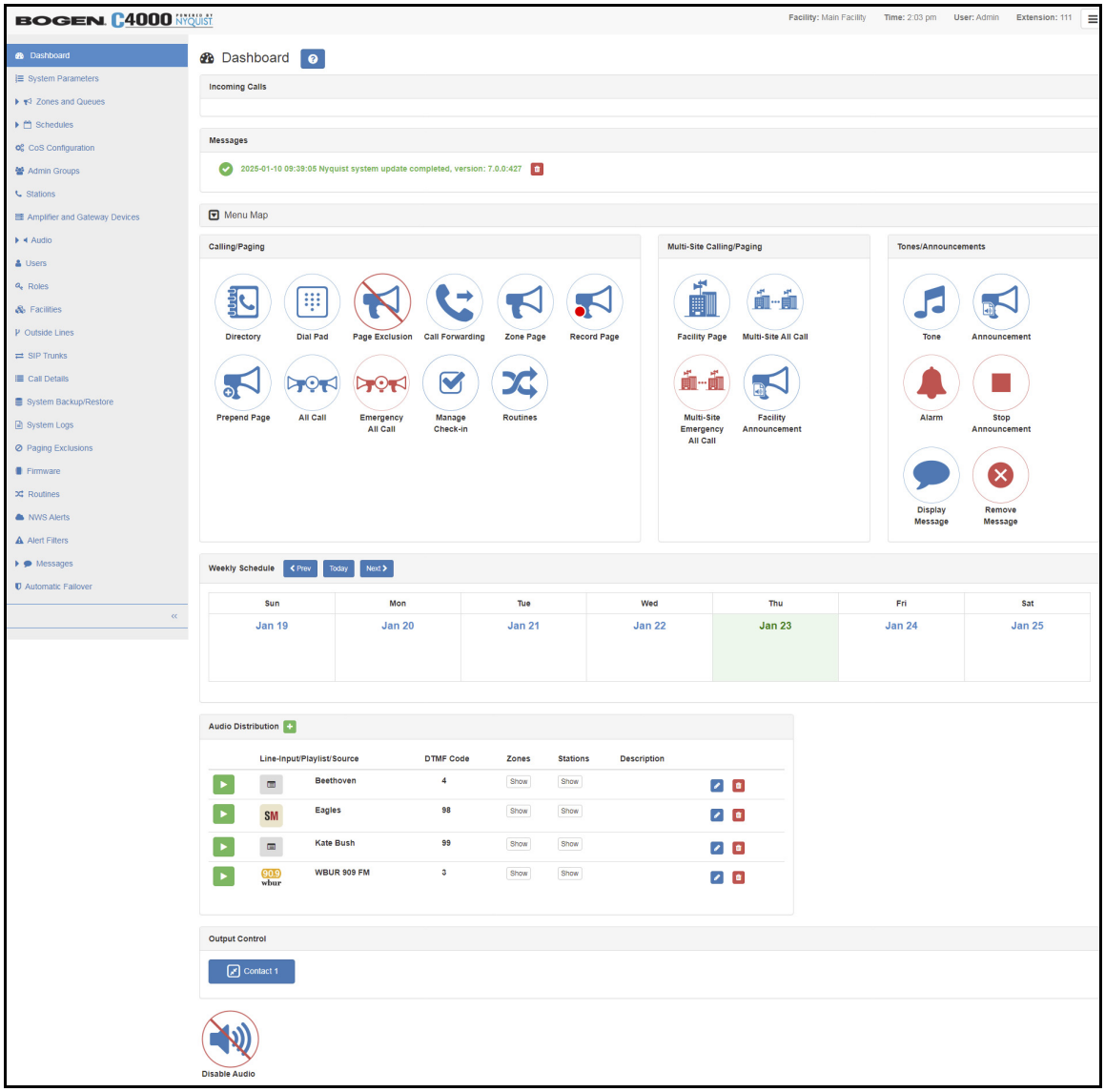


Figure 4. C4000 Dashboard for Admin Web Interface

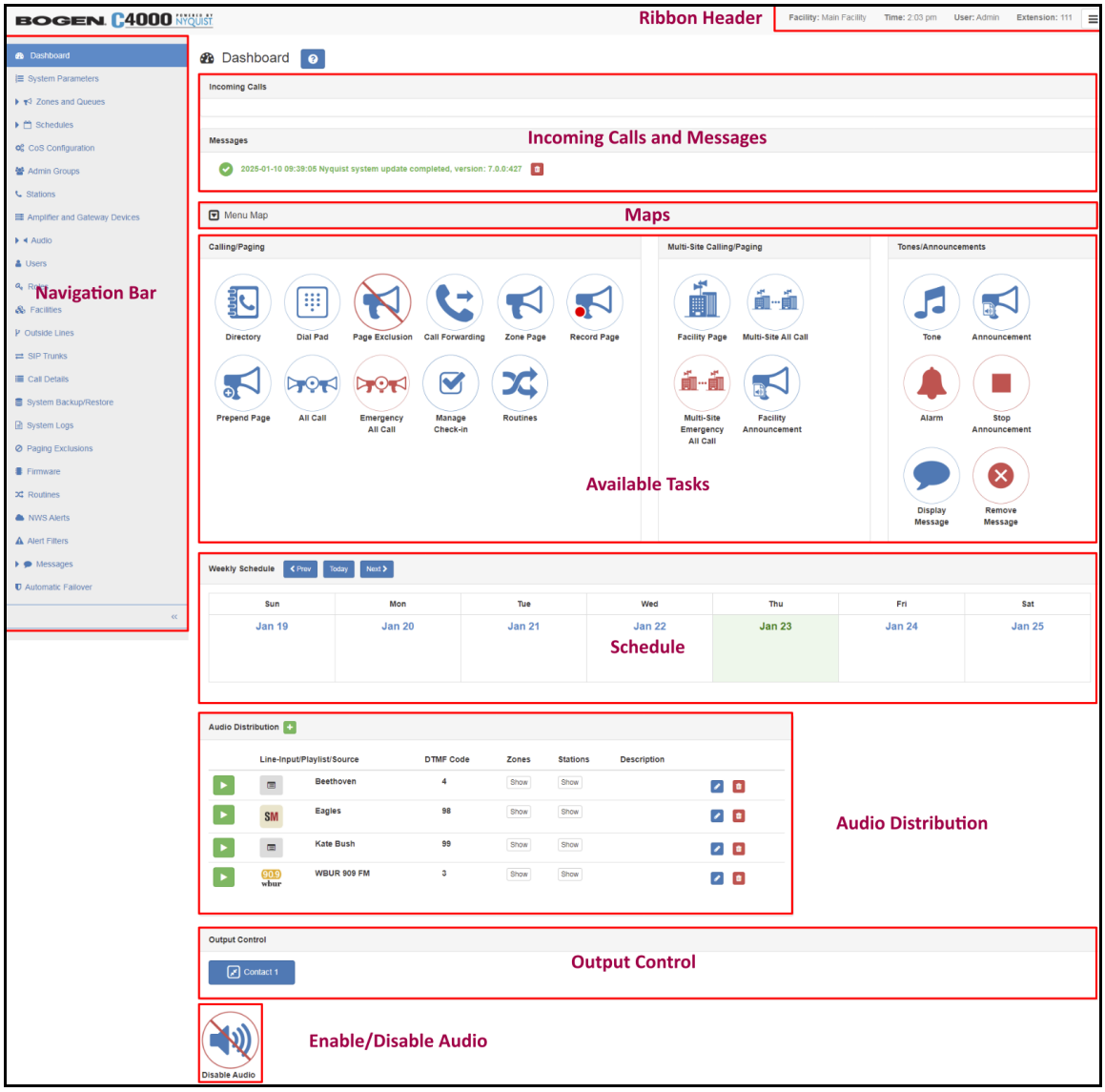


Figure 5. Dashboard Areas

The left side, or navigation bar, of the dashboard (*Figure 5, "Dashboard Areas," on page 11*) lists the areas of the C4000 system that you can access. Accessibility to C4000 features and functionality is controlled by the user's assigned role.

The right header ribbon provides the facility name, server time in hours and minutes, the username for the account, the extension for the station, and the collapsed menu icon (aka "hamburger button"). The facility name and server time will not appear if the screen is reduced in size, such as when viewing from a phone or tablet.

Incoming Calls and Messages appear on the top right dashboard pane. The Maps Panel appears below the Messages Panel.

When Maps is licensed and configured for a C4000 system, you can view the Maps Panel from the Dashboard. The panel appears below the Messages Panel.

The majority of the dashboard is set up to allow you to perform communications activities, view this week's schedules, and perform audio distribution.

The navigation bar does not appear for users not authorized to make changes to the C4000 configuration. Instead, those users see only standard tasks, such as calling an extension. For details about tasks commonly performed by office staff, see:

- *"Performing Tasks via the Dashboard" on page 375*
- *"Using the Maps Feature" on page 407*

Tip: It may be helpful to distribute printouts of key sections of this manual to front office staff, such as *"Performing Tasks via the Dashboard" on page 375* and *"Using the Maps Feature" on page 407*.

At the top of the dashboard, messages appear that can provide information about your system (see *Figure 6, "Dashboard Messages," on page 12*), such as any stations or devices that were connected to your server but now are not appearing to be connected or responding. (See *"Dashboard Messages" on page 367*.)

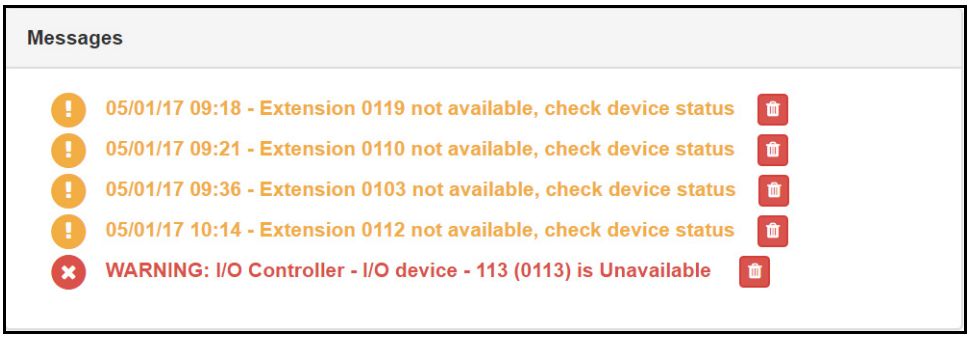


Figure 6. Dashboard Messages

If an I/O Controller rule's **Action** has been set to **Manual**, a dashboard button appears in the Output Control section of the dashboard that can be used to manually close or open specified output contact. (See *"Viewing I/O Controller Configuration Rules" on page 157*.)

On the lower part of the dashboard are options for Audio Distribution and an **Enable/Disable Audio** button that you can toggle to enable or disable audio.

For detailed information about performing tasks from the dashboard, see *"Performing Tasks via the Dashboard" on page 375*.

Making UI Selections

You can navigate and make UI selections by either using a mouse click or using touchscreen functionality. The UI provides buttons, which appear with a name and a graphic, and icons, which are graphics only.

Table 5. UI Icons

Icon	Description
	Add icon: Add an item.
	Edit icon: Edit an item.
	Delete icon: Delete an item.
	Information icon: Provides additional information, such as viewing release notes for firmware (see *"Viewing Release Notes for Firmware" on page 132*).
	Link icon: Links to a web page that contains related information or functionality.
	Update All: Apply a setting to all items in a list.
	Help icon: View feature help for the displayed page.
	Hamburger icon: Display a menu of options.

Configuring the C4000

Before configuring your C4000, you must first perform the initial setup, which is documented in the *Nyquist System Controller Setup Guide*. The initial setup process includes network configuration, among other things, some of which can only be performed through wizards. For example, configuring whether the C4000 will use a static IP address or DHCP can only be configured in the Network Wizard (which can also be accessed at `https://<server>/setup/network`).

You must configure your system and the C4000 features to best suit your organizational needs. For example, you must determine if your C4000 server is being used for just your site or for a multi-site environment.

Note: If the C4000 system server is used in a multi-site environment, All-Call and Emergency All-Call pages will be broadcast at all sites managed by that C4000 system server. If this is not the desired behavior, then each site should have its own C4000 system server. A single C4000 system server should not be used to manage multiple sites that are geographically separated because WLAN and power issues at one site could disrupt C4000 service at all locations.

The following table provides the suggested order for setting up your system and directs you to specific sections of the C4000 documentation for step-by-step instructions.

Table 6. C4000 Setup Tasks

Task	Reference
Configure the servers for Automatic Failover, if the appropriate license has been purchased.	See *"Automatic Failover Configuration" on page 86*.
Set the dialing length and other System Parameters to the desired values.	See *"Setting System Parameters" on page 67*.
Set the Class of Service (CoS) configurations.	See *"Adding CoS Parameters for a Station" on page 104*.
Determine the number of Admin Phones and Web Admin stations and configure these stations.	See *"Adding a Station" on page 185*.
Determine the number of Admin Groups, if any, that you need and create them.	See *"Adding an Admin Group" on page 260*.
If outside lines are being used, use the Discover Ports feature to configure outside lines and enable outside access for stations authorized to make or receive outside calls.	See *"Discover Ports" on page 126* and *"Editing Station Configuration Settings" on page 155*.
If staff IP phones will be used, determine how many are planned and configure these stations.	See *"Adding a Station" on page 185*.
If needed, configure the roles for the Web Admin interface.	See *"Adding a Role" on page 247*.
If needed, configure the users for the Admin Web interface.	See *"Adding a User" on page 252*.
Use Nyquist DHCP Server for initial discovery of Nyquist appliances and VoIP phones.	See *"DHCP Server" on page 47*.
If using VoIP speakers, I/O Controllers, MMPAs, VoIP Intercom Modules, or Audio Power Amplifiers, configure the stations using the C4000's Auto Discovery feature.	See *"Adding a Station" on page 185*.

Table 6. C4000 Setup Tasks

Task	Reference
Configure page, time, and audio zones and assign stations to these zones.	*Note:* If you want tones to interrupt active pages, you must create separate page and time zones, and the time zones must be created first. Creating time zones first sets the priority of time zones over page zones. Stations can be in multiple zones. See *"Adding a Zone" on page 215*.
If using tones to announce an alarm or an event, define the tones that will be available for C4000.	See *"Adding Tones" on page 333*.
If using playlists with C4000, create playlists and download songs.	See *"Adding Songs" on page 296* and *"Creating a Playlist" on page 300*.
Define the site start and end dates.	See *"Reviewing and Editing a Schedule" on page 266*.
Configure events for bell schedules, including tones and Scheduled Audio.	*Note:* If you want tones to play during active pages, you must create separate page and time zones, and the time zones must be created first. Creating time zones first sets the priority of time zones over page zones. Stations can be in multiple zones. See *"Adding an Event" on page 270*.
Schedule holidays.	See *"Adding a Holiday" on page 276*.
If a SIP trunk is being used, add the SIP trunk configuration to the C4000 and configure the station to use the SIP trunk for 911 calls.	See *"Adding SIP Trunk Configuration Parameters" on page 111* and *"Editing Station Configuration Settings" on page 155*.
If the C4000 system server will manage multiple facilities, add each facility to the C4000 system.	See *"Adding a Facility" on page 136*.

Getting Help

Help is available through the C4000 Admin Web UI and through Bogen's Technical Support. Technical Support is available between 9:00 a.m. and 5:00 p.m. Eastern Time, Monday through Friday. Technical Support contact information is as follows:

Technical Support: https://www.bogen.com/contact-tech-support
Telephone: 1-800-999-2809
Online training: https://www.bogen.com/BogenUniversity

Online help is available for most pages of the Admin Web UI via each page's **Help** button, .

Online help can also be accessed from the menu that appears in the upper right portion of the Admin Web UI's navigation pane. The menu contains the following options:

- **About**: Displays the version number and contact information for Bogen Communications LLC, links to the various license agreements, and links to the Bogen eLearning website.
- **Help Topics**: Provides help topics on using the C4000 system.
- **Admin Manual**: Accesses the PDF of this manual.
- **Nyquist Training Videos:** Navigates to the *Nyquist Training Videos* page (see *"Nyquist Training Videos" on page 16*).
- **Logout**: Logs the current user out of the C4000 system.

Nyquist Training Videos

The *Nyquist Training Videos* page, accessible via the hamburger ☰ menu of every page, displays a list of videos that provide training on various aspects of the Nyquist system. Each user can keep track of which training videos they have already watched.

Table 7. Nyquist Training Videos

Watched/ Unwatched	A user-settable flag that indicates whether or not the user has watched this video. This flag does not affect which videos can be watched; it is simply for the user's convenience.
Name	The name of the training video.
URL	A clickable link to the training video.
QR Code	Select the **Show** button to display a QR code that can be used to access the training video via a QR code reader, such as via a phone.

Configuring Your System

The Admin Web UI allows you to configure most of your Nyquist system, set passwords for the system and various system features, and gracefully restart or power down the Nyquist server through **System Parameters** (*see "Setting System Parameters" on page 67*). System configuration also includes the following:

- Setting parameters for what actions can be done from a specific station (*see "Using CoS Configuration" on page 100*)
- Setting what permissions are assigned to a user (*see "Managing Roles and Users" on page 246*)
- Configuring facilities for a multi-site server (*see "Configuring Facilities" on page 133*)
- Setting up stations, zones, and queues (*see "Managing Stations, Zones, and Queues" on page 141*)
- Updating firmware for Nyquist devices and stations (*see "Configuring Appliance Firmware" on page 126*)
- Setting parameters for SIP trunks (*see "Managing SIP Trunks" on page 104*)
- Disabling an outside line (*see "Editing Outside Lines" on page 125*)

Security

The C4000 provides several mechanisms that secure the C4000 environment.

VoIP security

SIP TLS and SRTP protocols can be enabled to provide secure SIP communications between participating appliances.

See *"VoIP Security" on page 18*.

Class of Service

Class of service (CoS) configurations define a call-in level and the system actions available to each CoS. Each station is then assigned a CoS to control the call-in level and available actions for that station.

See *"Using CoS Configuration" on page 100*.

Roles and Users

Access to the C4000 is granted via password-protected user accounts. User accounts are assigned to Roles, which specify the UI elements and actions that are available to users assigned to that role.

See *"Managing Roles and Users" on page 246*.

Passwords

Various passwords are used throughout the system for authentication purposes. These include web login passwords as well as passwords provided by appliances to interact with the C4000.

See *"Passwords" on page 19*.

Firewall Basic firewall functionality is available to block or allow access to the C4000 based on the client's IP address.

See *"Firewall" on page 50*.

Routines API key Access to the C4000's Routines API is only available to clients providing the system-wide API key.

See *"Invoking a Routine via the Routines API" on page 428*.

VoIP Security

Each station, SIP trunk, bridge, amplifier, and gateway device can be configured to authenticate and/or encrypt SIP sessions using the SIP TLS and/or SRTP protocols. These protocols authenticate and encrypt SIP and media streams, respectively, between the appliance (or trunk) and the C4000.

Although the C4000 allows secured appliances and trunks to communicate with unsecured appliances and trunks (i.e., the C4000's connection to one appliance may be secure, while it's connection to the other is not), it is strongly recommended that *all* SIP communications between *all* appliances be secured. Each appliance's configuration provides options to disable one or both of these protocols (i.e., **Enable SIP TLS** and **Enable SRTP**), but these are available primarily for troubleshooting or for devices that do not support these secure protocols.

Tip: To simplify this process, the **Nyquist Appliance VoIP Security** system tool (see *Table 24, "System Tools," on page 78*) enables the **Enable SIP TLS** and **Enable SRTP** settings for all Nyquist appliances. SIP trunks (see *"Managing SIP Trunks" on page 104*) and non-Nyquist appliances, however, must be configured individually.

Passwords

There are several different types of passwords that serve different purposes in the Nyquist system.

Table 8. Passwords

User Passwords	Each user has their own password. User passwords can be defined directly via the *Users* page (see *"Editing User Information" on page 256*) or via an LDAP server for systems that define their users via LDAP (see *"Lightweight Directory Access Protocol (LDAP)" on page 57*). *Tip:* Non-LDAP users can change their passwords via the Login page (see *"Accessing the Dashboard" on page 8*).
Web Passwords	Each Nyquist device that has a web interface requires a username and password to log into its web interface. The username and password are defined via the corresponding station, amplifier, or gateway device's **Web Password** configuration. Where a **Web Password** is not specified, the C4000's **Default Web Password** will be used. For details, see: • *Table 43, "View, Add, or Edit Station Configuration Parameters," on page 143* • • *Table 68, "Add/Edit Amplifier and Gateway Devices Parameters," on page 240*
Registration Password	Stations that will initiate or receive SIP calls must register with the Nyquist C4000 server each time they become available (e.g., after connecting to the network). To prevent unauthorized SIP clients from registering, a **Registration Password** is assigned to each station, and the Nyquist server, which remembers each station's password, authenticates the password during each station registration. Although each station can have a distinct registration password, it is very common to assign the same password to all SIP stations. To simplify manual configuration of stations, the C4000's **Default Registration Password** can be configured in the *System Parameters* page (see *Table 23, "Edit System Parameters Page," on page 69*). When a station is added, if its **Registration Password** is specified (*Table 43, "View, Add, or Edit Station Configuration Parameters," on page 143*), it will be used; but if not, the **Default Registration Password** will be used.
Nyquist Control Password	This password is used to secure Nyquist control messages between the C4000 controller and all associated Nyquist appliances to support certain Nyquist features, such as sound masking, amp protection mode, and station check-in. See *Table 24, "System Tools," on page 78* for details.

Table 8. Passwords (continued)

Facility Password	C4000 servers can communicate to other C4000 servers, where each server represents a facility. This enables such features as Facility Page, Multi-Site All Call, Multi-Site Emergency All Call, and Facility Announcement. Each server defines a **Facility Password** (see *Table 23, "Edit System Parameters Page," on page 69*), which must be specified by other servers when defining a remote facility (see *"Configuring Facilities" on page 133*).
DISA Passwords	The DISA passwords, **DISA Password** and **Security DISA Password**, can be used to secure access to the C4000's external DISA functionality. The **DISA Password** must be entered by an external caller to access DISA functionality when dialing in from an external line (i.e., a SIP trunk), such as accessing intercom calls, paging, etc. The **Security DISA Password** must be entered to authorize an external caller to enter Spy Mode from an external line (see *"Using Spy Mode" on page 528*). For more information, see **DISA Password** and **Security DISA Password** descriptions in *Table 23, "Edit System Parameters Page," on page 69*.

Understanding System Parameters

System parameters include key information that is unique to the system, including passwords, night ring characteristics, and telephony settings. (For more information on night ring behavior, see *"Configuring Night Call Options" on page 22*.)

Viewing System Parameters

Viewing system parameters can aid in troubleshooting. For example, if your calls are not being routed to the proper day or night Admin Station, you should check that the system parameters settings for **Day Start** and **Night Start** time are correct.

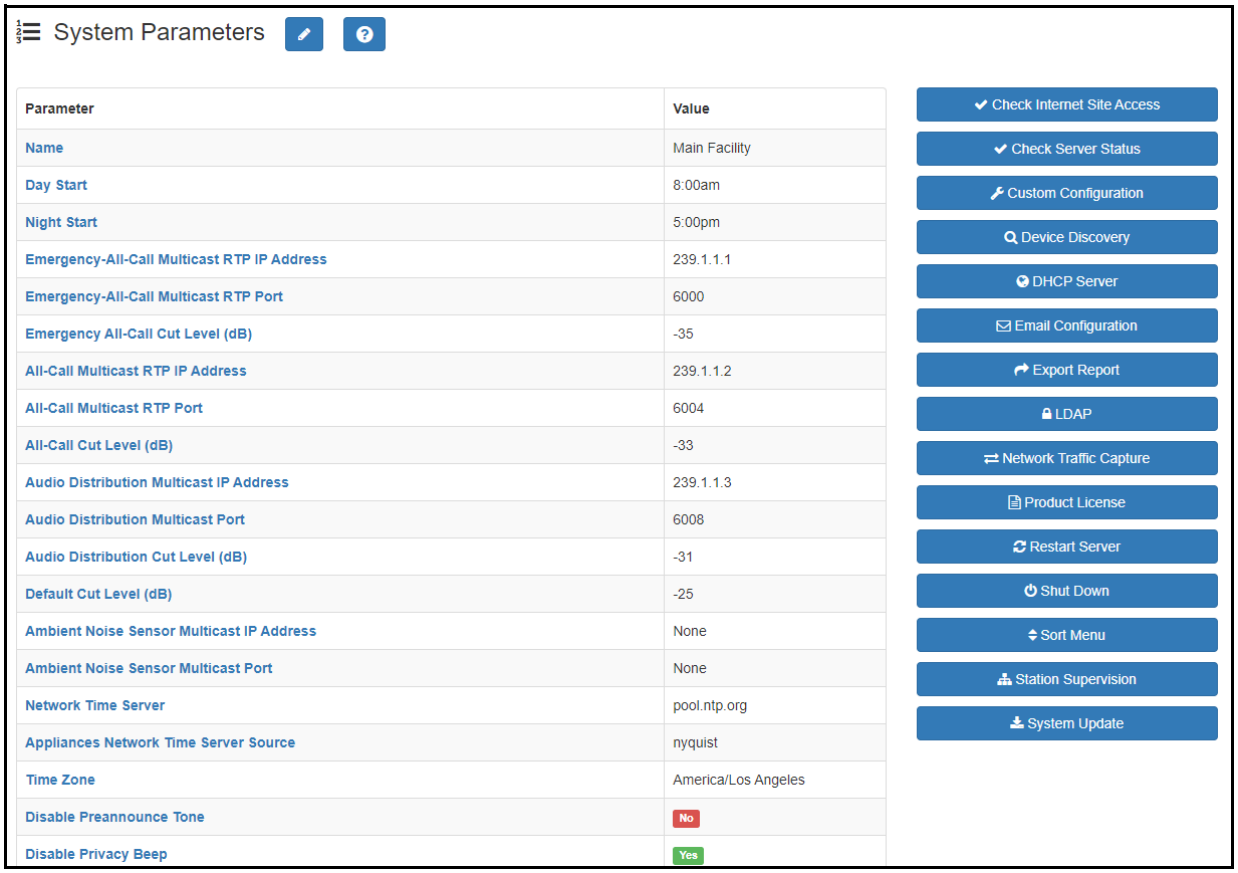


Figure 7. System Parameters Page

To view System Parameters:

From the navigation bar, select **System Parameters**.

The *System Parameters* page appears. For details, see *Table 23, "Edit System Parameters Page," on page 69* and *Table 24, "System Tools," on page 78*.

Using the System Parameters Page

From the *System Parameters* page, you can view many of the settings for the entire facility and perform the following tasks:

- Export a report. (*See "Exporting a Report" on page 23*.)
- Enter a product or feature license. (*See "Product License" on page 24 or "C4000 Software Licenses" on page 622*.)
- Sort the menu. (See *"Changing the Navigation Bar Order" on page 29*.)
- Restart the server. (See *"Restarting the Server" on page 29*.)
- Monitor stations and set station supervision criteria. (See *"Station Supervision" on page 30*.)
- Configure settings for Simple Mail Transfer Protocol (SMTP) email notifications. (See *"Email Configuration" on page 31*.)
- Check for and perform system updates. (See *"Performing a System Update" on page 34*.)

- Configure Automatic Software Download. (See *"Configuring Automatic Software Download" on page 41*.)
- Shut down the server. (See *"Shutting Down the Server" on page 43*.)
- Check Internet site access. (See *"Check Internet Site Access" on page 44*.)
- Check the server status. (See *"Check Server Status" on page 44*.)
- Configure the local DHCP server. (See *"DHCP Server" on page 47*.)
- Modify custom configuration settings. (See *"Custom Configuration" on page 46*.)
- Manage the Nyquist firewall. (See *"Firewall" on page 50*.)
- Capture network traffic on the Nyquist system. (See *"Network Traffic Capture" on page 52*.)
- Configure LDAP. (See *"Lightweight Directory Access Protocol (LDAP)" on page 57*).
- Configure NQ-DSC01 or NQ-S1810WBC flasher behavior for Nyquist system audio events. (See *"DSC01/WBC Flasher Configuration" on page 65*).

Configuring Night Call Options

The mechanism by which the system handles outside calls that are received during nighttime hours is determined by how the Night Ring options are configured for the SIP Trunk (see *Table 30, "Add/Edit/View SIP Trunk Page Parameters," on page 112*) and the System Parameters (see *Table 23, "Edit System Parameters Page," on page 69*, particularly the **Night Ring*** options).

Note: Despite the similar nomenclature, the Station's **Day Admin** and **Night Admin** settings (see *Table 43, "View, Add, or Edit Station Configuration Parameters," on page 143*) are not related to Night Call behavior.

During daytime hours (between **Day Start** and **Night Start**), outside calls are routed to the **Day Admin** extension defined in the SIP Trunk that received the outside call (see *Table 30, "Add/Edit/View SIP Trunk Page Parameters," on page 112*).

During nighttime hours (between **Night Start** and **Day Start**), outside calls are routed to the **Night Admin** extension defined in the SIP Trunk that received the outside call (*Table 30, "Add/Edit/View SIP Trunk Page Parameters," on page 112*). If the **Night Ring Enabled** and **Night Ring Admin** system parameters are both set (see *Table 23, "Edit System Parameters Page," on page 69*), the call is also routed to the system's **Night Ring Admin**.

If the call is not answered within 15 seconds, the system does one of several things (in priority order):

1. If **Night Ring All Stations** is enabled, the call will be routed to all stations.
2. If **Night Ring Admin Group** is specified, the call will be routed to all stations in the specified Admin Group.
3. If the **Night Ring Zones** list is specified, the call will be routed to the specified stations.
4. If none of these conditions is true, the call will continue ringing to the station's **Night Admin** extension and the system's **Night Ring Admin**.

The call will continue to ring for 30 minutes. If the call is not answered within that time, the call will be dropped.

The following diagram illustrates how settings for these options affect night calls.

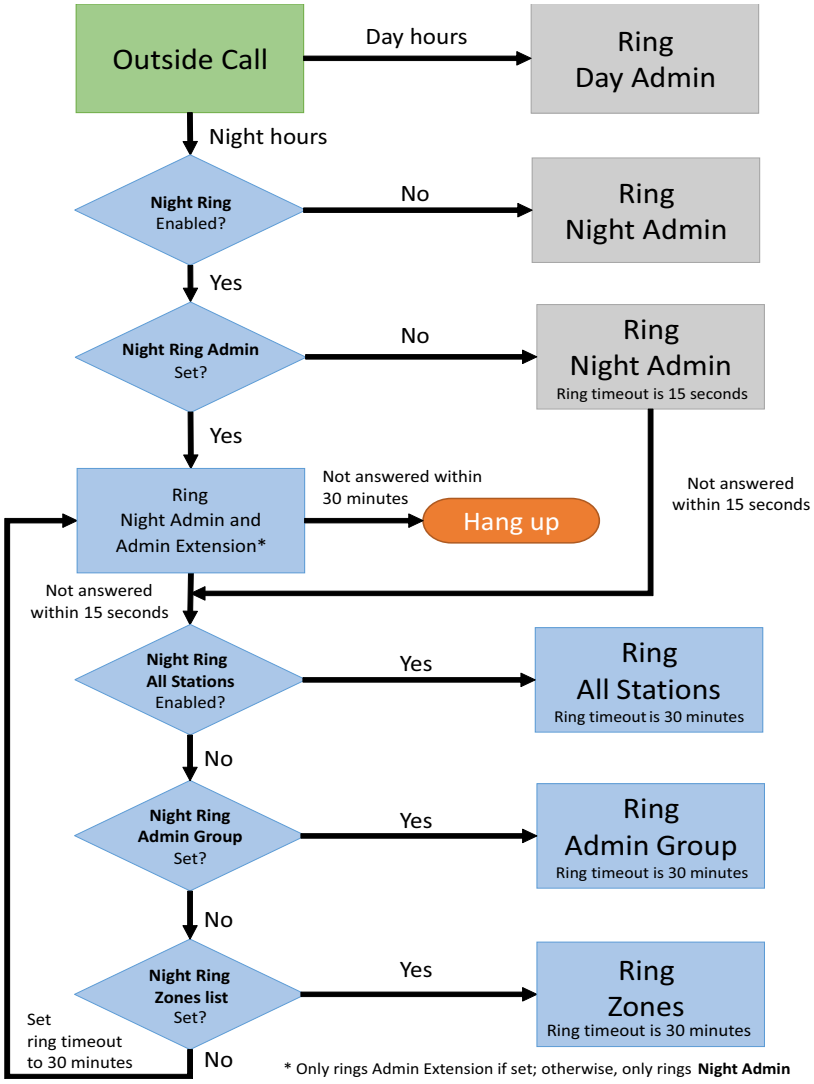


Figure 8. Night Ring Options

Exporting a Report

The Export Report feature generates an XML file in a Microsoft Excel format with a tab for each section of configurable variables, such as System Parameters, Zones, Stations, etc.

To export a report:

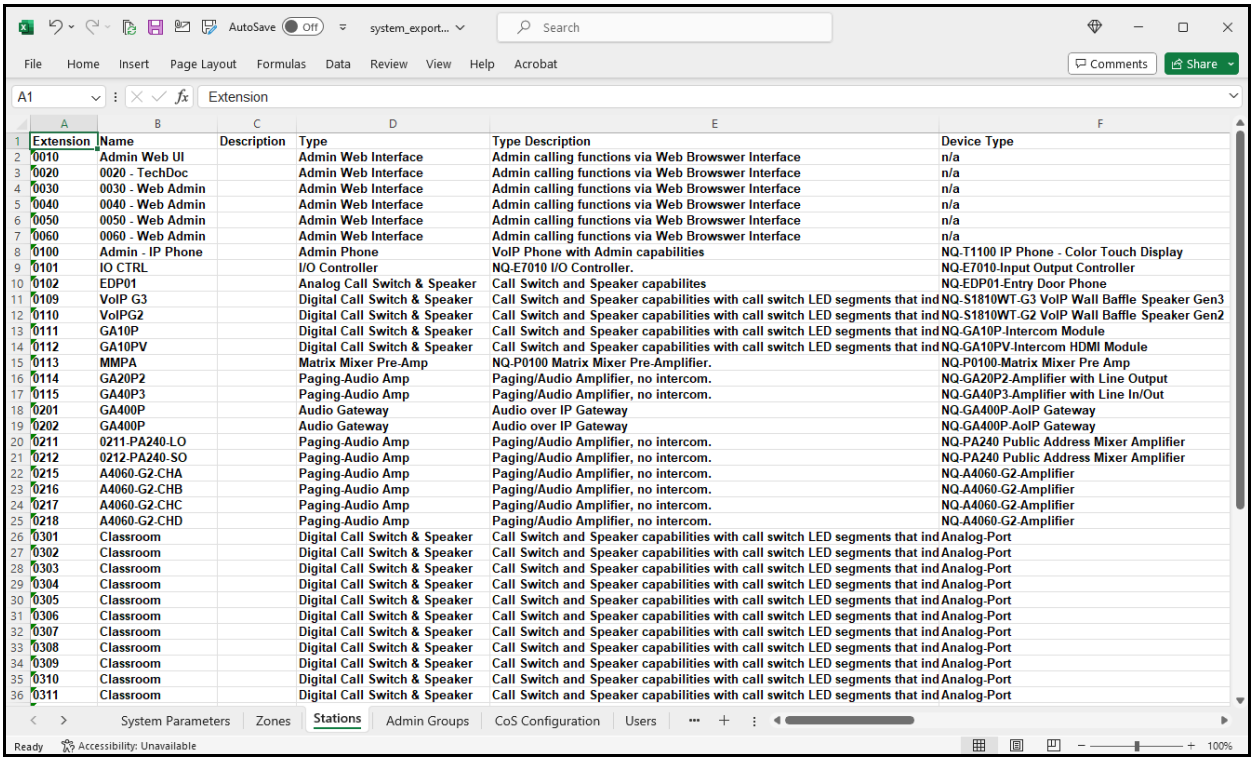
1. From the navigation bar, select **System Parameters**.
2. From the *System Parameters* page, select **Export Report**.

Warning This report contains decrypted passwords, API keys, and other security-sensitive information.

3 You may be prompted whether or not to download `system_export.xml`. If so, select an option to save the file.

4 Open the Excel application and open the downloaded file (typically located in the Downloads directory) to view the report (see *Figure 9, "System Report," on page 24*).

Tip: If you would like to access this report but do not have Excel available, please contact your Bogen dealer or Bogen Technical Support for assistance.



Extension	Name	Description	Type	Type Description	Device Type
0010	Admin Web UI		Admin Web Interface	Admin calling functions via Web Browswer Interface	n/a
0020	0020 - TechDoc		Admin Web Interface	Admin calling functions via Web Browswer Interface	n/a
0030	0030 - Web Admin		Admin Web Interface	Admin calling functions via Web Browswer Interface	n/a
0040	0040 - Web Admin		Admin Web Interface	Admin calling functions via Web Browswer Interface	n/a
0050	0050 - Web Admin		Admin Web Interface	Admin calling functions via Web Browswer Interface	n/a
0060	0060 - Web Admin		Admin Web Interface	Admin calling functions via Web Browswer Interface	n/a
0100	Admin - IP Phone		Admin Phone	VoIP Phone with Admin capabilities	NQ-T1100 IP Phone - Color Touch Display
0101	IO CTRL		I/O Controller	NQ-E7010 I/O Controller.	NQ-E7010-Input Output Controller
0102	EDP01		Analog Call Switch & Speaker	Call Switch and Speaker capabilites	NQ-EDP01-Entry Door Phone
0109	VoIP G3		Digital Call Switch & Speaker	Call Switch and Speaker capabilities with call switch LED segments that ind	NQ-S1810WT-G3 VoIP Wall Baffle Speaker Gen3
0110	VoIPG2		Digital Call Switch & Speaker	Call Switch and Speaker capabilities with call switch LED segments that ind	NQ-S1810WT-G2 VoIP Wall Baffle Speaker Gen2
0111	GA10P		Digital Call Switch & Speaker	Call Switch and Speaker capabilities with call switch LED segments that ind	NQ-GA10P-Intercom Module
0112	GA10PV		Digital Call Switch & Speaker	Call Switch and Speaker capabilities with call switch LED segments that ind	NQ-GA10PV-Intercom HDMI Module
0113	MMPA		Matrix Mixer Pre-Amp	NQ-P0100 Matrix Mixer Pre-Amplifier.	NQ-P0100-Matrix Mixer Pre Amp
0114	GA20P2		Paging-Audio Amp	Paging/Audio Amplifier, no intercom.	NQ-GA20P2-Amplifier with Line Output
0115	GA40P3		Paging-Audio Amp	Paging/Audio Amplifier, no intercom.	NQ-GA40P3-Amplifier with Line In/Out
0201	GA400P		Audio Gateway	Audio over IP Gateway	NQ-GA400P-AoIP Gateway
0202	GA400P		Audio Gateway	Audio over IP Gateway	NQ-GA400P-AoIP Gateway
0211	0211-PA240-LO		Paging-Audio Amp	Paging/Audio Amplifier, no intercom.	NQ-PA240 Public Address Mixer Amplifier
0212	0212-PA240-SO		Paging-Audio Amp	Paging/Audio Amplifier, no intercom.	NQ-PA240 Public Address Mixer Amplifier
0215	A4060-G2-CHA		Paging-Audio Amp	Paging/Audio Amplifier, no intercom.	NQ-A4060-G2-Amplifier
0216	A4060-G2-CHB		Paging-Audio Amp	Paging/Audio Amplifier, no intercom.	NQ-A4060-G2-Amplifier
0217	A4060-G2-CHC		Paging-Audio Amp	Paging/Audio Amplifier, no intercom.	NQ-A4060-G2-Amplifier
0218	A4060-G2-CHD		Paging-Audio Amp	Paging/Audio Amplifier, no intercom.	NQ-A4060-G2-Amplifier
0301	Classroom		Digital Call Switch & Speaker	Call Switch and Speaker capabilities with call switch LED segments that ind	Analog-Port
0302	Classroom		Digital Call Switch & Speaker	Call Switch and Speaker capabilities with call switch LED segments that ind	Analog-Port
0303	Classroom		Digital Call Switch & Speaker	Call Switch and Speaker capabilities with call switch LED segments that ind	Analog-Port
0304	Classroom		Digital Call Switch & Speaker	Call Switch and Speaker capabilities with call switch LED segments that ind	Analog-Port
0305	Classroom		Digital Call Switch & Speaker	Call Switch and Speaker capabilities with call switch LED segments that ind	Analog-Port
0306	Classroom		Digital Call Switch & Speaker	Call Switch and Speaker capabilities with call switch LED segments that ind	Analog-Port
0307	Classroom		Digital Call Switch & Speaker	Call Switch and Speaker capabilities with call switch LED segments that ind	Analog-Port
0308	Classroom		Digital Call Switch & Speaker	Call Switch and Speaker capabilities with call switch LED segments that ind	Analog-Port
0309	Classroom		Digital Call Switch & Speaker	Call Switch and Speaker capabilities with call switch LED segments that ind	Analog-Port
0310	Classroom		Digital Call Switch & Speaker	Call Switch and Speaker capabilities with call switch LED segments that ind	Analog-Port
0311	Classroom		Digital Call Switch & Speaker	Call Switch and Speaker capabilities with call switch LED segments that ind	Analog-Port

Figure 9. System Report

When the System Report appears, you can select a tab to view specific configuration settings.

Product License

The Product License page allows you to activate, update, or release licenses, check Internet site access, and view current licensing information.

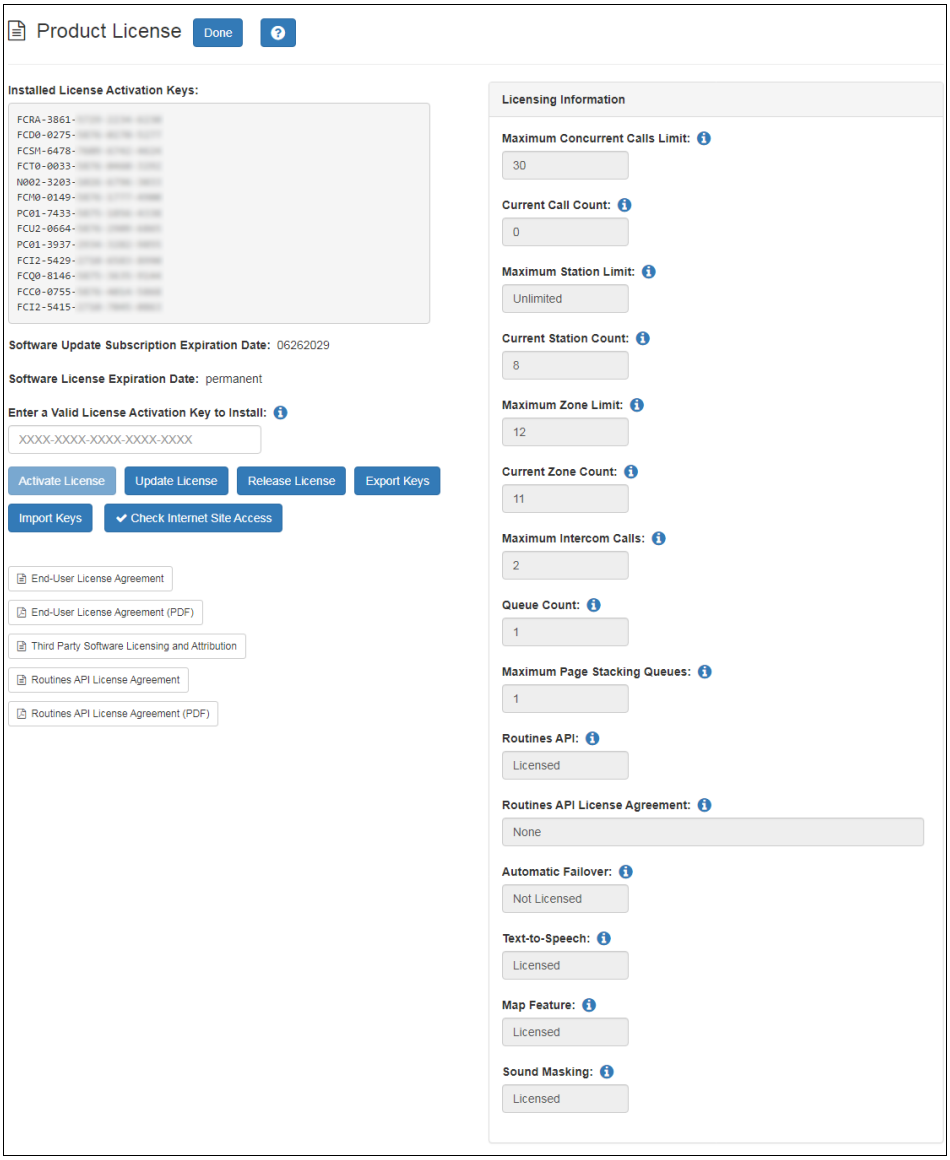


Figure 10. Product License Page

You must enter your product license activation key before you begin configuring the Nyquist system. Without a product license, you can only add a single station.

You can only enter one product activation key and any number of additional optional feature licenses. Your product license specifies the number of maximum concurrent calls that can be made and the maximum number of stations that can be added to a system.

The Product License page provides the following information:

Table 9. Product License Parameters

Installed License Activation Keys	Provides the activation keys installed on your server. See *"Understanding Activation Keys" on page 28*.
Software Update Subscription Expiration Date	Provides the expiration date in MMDDYYYY format for your software update subscription. If it has expired, then your system will not allow software updates.
Software License Expiration Date	Provides the software license expiration date for demo mode in dd-mmm-yyyy format. If not in demo mode, "permanent" is displayed.
Enter a Valid License Activation Key to Install	Enter the activation key for your product license or for optional features.

The Product License page also provides the following information about your currently installed license:

Table 10. Licensing Information

Maximum Concurrent Calls Limit	Displays the maximum number of concurrent calls allowed. For this field, calls mean telephone calls, pages, tones, alarms, and announcements.
Current Call Count	Displays the number of active calls in the system.
Maximum Station Limit	Displays the maximum number of stations allowed for your licensed system or displays **Unlimited** if your system has no maximum station limit. A Nyquist station is a device used to access the web interface, a speaker, a phone, or a Nyquist appliance (except for an I/O Controller. If you need to increase your station limit, contact Tech Support.
Current Station Count	Displays the number of stations registered with your Nyquist system server.
Maximum Zone Limit	Displays the maximum number of zones (regardless of type) allowed for your licensed system. If you need to increase your zone limit, contact Tech Support.
Current Zone Count	Displays the number of zones created for your system.
Maximum Intercom Calls	Displays the maximum number of concurrent intercom calls allowed for your licensed system. If you need to increase this limit, contact Tech Support.
Queue Count	Displays the number of zone queues created for your system.
Maximum Page Stacking Queues	Displays the maximum number of zone queues allowed for your licensed system. If you need to increase this limit, contact Tech Support.

Table 10. Licensing Information (continued)

Routines API	Displays **Licensed**. The Routines API is now available to all customers and does not require an extra license.
Routines API License Agreement	If the license has been accepted, displays the user name and user ID, as well as the date, time, and time zone when the license agreement was accepted; otherwise, displays **None**.
Automatic Failover	Displays **Licensed** if the Automatic Failover license is activated, otherwise it displays **Not Licensed**.
Text-to-Speech	Displays **Licensed** if the Text-to-Speech license is activated, otherwise it displays **Not Licensed**.
Map Feature	Displays **Licensed** if the Map Feature license is activated, otherwise it displays **Not Licensed**.
Sound Masking	Displays **Licensed** if the Sound Masking license is activated, otherwise it displays **Not Licensed**.

To enter a product license activation key:

1. From the navigation bar, select **System Parameters**.
2. From the System Parameters page, select **Product License**.
3. Type the activation key number.
4. Select one of the following buttons:

Table 11. Product License buttons

Activate License	This button becomes active only when data is entered into the Activation Key field. Select this button to activate the entered Activation Key. *Note:* Before activating a license key, use **Check Internet Site Access** (described below) to ensure that your Nyquist server can access hostedactivation.com.
Update License	Select this button to have the Nyquist server reactivate the Nodelocked license for the server. This can be done after **Release License** has been pressed. *Note:* Before updating a license key, use **Check Internet Site Access** (described below) to ensure that your Nyquist server can access hostedactivation.com.
Release License	Select this button if you want to release the license, which allows it to be moved to another server. *Note:* Before releasing a license key, use **Check Internet Site Access** (described below) to ensure that your Nyquist server can access hostedactivation.com.
Export Keys	Select this button to export a list of Activation License Keys to a `.tar` file that can then be saved to another computer or copied to storage media that can be secured offsite.

Table 11. Product License buttons

Import Keys	Select this button to import stored Activation License Keys if the Nyquist server was replaced. *Note:* If you attempt to import a LAK that has not been released, the activation fails. You must release the nodelock LAK and manually type the nodelock key.
Check Internet Site Access	Select this button to verify that your Nyquist server can access URLs required to run properly, as well as status for the default gateway, Network Time Protocol server, and Domain Name Servers, and to display the Nyquist server's public IP address. For more information, see *"Check Internet Site Access" on page 44*.

5 Select **Done**.

Understanding Activation Keys

Three types of licenses may appear in the **Current Activation Keys** list or be on entered in the **Activation Key** field on the Product License page:

- Nodelocked License Activation Key
- Product License Activation Key
- Feature License Activation Key

A Nodelocked License Activation Key has an *N* in the first position. The Product License Activation Key for C4000 starts with *PC* and is followed by the numerals 01 through 04, depending on the software bundle that was purchased.

The various Feature License Activation Keys start with *FC*. The third and fourth alphanumeric characters in the Feature License Activation Key provide information about the feature(s) purchased as described in the following table:

Table 12. Feature License Key Prefixes

Prefix	Meaning
FCCx	Concurrent Calls Expansion Pack License
FCDx	Software Update Subscription (SUS) Extension Extends the current SUS expiration date of a Bundle-x system by 3 years (e.g., if the system's current SUS expiration is 3/14/2024, installing this license key will extend it to 3/14/2027).
FCIx	Intercom Call License
FCMx	Map-based Paging License
FCQx	Queue Paging / Page Stacking License
FCTx	Text-to-Speech License
FCUx	System Software License Bundle Upgrades

Table 12. Feature License Key Prefixes (continued)

Prefix	Meaning
FCZx	Paging Zone License Expansion Pack
FCSM	Sound Masking License

For more information about licensing, see *"C4000 Software Licenses" on page 622*.

Changing the Navigation Bar Order

Through the **System Parameters** menu option, you can change the order of the selections that appear after Dashboard in the navigation bar.

To change the menu order:

1. From the navigation bar, select **System Parameters**.
2. From the *System Parameters* page, select **Sort Menu**.
3. Drag and drop the menu items until you have them in the order you prefer.
4. Select **Done**.

To return to the default settings for the menu order:

1. From the navigation bar, select **System Parameters**.
2. From the System Parameters page, select **Sort Menu** and then select **Reset Menu.**
3. Select **Done**.

Restarting the Server

Restarting the server should take less than a minute and is provided as a troubleshooting tool to use if the Nyquist system is not functioning. For example, if you are unable to page or make calls, you probably want to restart the server.

If you want to shut down the server, see *"Shutting Down the Server" on page 43*.

To restart the server:

1. From the navigation bar, select **System Parameters**.
2. From the System Parameters page, select **Restart Server** and select one of four options:
   - **Graceful**: System will restart after all current calls are completed.
   - **Now**: All current calls will be dropped.
   - **Force**: Use only if **Graceful** and **Now** do not work. The **Force** option will resolve more issues than the **Graceful** and **Now** options, including issues involving Recorded Paging (Queues), Rou-

tines, and Audio Distribution. This option will cause any running Routines to be terminated and will then start all routines that include a **Reboot** trigger.

- **Reboot**: Unlike the previous options, which just reboot the Nyquist services, this option performs a soft reboot of the operating system and all Nyquist services.

Station Supervision

You can set up parameters for alert notifications when a device, or station, goes offline. With this feature, you can set up email notifications, specify where records are to be stored, select what type of devices will be supervised, and select stations to be excluded from station supervision.

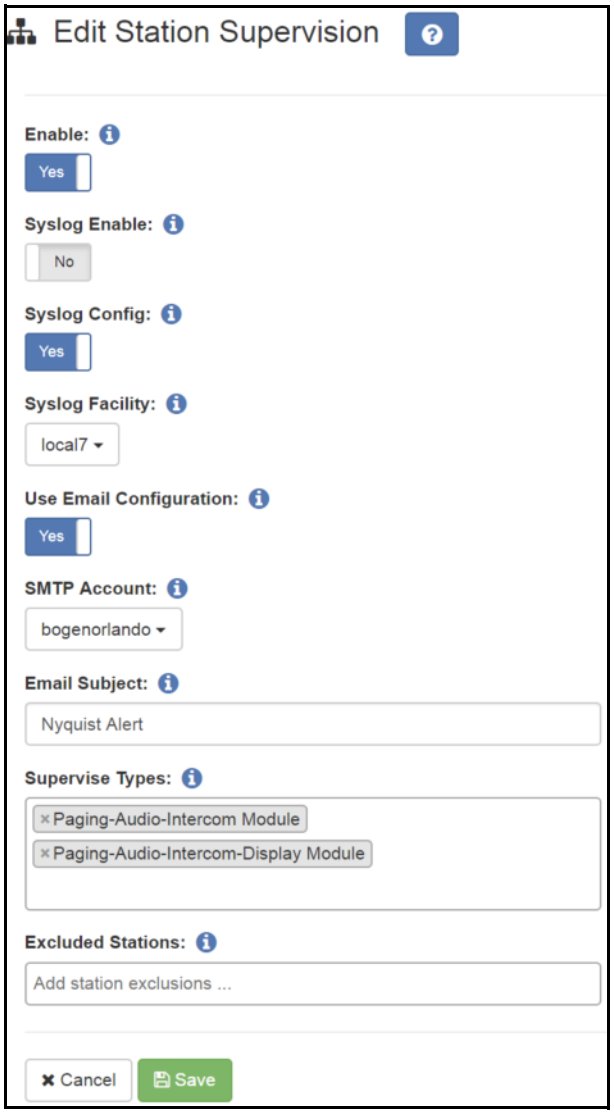


Figure 11. Edit Station Supervision

To set up station supervision parameters:

1 From the navigation bar, select **System Parameters**.

2 From the System Parameters page, select **Station Supervision**.

3 Select desired options from the Edit Station Supervision page.

4 Select **Save**.

Table 13. Edit Station Supervision Parameters

Enable	Use the slider to enable or disable the station supervision feature and the associated alerts creation. By default, this feature is disabled.
Syslog Enable	Use the slider to select if alerts will be recorded in the syslog file.
Syslog Config	Use the slider to select **Yes** to enable syslog configuration by the station supervision feature or select **No** if you are doing your own syslog configuration.
Syslog Facility	Select the syslog facility that will be used to report alerts to syslog.
Use Email Configuration	Use the slider to select **No** if you want to use SMTP parameters from the `/etc/msmtprc` file. If the default, **Yes,** is used, SMTP parameters from the SMTP configuration list will be used.
Send Email To	Enter email addresses separated by commas for all recipients who will receive an email message if a station goes down. If this field is left blank, email notification is disabled. *Note:* This option appears if **Use Email Configuration** is set to **No**. *Tip:* To send a text message, use one of the email address formats described in *Table 135, "Email Address Formats for Cellular Carriers," on page 461*.
SMTP Account	Specify the SMTP account that will be used for alert notification emails. *Note:* This option appears if **Use Email Configuration** is set to **Yes**.
Email Subject	Enter a subject line to appear on the email notifications. The default is **Nyquist Alert**.
Supervise Types	Select the station type or types that you want to be supervised.
Excluded Stations	Select the station extensions that are to be excluded from station supervision. If this option is left blank, no stations with the selected **Supervise Type** are excluded.

Email Configuration

The Email Configuration feature can be used to send SMTP email notifications when a station is not responding to the server. For example, if a Digital Call Switch (DCS) and speaker is offline, an automatic email can be sent to a facilities manager or IT personnel.

Note: SMTP is an Internet standard for email transmission.

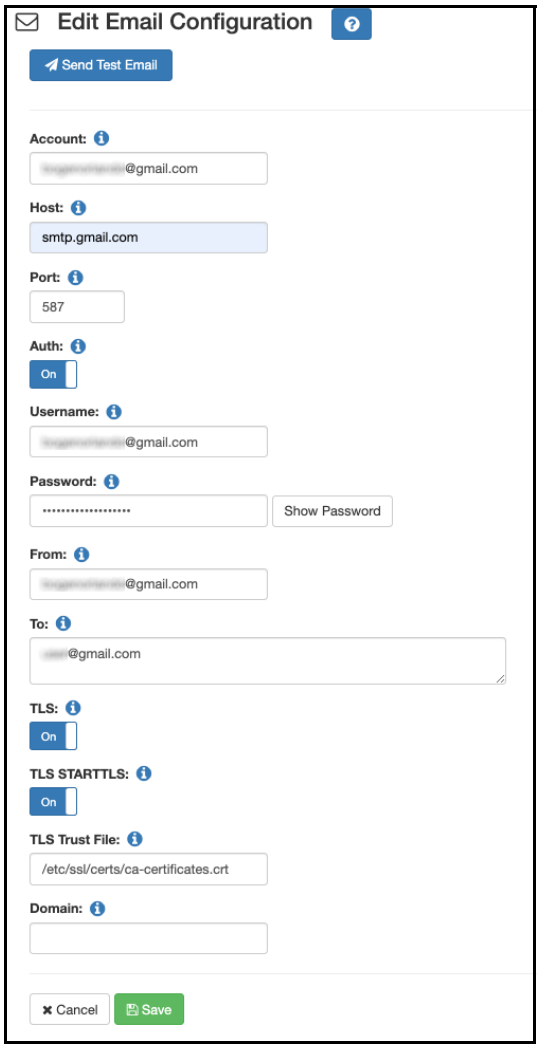


Figure 12. Edit Email Configuration

To set up email configuration:

1. From the navigation bar, select **System Parameters**.
2. From the *System Parameters* page, select **Email Configuration**.
3. Select desired options from the *Edit Email Configuration* page (see *Table 14 on page 33*).
4. Select **Save**.

Caution This email configuration can be used for any of several notifications (e.g., station supervision, I/O controller input and output notifications, custom routines, etc.). To disable email notifications, do not change the email configuration, as it may be used for other notifications. Instead, update the configuration of the notifications to be disabled.

Table 14. Edit Email Configuration

Send Test Email	Sends a test email using a saved Email Configuration. This allows you to quickly verify your email configuration settings for correctness by sending to an arbitrary email address using the configured email server and account.
Account	Enter the user-defined name for this account. The default account name is **Gmail**.
Host	Enter the SMTP server to send the email to. The value may be either a host name or a network address (e.g., `smtp.gmail.com`).
Port	Enter the port that the SMTP server uses to receive email transmissions. Typically, this is set to 25 for SMTP, 465 for SMTPS, or 587 for submission.
Auth	Use the slider to enable or disable SMTP authentication. By default, **Auth** is set to **On**, which is the recommended setting. When authentication is enabled, a user must provide a valid username and password to send email.
Username	Enter the username for SMTP authentication.
Password	Enter the password for SMTP authentication. *Note:* The password cannot contain single- or double-quote characters. *Note:* Some email servers, such as Gmail, do not support use of the standard user password and instead require the use of an App Password. For details on how to obtain a Gmail App Password, see https://support.google.com/mail/answer/185833.
Show Password	Select this button to show the password entered for SMTP authentication. *Note:* For security reasons, only the currently entered password will be displayed, not the saved password.
From	Enter the name that is to appear in the **From** field for the email.
To	Enter the email addresses for the recipients. Separate each email address by a comma. *Tip:* To send a text message, use one of the email address formats described in *Table 135, "Email Address Formats for Cellular Carriers," on page 461*.
TLS	Use the slide to enable or disable the use of TLS. When you have one email server send a message to another email server over TLS, the connection itself is encrypted so no one can intercept the payload information. But, the actual data itself is still unencrypted. It's secure and compliant because it was sent over an encrypted channel.
TLS STARTTLS	Use the slider to enable or disable the use of STARTTLS. STARTTLS is an email protocol command that tells an email server that an email client, including an email client running in a web browser, wants to turn an existing insecure connection into a secure one.

Table 14. Edit Email Configuration (continued)

TLS Trust File	Enter the location for the CA-Certificate trust file. The default location is `/etc/ssl/certs/ca-certificates.crt`.
Domain	Specify the domain of the server that is initiating the SMTP connection. If the email is rejected due to anti-SPAM programs, this domain name is used as the fully qualified domain name for the SMTP EHLO command.

Performing a System Update

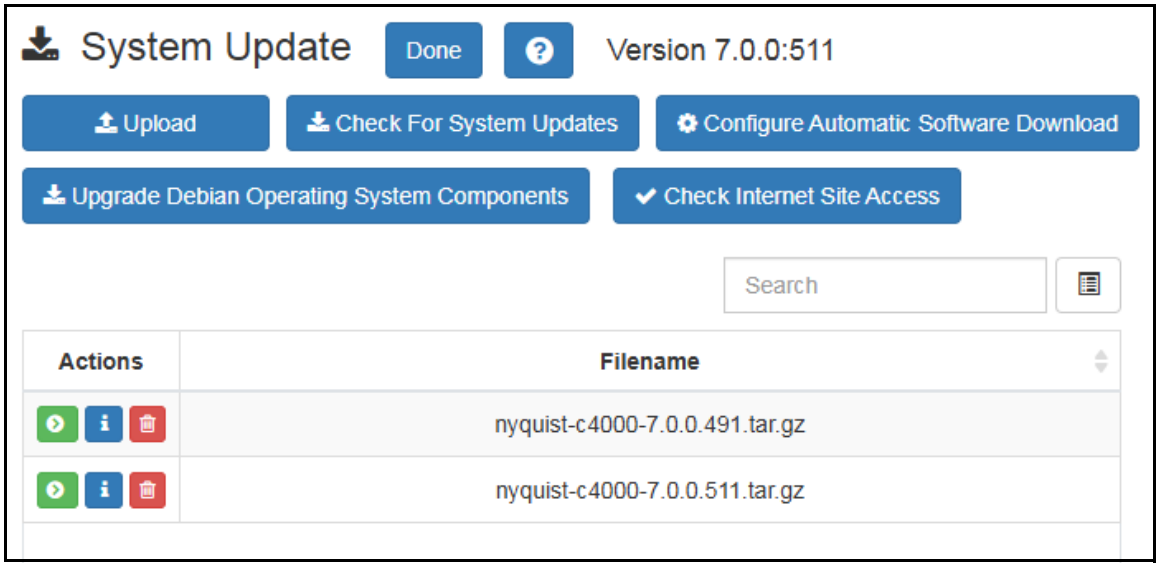


Figure 13. System Update

This feature updates the server software and configuration data for the C4000 server. From the *System Update* screen, you can choose to upload or check for new versions of the software as well as set configuration options for automatic software downloads.

Note: New appliances may have been introduced in a newer server release than the release you are using. To use these appliances, you must perform a *System Update*.

Software updates can be major releases, bug fixes, or even updates that are created specifically for your system.

Note: After a new software release is installed, permissions for features introduced by this new release must be set for the roles that will use these features. See *"Assigning and Editing Permissions" on page 248*

A list of downloaded software appears on the *System Update* screen. When you first access the *System Update* screen, the list will show only the default file that was installed. You can select **Check for**

Updates to obtain a list of software available for download or select **Upload** to browse for system update packages.

Note: Shortly before your Software Update Subscription (SUS) expires, you will receive a dashboard message explaining that you must contact your Bogen dealer to purchase a subscription renewal to access system updates. The message will include the subscription renewal part number (based on the number of currently licensed zones) and your Product License Key, both of which should be included when contacting your Bogen dealer.

Before performing a system update, you should perform the following tasks:

1. Perform a system backup and export the backup (see *"Backing Up Your Nyquist System and Files" on page 349*).
2. Export your product license activation keys (see *"Product License" on page 24*).
3. Execute **Check Internet Site Access** (see *"Check Internet Site Access" on page 44*) and ensure that all sites with "Install/Update" in the "During" column are accessible from the Nyquist server (i.e., Status is "SUCCESS").
4. If you are using the Automatic Failover feature (see *"Automatic Failover" on page 84*), execute **Check Server Status** (see *"Check Server Status" on page 44*) before you update the Primary server and verify that `Slave_IO_Running` and `Slave_SQL_Running` are both **Yes**. If one of these is **No** instead of **Yes**, perform a **Sync DB** operation between the Primary and Secondary servers before performing the system update. This is to ensure that your Secondary server contains the most update-to-date configuration data, as the Secondary server will temporarily become the Master server while the Primary sever is being updated.

To perform a system update:

1. From the navigation bar, select **System Parameters**.
2. From the *System Parameters* page, select **System Update**.

Caution If the Automatic Failover feature is being used, the system will not allow you to start a system update while accessing the C4000 via the Master IP Address. To update a system configured for Automatic Failover, see *"System Update Procedure" on page 95*.

---

3. If you want the system to check for new server software updates, select **Check for Updates**. A popup window appears with one of the following messages:
   - *No Nyquist System Software updates available.* When this message appears, select **OK** to exist the popup window.
   - *Can't check for updates. Check Internet connection and try again.*
   - Nyquist System Software download successful.
   - Nyquist System Software download failed, try again.

4 If you want to upload a file using the browser:

   a) Select **Upload**.

   b) Select **Choose file**.

   c) Locate the `.tar` or `.tar.gz` file.

   d) Select **Upload**.

5 If you want to update your system, select the **Run Update** icon for the file that you want to use for the update.

Note: During an update, volume control levels (Cut Levels) will be set to factory defaults. If you have changed these levels, you will need to make adjustments again.

A series of screens will appear when the System Update is running.

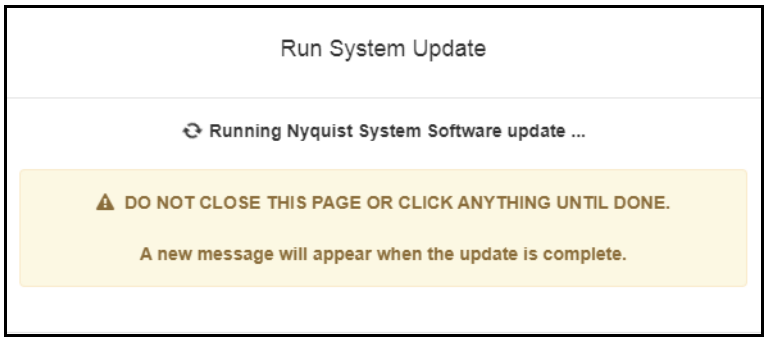


Figure 14. System Software Update Message

The first screen warns that the Nyquist System Software is being updated. Do not close the window or click anything on the computer screen until the update is completed.

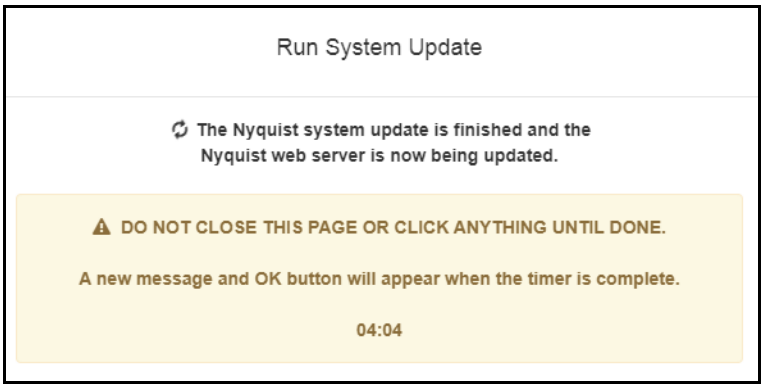


Figure 15. Nyquist Web Server Update Message

After the application software has been updated, the system will update any files, such as PHP files, needed for the Nyquist application. The screen that appears during this Nyquist web server update includes a progress clock that shows how many minutes and seconds remain before the update is complete. Again, do not close the message or click anything on the computer screen.

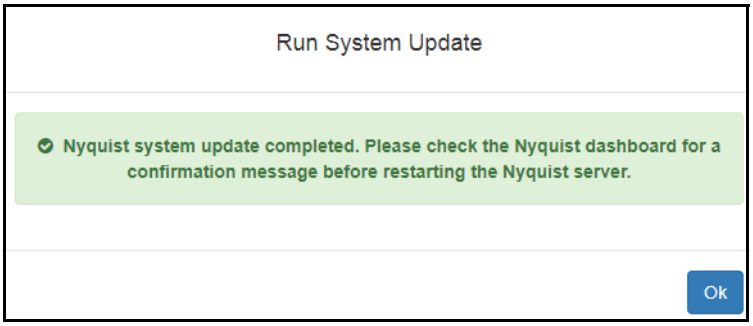


Figure 16. System Update Completed Message

6 When the system update completes, a message and an **OK** button appear. Select **OK** and check the Nyquist dashboard for a confirmation message before restarting the Nyquist server.

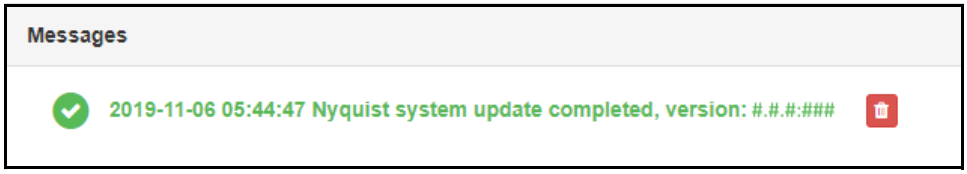


Figure 17. Dashboard Message After System Update

The dashboard message provides the date and time the update ran and the software version that was installed.

7 You might see a blank message box with an OK button. If so, click **OK**.

8 If a PHP message appears (e.g., *Figure 18, "PHP Message," on page 38*), press the refresh key (typically F5) repeatedly until the dashboard message appears.

```
<? php

/**
 * Laravel - A PHP Framework For Web Artisans
 *
 * @package  Laravel
 * @author   Taylor Otwell <taylorotwell@gmail.com>
 */

/*
|--------------------------------------------------------------------------
| Register The Auto Loader
|--------------------------------------------------------------------------
|
| Composer provides a convenient, automatically generated class loader for
| our application. We just need to utilize it! We'll simply require it
| into the script here so that we don't have to worry about manual
| loading any of our classes later on. It feels nice to relax.
|
*/

require __DIR__.'/../bootstrap/autoload.php';

/*
|--------------------------------------------------------------------------
| Turn On The Lights
|--------------------------------------------------------------------------
|
| We need to illuminate PHP development, so let us turn on the lights.
| This bootstraps the framework and gets it ready for use, then it
| will load up this application that we can run it and send
| the responses back to the browser and delight our users.
|
*/

$app = require_once __DIR__.'/../bootstrap/app.php';

/*
|--------------------------------------------------------------
| Run The Application
|--------------------------------------------------------------
|
| Once we have the application, we can handle the incoming request
```

Figure 18. PHP Message

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

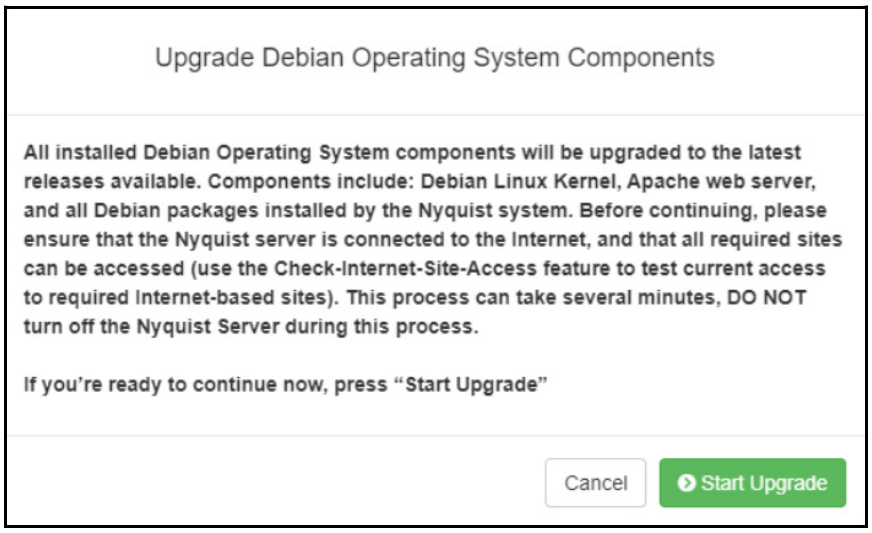
Upgrade Debian Operating System Components

You can use the **Upgrade Debian Operating System Components** feature to ensure that all Debian Operating System components (i.e., Linux Kernel, installed packages) are updated to the major Debian release version currently being used by the Nyquist system. Keeping Debian up-to-date can help improve security by ensuring that the latest versions of the Linux kernel and installed Debian packages are installed on the Nyquist server, as oftentimes these upgrades include security fixes. If a new vulnerability arises with the Debian Linux Kernel, Debian system, or installed Debian packages, you will be able to upgrade all Debian operating system components on the Nyquist server.

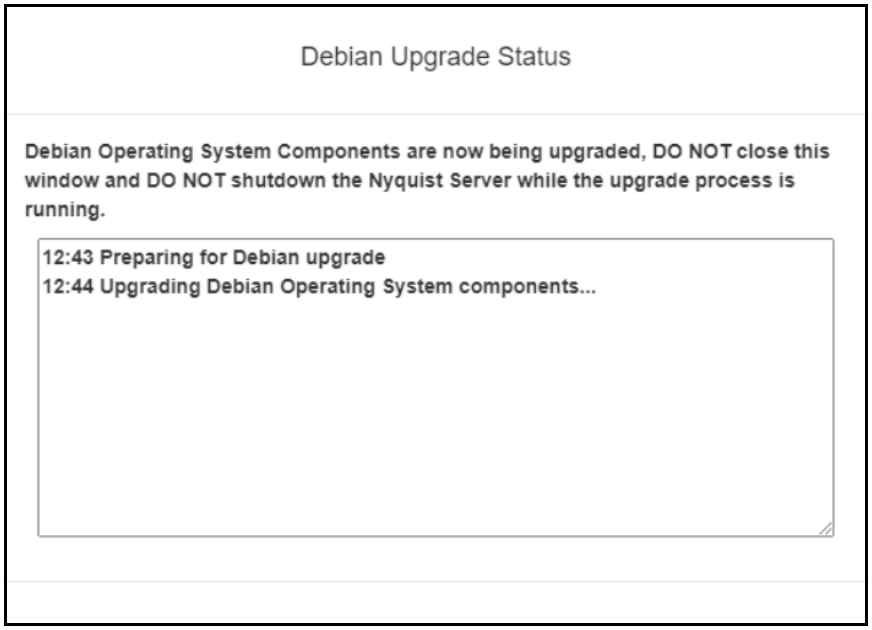
Use the following steps to upgrade the Debian Operating System components on your Nyquist server:

1 The Nyquist server will not be fully operational during the Debian Upgrade, so make sure you have a maintenance window available during a time when the Nyquist server is not needed. It is impossible to predict how long the upgrade process will take; it could take five minutes, or it could take over an hour.

2 On the *System Parameters* page, press the **Check Internet Site Access** button and verify that the following sites can be accessed:
   - deb.debian.org
   - security.debian.org
   - dl-ssl.google.com
   - bogen-ssu.bogen.com
3 Press the **Upgrade Debian Operating System Components** button on the *System Update* page, found under System Parameters.
4 Read the displayed text (see image below).
5 If you're ready to start the upgrade process, press the **Start Upgrade** button; otherwise press the **Cancel** button:

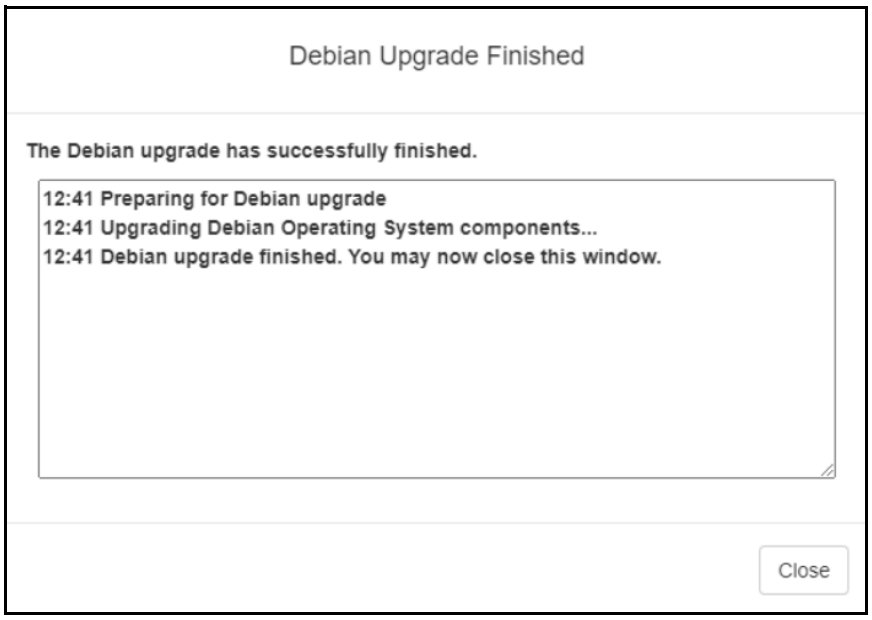


6 After you press **Start Upgrade**, a window entitled *Debian Upgrade Status* will open that displays the status of the Debian upgrade process:



Warning DO NOT shutdown the Nyquist Server while the upgrade process is running.

7 When the upgrade finishes, the *Debian Upgrade Finished* window will be displayed:



After the upgrade is finished, you may be instructed to shutdown and power-cycle the Nyquist server to complete the upgrade process.

After performing the Debian Upgrade, you can view a list of the Debian operating system components that were upgraded by displaying the dpkg.log file found in the **System** section of the *System Logs* page.

During the Debian upgrade process, one of the following messages may be displayed:

- ***Upgrading Debian Operating System components...***

  This message indicates that the Debian operating system is currently being upgraded. DO NOT power off or shutdown the Nyquist server.

- **Debian upgrades disabled by Bogen Administrator. No changes made.**

  This message indicates that the Debian operating system was not upgraded because Bogen has temporarily stopped Debian upgrades while possibly investigating a Debian upgrade issue.

- **Unable to access: deb.debian.org**

  This message indicates that the Debian operating system upgrade was not performed because your Nyquist server is not able to access the Debian upgrade server. Check your Internet connection and firewall settings, then try again.

- **Unable to access: bogen-ssu.bogen.com**

  This message indicates that the Debian operating system upgrade was not performed because your Nyquist server was not able to access the Bogen Communications System Software Update server. Check your Internet connection and firewall settings, then try again.

- **Please shutdown and power-cycle the Nyquist server to finish the Debian upgrade.**

This message indicates that the Debian operating system upgrade was successful and that your Nyquist Server must be shutdown and power-cycled to finish the upgrade process.

a) Shutdown your Nyquist Server by first selecting **Shut Down** in the *System Parameters* page.

b) After all lights have turned off on the Nyquist Server, turn off the power by flipping the power switch to the off position, wait 10 seconds, then turn the power back on by flipping the power switch to the on position.

- **WARNING: Possible Debian upgrade issues encountered. Contact Bogen Technical Support for assistance.**

  This message indicates that an unexpected issue was encountered during the Debian upgrade process. To resolve the issue, please contact Bogen Technical Support for assistance.

- **Apache web server was upgraded, restarting Apache server.**

  This message indicates that the Apache web server (used by the Nyquist web interface) was upgraded and restarted.

Configuring Automatic Software Download

From the Configure Automatic Software Download screen, you can schedule your Nyquist server to automatically check for and download server or firmware software updates.

Important: Downloaded software will *not* be automatically installed.

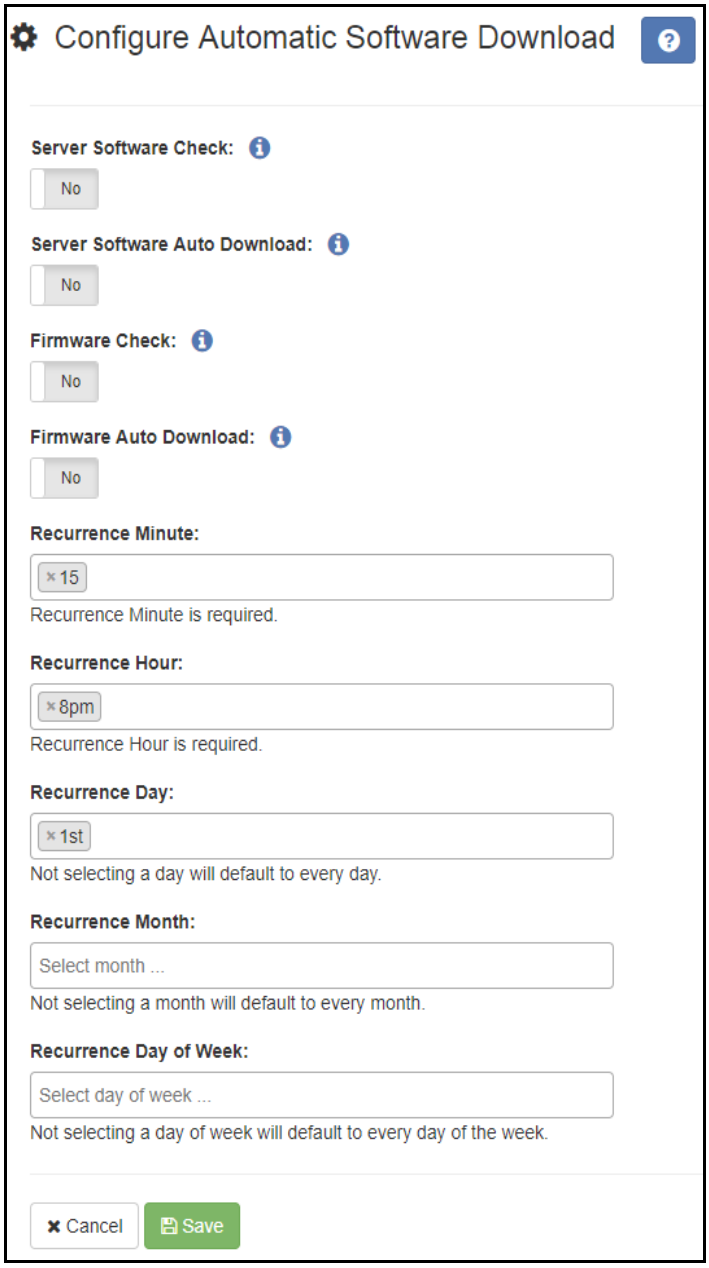


Figure 19. Configure Automatic Software Download

To configure automatic software downloads:

1. Do one of the following:
   a) From the navigation bar, select **System Parameters**, then from the System Parameters page, select **System Update**.
   b) From the navigation bar, select **Firmware**.
2. Select **Configure Automatic Software Download**.
3. Complete the options on the Configure Automatic Software Download screen.

4 Select **Save**.

Table 15. Configure Automatic Software Download Options

Server Software Check	When set to **Yes**, the server automatically checks for Nyquist server software updates and posts notifications to the dashboard when new software is available.
Server Software Auto Download	When set to **Yes**, the server automatically downloads Nyquist server software updates and posts notifications to the dashboard.
Firmware Check	When set to **Yes**, the server automatically checks for Nyquist device firmware updates and posts notifications to the dashboard when new software is available.
Firmware Auto Download	When set to **Yes**, the server automatically downloads Nyquist device firmware updates and posts notifications to the dashboard.
Recurrence Minute	Select the minute setting for automatic checks and downloads to occur. This field is required.
Recurrence Hour	Select the hour setting for automatic checks and downloads to occur. This field is required.
Recurrence Day	Select the day of the month for automatic checks and downloads to occur. If left blank, the setting defaults to every day of the month.
Recurrence Month	Select the month for automatic checks and downloads to occur. If left blank, the setting defaults to every month.
Recurrence Day of Week	Select the day of the week for automatic checks and downloads to occur. If left blank, the setting defaults to every day of the week.

Shutting Down the Server

Using the **Shut Down** button is the recommended way to gracefully stop Nyquist processes and power down the Nyquist server. Powering down the Nyquist server manually via the **Power** button is not recommended.

Note: If you are using the System Controller, the **Shut Down** button powers the component down but does not toggle the **Power** switch. To turn the System Controller back on, you must toggle the switch to the **Off** position and then toggle it to the **On** position.

To shut down the Nyquist server:

1 From the navigation bar, select **System Parameters**.

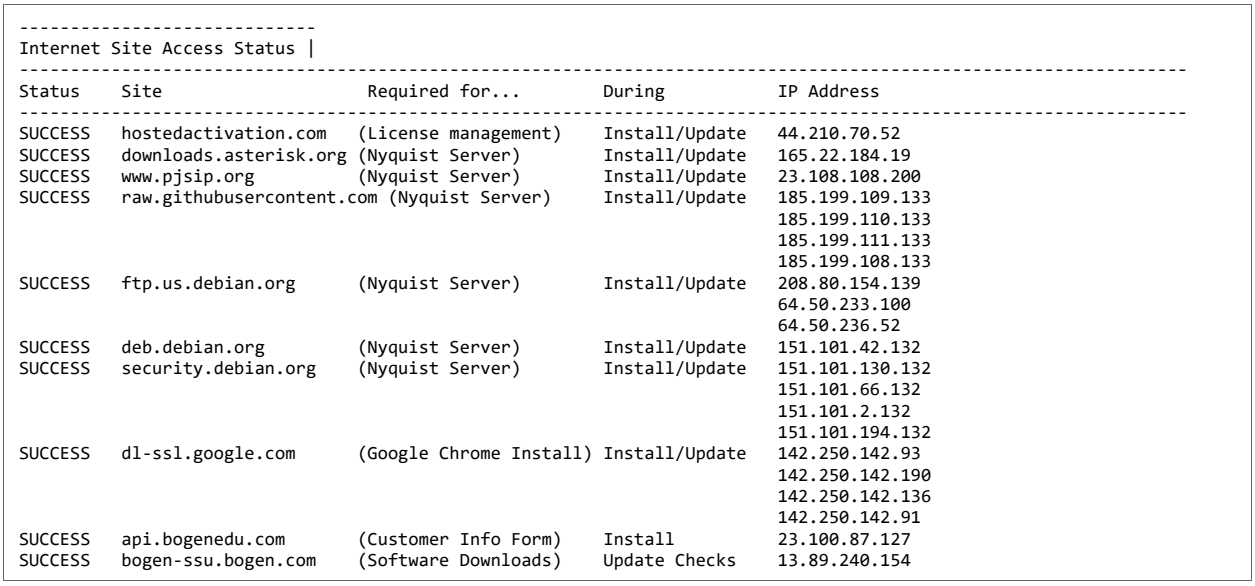
2 From the System Parameters page, select **Shut Down**.

3 When prompted, select **Continue**.

Check Internet Site Access

You can use the **Check Internet Site Access** button to verify that your Nyquist server can access URLs, commonly referred to as web addresses, that are required for Nyquist to run properly. This information can be used for resolving or debugging networking issues.

The **Check Internet Site Access** button appears on the *System Parameters* page, *System Update* page, and the *Product License* page.



```
----------------------------
Internet Site Access Status |
-------------------------------------------------------------------------------------------------------------------
Status    Site                    Required for...        During          IP Address
-------------------------------------------------------------------------------------------------------------------
SUCCESS   hostedactivation.com    (License management)   Install/Update  44.210.70.52
SUCCESS   downloads.asterisk.org  (Nyquist Server)       Install/Update  165.22.184.19
SUCCESS   www.pjsip.org           (Nyquist Server)       Install/Update  23.108.108.200
SUCCESS   raw.githubusercontent.com (Nyquist Server)     Install/Update  185.199.109.133
                                                                         185.199.110.133
                                                                         185.199.111.133
                                                                         185.199.108.133
SUCCESS   ftp.us.debian.org       (Nyquist Server)       Install/Update  208.80.154.139
                                                                         64.50.233.100
                                                                         64.50.236.52
SUCCESS   deb.debian.org          (Nyquist Server)       Install/Update  151.101.42.132
SUCCESS   security.debian.org     (Nyquist Server)       Install/Update  151.101.130.132
                                                                         151.101.66.132
                                                                         151.101.2.132
                                                                         151.101.194.132
SUCCESS   dl-ssl.google.com       (Google Chrome Install) Install/Update 142.250.142.93
                                                                         142.250.142.190
                                                                         142.250.142.136
                                                                         142.250.142.91
SUCCESS   api.bogenedu.com        (Customer Info Form)   Install         23.100.87.127
SUCCESS   bogen-ssu.bogen.com     (Software Downloads)   Update Checks   13.89.240.154
```

Figure 20. Check Internet Site Access

To check Internet site access:

1. From the navigation bar, select **System Parameters**.
2. From the *System Parameters* page, do one of the following:
   - Select **Check Internet Site Access**.
   - Select **System Update** and then select **Check Internet Site Access**.
   - Select **Product License** and then select **Check Internet Site Access**.

Tip: To export the report to a text file, select **Export**.

3. When finished viewing the *Check Internet Site Access* display, select **Close**.

Check Server Status

The *Check Server Status* window:

- Indicates if the default gateway, Network Time Protocol (NTP) servers, and Domain Name Servers (DNS) are configured and reachable (via ping).
- Reports the network interface and routing tables status.
- Displays the Nyquist server's public IP address, operation status, and software component versions.

- Shows disk space utilization and any pending SMART status warnings.
- Warns if one or more stations are still using the default password.
- Indicates which, if any, events are scheduled on overlapping zones, meaning that two or more target zones include the same station (see *"Zone Overlap Messages" on page 372*).
- Displays the Automatic Failover status (if the feature is enabled) as well as other server status details.

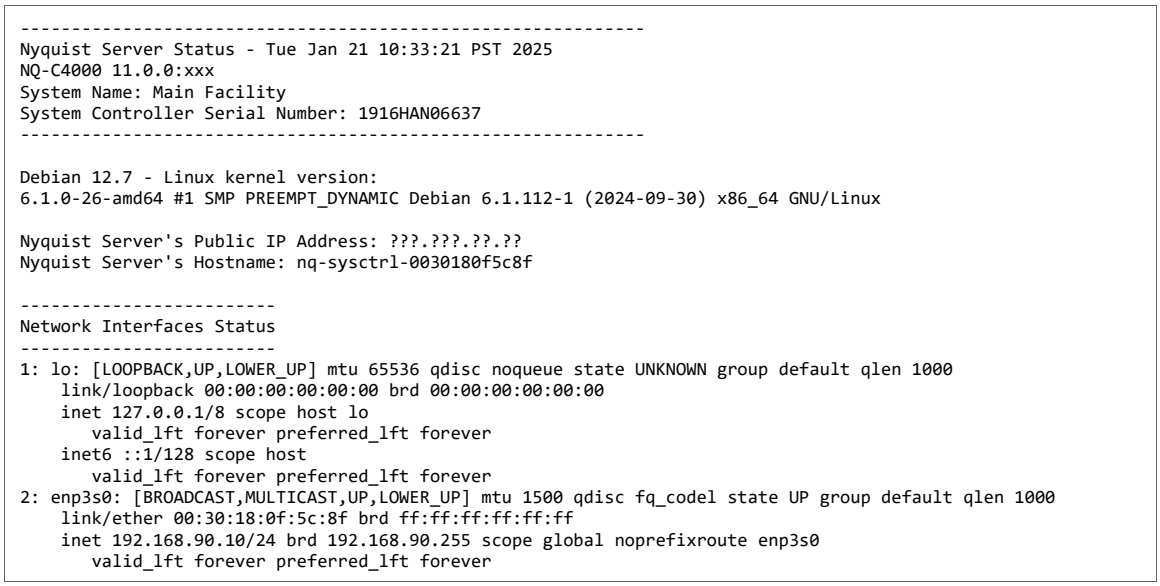


Figure 21. Check Server Status

To check server status:

1 From the navigation bar, select **System Parameters**.

2 From the *System Parameters* page, select **Check Server Status**.

Tip: To export the report to a text file, select **Export**.

3 When finished viewing the *Check Server Status* display, select **Close**.

SMART Diagnostics

The C4000 uses Self-Monitoring, Analysis, and Reporting Technology (SMART) to monitor the health of its hard drives. Any warning or error messages indicated by SMART will be available in the Check Server Status output under either the Temperature Sensor or Disk Space sections, such as:

> WARNING: Maximum operating temperature of 70C exceeded on SSD recorded by SMART monitor ### times! Maximum temperature recorded as ###.

SMART warnings will also be recorded in the syslog server log containing text like:

```
smartd[###]: Device /dev/sda
```

Entries that show a Reallocated_Sector_Ct value greater than zero indicate that the SSD is beginning to experience issues.

Custom Configuration

You can use the **Custom Configuration** button to customize any of the following three configuration files:

- *Actions and Custom Variables*

  Allows you to enter custom variable settings for Nyquist and Debian Linux-related services, as recommended by Bogen Technical Support.

- *Simple Network Management Protocol (SNMP) Configuration*

  Allows you to customize the SNMP configuration (e.g. setup private community string passwords, enable SNMP traps, etc.).

- *Syslog Configuration*

  Allows you to configure how system log entries are sent to remote hosts that manage syslogs of remote devices.

Note: To use **Custom Configuration**, the *Custom Configuration* permission must be enabled for the user.

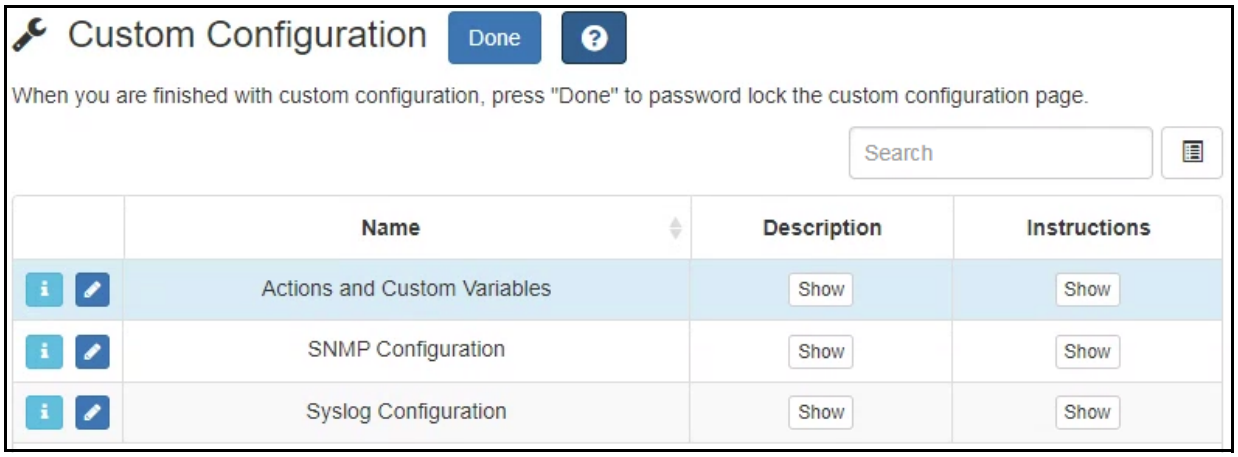


Figure 22. Custom Configuration

To edit custom configuration files:

1. From the navigation bar, select **System Parameters**.
2. From the System Parameters page, press the **Custom Configuration** button.
3. You will be prompted to enter your login password. After you enter your password, the web interface will display a list of configuration files that can be edited.
4. Move your mouse pointer over the description field of a configuration file to read the description for the configuration file.
5. Move your mouse pointer over the instructions field of a configuration file to read instructions related to editing the configuration file.

6 Press the information icon to view configuration file details.

   a) To edit a configuration file, press the **Edit** icon for one of the configuration files. A new window will open with the content of the configuration file.

   b) Make changes to the configuration file to meet your requirements.

   c) When you're finished making changes, press **Save and Implement Now** or **Save and Implement Later**. You can press **Cancel** if you want to abandon your changes.

7 Press the *Custom Configuration* page's **Done** button to relock the page.

Table 16. Custom Configuration options

Save and Implement Now	Saves your configuration changes and forces the Nyquist system to immediately implement the changes.
Save and Implement Later	Saves your configuration changes, but the Nyquist system will not immediately implement the changes. In this case, the changes will be implemented the next time the Nyquist server is rebooted or the next time you edit the file and press **Save and Implement Now**.

Important: If you are using Automatic Failover, changes made within the *Actions and Custom Variables* section will be automatically synchronized to the secondary server, except for the `purge_old_updates` and `fix_swap_issue` variables, which will still need to be manually replicated. Changes made to the *SNMP Configuration* and *Syslog Configuration* sections will also need to be manually replicated.

Warning In most cases, the Nyquist system will not validate the changes you make to configuration files; it is your responsibility to ensure the validity of changes that you make.

DHCP Server

The Nyquist server provides a DHCP server that can be used during the initial setup of a Nyquist system. This can be very helpful in the discovery and configuration of the various Nyquist devices, as well as third-party devices like the Grandstream HT813, Cisco ATA devices, and VoIP phones. It also provides clients with the Nyquist server's TFTP address (via DHCP option 66) to facilitate Nyquist device configuration.

Tip: The Nyquist C4000 server's TFTP service provides autoconfiguration information for many Nyquist devices. Its DHCP server uses extended DHCP option 66 to provide the address of its TFTP service to these devices. Many Nyquist and non-Nyquist devices can use the TFTP service to automatically retrieve configuration settings and notify the C4000 of their address, thereby simplifying the initial discovery and configuration of these devices.

This mechanism is referenced in many Nyquist device guides under their **TFTP Server from DHCP**

configuration setting.

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

The user would first configure a static IP address and subnet mask for Port-A of the Nyquist server, possibly using the *Network Wizard* (http://<server>/setup/network), then configure the DHCP service to provide a range of IP addresses that the server would assign to Nyquist and other network devices on that subnet. Once discovered, these devices can be configured, typically assigning each a static IP address.

This service would typically be disabled after all devices are discovered and configured. However, if no other DHCP server is available and only Nyquist devices are on the subnet, it could be used permanently, providing dynamic IP addresses to Nyquist devices.

Note: The DHCP server will use the same subnet mask as that which is configured for Port-A of this Nyquist server. This value can be viewed (usually in CIDR format) in the output of the **Check Server Status** command (see *"Check Server Status" on page 44*).

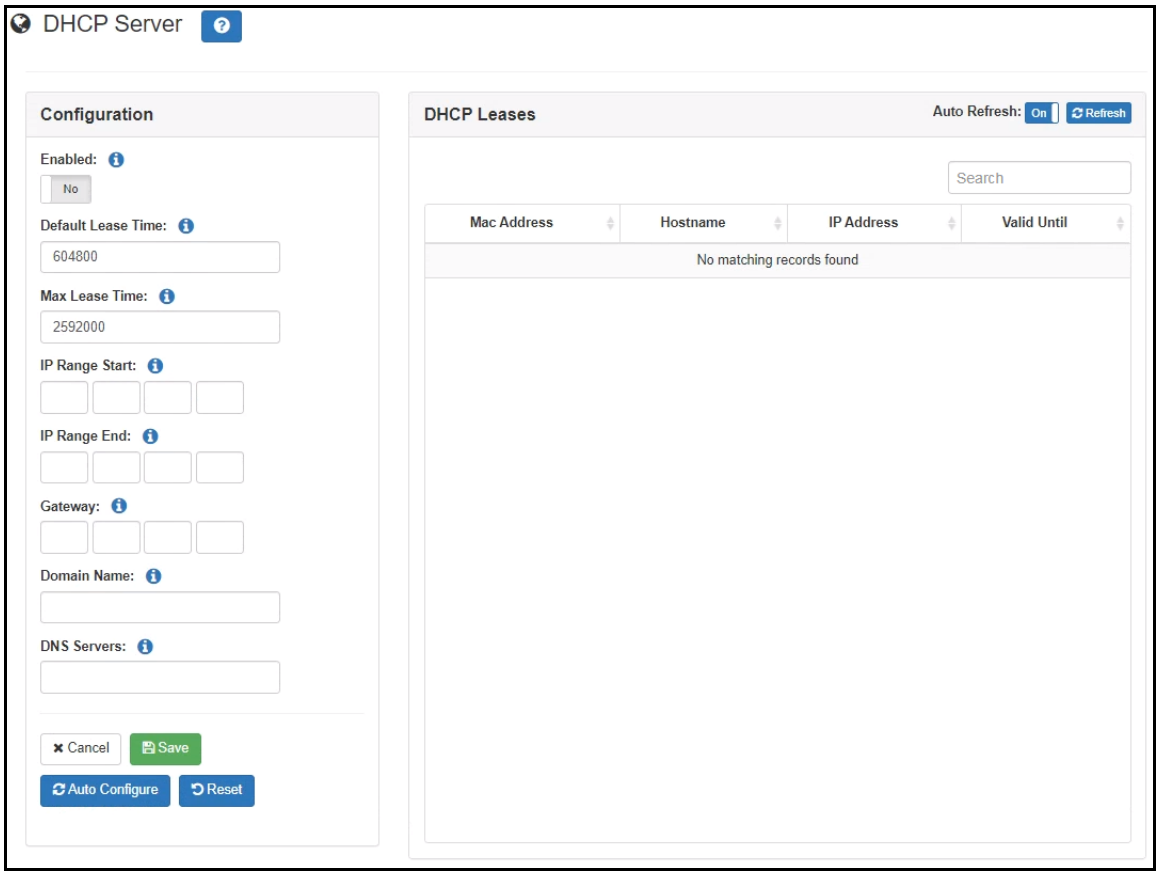


Figure 23. DHCP Configuration

Configuring the DHCP Server:

1 From the Navigator bar, select System Parameters.

2 From the *System Parameters* page, select **DHCP Server**.

3 If the DHCP Server has not yet been configured, you can populate the configuration properties with reasonable values by selecting the **Auto Configure** button.

4 Modify the values to the desired configuration. For details, see *"DHCP Configuration Parameters" on page 49*.

5 Press **Save** to persist the values.

6 To enable the DHCP feature and start allocating IP addresses via DHCP, toggle the **Enabled** switch to Yes, then press **Save**.

Table 17. DHCP Configuration Parameters

Enabled	Enables or disables the DHCP server for the subnet connected to Port-A. **Warning** When the DHCP server is enabled on Port-A, it will be authoritative! Do *not* enable the DHCP server while another DHCP server is providing DHCP addresses to the subnet defined on Port-A.
Default Lease Time	Length in seconds that will be assigned to a lease if the client does not request a specific expiration time. Decrease this value if you are only using the DHCP server to stage Nyquist devices.
Max Lease Time	Maximum length in seconds that will be assigned to a lease. Decrease this value if you are only using the DHCP server to stage Nyquist devices.
IP Range Start	Start of the IP address range from which to allocate addresses to devices on the Port-A subnet. After performing **Auto Configure**, you can increase this value to reserve a range of IP addresses on the subnet for fixed address assignments.
IP Range End	End of the IP address range from which to allocate addresses to devices on the Port-A subnet. After performing **Auto Configure**, you can decrease this value to reserve a range of IP addresses on the subnet for fixed address assignments.
Gateway	Gateway address sent to DHCP clients used for routing packets outside of the Port-A subnet. **Auto Configure** will set this value based on the current Port-A setup; you can still change it if needed. *Note:* If you are setting up the Nyquist DHCP server to provide IP Addresses and TFTP Server IP Address to Nyquist appliances, the Gateway IP address must be set to the Nyquist server's IP address; if you leave it blank, paging and audio distribution will not function. If you're using the Automatic Failover feature, the Gateway address must be set to the Master IP Address.
Domain Name	Domain name for devices operating on the subnet, excluding hostname. Leave this parameter blank if the Port-A subnet is private and not included in DNS managed domain. If the server has a domain name set, **Auto Configure** will use the server value. This is typically left blank.

Table 17. DHCP Configuration Parameters (continued)

DNS Servers	Comma-delimited list of DNS servers that devices on the subnet can use to resolve hostnames. **Auto Configure** will set this value; you can change it if needed.
Save	Saves the specified DHCP configuration.
Auto Configure	This button selects appropriate DHCP configuration values based on the existing server configuration. These values can be modified by the user before saving the settings. *Note:* These values will not be saved until the user clicks the **Save** button.
Reset	Sets all fields to their default values.
DHCP Leases	Displays a list of network devices that have been allocated IP addresses by the DHCP server.
Auto Refresh	If set to On, the list of DHCP leases will be periodically refreshed.
Refresh	Immediately refresh the list of DHCP leases.
MAC Address	The MAC address of the network card of the DHCP client.
Hostname	The hostname of the DHCP client.
IP Address	The IP address of the DHCP client. A link icon which provides a hyperlink to the device is displayed next to the IP address.
Valid Until	The date and time when the DHCP lease expires.

Firewall

The C4000 provides built-in firewall functionality that allows administrators to configure specific IP addresses and/or subnets as blacklisted or whitelisted for SIP traffic (ports 5060 and 5061). It also provides distinct blacklist and whitelist configurations for SSH clients (port 22).

Important: The C4000 provides an SSH interface for support purposes. Because an SSH session can provide full administrative access to the C4000, it is important to secure this interface, but SSH access should always be available via *some* IP address(es) to enable Bogen Support to troubleshoot issues in the event of system failures. Because such a failure could prevent access to the web interface, it is advisable to whitelist at least one IP address.

This firewall is particularly useful when Ethernet port B is connected to an Internet-facing network to allow access to public services, as a public interface is more susceptible to malicious attacks.

The C4000 can automatically blacklist an IP address for excessive SSH or station login failures. For example, an IP address that fails five consecutive attempts within a 10-minute period to log in via SSH or as a station will be automatically blacklisted for 10 minutes. The lockout period will increase by an additional 10 minutes for each five subsequent login failures while blacklisted. This makes it very difficult for an intruder to infiltrate the C4000 using brute force.

Tip: If a trusted IP address is accidentally added to a blacklist, you can manually remove it from the blacklist to restore connectivity. If necessary, the trusted IP address or subnet can be added to the appropriate whitelist to prevent it from being blacklisted.

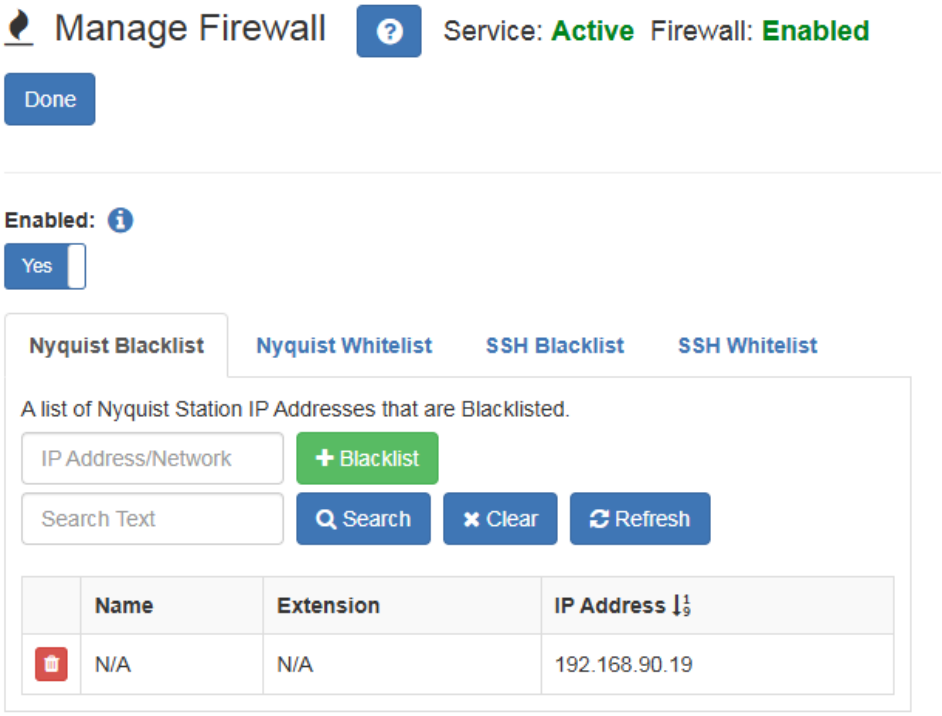


Figure 24. Manage Firewall

To manually add an IP address or subnet to a whitelist or blacklist:

1. Navigate to the *System Parameters* page.
2. From the *System Parameters* page, select **Manage Firewall**.
3. Select the Whitelist or Blacklist tab to which an IP address or subnet is to be added. The available lists are described in *Table 18, "Manage Firewall," on page 51*.
4. Enter an IP address or subnet specification (in CIDR notation) to be blacklisted or whitelisted and the **Blacklist** or **Whitelist** button. The item will be added to the list of IP addresses.

To remove an IP address or subnet from a whitelist or blacklist:

1. Navigate to the *System Parameters* page.
2. From the *System Parameters* page, select **Manage Firewall**.
3. Select the **Whitelist** or **Blacklist** tab to which an IP address or subnet is to be removed.
4. Select the **Delete** button next to the item to be removed from the list.

Table 18. Manage Firewall

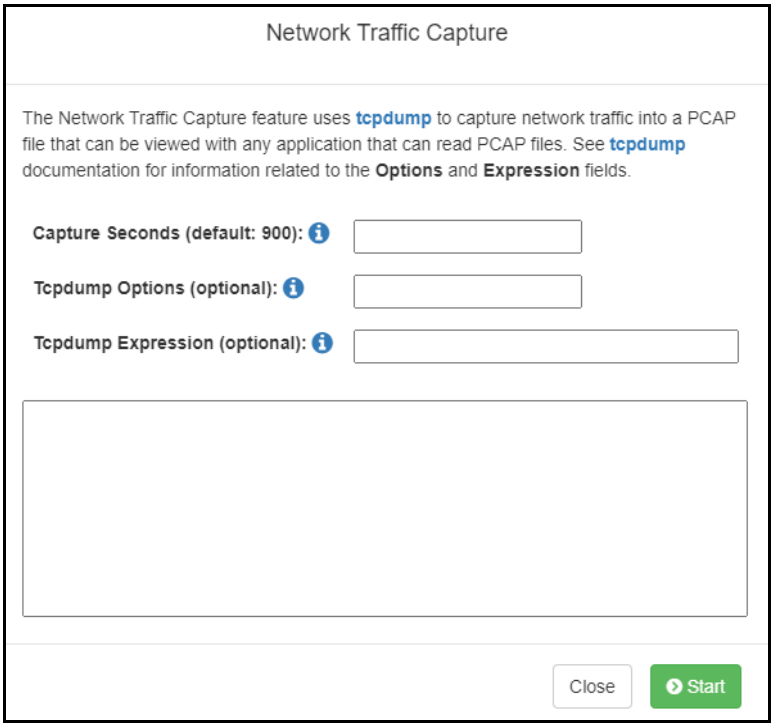
Enabled	Enables white- and black-listing of IP addresses and IP subnets for SIP traffic (ports 5060 and 5061) and SSH clients (port 22).
Nyquist Blacklist	A list of Nyquist station IP addresses or subnets that are blacklisted for SIP traffic.
Nyquist Whitelist	A list of Nyquist station IP addresses or subnets that are whitelisted for SIP traffic.
SSH Blacklist	A list of client IP addresses or subnets that are blacklisted for SSH connections.
SSH Whitelist	A list of client IP addresses or subnets that are whitelisted for SSH connections.
Whitelist	Adds an IP address or subnet to the whitelist.
Blacklist	Adds an IP address or subnet to the blacklist.
Search	Searches the list for the specified search text.
Clear	Clears the search text.
Refresh	Refreshes the list items that match the specified search text.

Network Traffic Capture

The **Network Traffic Capture** tool can be used to capture the network traffic present on the Nyquist system, typically for the purpose of troubleshooting networking issues. Network Traffic Capture uses the `tcpdump` command to capture network traffic to a PCAP file that will be downloaded to your computer. The PCAP file can be viewed by any application that can read PCAP files (e.g., Wireshark).

To use the **Network Traffic Capture** tool to capture network traffic:

1. Navigate to the C4000's Syste*m Parameters* page or the *Network Settings* page of an appliance's web UI.
2. Press the **Network Traffic Capture** button. The **Network Traffic Capture** popup window will be displayed.



3 Optionally change the parameters to meet your capture requirements (see *Table 19, "Network Traffic Capture Parameters," on page 53*):

If you leave all fields blank, the default action is to capture all packets on all interfaces for 15 minutes.

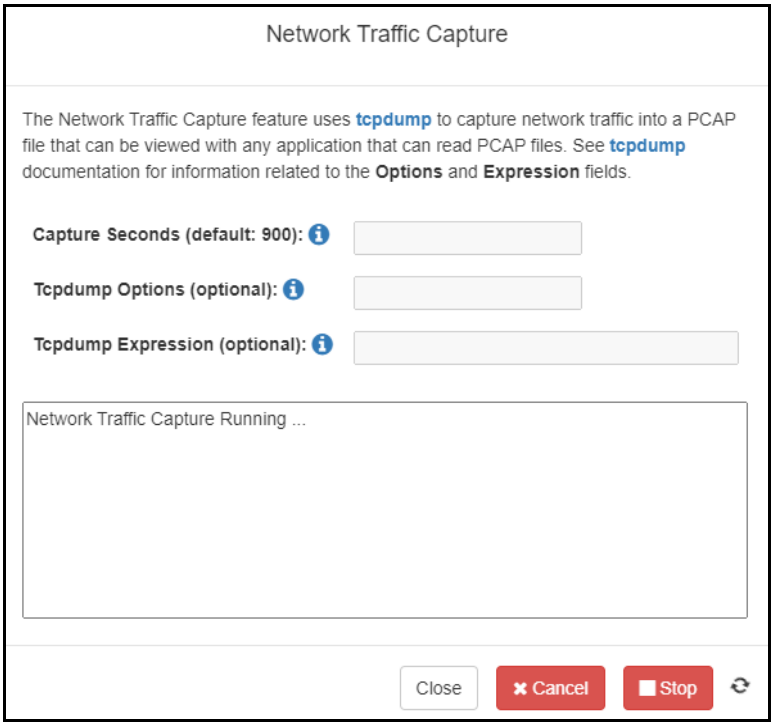
Table 19. Network Traffic Capture Parameters

Capture Seconds	The number of seconds to capture network traffic. If left blank, network traffic will be captured for 15 minutes (900 seconds). *Note:* The network capture will automatically stop if available disk space goes below 10 GB. Default: `900` **Caution** Long capture periods may result in a very large capture file, so make sure your server has sufficient disk space (see *"Check Server Status" on page 44* to determine the Nyquist server's available disk space).
Tcpdump Options	Command line options to apply to the `tcpdump` command. Only a few of the `tcpdump` options are supported, and none of the print-related modifier options are supported. If left blank, "`-i any`" is automatically used to capture network packets on all interfaces. Default: `-i any` *Note:* As a result of the implementation-specific context in which `tcpdump` is executing, the following options are *not* supported: `--monitor-mode --relinquish-privileges=user -W -G -F -I -r -z -Z -V` **Important:** Do not specify options unless you are knowledgeable about the `tcpdump` command. See *"Useful tcpdump options" on page 55*.
Tcpdump Expression	An optional expression to use on the `tcpdump` command. The expression is used to further filter the network traffic that you wish to capture. For more information regarding expression syntax and use, consult the `tcpdump` documentation (see https://www.tcpdump.org/manpages/pcap-filter.7.html) as well as the `tcpdump` example expressions shown below (see *"Example tcpdump expressions" on page 56*).

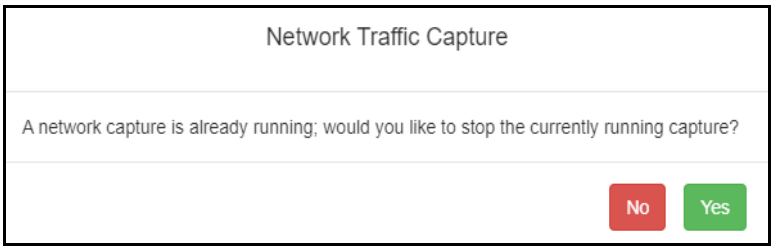
4 Press **Start** to begin the network traffic capture.

The window will now include a **Cancel** and **Stop** button, and inform you that the capture is running.

Note: If errors exist in values supplied in the Options or Expression field, the errors will be displayed in the text window and the capture will not be started.



5 Once the capture has started, you can either wait for the capture to complete, or press the **Close** button, allowing you to use the Nyquist dashboard to start Nyquist features while the network capture continues. After pressing **Close**, when you're ready to download the capture file, you can return to *Network Traffic Capture*. When you return, if the capture has finished, you can press the **Download** button to download the PCAP file. If the capture is still running, you will receive the following message asking you if you want to stop the capture.

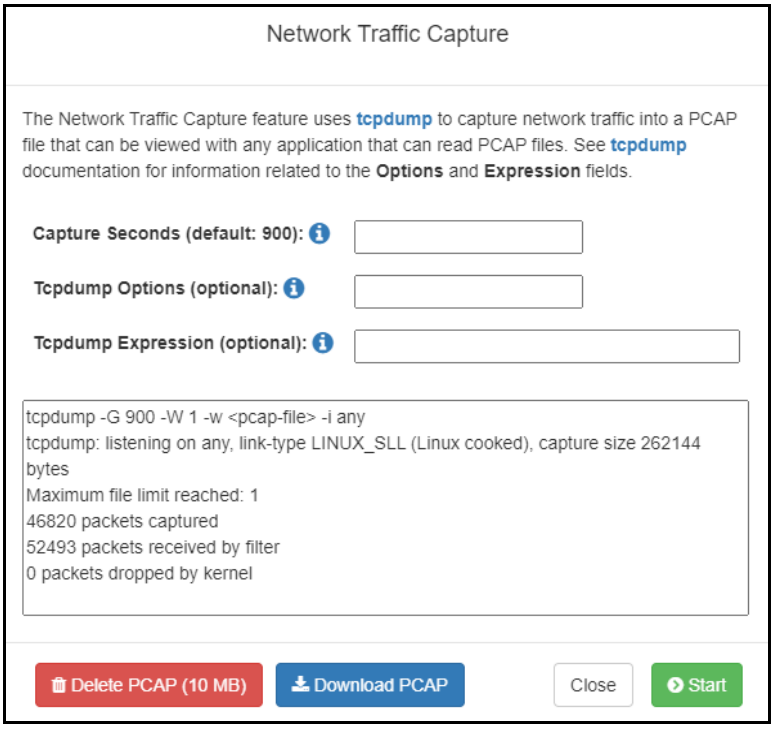


After stopping the capture by pressing **Yes**, you can then press the **Download** button on the Network Traffic Capture tool. If you press **No** instead, the network capture will continue.

6 While network traffic is being captured (and you have not pressed **Close**), you can press the **Stop** button to stop capturing traffic before the capture seconds has elapsed.

7 If, for any reason, you no longer want the captured network traffic, press **Cancel** to stop the capture process. Canceling the capture will not download the capture file; instead, the capture file will be deleted.

8 After the network capture has completed, the capture file can be downloaded to your client computer by selecting the **Download PCAP** button.



Information regarding the number of packets captured will be displayed. If you notice that "packets dropped by kernel" is greater than zero (0), be aware that not all packets were captured, most likely due to very busy network activity as seen by the Nyquist server.

Tip: You can try to fix a dropped packets issue by using the `tcpdump -B` option to increase the buffer size.

9 After the PCAP file has been download to your computer, you can press the **Delete PCAP** button to delete the PCAP file from the Nyquist server (to save disk space). If you do not delete the PCAP file, you can return to the *Network Traffic Capture* tool in the future and download it again, or delete it.

Important: The next time you start a download, any previous PCAP files are automatically deleted.

Useful tcpdump *options*

- To view the current version of the `tcpdump` command, enter the following into the **Tcpdump Options** field:

  ```
  --version
  ```

  This is useful to ensure that you're referencing the correct version of the `tcpdump` documentation.

- To view the list of available network interfaces, enter the following into the **Tcpdump Options** field:

  ```
  -D
  ```

  This is useful if you wish to use interface filters in the **Tcpdump Expression** field.

  Sample output:

  ```
  1.enp3s0 [Up, Running]
  2.enp4s0 [Up, Running]
  3.any (Pseudo-device that captures on all interfaces) [Up, Running]
  ```

In the above example on Nyquist System Controllers, `enp3s0` is Port-A, `enp4s0` is Port-B, and `any` refers to both interfaces.

In very rare cases on Nyquist System Controllers, you may see `eth0` and `eth1` instead; in this case, `eth0` is Port-A and `eth1` is Port-B.

- To capture packets from only a specific network interface, enter the following into the **Tcpdump Options** field, where `<interface-name>` is the name of the interface (as returned by the aforementioned `-D` option, e.g., `enp3s0`):

  ```
  -i <interface-name>
  ```

For details about `tcpdump` options, see https://www.tcpdump.org/manpages/tcpdump.1.html.

Example tcpdump *expressions*

To capture all packets to and from IP address `192.168.90.15`:

```
net 192.168.90.15
```

To capture RTP packets:

```
portrange 10000-20000
```

To capture SIP packets (when SIP TLS is *not* enabled):

```
port 5060
```

To capture SIP and RTP packets (when SIP TLS is *not* enabled):

```
udp port 5060 or udp portrange 10000-20000
```

To capture SIP packets when SIP TLS is enabled, modify the previous commands to use port 5061. Be aware, however, that the packets will be captured, but not decoded, as SIP TLS packets are encrypted.

Caution If the C4000 does not have at least 10 GB of available disk space, the network capture will not start (see *"Check Server Status" on page 44* to determine the Nyquist server's available disk space).

In general, the largest consumers of disk space are: old system backups, obsolete system updates, obsolete firmware updates, audio files (e.g., announcements, tones, songs), and recorded voice conversations.

You can manually remove system backups (see *"Deleting a Backup File" on page 352*); obsolete system updates (see *"Performing a System Update" on page 34*); obsolete firmware updates (see *"Deleting Listed Firmware" on page 133*); and unneeded announcements (see *"Deleting an Announcement" on page 331*), tones (see *"Deleting a Tone" on page 341*), songs (see *"Deleting a Song" on page 299*), and voice recordings (see *"Managing Recordings" on page 342*).

To automatically remove obsolete Nyquist system updates, you can set `purge_old_updates=true` under **Actions and Custom Variables** (see *"Custom Configuration" on page 46*).

Lightweight Directory Access Protocol (LDAP)

The Nyquist C4000 can be configured to obtain user account and group information from an Active Directory (AD) server using the LDAP protocol. This minimizes or eliminates the need to maintain user information in the Nyquist system. Once configured, users can be imported from the AD server, assigned to Nyquist roles, and authenticated upon login. It can also be configured to regularly update this information from the AD server (based on a configured schedule).

Important: Nyquist servers currently only support LDAP connections to a Microsoft Active Directory (AD) server.

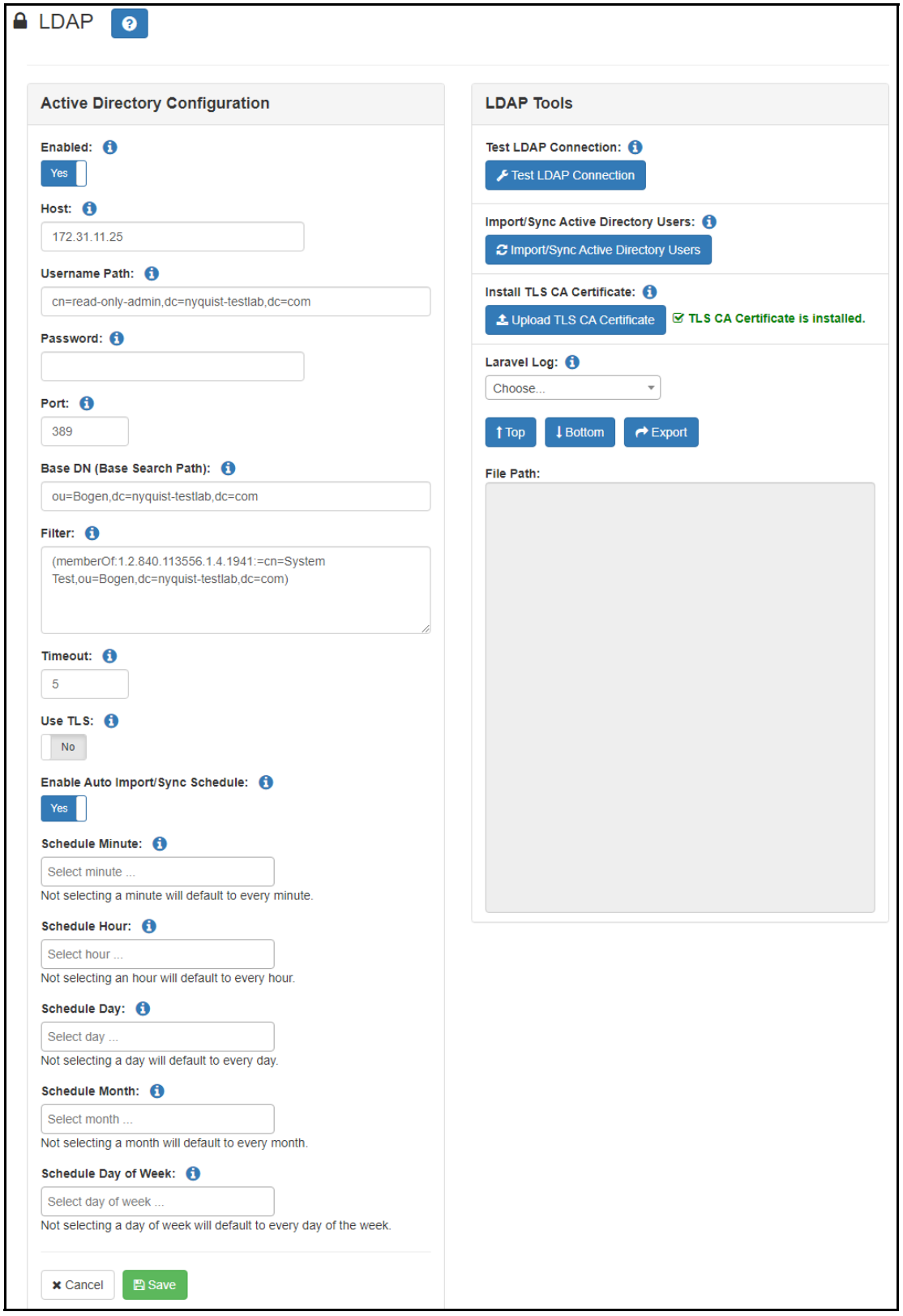


Figure 25. LDAP Settings

Table 20. Active Directory Configuration Settings

Enabled Indicates if user account information will be retrieved from an Active Directory server via LDAP.

Host The IP address or hostname of the Active Directory server.

Username Path Specifies the user name of the Active Directory user account to be used to make the LDAP queries against the Active Directory server.

Note: This value can be specified using the X.500 Directory Specification Distinguished Name (DN) format, User Principal Name (UPN) format, or down-level logon name format.

The following are examples of valid values:

```
CN=admin,DC=bogen,DC=com
admin@bogen.com
bogen\admin
```

Password The password of the user specified in **Username Path**.

Port The TCP and UDP port on which the LDAP service is available. This is typically port 389 (or port 636 for LDAP over TLS).

Base DN (Base Search Path) The Active Directory directory to be used as the base path in which to search for users.

Note: This value is specified as an X.500 Directory Specification Distinguished Name (DN) value.

The following is an example of a valid value:

```
OU=nyquist,DC=bogen,DC=com
```

Filter Specifies an Active Directory filter string to specify which Active Directory users will be imported as Nyquist users. This filter is applied to the Base DN. If no filter is specified, all entries found within the Base DN path will be included.

Important: This value must not include carriage return or line feed characters.

Caution Once a user has been imported, that user will not be removed from the Nyquist Users list if, in the future, that user no longer matches this filter (e.g., if the Active Directory directory entries have changed or this filter has changed).

For a detailed discussion on LDAP syntax filter strings, see *"LDAP Syntax Filter" on page 62*.

Timeout The number of seconds to wait for a response from the LDAP server.

Table 20. Active Directory Configuration Settings (continued)

Use TLS	Indicates whether or not to use TLS to establish a secure connection to the Active Directory server whenever Active Directory users are imported or synchronized.
	Important: A TLS Certification Authority (CA) certificate must be uploaded via **Install TLS CA Certificate** for a TLS connection to be established.
Enable Auto Import/Sync Schedule	If enabled, the C4000 will periodically update the list of users from the Active Directory server. The configurable details of the schedule are only visible when enabled.
Schedule Minutes	Sets one or more minutes after the hour on which the scheduled Import/Sync operation will occur. If left blank, the operation will default to every minute.
Schedule Hours	Sets one or more hours of the day on which the scheduled Import/Sync operation will occur. If left blank, the operation will default to every hour.
Schedule Days	Sets one or more days of the week on which the scheduled Import/Sync operation will occur. If left blank, the operation will default to every day.
Schedule Months	Sets one or more months of the year on which the scheduled Import/Sync operation will occur. If left blank, the operation will default to every month.
Schedule Days of Week	Sets one or more days of the week on which the scheduled Import/Sync operation will occur. If left blank, the operation will default to every day of the week.

For further details about the X.500 Directory Specification Distinguished Name (DN) format, the following may be helpful:

- https://learn.microsoft.com/en-us/previous-versions/windows/desktop/ldap/distinguished-names
- https://datatracker.ietf.org/doc/rfc4514/
- https://ldap.com/ldap-dns-and-rdns

There are several tools provided to assist in configuring the C4000 to interoperate with LDAP/Active Directory, as described in *"LDAP Tools" on page 61*.

Table 21. LDAP Tools

Test LDAP Connection	Uses the LDAP configuration settings to verify that a connection can be successfully made to the Active Directory server using the specified host, username path, password, and port. The operation and completion status of the connection attempt will be displayed next to this button for approximately five seconds. **Important:** The connection attempt will be made using the saved configuration values, not necessarily the displayed values. Be sure to save any configuration changes before testing.
Import/Sync Active Directory Users	Imports the user accounts specified by the Active Directory host and Base DN (and filtered by the Filter Path) into the Nyquist server's Users list. If user accounts have already been imported, they will be synchronized (i.e., updated based on the Username). The operation and completion status of the import operation will be displayed next to this button for approximately five seconds. **Important:** The import/sync operation will be made using the saved configuration values, not necessarily the displayed values. Be sure to save any configuration changes before importing.
Upload TLS CA Certificate	Uploads a PEM file containing the public Certification Authority (CA) certificate of the Active Directory server. If **Use TLS** is enabled, the uploaded CA certificate will be used to validate the Active Directory server connection whenever Active Directory users are imported or synchronized. *Note:* An adjacent message will indicate whether or not a CA certificate has been installed.
Laravel Log	This section allows you to view the current and archived `laravel.log` files in the **File Path** edit box. These provide details on LDAP operations that have been performed and/or failed. Selecting a log file will display its contents in the text box below. There are three buttons that provide extra functionality: **Top:** Scrolls the log file listing to the top of the file. **Bottom:** Scrolls the log file listing to the bottom of the file. **Export:** Exports the displayed log file to a text file. Be sure to select the log file in the **Laravel Log** combo box first.

Importing the Active Directory Server's TLS Certification Authority

To securely connect to an Active Directory server using TLS (which is highly recommended), **Use TLS** must be enabled and the Active Directory server's CA certificate must be uploaded to the C4000 so it

can validate the identity of the server. A PEM file containing the CA certificate can be uploaded via the **Upload TLS CA Certificate** button.

For details on how to obtain the Active Directory CA certificate, please refer to Microsoft's documentation.

Once the CA certificate has been exported to a CER file, it can be converted to a PEM file by renaming the file to `<cacertfile>.pem`. Import the CA certificate into the LDAP settings via the **Upload TLS CA Certificate** button in **LDAP Tools** (see *Figure 21, "LDAP Tools," on page 61*).

LDAP Syntax Filter

You may want to include restrictions to limit which Active Directory entries are imported as users into your Nyquist system. LDAP filters are very flexible, allowing for very precise specification of which users to include and/or exclude.

The following Microsoft articles provide detailed descriptions and numerous examples of LDAP syntax filters for the Active Directory platform, which may be helpful:

- https://learn.microsoft.com/en-us/windows/win32/adsi/search-filter-syntax
- https://learn.microsoft.com/en-us/archive/technet-wiki/5392.active-directory-ldap-syntax-filters

Important: Keep in mind that changing the Filter Path will not remove Users that were previously imported but no longer match the filter. If you do not wish to keep those user accounts in the Nyquist system, you will need to manually delete them. If you do keep them, remember that they will *not* be synchronized if they do not match the currently specified LDAP filter.

Tip: For details on the LDAP filter capabilities and syntax, see RFC4515 (https://www.rfc-editor.org/rfc/rfc4515) or search the web for "LDAP filters" (e.g., https://ldap.com/ldap-filters). Note that Microsoft's Active Directory supports several platform-specific extensions that may be relevant (see https://learn.microsoft.com/en-us/windows/win32/adsi/search-filter-syntax).

Note: The C4000 automatically disables or enables Nyquist users based on the status of the corresponding Active Directory accounts, so there should be no need to filter based on the ACCOUNTDISABLE bit of the Active Directory `userAccountControl` attribute.

LDAP Filter Examples

The following are examples of LDAP syntax filters that may be helpful. They do not show the full capabilities of the LDAP syntax filter mechanism, but are provided simply for illustrative purposes. They assume an LDAP structure in which all users and groups are defined within `CN=users,DC=bogen,DC=com`. The structure of your LDAP environment will be different.

The following LDAP filter retrieves all users that are direct members of the Engineering group:

```
(memberOf=CN=Engineering,CN=users,DC=bogen,DC=com)
```

Note: The `memberOf` property of an LDAP user object specifies a list of groups to which the user belongs.

The following Active Directory-specific example—which uses a Microsoft LDAP extensible matching rule to perform a recursive search—retrieves all users that are direct *or indirect* members of the Engineering group, which includes members of any group that is a direct or indirect member of the Engineering group:

```
(memberOf:1.2.840.113556.1.4.1941:=CN=Engineering,CN=users,DC=bogen,DC=com)
```

Tip: For more information on Microsoft Active Directory's extensible matching rules (e.g., the dot-separated series of number in the previous example), see https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-adts/0bb88bda-ed8d-4af7-9f7b-813291772990. The one shown in the previous example, LDAP_MATCHING_RULE_TRANSITIVE_EVAL (1.2.840.113556.1.4.1941), is documented at https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-adts/1e889adc-b503-4423-8985-c28d5c7d4887.

The following example queries the Active Directory for all users in the Engineering or Operations groups:

```
(|(memberOf:1.2.840.113556.1.4.1941:=CN=Engineering,CN=users,DC=bogen,DC=com)
(memberOf:1.2.840.113556.1.4.1941:=CN=Operations,CN=users,DC=bogen,DC=com))
```

The following example further restricts users to those that have an object category of "person", an object class of "user", and are members of the Engineering or Operations groups:

```
(&(objectCategory=person)(objectClass=user)(|(memberOf:1.2.840.113556.1.4.1941:=C
N=Engineering,CN=users,DC=bogen,DC=com)(memberOf:1.2.840.113556.1.4.1941:=CD=Oper
ations,CD=users,DC=bogen,DC=com)))
```

Testing an LDAP syntax filter

There are many tools available for viewing Active Directory structures and data, such as:

- Microsoft's LDP (available as part of the RSAT feature),
- Sysinternals Active Directory Explorer (https://learn.microsoft.com/en-us/sysinternals/downloads/adexplorer),
- the PowerShell ActiveDirectory module (for command-line access), and
- many other tools, such as those listed at https://ldap.com/ldap-tools.

These tools can be very useful for exploring your Active Directory/LDAP structure to help you define your filters, and some (e.g., LDP, PowerShell, etc.) can be helpful for experimenting with LDAP filter expressions.

Testing LDAP filter with PowerShell

The following sample PowerShell script shows a useful technique for testing an LDAP filter without actually importing the users. Modify the `$user` and `$adserver` values to the appropriate values for your environment, and modify the `$ldapfilter` as needed to experiment with different filter values. (These commands can be executed as a script or at the command line.)

Note: If executing from a Windows client environment (i.e., not Windows Server), the following PowerShell code requires the Remote Server Administration Tools (RSAT) be installed. For details on installing RSAT, see https://learn.microsoft.com/en-US/troubleshoot/windows-server/system-management-components/remote-server-administration-tools.

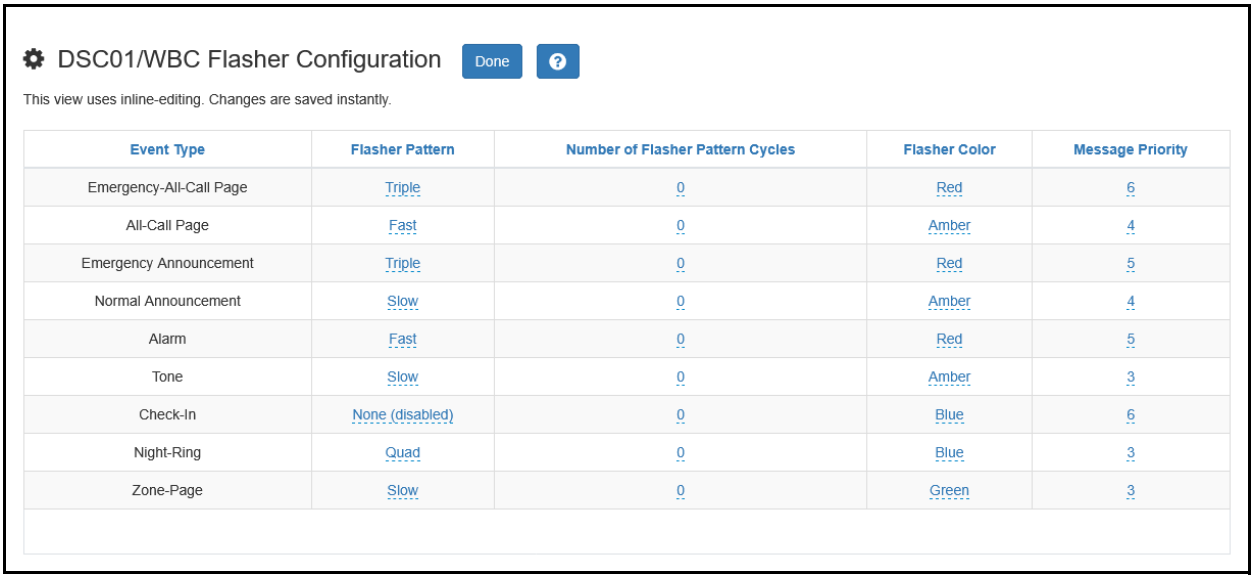
```
# Specify the AD server address and credentials
$adserver = '192.168.11.25'
$user = 'read-only-admin@bogen.com'
$cred = Get-Credential -UserName $user

# Specify the LDAP filter to test. Remember: no line breaks!
$ldapfilter = '(&(objectCategory=person)(objectClass=user)
(|(memberOf:1.2.840.113556.1.4.1941:=CN=Software,OU=Bogen,DC=nyquist-
testlab,DC=com)(memberOf:1.2.840.113556.1.4.1941:=CN=System Test,OU=Bogen,DC=nyquist-testlab,DC=com)))'

# Use the filter to retrieve a list of users.
Get-ADUser -Server $adserver -AuthType Negotiate -Credential $cred -LDAPFilter $ldapfilter
```

Tip: Append "`| Format-Table`" to the `Get-ADUser` command to view the results as a table or "`| Out-GridView`" to view the results in a spreadsheet-like window.

Note: This code explicitly specifies the `-Server` parameter of the `Get-ADUser` cmdlet, which is unnecessary if the current environment is part of the AD domain.

DSC01/WBC Flasher Configuration

The flashers of any NQ-DSC01 or NQ-S1810WBC speakers attached to the Nyquist system can be configured to indicate the activation of Nyquist audio events, such as Emergency-All-Call Page, Emergency Announcement, Alarm, etc.



Event Type	Flasher Pattern	Number of Flasher Pattern Cycles	Flasher Color	Message Priority
Emergency-All-Call Page	Triple	0	Red	6
All-Call Page	Fast	0	Amber	4
Emergency Announcement	Triple	0	Red	5
Normal Announcement	Slow	0	Amber	4
Alarm	Fast	0	Red	5
Tone	Slow	0	Amber	3
Check-In	None (disabled)	0	Blue	6
Night-Ring	Quad	0	Blue	3
Zone-Page	Slow	0	Green	3

Figure 26. NQ-S1810WBC Flasher Configuration

To configure the NQ-DSC01 or NQ-S1810WBC flasher parameters:

1. From the navigation bar, select **System Parameters**.
2. From the *System Parameters* page, select **DSC01/WBC Flasher Configuration**.
3. On the *DSC01/WBC Flasher Configuration* page that appears, make the desired changes. For parameter descriptions, see *Table 22 on page 66*.

Table 22. DSC01/WBC Flasher Configuration

Event Type	The audio event during which the NQ-DSC01 or NQ-S1810WBC flashers can be enabled.
Flasher Pattern	Specifies the on/off pattern the flasher will display. Valid values are: • **No Change**: The message will not cause the selected flasher to change from its current flasher setting. • **Off**: The selected flasher will be turned off unless a higher priority message is using the flasher. When the flasher is turned off, it will remain off until another message is sent with a new flasher setting. • **Slow**: The selected flasher will blink at a rate of once per second for the duration of the message. • **Fast**: The selected flasher will blink at a rate of twice per second for the duration of the message. • **Double**: Flash two (2) times within one second with a 1-second pause and repeat. • **Triple**: Flash three (3) times within 1.5 seconds with a 1-second pause and repeat. • **Quad**: Flash four (4) times within two seconds with a 1-second pause and repeat.
Number of Flasher Pattern Cycles	Specifies the number of times that the flasher pattern will repeat. Valid values are 1 through 65536 or specify zero (0) to flash continuously for the duration of the message.
Flasher Color	Specifies the color of the LED flasher. Valid values are: • **Amber** • **Blue** • **Green** • **Orange** • **Red** • **Violet** • **White** • **Yellow**
Message Priority	Specifies the display message priority for the flasher, where zero is the lowest and six is the highest. For details, see *"Message Priorities and Precedence" on page 499*.

Setting System Parameters

To set system parameters:

1. From the navigation bar, select **System Parameters**.
   The *System Parameters* page displays all key system parameters.
2. To change the settings, select the **Edit** icon.
3. On the *Edit System Parameters* page that appears, make changes to the appropriate settings.
4. After entering all changes, select **Save**.

Using the Edit System Parameters Page

The *Edit System Parameters* page contains the parameters that can be set for the entire facility. It is accessed by selecting the **Edit** icon on the *System Parameters* page. Through the *Edit System Parameters* page, you can also set passwords for the system and various system features, including setting passwords for page and announcement types and alarms and tones.

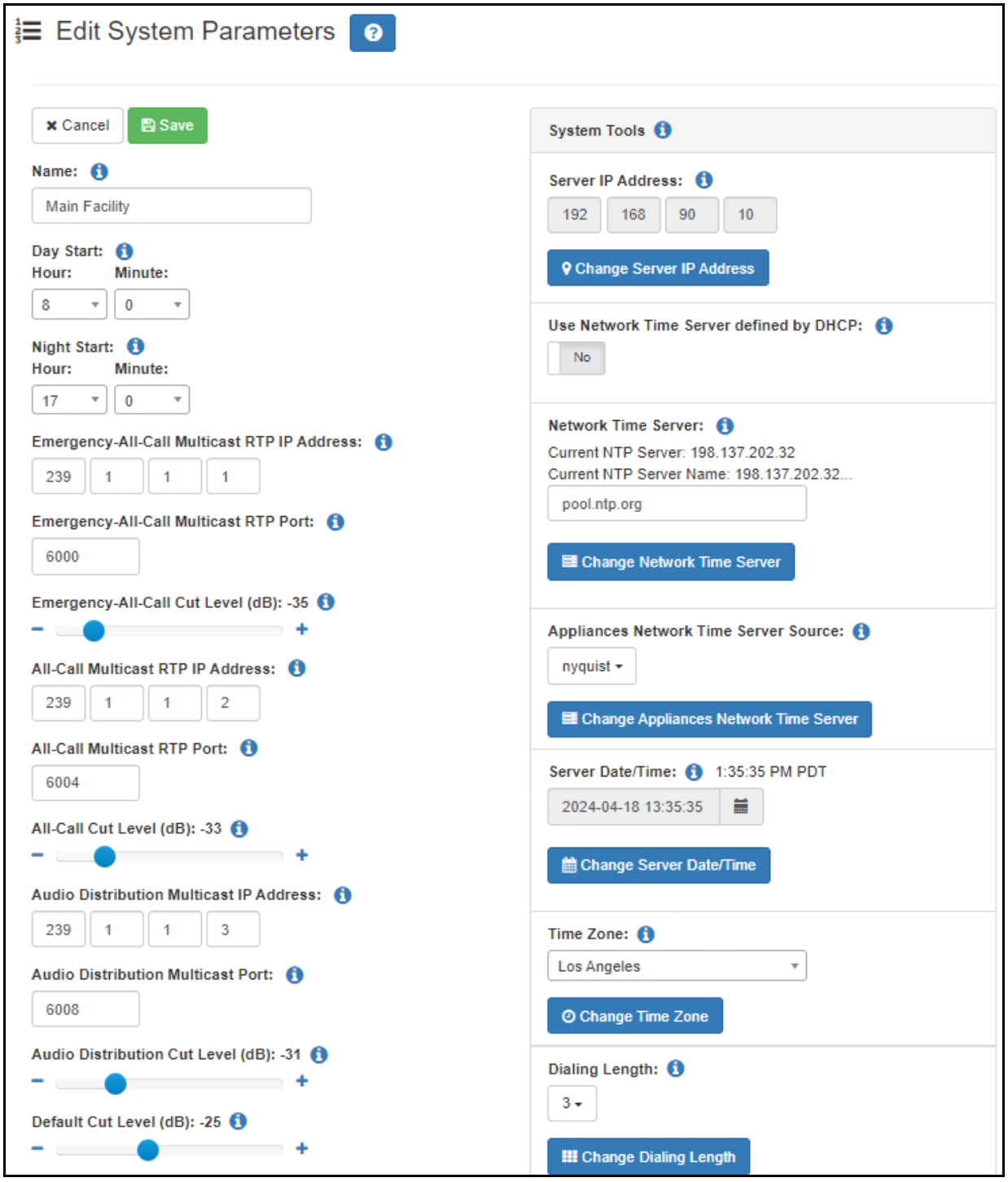


Figure 27. Edit Systems Parameters Page

The following tables describes the system parameters (*Table 23 on page 69*) and System Tools (*Table 24*

on page 78) available on this page:

Table 23. Edit System Parameters Page

Name	Specifies the name given to the entire facility. The name can be up to 30 characters.
Day Start	Identifies when the system switches to its "Day" mode of operation and specifies the time period for which the Day Admin Station is active. Telephones with night-only outside line access are prevented from placing outside line calls during this time. Use the down arrows to select the **Hour** and **Minute** values. Valid times range from 00:00 to 23:58, but must be less than the Night Start time.
Night Start	Identifies when the system switches to its "Night" mode of operation and specifies the time period for which the Night Admin Station is active. During this time, telephones with the night-only outside line access can place outside line calls. Use the down arrows to select the **Hour** and **Minute** values. Valid times range from 00:01 to 23:59 and must be larger than the Day Start time.
Emergency-All-Call Multicast RTP IP Address	Identifies the IP address to use for multicast RTP paging for Emergency-All-Call. Receiving IP telephones must also have this IP address configured. Bogen suggests an address in the range 239.0.0.0–239.255.255.255, but recommends consulting with your IT department to avoid conflicts.
Emergency-All-Call Multicast RTP Port	Identifies the first of four RTP ports to use for multicast RTP paging for Emergency-All-Call. Receiving IP telephones must also have this RTP port configured. Recommended range: 6000 to 7499 Suggested value: 6000 (i.e., ports 6000–6003)
	Caution Ensure that this port range does not overlap other port range assignments, such as **All-Call Multicast RTP Port**, **Audio Distribution Multicast Port**, **RTP Start Port** through **RTP End Port**, or Multicast ports used for Zones.
Emergency-All-Call Cut Level (dB)	Sets the cut volume for Emergency-All-Call audio. The cut volume range is −42 to 0 dB.
All-Call Multicast RTP IP Address	Identifies the All-Call Multicast RTP IP address. Receiving IP telephones must also have this IP address configured. Bogen suggests an address in the range 239.0.0.0–239.255.255.255, but recommends consulting with your IT department to avoid conflicts.

Table 23. Edit System Parameters Page

All-Call Multicast RTP Port	Identifies the first of four RTP ports to use for multicast RTP paging for All-Call. Receiving IP telephones must also have this RTP port configured. Recommended range: 6000 to 7499 Suggested value: 6004 (i.e., ports 6004–6007) **Caution** Ensure that this port range does not overlap other port range assignments, such as **Emergency-All-Call Multicast RTP Port**, **Audio Distribution Multicast Port**, **RTP Start Port** through **RTP End Port**, or Multicast ports used for Zones.
All-Call Cut Level (dB)	Sets the cut volume for All-Call audio. The cut volume range is −42 to 0 dB.
Audio Distribution Multicast IP Address	Identifies the RTP multicast IP address to use for audio distribution to all stations (All Speakers). For more information about audio distribution, see *"Managing Audio" on page 290*. Bogen suggests an address in the range 239.0.0.0–239.255.255.255, but recommends consulting with your IT department to avoid conflicts.
Audio Distribution Multicast Port	Identifies the first of four RTP multicast ports to use for audio distribution to all stations. Recommended range: 6000 to 7499 Suggested value: 6008 (i.e., ports 6008–6011) **Caution** Ensure that this port range does not overlap other port range assignments, such as **Emergency-All-Call Multicast RTP Port, All-Call Multicast RTP Port**, **RTP Start Port** through **RTP End Port**, or Multicast ports used for Zones.
Audio Distribution Cut Level (dB)	Sets the cut volume for audio distributions played to all stations (All Speakers). The cut volume range is −42 to 0 dB. See *"Using Audio Distribution" on page 402* for information on controlling audio distribution played to zones.
Default Cut Level (dB)	Defines the default cut volume level for a new zone. The cut volume range is −42 to 0 dB. For information about zones, see *"Viewing Zone Information" on page 214*.
Ambient Noise Sensor Multicast IP Address	Identifies the multicast IP address to use by ambient noise sensors (ANSs) to send volume data.
Ambient Noise Sensor Multicast Port	Identifies the multicast port number to be used by ANSs to send volume data.

Table 23. Edit System Parameters Page

Disable Preannounce Tone	Indicates if the preannounce tone is disabled. If disabled, the tone is not heard when connecting to a speaker or prior to a page.
Disable Privacy Beep	Indicates if the privacy beep feature is disabled.
Emergency Tone	Identifies the preannounce tone played before an Emergency-All-Call is made.
All Call Tone	Identifies the preannounce tone played before an All-Call is made.
Intercom Tone	Identifies the preannounce tone played before an intercom call is made.
Intercom Wait Tone	Indicates if an intercom caller will hear a continuous ringing while the call is being initiated which stops when the connection to the call recipient is established. *Note:* The "ringing" is not a typical ringtone. It does not include the silence between rings. Instead, the user will hear a continuous ring until the call is established and ready for communication. The length of the ringing depends on the length of the Intercom Tone specified in the system parameters (see above).
Appliance Backup Scheduled Tone	Identifies the tone played by appliances if they are unable to communicate with the C4000 System Controller at the scheduled time. *Note:* The device will continue to play scheduled tones for up to 72 hours.
Default Registration Password	Provides an optional default SIP registration password to be used when adding new stations. This password will be used each time the station registers with the C4000 for SIP communications. The Nyquist controller remembers the station-specific SIP registration password of *each* station that will register with it for SIP communications. Specifying a **Default Registration Password** simplifies the process of adding a new station. If the station's **Registration Password** is not specified, the Nyquist controller's **Default Registration Password** will be used. However, if the Nyquist controller's **Default Registration Password** is not specified, the station's **Registration Password** is required. The minimum length is five characters.
Default Web Password	Provides an optional default web password to be used when adding a new appliance (i.e., station, bridge, or amplifier). If the appliance's **Web Password** is not specified, the Nyquist controller's **Default Web Password** will be used. However, if the Nyquist controller's **Default Web Password** is not specified, the station's **Web Password** is required. The minimum length is five characters. *Note:* Nyquist appliances have distinct web passwords for non-standalone versus standalone modes. **Default Web Password** only applies to non-standalone mode.

Table 23. Edit System Parameters Page

Admin Queue Timeout	Specifies the maximum amount of minutes that a call switch or handset station can remain on an administrative queue. When the time is exceeded, the call switch or handset station is removed from the queue. Valid timeout values range from 1 to 999 minutes.
Night Ring Enabled	Indicates if a night ring is enabled. When enabled, you can optionally set a **Night Ring Admin** and optionally set one additional option from the following list: • **Night Ring All Stations** • **Night Ring Admin Group** • **Night Ring Zones** (For more information on night ring behavior, see *"Configuring Night Call Options" on page 22*.)
Night Ring Admin	Identifies the specific Admin Station that handles outside line calls received during night hours. Outside line calls not answered within 15 seconds ring all or selected stations. If **Night Ring Admin** is the only option set, then the specified Admin extension rings for 30 minutes and hangs up if the call is not answered within that time. *Note:* If **Night Admin** is also included in the call, both **Night Admin** and **Night Ring Admin** ring. An analog phone cannot be used as a Night Ring Admin even if the station has the admin CoS enabled.
Night Ring All Stations	Indicates if all stations receive night rings during night hours. When enabled, any ringing station can answer the call. The specified stations will ring for up to 30 minutes, then hang up if the call is not answered within that time. *Note:* NQ-P0100 Matrix Mixer Pre-Amp stations will also ring.
Night Ring Admin Group	Identifies the Admin Group that handles outside line calls received during night hours. The Admin Group is called if the **Night Admin** and **Night Ring Admin** do not answer within 15 seconds. The specified stations will ring for up to 30 minutes, then hang up if the call is not answered within that time.
Night Ring Zones	Identifies which zones receive night rings when outside calls are received during night hours. The specified stations will ring for up to 30 minutes, then hang up if the call is not answered within that time.
Parking Lot	Defines the range of numbers to use for call parking. The first number listed is used to initiate call parking, which is a feature that allows you to put a call on hold at one telephone set and continue the conversation from any other telephone set.
Record Monitoring	Indicates if call and location monitoring will be recorded.

Table 23. Edit System Parameters Page

Emergency Link	Specifies the station that functions as the system's Emergency Link Station. An Emergency Link Station is the station that an emergency call (but not a 911 call) is routed to if the station's associated Admin Station is busy, rejects the call, or fails to answer within 15 seconds. A value of 999 means that this feature is disabled. If the Emergency Link Station is a ringable device (a Nyquist phone), the station will ring and the call will be displayed on the station's display (if so equipped) as an "Emergency Call." If the Emergency Link Station is not a ringable device (a Nyquist VoIP speaker), the station will auto-answer, preannouncing the call as an "Emergency." The Admin Station will continue to ring if an emergency call is auto-answered by a non-ringable Emergency Link Station device. The Admin Station can retrieve the call by answering it, and the Emergency Link Station device will then drop the call. As with any Emergency Call, all calls to an Emergency Link Station will be recorded.
Max Restricted Digits	Specifies the maximum number of digits that can be dialed if a station has been assigned restricted outside line access.
DISA Password	Identifies the four-digit password required for normal Direct Inward System Access (DISA) operations (e.g., intercom calls, paging via incoming DISA).
Security DISA Password	Identifies the four-digit password required to access Nyquist through a security DISA line, which is used to monitor another station (see *"Using Spy Mode" on page 528*).
CDR Storage Duration	Identifies the number of days that a record of call details will be kept. The maximum value for CDR Storage Duration is 365 days.
Trunk Priority	Identifies the first trunk type to use for placing outbound calls.
Bump on Emergency	Indicates if emergency calls to the Admin Station will bump existing non-emergency calls.
Bump on 911	Indicates if outbound calls to 911 will bump trunk calls if no available outbound trunk is available.
Allow Local Emergency-All-Call Page Interrupt	When enabled, allows a locally initiated Emergency-All-Call page to interrupt an ongoing Multi-Site-Emergency-All-Call page or Emergency-All-Call page, after entering the system PIN code.
Allow Multi-Site-Emergency-All-Call Page Interrupt	When enabled, Emergency-All-Call pages can be interrupted by Multi-Site-Emergency-All-Call pages.

Table 23. Edit System Parameters Page

Auth Code	Allows users to enable the features of a specific station while using a different telephone or web station (on which the Walking Class of Service CoS feature is enabled). This four-digit code activates features of the specified station on the station being used by using the Walking CoS DTMF code (see *"Walking CoS" on page 583*): `3*{auth-code}*{extension}` This should be followed by the DTMF dial code(s) of the desired feature(s).
Facility Password	Identifies the password to be used by facility servers that are registering with this server. The maximum password size is 12 characters.
Remote Facility CoS	Identifies the CoS for remote facility access.
RTP Start Port	Identifies the start port number for UDP RTP traffic. The default value is 10000.
RTP End Port	Identifies the stop port number for UDP RTP traffic. The default value is 20000.

Caution Ensure that the port range from **RTP Start Port** to **RTP End Port** does not overlap other port range assignments, such as **Emergency-All-Call Multicast RTP Port, All-Call Multicast RTP Port, Audio Distribution Multicast Port**, or Multicast ports used for Zones.

Enable RTP Checksums	Indicates if UDP checksums are enabled for RTP traffic. A checksum is a count of the number of bits in a transmission that is included with the transmission so that the receiver can check to see if the same number of bits arrived.
Enable ICE Support	Indicates if Interactive Connectivity Establishment (ICE) support is enabled to enhance peer-to-peer VoIP communications performance. *Note:* Disabling ICE support could result in audio issues when making calls using the Web Interface.
STUN Server	Identifies the host name or IP address and optional port for the Session Traversal Utilities for NAT (STUN) server that is used when determining the external IP address and port for an RTP session. (Do not include the stun: prefix.) *Note:* A port number is optional. If omitted, the default value of 3478 will be used.
TURN Server	Identifies the host name or IP address for the Traversal Using Relays around NAT (TURN) server that is to be used as a relay. (Do not include the turn: prefix.) *Note:* A port number is optional. If omitted, the default value of 3478 will be used.
TURN Username	Identifies the user name used to authenticate with the TURN server.

Table 23. Edit System Parameters Page

TURN Password	Identifies the password used to authenticate with the TURN server.
Retention Recordings	Identifies the number of days to retain recordings. Recordings that are older than the retention period are automatically deleted. You can set a maximum retention period of 99,999 days.
Backup Retention System	Identifies the number of days to retain system backup files. System backups that are older than the retention period are automatically deleted, provided at least one system backup file remains. You can set a maximum retention period of 99,999 days.
Backup Retention Recordings	Identifies the number of days that backups of recordings are retained. Backups that are older than the retention period are automatically deleted, provided at least one backup remains. You can set a maximum retention period of 99,999 days.
Backup Retention Voicemail	Identifies the number of days that voicemail backups are retained. Backups that are older than the retention period are automatically deleted, provided at least one backup remains. You can set a maximum retention period of 99,999 days.
Backup Recordings Enabled	If enabled, call recordings will be backed up according to the specified frequency and retention period (see *"Editing Backup Settings" on page 354*). *Note:* This setting is also available via the *System Backup/Restore* page's **Backup Recordings Enabled** setting.
Backup Voicemail Enabled	If enabled, voicemails will be backed up according to the specified frequency and retention period (see *"Editing Backup Settings" on page 354*). *Note:* This setting is also available via the *System Backup/Restore* page's **Backup Voicemail Enabled** setting.
System Password	Displays the password that must be entered whenever a user is prompted for the System Password (e.g., starting or stopping a routine via DTMF that is not configured to be started or stopped via DTMF).
Multi-Site-Emergency-All-Call Password	Identifies the 4-digit password to use if a caller is required to enter a password when starting a Multi-Site-Emergency-All-Call page. A password of four zeros (0000) requires the caller to enter 1 for confirmation when starting a Multi-Site-Emergency-All-Call page.
Multi-Site-All-Call Password	Identifies the 4-digit password to use if a caller is required to enter a password when starting a Multi-Site-All-Call page. A password of four zeros (0000) requires the caller to enter 1 for confirmation when starting a Multi-Site-All-Call page.
Facility-Page Password	Identifies the 4-digit password to use if a caller is required to enter a password when starting a Facility page. A password of four zeros (0000) requires the caller to enter 1 for confirmation when starting a Facility page.

Table 23. Edit System Parameters Page

Emergency-All-Call Password	Identifies the 4-digit password to use if a caller is required to enter a password when starting an Emergency-All-Call page. A password of four zeros (0000) requires the caller to enter 1 for confirmation when starting an Emergency-All-Call page.
All-Call Password	Identifies the 4-digit password to use if a caller is required to enter a password when starting an All-Call page. A password of four zeros (0000) requires the caller to enter 1 for confirmation when starting an All-Call page.
Emergency-Announcement Password	Identifies the 4-digit password to use if a caller is required to enter a password when starting or stopping an Emergency Announcement. A password of four zeros (0000) requires the caller to enter 1 for confirmation when starting or stopping an Emergency Announcement.
Announcement Password	Identifies the 4-digit password to use if a caller is required to enter a password when starting or stopping an Announcement. A password of four zeros (0000) requires the caller to enter 1 for confirmation when starting or stopping an Announcement.
Facility-Announcement Password	Identifies the 4-digit password to use if a caller is required to enter a password when starting or stopping a Facility Announcement. A password of four zeros (0000) requires the caller to enter 1 for confirmation when starting a Facility Announcement.
Facility-Emergency-Announcement Password	Identifies the 4-digit password to use if a caller is required to enter a password when starting or stopping a Facility Emergency Announcement. A password of four zeros (0000) requires the caller to enter 1 for confirmation when starting a Facility Emergency Announcement.
Zone-Page Password	Identifies the 4-digit password to use if a caller is required to enter a password when starting a zone page. A password of four zeros (0000) requires the caller to enter 1 for confirmation when starting a zone page.
Alarm Password	Identifies the 4-digit password to use if a caller is required to enter a password when starting or stopping an Alarm. A password of four zeros (0000) requires the caller to enter 1 for confirmation when starting or stopping an Alarm.
Tone Password	Identifies the 4-digit password to use if a caller is required to enter a password when starting or stopping a tone. A password of four zeros (0000) requires the caller to enter 1 for confirmation when starting or stopping a Tone.
Audio Distribution Password	Identifies the 4-digit password to use if a caller is required to enter a password when starting or stopping an audio distribution. A password of four zeros (0000) requires the caller to enter 1 for confirmation when starting or stopping an audio distribution.
Disable Emergency All-Call and Intercom when Audio Disabled	If **Audio Disabled** is enabled (see *"Enabling and Disabling Audio" on page 404*), this indicates whether or not Emergency All-Call and Intercom calls will also be disabled.

Table 23. Edit System Parameters Page

Zone Control Password	Identifies a password to access the Zone Control view (see *"Zone Control: Volume and Audio Distribution Panel" on page 344*).
Enable Callback Request Indicator	Indicates if the Callback Request Indicator feature is enabled for this system (see *"Managing Calls via the Dashboard" on page 393*). *Note:* This feature only applies to Digital Call Switch G2 stations with a CoS-based call-in level of Normal+Emergency or Urgent+Emergency.
Callback Request Indicator Expiration	Identifies for how many hours a Callback Request Indicator will remain active before being turned off. A value of zero (0) indicates no expiration.
Enable Nyquist STUN Server for Web Interface	Configures web interface stations to use the local Nyquist server as the ICE server. **Caution** This feature may resolve issues placing calls from the web interface dashboard, but should be used as a last resort after all other solutions have failed.
Enable Queued Paging Instruction Message	When enabled (Yes), verbal instructions are provided before a queued message is recorded via Record Page. When disabled (No), only a beep tone is played to indicate the start of recording.
Enable Queue All-Call Page	When enabled (Yes), All-Call pages will be recorded and queued for playing to all speakers. Queued All-Call pages have higher priority than queued zone pages and will interrupt any that are currently playing, which will be replayed after completion of the All-Call page.
Talkback Hold Time (ms)	The length of time (in milliseconds) that talkback is disabled after a voice is detected from the admin phone.
Talkback Threshold (dB)	The level at which a voice is considered "detected" on the admin phone. Higher levels are recommended for loud environments.
Enable LLDP Discovery	Enable all Nyquist appliances to advertise themselves to the network using Link Layer Discovery Protocol (LLDP, specifically LLDP-MED) for network inventory and diagnostics. This feature is disabled by default. *Note:* VLAN auto-provisioning and configuration is not currently supported.

System Tools

The *Edit System Parameters* page contains a section called System Tools. These settings are managed independently from the parameters listed in *Table 23, "Edit System Parameters Page," on page 69* (i.e.,

they are not controlled by the **Cancel** and **Save** buttons, but instead take effect immediately). The following table describes parameters for this section.

Table 24. System Tools

Server IP Address	Identifies the Nyquist system server IP address that will be used by Nyquist devices to register and communicate with the Nyquist system server. *Note:* This is the IP address to specify as an appliance's **TFTP Server**, from which it can retrieve its *Configuration* settings via the **Get Configuration from Server** button. The C4000's IP configurations for both Port A and Port B are specified using the *Network Wizard*, which can configure each port to either use a static IP address or obtain its IP configuration from an external DHCP server (or, for Port B, to disable it). The **Change Server IP Address** button provides the option to select which previously configured C4000 IP address Nyquist devices will register and communicate with. Use the mouse or down arrow to select which IP address (i.e., which Ethernet port, Port A or Port B) to use. **Caution** The Nyquist DHCP service does not operate on the Port B network. If the Nyquist DHCP service is to be used, do not select the Port B IP address. *Note:* If this Nyquist Server is configured for Automatic Failover (see *"Automatic Failover" on page 84*), this will show the Master IP address and the user should not attempt to change this value. If the Master IP address must be changed, you should: 1 disable Automatic Failover, 2 change the server IP address (via the Network Wizard), 3 and reconfigure Automatic Failure. *Tip:* The network settings (i.e., IP address, subnet, gateway, DHCP server, and/or DNS servers) of both network ports can be viewed and changed using the Network Wizard, which can be accessed via the following URL: https://<server>/setup/network
Use Network Time Server defined by DHCP	When enabled, the C4000 will use the Network Time Protocol (NTP) server defined via DHCP option 42.

Table 24. System Tools (continued)

Network Time Server	Identifies a comma-delimited list of IP addresses and/or domain names of Network Time Protocol (NTP) servers to be used. The C4000 will communicate with each NTP server and choose the best one from the list. The maximum length of this list is 768 characters, including commas. To change the NTP server, specify one or more IP addresses and/or domain names, then select **Change Network Time Server**. If unspecified, the default setting is time.google.com.
Appliances Network Time Server Source	Identifies the time source for all appliances on the Nyquist network (excluding the C4000 itself, which gets its NTP source via the **Network Time Server** configuration). The appliances may use one of the following sources: • **nyquist** When this option is selected, all Nyquist appliances will use this Nyquist system server as the NTP server. This is the default option. • **dhcp** When this option is selected, all Nyquist appliances will use the NTP server provided via DHCP option 42. If the built-in Nyquist DHCP Server feature is being used, all Nyquist appliances will use the Nyquist server for NTP service via the Server IP Address. • **ntpserver** When this option is selected, all Nyquist appliances will use the Network Time Server defined in the **Network Time Server** setting (above). To change the time source for the appliances, use the down arrow to select the desired source, and then select **Change Appliances Network Time Server**.
Server Date/Time	Identifies the date and time of the server. To change the Server Date/Time, use the **Calendar** icon to select the new date, and then select **Change Server Date/Time**.
Time Zone	Sets the time zone for the server. To change the time zone, select a new time zone from the drop-down menu, and then select **Change Time Zone**. The available time zone options are based on the IANA time zone database. *Note:* A time zone change will not take effect until after the C4000 server has been rebooted. You will be prompted to reboot, either now or later. If you do not reboot immediately after making the change, be sure to do so as soon as possible to avoid time zone-related issues, such as authentication failures.

Table 24. System Tools (continued)

Dialing Length	Specifies the number of digits required to dial within the system. Valid values are 3, 4, 5, or 6. To change the dialing length, select a new value from the drop-down menu, and then select **Change Dialing Length**. You must reboot all Nyquist appliances and IP phones. A system backup is automatically created.
Routines API Key	The Routines API Key is used as an authorization passcode by Routines API (REST) calls. Every Routines API call must include an HTTP header called `Authorization` whose value is the string, "Bearer xxxxxxxx", where xxxxxxxx is the **Routines API Key**. If this value is missing or incorrect, the call will fail. For further details, see *"Using the Routines API" on page 428*.
Reset	Invalidates the current **Routines API Key** and randomly generates a new one. This will prevent a potentially compromised key from being used, as all subsequent calls using the old key will fail. This new key should be securely communicated to all valid users of the Routines API. Be aware that this operation immediately invalidates the key. You will be prompted with a warning after clicking this button to prevent accidental resets.
Additional IP addresses and/or DNS names to include in the Server Certificate	Additional IP addresses and/or DNS names, as a space-separated list, to include in the generated server certificate's Subject Alternative Names (SAN) field. This indicates to a client that this certificate is valid for a server at any of the specified IP addresses or DNS names. A domain wildcard may be included (e.g. *.your-domain.com). This is primarily intended for adding an alternate IP address and/or DNS name, such as a public-facing network connected to Ethernet Port-B or a valid DNS name, that your site is supporting for the Nyquist server. *Note:* Automatic Failover configurations automatically include the Master, Primary, and Secondary IP addresses in the SAN, so this need not be set explicitly.
Generate Server Certificate	Generates a server certificate for this Bogen server. The certificate will include any additional IP addresses and/or DNS names specified in the aforementioned "Additional IP addresses..." setting as part of the certificate's Subject Alternative Name (SAN) field. **Important:** After a system update, the bogen`CA.crt` file needs to be recreated before it can be downloaded to a client again (see *"Client Requirements" on page 8*). Use this button to re-generate the certificate.
Download Bogen CA Certificate	Initiates a download of a CRT file containing the public Bogen Certification Authority (CA) certificate. This CA certificate should be installed on any devices that will connect to this Bogen server, whether through a browser or through the Routines API, so that they can authenticate it as a valid Bogen server.

Table 24. System Tools (continued)

Remote Calendar Control	Configures which Facilities, if any, will be allowed remote access to this system's Calendars. • **Disabled**: Remote Facilities are not permitted to control this system's calendar (although this Facility may still be able to access a remote Facility's calendar). • **Allow Facilities**: All enabled Facilities from the Facilities view are permitted to remotely access and control this system's calendar. • **Allow Access List**: All specified Facilities (as specified by IP addresses in the **Calendar Control Access List** field) are permitted to remotely access and control this system's calendar. See **Calendar Control Access List** for more information. *Note:* If none of the Facilities are using Automatic Failover, **Allow Facilities** is the easiest way to enable Remote Calendar Control. If any of the Facilities are using Automatic Failover, you will need to use **Allow Access List** to enable Remote Calendar Control. *Note:* Only users whose Role has the **Remote Calendar Control** permission will be able to access remote calendars.
Calendar Control Access List	This field is only shown if **Remote Calendar Control** is configured as **Allow Access List**. A space-separated list of IP addresses specifying the remote Facilities that are permitted to manage this system's calendar. This list should include the Primary IP Address, Secondary IP Address, and Server IP Address of each Facility that uses Automatic Failover, as well as the Server IP Address for each server that does not use Automatic Failover.
Update Remote Calendar Control	When pressed, the **Remote Calendar Control** and optional **Calendar Control Access List** changes will take effect.
Nyquist Control Password	Specifies a password used to secure Nyquist control messages between the C4000 controller and associated Nyquist appliances. The password specified on each Nyquist appliance must match the password specified here for that appliance 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 current user's password has been modified from the Bogen-defined default value. Similarly, this password cannot be set on a Nyquist appliance unless the Web Password for that appliance's Station, Amplifier, or Gateway device has been changed from the Bogen-defined default value.
Save Password	Saves the value specified in the **Nyquist Control Password** field as the current Nyquist control password.

Warning	After the password has been modified and saved, features that depend on this password will not work until this password has been updated on all Nyquist devices.

Table 24. System Tools (continued)

Show Saved Password	Displays the current Nyquist control password.
Update Nyquist Devices	Updates the Nyquist control password on connected Nyquist devices using the current Nyquist control password.

Warning Nyquist devices that are not currently connected will not be updated. These may need to be updated manually on the device's web interface, or use this button again when they are connected.

Schedule Site Settings: Label Singular	Specifies a word or phrase to be used throughout the schedules in place of the word "site."
Schedule Site Settings: Label Plural	Specifies a word or phrase to be used throughout the schedules in place of the word "sites."
Schedule Site Settings: Icon	Specifies the icon to be used throughout the schedules to represent one or more sites.
Schedule Site Settings: Save Settings	Apply changes to the site labels and icons.
Certificate Authority File Upload	Select and upload a PEM or CRT file containing an X.509 certificate authority (CA), which can be used to authenticate secure SIP TLS and/or SRTP connections. The certificate must identify a CA in the certificate chain (i.e., certification path) of the SIP trunk server's certificate.

Important: The C4000 can authenticate certificates issued by most public CAs. A Certificate Authority file only needs to be specified if the C4000 cannot authenticate an SIP trunk certificate's issuing CA.

A file can be uploaded from your local machine or via a remote URL. For example, the Twilio CA file can be found at:

https://docs-resources.prod.twilio.com/documents/ca-bundle-sip.crt

Note: The uploaded certificate may not be available for use until after the **Save** button has been selected.

Table 24. System Tools (continued)

Call Assurance Audio	Identifies the audio to be played to the caller to indicate that a call to the admin station has been placed. To choose a new file, select **Choose File**, browse to select the new file to be used for the Call Assurance audio, and press **Save Call Assurance Audio**. The supported audio formats are: • WAV (8 kHz, 16-bit, mono) • GSM *Tip:* There are websites (e.g., https://convertio.co) that can convert audio files into an appropriate audio format.
Urgent Call Assurance Audio	Identifies the audio to be played to the caller to indicate that an urgent call to the admin station has been placed. To choose a new file, select **Choose File**, browse to select the new file to be used for the Urgent Call Assurance audio, and press **Save Urgent Call Assurance Audio**. The supported audio formats are: • WAV (8 kHz, 16-bit, mono) • GSM

Table 24. System Tools (continued)

Emergency Call Assurance Audio	Identifies the audio to be played to the caller to indicate that an emergency call to the admin station has been placed. To choose a new file, select **Choose File**, browse to select the new file to be used for the Call Assurance audio, and press **Save Emergency Call Assurance Audio**. The supported audio formats are: • WAV (8 kHz, 16-bit PCM, mono) • GSM
Nyquist Appliance VoIP Security **Enable Security** **Disable Security**	Enables or disables SIP TLS and SRTP security for *all* currently configured Nyquist appliances (and *only* Nyquist appliances; not SIP trunks or non-Nyquist devices). *Tip:* We recommend selecting **Enable Security** after adding Nyquist devices to ensure SIP devices are communicating as securely as possible. Be sure to also configure non-Nyquist devices to use SIP TLS and SRTP wherever possible. Alternatively, SIP TLS and SRTP security can be enabled or disabled independently for each device (see *"Editing Station Configuration Settings" on page 155*). To identify the security status of a given station, examine the **Registered** status in the device's **Device Status** listing (see *"Viewing Station Configuration Settings" on page 142* or *"Simplified Configuration" on page 220*). If the device is registered with SIP TLS enabled, the text, **(Secure SIP enabled)**, will be appended to the **Registered** status. If the station is configured for SIP TLS but is not registered, the status listing will include **Configured for Secure SIP with TLS**. *Note:* This option is only available if the **Nyquist Appliance VoIP Security** permission is assigned to the user's role and if all Nyquist appliances are using firmware version 5.0 or later.

Automatic Failover

Nyquist servers provide the ability to configure two Nyquist servers to act as a Master and Slave. If and when the Master Nyquist server fails, the Slave server can automatically take over, thereby ensuring reliable functionality.

The basic mechanism by which Automatic Failover works is conceptually very simple. Each of two servers, a primary and a secondary, are assigned IP addresses. A third IP address, known as the Master IP Address, is then assigned to the primary server. This master IP address is used by users and devices to access the Nyquist system, and the server providing service via the master IP address is known as the Master server. The secondary server is known as the Slave server, which monitors the Master server.

If the Master server fails for any reason, the Slave server detects the failure, assigns the master IP address to itself, and takes over as the Master. When the primary server recovers, the secondary server releases the master IP address, becoming the Slave, and the primary server reassigns the master IP address to itself, once again becoming the Master.

The Automatic Failover feature also includes another concept: Standby mode. A server in Standby mode will relinquish the Master role, if it is currently the Master, and will not resume as Master until explicitly removed from Standby. This is useful when you wish to force the secondary server to assume Master functionality, such as for primary server maintenance purposes.

The configured Automatic Failover role (primary or secondary) and mode (master or slave) of a server is displayed on the *Login* screen, indicating to the user which server is being accessed. The role and mode are also indicated in the header of each page as a yellow (slave) or green (master) shield icon followed by an S (secondary server) or P (primary server), as shown below in *Table 25*.

Table 25. Automatic Failover Role and Mode Indicators

Indicator	Role and Mode
P (green)	Primary server in master mode
S (green)	Secondary server in master mode
P (yellow)	Primary server in slave mode
S (yellow)	Secondary server in slave mode

Important: When logged in to the web station of a slave-mode server, the Dashboard will display an error indicating that the station is not connected to the server (and may recommend verifying the Bogen CA installation). This is normal and simply indicates that the slave-mode server is not active as a SIP server and, therefore, this web station cannot initiate or receive calls, announcements, pages, or tones, as well as many other functions.

In general, a slave-mode server should only be used as described in the following sections. It should not be used for normal operations or to make configuration changes, as most functions will not work, and configuration changes will be lost when the master server resumes operation.

Recoverable Failures

There are any number of server failures which will cause the Automatic Failover mechanism to promote the secondary server to Master. The following list is not comprehensive, but provides a number of examples.

Hardware Failures

- Catastrophic server failure causing server to no longer power up or boot
- Loss of power
- Damaged Ethernet hardware (NIC)
- Damaged RAM
- Ethernet cable no longer supplying network connection (e.g., cable pulled out, cable damaged, failed network switch, network switch isolated from network, etc.)
- Catastrophic SSD failure

Software Failures

- Catastrophic software failure that prevents system from booting
- Operating System failure (becomes unresponsive or reboots)
- Repeated Operating System service failures (e.g., web server, database server, DHCP server, etc.)
- Repeated Nyquist service failures (Communication service, Device Monitor, Queue Manager)
- System becomes unresponsive, due to software issue
- Disk full, resulting in software failures
- System Update being performed on Primary server (this is a normal cause of failover, though it's not really a failure.)

Note: Some of these conditions may only be temporary. The primary server may resume the primary role after a successful reboot or it becomes responsive again.

Automatic Failover Configuration

To use the Automatic Failover functionality, the administrator must configure the two servers with their static IP addresses—both on the same subnet—and with the master IP address. The administrator will then step the two servers through several coordination phases—Initialization, Database, Services, and Resources—at the end of which the primary server will be in master mode and the secondary server will be in slave mode, ready to take over and provide service.

Allocate three IP addresses to be used for the servers, all within the same subnet, and ensure that these addresses are reserved (i.e., will not be used by other machines or allocated by a DHCP server). You will also need to select an authentication password, which is used by each of the servers to verify that it is a legitimate failover partner.

If there are any firewalls between the primary and secondary servers, the following network ports must be opened for both inbound and outbound traffic before proceeding.

- UDP 5405
- TCP 2224
- TCP 3121

Note: The servers do not share USB-based audio files. If the primary server is using USB-based audio distribution files, make sure that the secondary server has an exact copy of the USB flash drive being used by the primary server.

To configure the primary and secondary servers:

1. Determine the IP addresses and authentication password to be used by the servers:
   - Master IP address
   - Primary IP address
   - Secondary IP address
   - Authentication password
     The authentication password must match on both the primary and secondary servers for the Automatic Failure mechanism to work.
2. Activate a Nyquist system controller to use as a primary server. Assign the master IP address (*not* the primary IP address) to Port-A of the system.
3. Activate a Nyquist system controller to use as a secondary server. Assign the secondary IP address to Port-A of the system.
4. Ensure the secondary server contains an **Automatic Failover** license before proceeding any further with the configuration process. This can be verified by clicking the **Product License** button on the **System Parameters** page of the secondary server. If the **Automatic Failover** property of the **Licensing Information** section shows "Licensed," the feature is enabled. Note the primary server will report this as "Not Licensed" until after **Automatic Failover** is fully configured. If needed, contact Bogen or an Authorized Reseller to purchase the **Automatic Failover License Key**.
5. Install the server's Certification Authority on your local machine (see *"Bogen Digital Certification Authority" on page 588*).

Note: Browser security warnings will not immediately be eliminated as the servers may not yet have a certificate with the appropriate IP addresses associated with it, but these warnings should stop within the next couple steps.

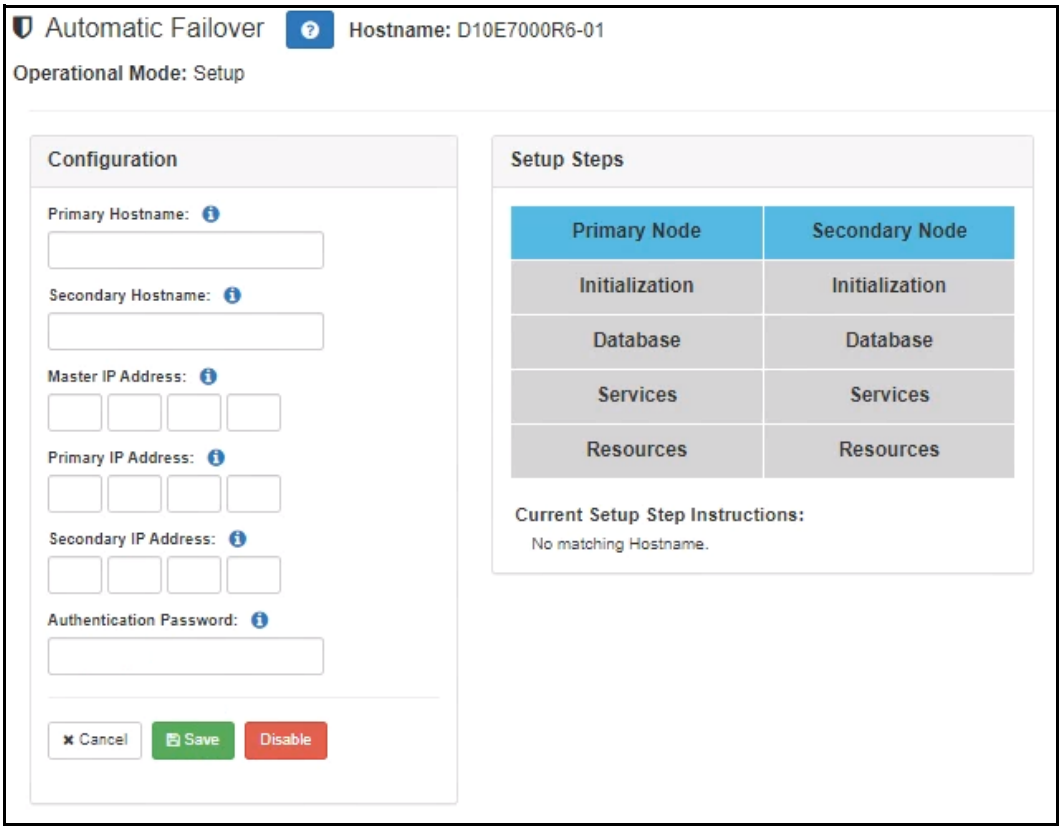


Figure 28. Automatic Failover Configuration

Note: Subsequent instructions will indicate on which server to perform the operations, with sub-items providing the steps to perform.

---

6 *Primary server*

a) Open a browser window or tab and navigate to the Dashboard using the Master IP address, then to the **Automatic Failover** area.

b) Enter the hostname and IP address for each of the primary and secondary servers.

c) Enter the master IP address (i.e., the same address which your browser is currently addressing).

d) Enter the secret authentication password.

e) Press the **Save** button and wait for confirmation.

f) To continue the process on the primary server, you will need to login again using the *primary* IP address (instead of the *master* IP address).

7 *Secondary server*

a) Open a new browser window or tab and navigate to the Dashboard using the secondary IP address, then to the **Automatic Failover** area.

Tip: As you will be alternating between the primary and secondary servers frequently, it may be easiest to keep them in separate browser windows.

---

b) Enter the hostname and IP address for each of the primary and secondary servers.

c) Enter the master IP address.

d) Enter the same secret authentication password used on the primary server.

e) Press the Save button and wait for confirmation.

From this point forward, the **Setup Steps** section of the **Automatic Failover** page will indicate instructions to perform for each step. These instructions should directly correspond to the steps provided here.

This stage of the configuration process will walk you through a sequence of configuration steps, requiring you to alternate between the browser windows of the Primary and Secondary servers. The following table summarizes these Setup Steps (i.e., button clicks) and on which server (i.e., browser) each step should be performed.

Note that the sequence of buttons to be clicked for each stage (i.e., Initialization, Database, Services, and Resources) follows the same pattern:

- Primary Server, Primary Node button
- Secondary Server, Primary Node button
- Secondary Server, Secondary Node button
- Primary Server, Secondary Node button

Primary Server			
#	Primary Node	#	Secondary Node
1	Initialization	4	Initialization
5	Database	8	Database
9	Services	12	Services
13	Resources	16	Resources

Secondary Server			
#	Primary Node	#	Secondary Node
2	Initialization	3	Initialization
6	Database	7	Database
10	Services	11	Services
14	Resources	15	Resources

8 *Primary server*

a) Press the **Initialization** button under **Primary Node** and wait for confirmation.

9 *Secondary server*

a) Press the **Initialization** button under **Primary Node** and wait for confirmation.

b) Press the **Initialization** button under **Secondary Node** and wait for confirmation.

10 *Primary server*

a) Press the **Initialization** button under **Secondary Node** and wait for confirmation.

b) Press the **Database** button under **Primary Node**.

c) Refresh the web page until the **Database** button turns green. If errors are displayed, continue refreshing the web page until the **Database** button turns green.

11 *Secondary server*

a) Press the **Database** button under **Primary Node** and wait for confirmation.

b) Press the **Database** button under **Secondary Node**.

c) Refresh the web page until the **Database** button turns green. If errors are displayed, continue refreshing the web page until the **Database** button turns green.

12 *Primary server*

a) Press the **Database** button under **Secondary Node** and wait for confirmation.

b) Press the **Services** button under **Primary Node** and wait for confirmation.

13 *Secondary server*

a) Press the **Services** button under **Primary Node** and wait for confirmation.

b) Press the **Services** button under **Secondary Node** and wait for confirmation.

14 *Primary server*

a) Press the **Services** button under **Secondary Node** and wait for confirmation.

b) Press the **Resources** button under **Primary Node** and wait for confirmation. If errors are displayed, refresh the web page.

c) If a login screen is displayed, log back into the web interface, open the **Automatic Failover** area and confirm that the **Resources** button is green.

15 *Secondary server*

a) Press the **Resources** button under **Primary Node** and wait for confirmation.

b) Press the **Resources** button under **Secondary Node** and wait for confirmation.

16 *Primary server*

a) Press the **Resources** button under **Secondary Node** and wait for confirmation.

If all setup buttons are green at this point, the **Primary Node** is in master mode and the **Secondary Node** is in slave mode. The system has been successfully configured for Automatic Failover.

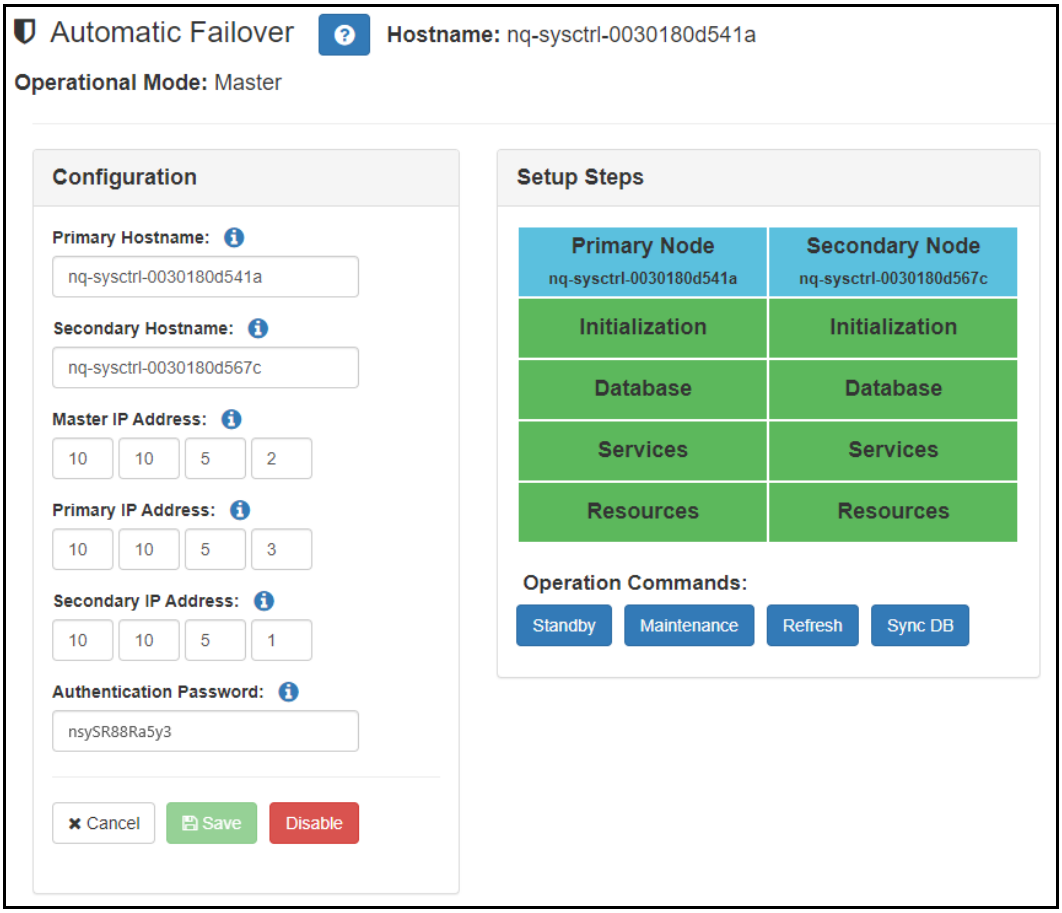


Figure 29. Automatic Failover Operations mode

Note: The Automatic Failover page can be accessed via the Primary or Secondary IP address, or via the Master IP address. When accessed via the Primary or Secondary IP address, it displays and allows the user to access the Operation Commands, as shown in *Figure 29*. When accessed via the Master IP address, links to the Primary and Secondary servers are shown instead.

Table 26. Automatic Failover Parameters

Hostname	Name of the current server.
Operational Mode	Indicates the current state of the Automatic Failure configuration or operation on this server. Possible values are: • Setup • Master • Slave • Standby • Maintenance
Primary Hostname	Name of the Primary server.
Secondary Hostname	Name of the Secondary server.

Table 26. Automatic Failover Parameters (continued)

Master IP Address	The IP address that is used by Nyquist devices, the Nyquist web interface, SIP-based telephony devices, and Routines API clients of the Nyquist system to communicate with the Nyquist system. The Master IP Address is also known as the Server IP Address.
Primary IP Address	The IP address of the primary server, used for communicating with the secondary server and for performing specific Automatic Failover operations through the web interface.
Secondary IP Address	The IP address of the secondary server, used for communicating with the primary server and for performing specific Automatic Failover operations through the web interface.
Authentication Password	Password used for authentication between the primary and secondary servers.
Save	Saves the currently shown configuration settings.
Disable	Disables the Automatic Failover functionality for this server, returning this server to a standalone server. To temporarily disable Automatic Failover, use the Standby or Maintenance modes instead. **Caution** This action will completely remove the Automatic Failover configuration and is not reversible without performing the setup process over again.
Setup Steps	Shows which setup step is currently being performed during the Automatic Failover setup process. Successfully completed steps are displayed in green.
Standby	Places the current server in Standby mode, which causes the server to surrender the Master role to the partner server and to subsequently refuse to accept the Master role.
Unstandby	Removes the current server from Standby mode and potentially resumes the Master role.

Table 26. Automatic Failover Parameters (continued)

Maintenance	Places the current server in Maintenance mode. *Note:* Do not place your server into Maintenance mode unless instructed to do so by Technical Support. While in Maintenance mode, a server will neither assume nor relinquish the Master role due to failures, but will maintain its current role. For example, if the Primary server is in Maintenance mode and suffers a software error or controlled software restart, it will not relinquish the Master role to the Secondary server. Similarly, if the Secondary server has assumed the Master role and is then placed into Maintenance mode, it will not assume the Master role when the Primary server recovers until the Secondary server is taken out of Maintenance mode. *Note:* Although a server will not explicitly assume or relinquish the Master role while in Maintenance mode, the other server may still assume the Master role if the server in Maintenance mode is incommunicado due to a shutdown, reboot, or other network issues.
Unmaintenance	Removes the current server from Maintenance mode. *Note:* Do not place your server into Maintenance mode unless instructed to do so by Bogen Technical Support.
Refresh	Refreshes the Automatic Failover status. This clears previous failures that may have caused failover from Master to Slave.
Sync DB	Synchronizes the database between Master and Slave servers. To synchronize the databases, first execute **Sync DB** while logged into the Primary server IP address. Wait for confirmation that the operation has completed, then execute **Sync DB** while logged into the Secondary server IP address. *Note:* You *must* execute the **Sync DB** command on the Primary server first.

Automatic Failover Process

The failover process, once configured, will automatically occur if the primary server fails. The failure may be an internal error that is detected by the primary server itself, or it may be a catastrophic failure, such as a hardware failure, where the secondary server loses contact with the primary and assumes the Master role.

Warning It is STRONGLY recommended that system configuration changes NOT be made while the Secondary server is acting as the Master server. Any such changes will not be replicated to the Primary server. If changes *must* be made (e.g., while awaiting a replacement Primary server), be sure to perform the same changes on the Primary server when it is placed in service.

Initiating a Server Shutdown

If you need to shutdown the primary server and you want the secondary server to provide service during the primary server's downtime, put the primary server into Standby mode by pressing the **Standby** button before performing the shutdown. Later, when the primary server boots up, it will remain in Standby mode. When you are ready for it to resume the master role, take it out of Standby mode by pressing the **Unstandby** button.

A secondary server in Slave mode can be shutdown immediately. When it boots up, it will automatically resume in Slave mode.

Before shutting down a secondary server in Master mode, make sure the primary server is available and in Master mode. If the primary server is in Standby mode, take it out of Standby mode and wait for it to assume the Master role before shutting down the secondary server.

Primary Server Permanent Failure

If the Primary server permanently fails, forcing the use of the Secondary server as the Master, you will need to setup a new System Controller to use as the Primary, disable Automatic Failover on the Secondary, and then perform the Automatic Failover configuration on the two servers.

Caution	Although the secondary server will provide full functionality, the Automatic Failover license will not operate indefinitely without a primary server. Please contact Bogen or an Authorized reseller for information on replacing the primary server.

Restore the System from a System Backup

To restore an Automatic Failover-configured system from a system backup, follow these steps:

1. Perform the system restore on the primary server using a system backup that was created after the **Automatic Failover** setup (see *"Restoring a Backup File" on page 358*).
2. On the **Automatic Failover** page of the primary server, press **Sync DB** under **Operation Commands** and wait until it finishes.
3. On the **Automatic Failover** page of the secondary server, press **Sync DB** under **Operation Commands** and wait until it finishes.
4. On the **Automatic Failover** page of the primary server, press the **Refresh** button.
5. On the **System Parameters** page, press **Check Server Status**.
6. In the **Automatic Failover Status** section, check that the following statements are true:
   - "**MySQL Master Status, File**" is equal to "**MySQL Slave Status, Master_Log_File**"
   - "**MySQL Master Status Position**" is equal to "**MySQL Slave Status, Read_Master_Log_Pos**"
   - "**MySQL Slave Status, Slave_IO_Running**" is **Yes**
   - "**MySQL Slave Status, Slave_SQL_Running**" is **Yes**
7. If any statements in step #6 are false, repeat the procedure starting with step #2
8. If statements listed in step #6 are not true, even after repeating the steps, contact technical support.

Note: System Restore will only restore configuration data; it will not repair all issues that may be related to the **Automatic Failover** feature. If system restore does not solve the problem you're experiencing, then disable the **Automatic Failover** feature and repeat the **Automatic Failover** setup process. If your problem is still not resolved, please contact technical support.

System Update Procedure

Important: Please read the Release Notes for the system update that you're about to use. The release notes may include changes to this procedure.

The following procedure should be followed to perform System Updates on the Primary and Secondary servers when Automatic Failover is enabled:

Update the Primary Server

1. Access the Primary server using the Primary server's IP address.

Warning While using the Automatic Failover feature, the system will not allow you to start a System Update from the Master IP Address. Updates must be applied via the Primary and Secondary Server IP addresses.

2. If you are performing system updates on systems that are currently providing service, place the Primary server into standby mode, and wait until the Secondary server has assumed the master role.
3. Start the System Update on the Primary server (see *"Performing a System Update" on page 34*) and wait until the update has finished.
4. In the unlikely event that the update fails, stop the procedure and contact Technical Support. The Secondary server will continue to provide service until the issue is resolved on the Primary server.
5. If you placed the Primary server into standby mode, take the Primary server out of standby mode, and wait until the Primary server has assumed the master role.

Note: If the Primary server assumed the master role after the system update, this step can be skipped.

Update Secondary Server

6. Access the Secondary server using the Secondary server's IP address.
7. Start the System Update on the Secondary server (see *"Performing a System Update" on page 34*) and wait until the update has finished.

Verify Operation

8 Access the Primary server using the Primary server IP address.

9 On the **System Parameters** page, press **Check Server Status**.

10 In the **Automatic Failover Status** section, check that the following statements are true:

- "**MySQL Master Status, File**" is equal to "**MySQL Slave Status, Master_Log_File**"
- "**MySQL Master Status Position**" is equal to "**MySQL Slave Status, Read_Master_Log_Pos**"
- "**MySQL Slave Status, Slave_IO_Running**" is **Yes**
- "**MySQL Slave Status, Slave_SQL_Running**" is **Yes**

11 If any statements in the previous step are false, continue to the next step, otherwise the system update procedure is finished.

12 On the **Automatic Failover** page of the primary server, press **Sync DB** under **Operation Commands** and wait until it finishes.

13 On the **Automatic Failover** page of the secondary server, press **Sync DB** under **Operation Commands** and wait until it finishes.

14 On the **Automatic Failover** page of the primary server, press the **Refresh** button.

15 On the **System Parameters** page, press **Check Server Status**.

16 In the **Automatic Failover Status** section, check that the following statements are true:

- "**MySQL Master Status, File**" is equal to "**MySQL Slave Status, Master_Log_File**"
- "**MySQL Master Status Position**" is equal to "**MySQL Slave Status, Read_Master_Log_Pos**"
- "**MySQL Slave Status, Slave_IO_Running**" is **Yes**
- "**MySQL Slave Status, Slave_SQL_Running**" is **Yes**

17 If any statements in step #16 are false, repeat the procedure starting with step #12

18 If statements listed in step #16 are not true, even after repeating the steps, contact technical support.

Configuration Limitations

- Changes to Network Time (NTP) Server (see *"System Tools" on page 77*) should be applied to both Primary and Secondary servers.

Note: As a safety feature, the NTP server of the Primary server will be automatically applied to the Secondary server when the Secondary server becomes the Master server. To ensure they are both synchronized, however, it is recommended that changes be applied to both at the same time.

- Changes to Time Zone (see *"System Tools" on page 77*) must be applied to both Primary and Secondary servers.
- Changes made via *Custom Configuration* (see *"Custom Configuration" on page 46*) must be applied to both Primary and Secondary servers.

Failover Limitations

- Queued paging messages are not copied to the Secondary server. If the Secondary server becomes the Master server, the queued paging messages that were created on the Primary server will not be played.
- Ongoing check-in processes are not migrated between Primary and Secondary servers. If a check-in is started on the Primary server, and during the check-in process the Secondary server becomes the Master, the current check-in process is not migrated to the Secondary server.
- Audio Distributions are terminated and no attempt is made to resume Audio Distributions that were playing before the failover.
- Routines that were operating are terminated, and thus the state of various features may not be updated if a Routine was responsible for updating the state. For example:
  - Display messages (missing delete command)
  - I/O Contact state (missing open/close command)

  One way to work around this issue is to create Routines with reboot triggers that are responsible for setting features to a known state after a failover occurs, when applicable.
- Recordings and Voicemail made while the Secondary server is providing service are not copied to the Primary server when it resumes service.

Failover Routines and Triggers

The following table lists Routine triggers that can be used to execute Routines upon Automatic Failover events. The "Executed on node" column indicates on which node the Routine actions will execute.

Table 27. Failover Event Routine Triggers

Routine Trigger	Automatic Failover Event	Executed on node
af-primary-avail	The Secondary server is now able to contact the Primary server.	Secondary Primary (*rejoin)
af-primary-error	An error has occurred on the Primary server that requires attention.	[Not used in this release]
af-primary-master	The Primary server is now in master mode providing service.	Primary (Master)

Table 27. Failover Event Routine Triggers (continued)

af-primary-maint	The Primary server is now in maintenance mode. If the Primary server is currently the master, it will continue to provide service. While in maintenance mode, failover to the Secondary server will only occur if the Primary server is shutdown, reboots, or losses network connectivity. The server should not be left in maintenance mode unless instructed to do so by technical support.	Primary
af-primary-standby	The Primary server is now in standby mode and is not providing service.	Primary
af-primary-unavail	The Secondary server is unable to contact the Primary server. This may indicate a primary server failure or be due to a network connection issue on the primary or secondary server.	Secondary
af-secondary-avail	The Primary server is now able to contact the Secondary server.	Primary Secondary (*rejoin)
af-secondary-error	An error has occurred on the Secondary server that requires attention. Example: MySQL may be out of sync with Primary server.	[Not used in this release]
af-secondary-master	The Secondary server is now in master mode providing service.	Secondary (Master)
af-secondary-maint	The Secondary server is now in maintenance mode. If the Secondary server is currently the master, it will continue to provide service. If the Secondary server is currently the slave, it will not assume the master role if the Primary server fails. The server should not be left in maintenance mode unless instructed to do so by technical support.	Secondary
af-secondary-slave	The Secondary server is now in slave mode, is not providing service, and is waiting for failover.	Secondary

Table 27. Failover Event Routine Triggers (continued)

af-secondary-standby	The Secondary server is now in standby mode, is not providing service, and is unavailble for failover.	Secondary
af-secondary-unavail	The Primary server is unable to contact the Secondary server. This may indicate a secondary server failure or be due to a network connection issue on the primary or secondary server.	Primary

* "rejoin" indicates that the node has rejoined after being offline

Recommendations

- If a Routine includes an action to display a message to GA10PV display devices, consider specifying a unique identifier for that message. This will make it easier to delete the message when it is no longer relevant, such as when the failover state changes. For example, when the secondary server becomes the Master, a display message might be created for that event. Later, when the primary becomes Master again, a Routine started by the **af-primary-master** trigger will be able to delete the previously displayed message related to the secondary becoming the Master by using the message identifier specified by the secondary server when it created the message.
- Most triggers will *not* cause Routines to be executed on *both* servers. Keep that in mind when you're planning which actions to perform. For example, a Routine triggered by **af-secondary-slave** will execute actions only on the Slave server, so attempting to perform actions that affect Nyquist devices will not take affect because the Nyquist devices are only communicating with the Master server.
- Remember that Routines that execute on a non-Master node cannot display messages on, or otherwise communicate with, Nyquist devices.
- Every time a server becomes the Master, the **Reboot** trigger is also fired. This allows the **Reboot** trigger to be used to initialize the server environment. The **af-primary-master** and **af-secondary-master** triggers should be used for actions that should only occur when the failover mechanism has caused the switch.
- Whenever you use a Routine trigger related to a server being unavailable (e.g., **af-secondary-unavail**), keep in mind that the reason could be that the reporting server is no longer attached to a network and thus Routine actions that require network connectivity could fail.
    - Similarly, remember that the **af-secondary-unavail** and **af-primary-unavail** triggers may *both* fire, each on a different server, if both servers are still functioning but are unable to communicate for any reason. The Routines should be designed with this possibility in mind.

Tip: Whenever Routines are configured to be triggered by any of the Automatic Failover event triggers, we highly recommend that you thoroughly test everything to ensure that the expected actions are performed. It may be safest to test outside of normal operating hours.

Using CoS Configuration

Class of Service (CoS) configurations define the Nyquist features that stations are permitted and the Call-in Level that stations will use when calling an Admin Station. All stations in the Nyquist system must have an associated CoS to specify the feature privileges granted to that station. An unlimited number of CoS definitions can be configured and assigned. Once created, a CoS can be assigned to a station as a **Day CoS** and/or **Night CoS**. (See *"Editing Station Configuration Settings" on page 155*.)

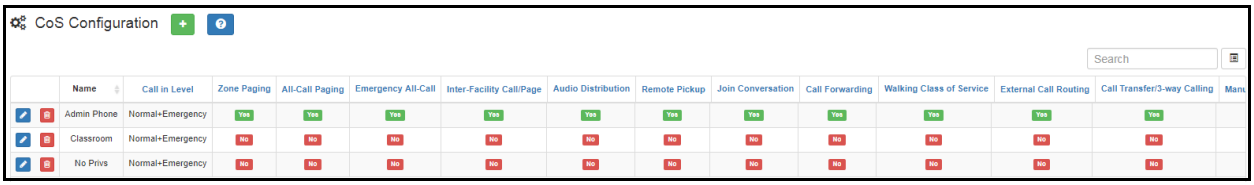


Figure 30. CoS Configuration Page

The following table describes the CoS parameters:

Table 28. CoS Configuration Page Parameters

Name	User-provided name for the CoS.
Call in Level	For call-switch station types, identifies the call as **Normal+Emergency**, **Urgent+Emergency**, or **Emergency-Only**. The system defaults to **Normal+Emergency**. • **Normal+Emergency**: Initiates a normal- or emergency-level call. Pressing the Analog/Digital Call Switch once triggers a normal-level call to the administrator. Pressing a Digital Call Switch three times, or pressing an Analog Call Switch four times, triggers an emergency-level call to the administrator. After placing a normal-level call with a Digital Call Switch, before it has been answered, the call can be elevated to an emergency-level call by pressing the call switch one more time. After placing a normal-level call with an Analog Call Switch, before it has been answered, the call can be elevated to an emergency-level call by pressing the call switch four times. • **Urgent+Emergency**: Initiates an urgent- or emergency-level call. Pressing the Analog/Digital Call Switch once triggers an urgent-level call to the administrator. Pressing a Digital Call Switch three times, or pressing an Analog Call Switch four times, triggers an emergency-level call to the administrator. After placing an urgent-level call with a Digital Call Switch, before it has been answered, the call can be elevated to an emergency-level call by pressing the call switch one more time. After placing an urgent-level call with an Analog Call Switch, before it has been answered, the call can be elevated to an emergency-level call by pressing the call switch four times. • **Emergency Only**: Initiates an emergency-level call by pressing the call switch one time. *Note:* The Callback Request Indicator feature cannot be used with stations that have Call in Level set to **Emergency Only**.

Table 28. CoS Configuration Page Parameters

Call in Level (cont'd)	*When an emergency call is placed to an Admin:* • Caller ID will include "Emergency". • Timeout to roll over to Admin Group for unanswered call to Admin is 15 seconds instead of 30 seconds. • Routines with **Emergency-Call** trigger will execute. • I/O controllers will be notified that Emergency Call was placed. • Station recording will be automatically enabled. • If **Emergency Link** is enabled, Emergency Link Station will be called. • If **Bump on Emergency** is enabled, existing Admin Call currently connected to Normal call will be bumped.
Zone Paging	Specifies if Zone Paging, Zone-based Announcements, and Record Announcements are enabled for the associated station.
All-Call Paging	Specifies if the associated station can simultaneously page or play announcements to all speakers within the facility.
Emergency All-Call	Specifies if the associated station can place a top priority all-call page.
Inter-Facility Call/Page	Specifies if the associated station can call or page another facility.
Audio Distribution	Specifies if the associated station can start and stop audio distributions.
Remote Pickup	Specifies if the associated station can remotely answer internal and incoming outside line calls by dialing `7*<extension-to-pickup>`.
Join Conversation	Enables the caller to interrupt or join an existing call. If a call is placed to a busy station, the system waits 10 seconds and then bumps or interrupts the call with the new caller, or the caller can dial an access string to join the existing call. This feature applies to administrative display phones only.
Call Forwarding	Permits a user to redirect or route incoming calls to another station.
Walking Class of Service	Enables the CoS settings of the station to be temporarily overridden with the CoS of a different station via the Walking CoS DTMF code (see *"Walking CoS" on page 583*).
External Call Routing	Enables the station to transfer a call to an outside line.
Call Transfer/3-way Calling	Allows the associated station user to contact a third-party while on a call, establish a three-way conversation and then drop off allowing the two other parties to remain connected.
Manually Activate Tone Signals	Enables a user to initiate tones outside of the schedule.
Call Any Station	Enables a station to call any station.
Manage Recordings	Allows the station user to manage recordings, such as emergency call recordings.

Table 28. CoS Configuration Page Parameters

Monitor Calls	Allows the station user to monitor active calls.
Monitor Locations	Allows the station user to monitor locations (not active calls).
Conference Admin	Allows the station user to join a conference as an administrator.
Conference User	Allows the station user to join a conference as a user.
Voicemail	Allows the station user to receive voicemail.
Record Calls	Allows the station user to begin recording an active call by pressing *3 any time during the call. This option is for use with admin phones when a Normal, Urgent, or Emergency intercom call is being made.
Activate Alarm Signals	Allows the station to activate alarms.
Disable Audio	Allows a station with contact closure to disable audio during a fire alarm or other emergency, allows an Admin web interface station to manually disable audio via the dashboard, and allows an Admin Phone to disable audio via DTMF code. *Note:* There also exists a related Role permission, Enable/Disable Audio Button, that determines whether or not users will see the Enable Audio and Disable Audio buttons on their Dashboard. The Role permission does not, however, prevent the user from using this feature through other mechanisms, such as via an Admin phone or the Routines API.
Enable Audio	Allows enabling of audio previously disabled during an emergency event, allows an Admin web interface station to manually enable audio via the dashboard, and allows an Admin Phone to enable audio via DTMF code. *Note:* See Disable Audio note regarding related Role permission.
Allow Callee Auto-answer	Allows call auto-answer by the callee for calls placed by this station.
Multi-Site Paging	Allows station to perform multi-facility paging and multi-facility announcements.
Inter-Facility Features	Allows the station to call extensions on remote facilities for voice mail and access to recorded calls and to stop audio.
Manage Output Contacts	Allows the station to activate or reset output contacts on I/O Controllers. For more information about managing output contacts, see *"Configuring I/O Controller Output Rules" on page 164*.
Execute Routines	Allows the station to execute routines via DTMF codes. For more information about managing routines, see *"Using Routines" on page 425*.
Call Speaker Stations	Allows the station to call speaker stations (i.e., stations that do not have the ability to hang up), such as VoIP speaker stations and amplifier stations.

Editing CoS Parameters for a Station

To edit CoS Parameters for a station:

1. On the navigation bar, select **CoS Configuration**.
2. For the station that you want to edit CoS settings, select the **Edit** icon.
3. Make the desired changes. You can use the **All On** button to turn all features on or the **All Off** button to turn all features off. For information about the settings, see *Table 28, "CoS Configuration Page Parameters," on page 101*.
4. After all changes are made, select **Save**.

Deleting CoS Parameters for a Station

To delete CoS Parameters for a station:

1. On the navigation bar, select **CoS Configuration**.
2. For the station that you want to delete CoS settings, select the **Delete** icon.
3. When prompted, select **Delete**.

Adding CoS Parameters for a Station

To add CoS Parameters for a station:

1. On the navigation bar, select **CoS Configuration**.
2. Select the **Add** icon.
3. Complete the parameters for the station. For information about the settings, see *Table 28, "CoS Configuration Page Parameters," on page 101*.
4. After all changes are made, select **Save**.

Managing SIP Trunks

A Session Initiation Protocol (SIP) trunk is an IP-based network connection between Nyquist and an Internet Telephony Service Provider (ITSP) (also known as a *VoIP telephone service provider*). It allows you to use Voice over IP (VoIP) telephony beyond the facility's firewall without the need for a Public Switched Telephone Network (PSTN), providing a configuration that is easier and less expensive to operate and maintain. SIP trunks can carry VoIP calls, video calls, Enhanced 911, and other real-time communication (RTC) services.

A SIP Tie-Trunk (or a SIP Tie-Line) functions similarly to a SIP trunk, but serves as an IP-based interconnection between Nyquist and a local (premises-based) or hosted IP-PBX. For information about using SIP Tie-Trunks with Nyquist, refer to *"Configuring SIP Tie-Trunks Between Nyquist and PBX Systems" on page 110*.

Before you can set SIP parameters in Nyquist, you must first set up the system's Direct Inward System Access (DISA) function by creating a station with the **Station Type** set to **DISA Line** (see *"Adding a Station" on page 185*). This station will be used to configure station-specific settings for the SIP trunk, such as its CoS.

Important: We strongly recommend that the technician performing the installation be knowledgeable about SIP implementation and testing. The firewall setting must allow port 5060 for non-secured SIP and/or 5061 for SIP TLS and ports 10000–20000 (or whichever port range is configured via **RTP Start Port** and **RTP End Port**, as specified in *Table 23, "Edit System Parameters Page," on page 69*) for the RTP traffic. Any other type of SIP connectivity could be available on a per-case basis.

How Nyquist Handles Incoming SIP Calls

Note: If a SIP trunk is configured but disabled, incoming calls from the SIP trunk are ignored.

When a SIP trunk is enabled and Nyquist receives an incoming call on that SIP trunk, Nyquist routes the call based on the SIP trunk's **Access** parameter. The **Access** parameter is set when adding or editing the SIP trunk configuration (see *"Editing a SIP Trunk Configuration" on page 123* and *"Adding SIP Trunk Configuration Parameters" on page 111*) and must match the ITSP switch configuration.

Based on the **Access** parameter setting, Nyquist does one of the following:

- Routes the call to a DISA function/station (see *"Route call to DISA" on page 106*)
- Routes the call to a Security DISA function/station (see *"Route call to Security DISA" on page 107*)
- Routes the call to a defined Day Admin or Night Admin (see *"Route call to a defined Day Admin or Night Admin" on page 107*)

Important: For incoming calls over SIP Trunks, authorization is based on *IP Address* or *Hostname*, as defined in the SIP Trunk's **Host** setting. As a result, the SIP trunk provider or PBX is not required to register with the Nyquist system to place calls into the Nyquist system. The Nyquist system accepts SIP INVITES from the SIP Trunk's configured **Host**.

Table 29. Incoming/Outgoing SIP calls by Access

Access	Route incoming calls to DISA	Route incoming calls to Security DISA	Route incoming calls to Day/Night Admin	Allow outgoing calls
911 Only				
DISA - Bi-directional - No password	Y			Y
DISA - Bi-directional - Password	Y			Y
DISA - Incoming only - No password	Y			
DISA - Incoming only - Password	Y			
Incoming Only			Y	
No Access				
Outgoing Only				Y
PBX Connection - Bi-directional, Allow DISA, No password	Y			Y
PBX Connection - Bi-directional, Allow DISA, Password	Y			Y
PBX Connection - Bi-directional, No DISA			Y	Y
PBX Connection - Bi-directional, Security DISA		Y		Y
PBX Connection - Incoming only, Allow DISA, No password	Y			
PBX Connection - Incoming only, Allow DISA, Password	Y			
PBX Connection - Incoming only, No DISA			Y	
PBX Connection - Incoming only, Security DISA		Y		
Security DISA - Bi-directional - Listen only		Y		Y
Security DISA - Incoming only - Listen only		Y		
Unrestricted			Y	Y

Route call to DISA

The following **Access** settings route the incoming SIP trunk call to the DISA functionality:

- DISA - Bi-directional - No password
- DISA - Bi-directional - Password

- DISA - Incoming only - No password
- DISA - Incoming only - Password
- PBX Connection - Incoming only, Allow DISA, No password
- PBX Connection - Incoming only, Allow DISA, Password

When the Nyquist system receives an incoming call, the caller will hear a dial tone. The caller can then dial any Nyquist extension or any Dual Tone Multi-Frequency (DTMF) code associated with a Nyquist feature. For example, after hearing the dial tone, the caller can dial #0911 to start an Emergency All-Call page. (See *"Nyquist DTMF Feature Dialing Codes" on page 574* for a list of DTMF codes.)

When incoming calls are routed to the DISA function, the SIP trunk **Extension** setting is used to map the SIP trunk to a station of type **DISA Line**; the station's CoS configuration is used to determine which Nyquist functions are available to the incoming DISA user. (See *"Adding CoS Parameters for a Station" on page 104*.) The **Extension** parameter is used as the caller ID when a DISA user dials a station extension.

Route call to Security DISA

The following **Access** settings route the incoming SIP trunk call to Security DISA functionality:

- Security DISA - Bi-directional - Listen only
- Security DISA - Incoming - Listen only
- PBX Connection - Bi-directional, Security DISA
- PBX Connection - Incoming only, Security DISA

The caller must enter a valid extension to be monitored and can only listen to calls or station locations.

Route call to a defined Day Admin or Night Admin

The following **Access** settings route the incoming SIP trunk call to the defined Day or Night Admin:

- Unrestricted
- Incoming Only

If the Day or Night Admin does not answer the incoming call, the call is routed, or rolled over, to the Admin Group. (See *"Using Admin Groups" on page 258*.)

If the call is not answered during night hours, and the **Night Ring** option is enabled, the call is routed using the Night Ring functionality. (See *"Configuring Night Call Options" on page 22*.)

How Nyquist Handles Outgoing SIP Calls

Important: Nyquist users can initiate outside calls by dialing a number that starts with the outside call prefix: 98.

Outside calls are only sent to SIP Trunks that have one of the following **Access** settings:

- DISA - Bi-directional - No Password
- DISA - Bi-directional - Password
- Security DISA - Bi-directional - Listen only
- Unrestricted
- Outgoing Only
- PBX Connection - Bi-directional, No DISA
- PBX Connection - Bi-directional, Allow DISA, No password
- PBX Connection - Bi-directional, Allow DISA, Password
- PBX Connection - Bi-directional, Security DISA

Important: Use the PBX Connection options only if the PBX accepts 7-digit and 10-digit domestic and 12-digit international PSTN telephone numbers and can initiate outbound calls to specified telephone numbers.

When outside calls are placed, the outbound caller ID is set to the Direct Inward Dial (DID) defined for the SIP Trunk. (See *"Editing a SIP Trunk Configuration" on page 123* or *"Adding SIP Trunk Configuration Parameters" on page 111*.)

When **Access** is set to **911 Only**, only outgoing 911 calls may be routed on the associated SIP trunk. The **DID** parameter is not used for outgoing 911 calls; it is expected that the SIP trunk provider has mapped the Billing Telephone Number (BTN) to E911 service.

All outgoing calls are routed through the SIP trunk provider using the following SIP trunk configuration parameters:

- Host IP Address
- Username
- Password

If the SIP trunk provider expects all called numbers to be prefixed with a specific code, the **Dial Prefix** setting can be used to satisfy the requirement.

If the SIP trunk provider expects all called 7-digit numbers to be prefixed with a specific local area code, the **Local Area Code** setting can be used to satisfy the requirement. (See *"Adding SIP Trunk Configuration Parameters" on page 111*.)

Dialing PBX Extensions via Nyquist SIP Trunks

If the Nyquist system has one configured SIP trunk that is attached to a PBX system, Nyquist users can dial PBX extensions via the Nyquist SIP trunk. The SIP trunks can be setup using DAHDI hardware, Grandstream HT813 FXO ports, or configured SIP Trunks.

Calls initiated via the Nyquist system that start with *** will be routed through an available Nyquist SIP trunk, presumably to an attached PBX system.

For example, dialing ***123 will cause the Nyquist system to place a call to 123 using an available SIP trunk (which should be attached to a PBX system).

Any combination of characters can follow the *** prefix. This allows complete flexibility to match the dial plan syntax of the attached PBX system.

For example, if the PBX is programmed to accept calls to extensions when prefixed with #, the Nyquist user can dial ***#123 to place a call to extension 123.

Notes

- When a Nyquist station uses the *** prefix to dial a PBX extension via a Nyquist SIP trunk, the Nyquist station must have **Outside Access** enabled. If the calling station's **Outside Access** parameter is set to **No Access**, the calling station will hear "access denied" and the call will not be placed. Any choice other than **No Access** will allow the station to place calls using the *** prefix; but if the **Restricted Day/Night** options are used, they will also be in affect to control access to day or night only.
- If the PBX extension length matches the Nyquist Dialing Length, you can add Admin PBX Extension stations to the Nyquist system to allow Nyquist users to call the PBX extension via the Admin PBX Extension without the need to use the *** prefix. For example, if your PBX has extensions 401, 402, and 403, and the Nyquist Dialing Length is three (3), you can add three Nyquist Admin PBX Extension stations using 401, 402, and 403 as the extensions. After that, Nyquist users can simply dial 401 to call PBX extension 401, 402 to call PBX extension 402, and 403 to call PBX extension 403.
- The SIP Trunk DID field can be set to whatever value is required by the PBX system that will be receiving calls from the Nyquist system. For example, if the PBX system wants to see the Nyquist incoming call as extension 123, the SIP Trunk DID can be set to 123 to make sure that—from the PBX system's perspective—the incoming call is coming from the caller id equal to 123.
- To enable this feature, the SIP Trunk Access setting should use one of the available choices that start with "PBX Connection".

Limitations

- Only one PBX system connection via a single SIP trunk is supported. Multiple PBX system connections is not supported because Nyquist does not yet have a method to allow users to select a specific PBX system for calls to PBX systems using the *** prefix.
- Nyquist does NOT support the use of '***' to dial PBX extensions via SIP trunks if the Nyquist system is also being used to dial PSTN DIDs via a SIP trunk attached to the PSTN (e.g. using PSTN SIP Trunk provider, or FXO attached to PSTN, instead of being attached to a PBX system).

On the other hand, if a PBX system is programmed to route incoming PSTN DID extensions through the PSTN, and Nyquist is attached to a single such PBX system, then Nyquist outbound calls via the PBX system are also supported.

Configuring SIP Tie-Trunks Between Nyquist and PBX Systems

If you want all incoming calls from the PBX to always use DISA to prompt the caller for Nyquist dial codes, then use one of the **Access** options that starts with **DISA** (e.g., **DISA - Incoming only - No password**).

If you want all incoming calls from the PBX to directly pass in dial codes that have already been collected from the user by the PBX or created by the PBX, then choose one of the **Access** options that starts with **PBX Connection** (e.g., **PBX Connection - Incoming only, Allow DISA, No password**).

When any of the following **Access** options are configured for the SIP Tie-Trunk, the Nyquist server expects that dialing digits will be provided by the PBX system (the dialing digits should be included in the SIP INVITE from the PBX), and Nyquist will immediately initiate a Nyquist call based on the digits provided:

- PBX Connection - Incoming only, No DISA
- PBX Connection - Incoming only, Allow DISA, No password
- PBX Connection - Incoming only, Allow DISA, Password
- PBX Connection - Bi-directional, No DISA
- PBX Connection - Bi-directional, Allow DISA, No password
- PBX Connection - Bi-directional, Allow DISA, Password

If the PBX Connection option includes **Allow DISA**, the PBX may start the DISA function by sending dialing code 950. The DISA function will also be started if the PBX does not pass any dialing digits in the SIP INVITE.

If **PBX Connection - Incoming only, No DISA** is used, the SIP Trunk must still have a DISA station type linked to the SIP trunk extension to provide the Nyquist CoS settings to be used for incoming calls, but when incoming connections are made from the PBX, the Nyquist system will ignore dialing code 950. The DISA function cannot be requested if the **No DISA** option is used.

The dialing digits provided by the PBX can be any of the DTMF codes supported by the Nyquist system. Access to various Nyquist features is granted based on the Nyquist CoS settings of the DISA station extension defined in the SIP Trunk.

If the PBX is not able to pass through the hashtag (#) symbol in the dialing digits, alternative dialing codes may be used to replace Nyquist extensions that start with #. For details, see *"Alternate Dialing Codes" on page 586*.

When the following **Access** options are configured for the SIP Tie-Trunk, upon connection from the PBX system (via SIP INVITE), the Nyquist system automatically activates the Security DISA function:

- PBX Connection - Incoming only, security DISA

- PBX Connection - Bi-directional, Security DISA

The caller must enter an access PIN, followed by the extension number of the station to monitor.

Another available option for connecting Nyquist with PBX Systems is the use of the Grandstream HT813 FXO Port. Please see *"Using a Grandstream HT813 Adapter" on page 190* for details.

Adding SIP Trunk Configuration Parameters

Before adding a SIP trunk, the following parameters must be configured or known:

- Extension for the Nyquist DISA line station associated with the specified SIP trunk; the station must have its **Station Type** specified as **DISA Line** (see *"Viewing Station Configuration Settings" on page 142*).
- Dial prefix and format used to connect to an outside line
- Local area code
- Username and password for the DISA line
- DID phone number associated with the DISA line
- Allowed codecs

Note: If available, the OPUS codec will be treated as the preferred codec by all Nyquist and standalone appliances.

- Admin Group set up for the SIP extension (see *"Using Admin Groups" on page 258*)
- Whether or not the ITSP supports SIP TLS and/or SRTP.

Important: If SIP is to be secured and the ITSP is using an unrecognized CA (e.g., a self-signed CA), a PEM file containing the CA will need to be installed.

Before you can define a SIP trunk, you must first define the system's Direct Inward System Access (DISA) function by creating a station with the **Station Type** set to **DISA Line** (see *"Adding a Station" on page 185*). This station will be used to configure station-specific settings for the SIP trunk, such as its CoS.

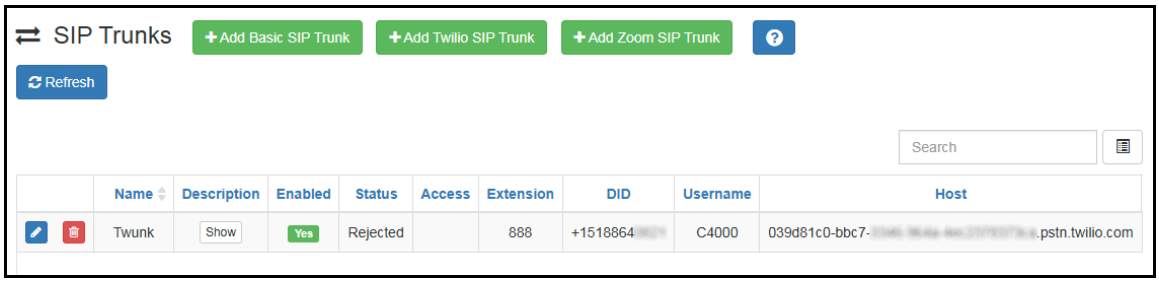


Figure 31. SIP Trunks page

The C4000 supports several different SIP trunk types:

- Generic (see *"Generic SIP Trunk" on page 112*)
- HT813 (see *"Basic HT813 Setup" on page 190*)
- Twilio (see *"Twilio SIP Trunk" on page 115*)
- Zoom (see *"Zoom SIP Trunk" on page 116*)
- RingCentral (see *"RingCentral SIP Trunk" on page 118*)

Tip: For an overview of SIP trunks, see *"Managing SIP Trunks" on page 104*.

Generic SIP Trunk

To add a Basic SIP trunk:

1. On the navigation bar, select **SIP Trunks**.
2. On the *SIP Trunks* page, select the **Create New Trunk > Generic SIP Trunk** icon.
3. On the *Add SIP Trunk* page, complete the parameters (see *Table 30, "Add/Edit/View SIP Trunk Page Parameters," on page 112*).
4. Select **Save.**

Table 30. Add/Edit/View SIP Trunk Page Parameters

Name	Enter the name for the SIP trunk. The name cannot contain spaces or slashes (/) and cannot exceed 16 characters.
Extension	Select the extension of the **DISA Line** station to be associated with the SIP trunk.
Dial Prefix	Enter the dial prefix required by the ITSP to complete an outbound call over the SIP trunk. For example, +1, :9, 9+1, etc.
Local Area Code	Enter the local area code if the ITSP requires 7-digit telephone numbers be prefixed with the area code. Otherwise, this field is left blank.
Enabled	Specify if the SIP trunk is enabled. *Tip:* The SIP trunk should be fully configured before it is enabled to avoid erratic system behavior.
Status **(view only)**	Provides the registration status of the SIP trunk. If the credentials are used by the SIP endpoint, the **Status** might be **Registered**. If the SIP endpoint does not use credentials, the **Status** might be **Rejected** but this will not impeded a successful SIP connection.

Table 30. Add/Edit/View SIP Trunk Page Parameters (continued)

Type	Identifies the SIP trunk's type. Valid values are: • Generic • HT813 • Twilio • Zoom • RingCentral
Call Recording (view only)	Indicates if incoming and outgoing calls are being recorded.
Access	Select the outside access permissions for the SIP trunk. The available options, which may be restricted to those supported by the trunk type being added, are listed in *Table 29, "Incoming/Outgoing SIP calls by Access," on page 106*. For details, see *"How Nyquist Handles Incoming SIP Calls" on page 105*, *"How Nyquist Handles Outgoing SIP Calls" on page 108*, and *"Configuring SIP Tie-Trunks Between Nyquist and PBX Systems" on page 110*.
Username	Enter the user name that is required to access the SIP trunk. *Note:* This field is required. If the SIP trunk does not provide an authentication credential (e.g., it authenticates using the C4000's public IP address), specify any value.
Password	Enter the password that is required to access the SIP trunk. The password is provided by the SIP trunk provider or hosted VoIP provider.
Password Confirmed	Re-enter the SIP trunk password.
Host	Enter the host name or IP address for the ITSP. *Note:* This is often referred to as a *termination URI*.
DID	Enter the telephone number that the SIP trunk or hosted VoIP provider has assigned to the SIP trunk (no spaces or dashes). This number will be displayed by caller ID.
Outbound Proxy	Specify the outbound proxy address specified by the SIP trunk provider.
Authorization ID	Specify the authorization ID required by the SIP trunk providers.
Day Admin	Select the Admin Station to call during daytime hours.
Night Admin	Select the Admin Station to call during nighttime hours.
Admin Group	Select the Admin Group to call if the day or night Admin Stations do not answer the call.
Call Recording	Indicates if incoming and outgoing calls are to be recorded.

Table 30. Add/Edit/View SIP Trunk Page Parameters (continued)

Allow Outbound Intercom Calls

Indicates if call-switch–based stations are allowed to place calls to PBX-based Admin extensions via the SIP Trunk using Day/Night Admin-PBX-Extension.

See *"Routing Intercom Calls to PBX Extensions via SIP Trunk" on page 207*) for further details.

Enable SIP TLS

Enables support for SIP over TLS 1.2 on the SIP trunk. This uses certificates to secure SIP signaling packets (i.e., call setup, modification, and termination) between the endpoints and servers to provide privacy, integrity, and authentication to SIP communications.

This is disabled by default, but we highly recommend enabling it.

See *"VoIP Security" on page 18* for further details.

Enable SRTP

Enables support for Secure Real-Time Transport Protocol (SRTP) on the trunk. This adds encryption, message authentication, integrity, and replay protection for RTP voice call audio streams.

This is disabled by default, but we highly recommend enabling it.

See *"VoIP Security" on page 18* for further details.

Device Certificate (optional)

Select a previously uploaded X.509 device certificate PEM file that will identify this device to the SIP trunk to secure SIP TLS and/or SRTP connections or upload a new file using the **Device Certificate File Upload** control.

Important: If a device certificate is not provided, the built-in Bogen CA-signed certificate will be used (see *"Bogen Digital Certification Authority" on page 588*). This setting only needs to be specified if the SIP trunk will not accept the Bogen CA-signed certificate.

Note: This field appears only if **Enable SIP TLS** or **Enable SRTP** is enabled.

Device Certificate File Upload

Select and upload a PEM file containing the **Device Certificate**.

Important: The uploaded certificate may not be available for use until after the **Save** button has been selected.

Note: This parameter only appears if **Enable SIP TLS** or **Enable SRTP** is enabled.

Allow

Specify a list of media codecs that are allowed.

Tip: The PSTN standard codec, G.711, can be specified via either the *alaw* or *ulaw* companding algorithm.

Table 30. Add/Edit/View SIP Trunk Page Parameters (continued)

Client URI	Specify the optional URI with which to identify the C4000 in the SIP messages' *From* headers when communicating with a cloud-based trunk. This is used to identify this client to trunk providers that only allow clients from a pre-specified address to register. This setting is not typically required, but when it is, it typically follows the following format: sip:<number>@<user.domain.com> *Note:* This setting is sometimes referred to as an *origination URI*.
Description	Provide user-provided description for the SIP trunk.
Custom Settings	Provide custom setting configurations that are provided by Technical Support (see *"SIP Trunk Custom Configuration Settings" on page 120*).

Twilio SIP Trunk

To add a Twilio SIP trunk:

Note: Before a Twilio SIP trunk can be added to the C4000, a Twilio account must be created at https://www.twilio.com and an Elastic SIP Trunk must be created.

---

1. On the navigation bar, select **SIP Trunks**.
2. On the *SIP Trunks* page, select the **Create New Trunk** > **Twilio SIP Trunk** button.
3. On the *Add Twilio SIP Trunk* page, specify the **API Key SID** and **API Key Secret** in the **Twilio API Settings** section.

Table 31. Twilio Settings

Twilio API Settings	The C4000 uses Twilio API keys to access the Twilio REST API, allowing it to retrieve a list of available DID numbers (upon selecting **Fetch Twilio Account DID Numbers**), and to create and configure a Twilio trunk (upon selecting **Save**). *Note:* The API Key is only used to create and initialize the Twilio SIP trunk. Once created, the API Key is no longer needed or used by the C4000.
API Key SID	Provide a Twilio API key. Twilio API keys can (as of publication time) be created via Twilio's *API keys & tokens* page, accessible from the *Account Settings* page. Any type of Twilio key can work, including the Account SID or Auth Token. For more information, see https://www.twilio.com/docs/iam/api-keys.

Table 31. Twilio Settings

API Key Secret	The secret for the specified Twilio API key.
Fetch Twilio Account DID Numbers	Uses the specified Twilio API key to retrieve a list of phone numbers, both reserved and available for purchase, that can be assigned to this trunk.

The C4000 uses the keys to access the Twilio REST API, which is used to retrieve Twilio trunk DID values. As of publication, Twilio API keys can be created via Twilio's *API keys & tokens* page, accessible via the *Account management* menu. Any type of Twilio key can work, including the Account SID or Auth Token.

4. Select the **Fetch Twilio Account DID Numbers** button. This will use the specified keys to retrieve DID numbers that can be used for the new trunk.
5. Select a telephone number from the **DID** field. Numbers listed under **Reserved Twilio Phone Numbers** have already been reserved by your Twilio account. Those listed under **New Available Twilio Phone Numbers** are available for purchase.
6. Specify the **Name**, **Extension**, **Local Area Code**, **Enabled**, and **Outside Access**.
7. Complete the parameters (see *Table 30, "Add/Edit/View SIP Trunk Page Parameters," on page 112*).
8. Select **Save.**
9. Configure Twilio's termination credentials via the Twilio Dashboard to specify how the C4000 will authenticate with the newly created Twilio trunk. The credentials can consist of an IP access control list, a credentials list, or both.
   - If you choose to authenticate using an IP access control list, specify the public IP address of this C4000. This will need to be updated if the C4000's IP address is ever changed.
   - If you choose to authenticate using credentials, configure the same credentials in the newly created SIP trunk (see **Username** and **Password** in *Table 30, "Add/Edit/View SIP Trunk Page Parameters," on page 112*).

Zoom SIP Trunk

The C4000 can access Zoom as a SIP trunk.

Caution	A Zoom SIP trunk will allow users to receive incoming calls, but will not allow them to place outgoing calls.

Before defining a phone in Zoom, you must create a Zoom account (https://zoom.us) and place a Technical Support request with Zoom asking them to enable generic device provisioning of unsupported phone models for your Zoom account. This will allow the account to add a generic device (i.e., the C4000) as a phone. Include the brand (Bogen), model (NQ-SYSCTRL), and quantity (one) of the device to be used.

We recommend defining a Zoom phone and extension that is dedicated to the system controller, then assign separate extensions to individual users. This prevents confusion that would be caused be assigning a user's extension to the system controller.

Tip: ~~To place a call to a Zoom extension number, dial: ***<Zoom extension>.~~

Zoom generic device request questions

A request must be placed with Zoom Technical Support to enable generic device provisioning on unsupported phone models. The information requested by Zoom may vary. The following are the answers to questions that have been asked by Zoom about the device to be used (i.e., the Nyquist C4000):

1. What is the device and model to be used?

   Bogen NQ-SYSCTRL
2. How many units are you looking to configure manually?

   One (typically)
3. Does it support SIP registration?

   Yes
4. Does it support the use of a wildcard SSL certificate?

   Yes
5. Does it support TLS 1.2/SRTP security protocol?

   Yes
6. What are its TLS 1.2/AES-256 cipher sets?
   - ECDHE-RSA-AES256-GCM-SHA384
   - AES256-SHA256
   - DHE-RSA-AES256-GCM-SHA384
   - DHE-RSA-AES256-SHA256
   - AES256-GCM-SHA384
   - DHE-RSA-AES128-GCM-SHA256
   - DHE-RSA-AES128-SHA256
   - AES128-GCM-SHA256
   - ECDHE-ECDSA-AES256-GCM-SHA384
   - DHE-RSA-AES256-GCM-SHA384

Important: Be aware that requesting provisioning of unsupported devices may entail returning a signed waiver to Zoom Technical Support.

To add a Zoom SIP trunk:

1. Define a phone via Zoom.

   Before a Zoom SIP trunk can be added to the C4000, a Zoom phone number must be created. For details, see the Zoom support article, *How to add generic devices*.

   When provisioning the phone device within Zoom, specify the MAC address of the C4000's external network port, which is displayed on the chassis of the System Controller. (*Hint*: It begins with `00:30:18`.) The MAC address can be found (among other techniques) via:
   - the C4000's *Check Server Status* (see *"Check Server Status" on page 44*),
   - your DHCP server's client list, or
   - the PowerShell command:

     ```
     Get-NetNeighbor -LinkLayerAddress 00-30-18-*
     ```

The **Device Type** must be specified as **Other**, which is only available after Zoom Technical Support has activated Enable Generic Device Model.

Make a note of the phone number to which the device is assigned. This will be used subsequently to specify the DID number in the Bogen SIP Trunk definition.

2 Select the **Actions** button and select **Provision**. This will display the SIP provisioning information needed in subsequent steps.

3 On the C4000 navigation bar, select **SIP Trunks**.

4 On the *SIP Trunks* page, select the **Create New Trunk > Zoom SIP Trunk** button.

5 Specify the SIP trunk parameters using the Zoom SIP account values displayed by the aforementioned Zoom provisioning page, mapping the fields according to *Table 32, "SIP Trunk to Zoom SIP parameters," on page 118*. Specify the DID using the phone number (digits only) assigned to the Zoom phone (i.e., see the **Assigned to** field of the Zoom device).

Table 32. SIP Trunk to Zoom SIP parameters

SIP Trunk parameters	Zoom SIP account Provisioning parameters
Access	Incoming only access only
Username	Username
Password	Password
Host	SIP Domain
Outbound Proxy	Outbound Proxy
Authorization ID	Authorization ID
DID	Zoom phone number (no spaces or dashes, prefix with + and the country code)

6 Complete the parameters (see *Table 30, "Add/Edit/View SIP Trunk Page Parameters," on page 112*).

7 Select **Save**.

8 If the SIP trunk status does not change to **Registered**, use Zoom's Resync action, available in the Zoom phone profile via the Actions dropdown button.

RingCentral SIP Trunk

RingCentral is a Nyquist-compatible cloud telephony provider. With a RingCentral trunk, stations on the Nyquist network can dial out to external phone numbers or to RingCentral extensions. Users can also dial into the Nyquist network from a RingCentral extension or from any device on the PSTN (e.g., a cell phone).

Caution Instructions specific to the RingCentral website are beyond Bogen's control and may change at any time.

To add a RingCentral SIP trunk:

1 Before configuring the C4000 SIP trunk, prepare your RingCentral account for manual SIP settings (see the RingCentral article, *Getting the SIP settings for manual provisioning*).

   a) Create a user phone in RingCentral. When asked to select a device, select **Existing Phone** from the **Other Phones** section. Complete the creation of the user phone.

   b) Select **Phone System**, then **Phones & Devices** > **User Phones**, then select the configured **Device** (e.g., **Existing Phone**). Select **Change Phone** and change the phone type to **Bring Your Own Device**. When asked for the device model, select **Set up manually using SIP**.

   c) If the C4000 will be configured to use TLS (see **Enable SIP TLS** and **Enable SRTP** in *Table 30, "Add/Edit/View SIP Trunk Page Parameters," on page 112*), select **Yes** to indicate the device will support TLS 1.2. If not, select **No**.

   d) The SIP provisioning information will be displayed. You will need the displayed values for the subsequent steps.

Tip: Press the **Copy** button to copy all this information to the clipboard and paste it elsewhere for reference..

Table 33. SIP Trunk to RingCentral SIP parameters

SIP Trunk parameters	RingCentral Provisioning parameters
Dial Prefix	<blank>
Local Area Code	<blank>
Username	User Name
Password and Password Confirmed	Password
Host	SIP Domain (without the port)
DID	RingCentral phone number (no spaces or dashes, prefixed with + and the country code)
Outbound Proxy	<Outbound Proxy>:<Outbound Proxy Port> *Note:* You may need to select an outbound proxy.
Authorization ID	Authorization ID
Client URI	sip.ringcentral.com *Note:* This is auto-populated.
Custom Settings	`:ENDPOINT:from_user='<DID>':ENDPOINT:` *Note:* This is auto-populated.

   e) Select **Done** when ready.

   f) Select the **Set Up and Assign** button, then complete the **Assign unassigned phone** wizard.

2 On the C4000 navigation bar, select **SIP Trunks**.

3 On the *SIP Trunks* page, select the **Add RingCentral SIP Trunk** button.

4 On the *Add RingCentral SIP Trunk* page, specify the **Name**, **Extension**, and **Dial Prefix**.

5 Set **Enabled** to Yes.

6 **Access** should be defined as **DISA - Bi-directional - No Password** or **DISA - Bi-directional - Password**.

7 Specify the settings specified in *Table 33, "SIP Trunk to RingCentral SIP parameters," on page 119*.

8 Set **Enable SIP TLS** and **Enable SRTP** to Yes.

If you will not be using TLS and SRTP to connect to this trunk, set these to **No** and make sure this was indicated when provisioning the RingCentral line.

Note: If **Enable SIP TLS** and **Enable SRTP** are disabled, they will be automatically set to Yes after creation.

---

9 For **Allow**, select opus and g722.

10 Select **Save**.

If everything is configured correctly, the status of the SIP Trunk will soon be reported as **Registered**.

Tip: To place a call to a RingCentral PBX number, dial: ***<RingCentral extension>.

SIP Trunk Custom Configuration Settings

The **Custom Settings** parameter can be used if additional parameters are needed during SIP trunk configuration to satisfy SIP trunk provider requirements. Bogen Technical Support will provide any necessary custom settings. In most cases, **Custom Settings** are not required.

Custom Settings can be entered when adding or editing SIP Trunk parameters (see *"Adding SIP Trunk Configuration Parameters" on page 111* or *"Editing a SIP Trunk Configuration" on page 123*) using the following format:

```
:<TABLE-NAME>:<variable>=<value>:<TABLE-NAME>:
```

where <TABLE-NAME> is ENDPOINT, AOR, AUTH, or SIPTRUNK; <variable> is a valid variable from one of the pjsip tables (i.e., ps_endpoints, ps_aors, ps_auths) or the sip_trunk table; and <value> is a valid value for the specified variable.

For example, the following custom settings are required to authenticate with some external SIP trunk providers:

```
:AUTH:realm='':AUTH:
:SIPTRUNK:context='777':SIPTRUNK
```

Contact Bogen Technical Support for information regarding custom settings for your specific IP-PBX type and configuration.

Registering as a Third-Party SIP Endpoint

You can configure a Nyquist SIP trunk to register with a third-party SIP endpoint with an IP-PBX. This will allow users to dial an IP-PBX–defined extension to initiate Nyquist features, such as paging.

The steps to register the Nyquist SIP trunk as a third-party SIP endpoint for an IP-PBX are:

1 **Define a Third-Party SIP Phone/Endpoint on your IP-PBX system.**

On the IP-PBX system, set up a third-party SIP phone/endpoint as you would for a standard single-line basic SIP IP phone with a username and password to use for authentication. Typically, the username would be the extension number. The Nyquist system will attempt to register with your IP-PBX system as a SIP endpoint extension using the provided username (extension) and password pair. Your IP-PBX users will dial the provided IP-PBX extension to access the Nyquist system.

2 **Define a DISA station on Nyquist system.**

On the Nyquist System, create a station with a **Station Type** of **DISA Line**. This station's extension will define the feature CoS permissions to be used when the IP-PBX calls into the Nyquist system.

Note: The station extension used for the DISA Line must be different than the extension being used by your IP-PBX.

---

3 **Define a SIP Trunk on Nyquist system.** Configure a Nyquist SIP Trunk using the username (PBX extension) and password that was defined on your IP-PBX in step 1.

For example, suppose the IP-PBX has defined extension 511 as the SIP endpoint with password `testpassword`. The Nyquist SIP trunk must use **511** in the **Name**, **Username**, and **DID** parameters on the *Add SIP Trunk* page. Nyquist station extension 500 is defined as a **DISA** station.

When an IP-PBX user calls 511, the Nyquist system will see an incoming call to extension 511. Nyquist converts to the DISA station extension 500 (to provide CoS definitions for 511 and Caller-ID to the Nyquist system). DISA will be started, allowing the IP-PBX caller to initiate a feature on the Nyquist system. When DISA starts, the IP-PBX user hears a dial tone. The IP-PBX user can then enter DTMF/dial-pad based feature commands to start paging and other Nyquist features.

Table 34. Third-Party SIP Endpoint Example Configuration

Name	511 (Username/extension provided by IP-PBX)
Extension	500 (DISA station extension defined on the Nyquist system. On Nyquist, it will look like the call came from this extension.))
Dial Prefix	NOT USED
Local Area Code	NOT USED
Enabled	Yes

Table 34. Third-Party SIP Endpoint Example Configuration (continued)

Access	• PBX Connection - Incoming only, Allow DISA, No password • PBX Connection - Incoming only, Allow DISA, Password
Username	511 (Username/extension provided by IP-PBX)
Password	testpassword (Password provided by IP-PBX)
Host	10.10.5.100 (The IP-PBX's IP Address or fully qualified domain name, for example, myhost.mycompany.com)
DID	511 (Username/extension provided by IP-PBX)
Day Admin	NOT USED (Pick any valid Nyquist Admin extension)
Night Admin	NOT USED (Pick any valid Nyquist Admin extension)
Admin Group	NOT USED (Pick any valid Nyquist Admin extension)
Allow	g722 (or ulaw or other codec if needed)
Client URI	NOT USED *Note:* This is the C4000's fully qualified domain name (e.g., system-controller.mycompany.com). It can usually be left blank.

Custom Settings	`:AUTH:realm='':AUTH:`
	`:SIPTRUNK:context='511':SIPTRUNK:`
	Note: If realm='' does not work, try realm='<server_ip_address>'or realm='<server_hostname>'

Viewing SIP Trunks

To view available SIP trunks for your facility:

On the navigation bar, select **SIP Trunks**.

For details, see *Table 30, "Add/Edit/View SIP Trunk Page Parameters," on page 112*.

Editing a SIP Trunk Configuration

You cannot edit the name given to a SIP trunk, but you can edit other fields, such as the **Dial Prefix** and **Local Area Code**.

Figure 32. Edit SIP Trunks Page

To edit a SIP Trunk's configuration:

1. On the navigation bar, select **SIP Trunks**.
2. On the *SIP Trunks* page, select the **Edit** icon for the SIP trunk that you want to edit.
3. On the *Edit SIP Trunk* page, make the desired changes. (See *Table 30, "Add/Edit/View SIP Trunk Page Parameters," on page 112*.)
4. Select **Save**.

Deleting a SIP Trunk Configuration

If you are no longer paying for or using a SIP trunk service via an external provider, you may want to delete a previously added SIP trunk.

To delete a SIP trunk:

1. On the navigation bar, select **SIP Trunks**.
2. On the *SIP Trunks* page, select the **Delete** icon next to the SIP trunk that you want to delete.
3. Select **Delete**.

Viewing Outside Line Status

The status of every outside line in a facility can be quickly determined by using the Outside Lines feature.

To view the outside lines:

On the navigation bar, select **Outside Lines**.

Table 35. Outside Lines Page Parameters

Name	Identifies the system port name for the outside line.
Description	Identifies the user-provided description of the outside line's purpose.
Enabled	Specifies if the outside line is enabled.
Status	Provides the status of the line.
Port Type	Identifies system port type used for this line.
Access	Identifies level of access allowed on this outside line. The available options are shown in *Table 29, "Incoming/Outgoing SIP calls by Access," on page 106*.
Dial Prefix	Identifies the digit or digits that must be dialed to obtain an outside line.
Extension	Identifies the station extension that is associated with the outside line (DISA station mapping and caller ID for incoming DISA).
DID	Identifies the DID telephone number associated with the outside line.
Day Admin	Identifies the Admin Station to call during daytime hours.
Night Admin	Identifies the Admin Station to call during nighttime hours.
Admin Group	Identifies the Admin Group to call if the Day or Night Admin Stations do not answer the call.

Editing Outside Lines

You can edit information or disable an outside line through the *Edit Outside Line* page.

To edit an outside line:

1. On the navigation bar, select **Outside Lines**.
2. Select the **Edit** icon next to the outside line name.
3. Make desired edits.
4. Select **Save**.

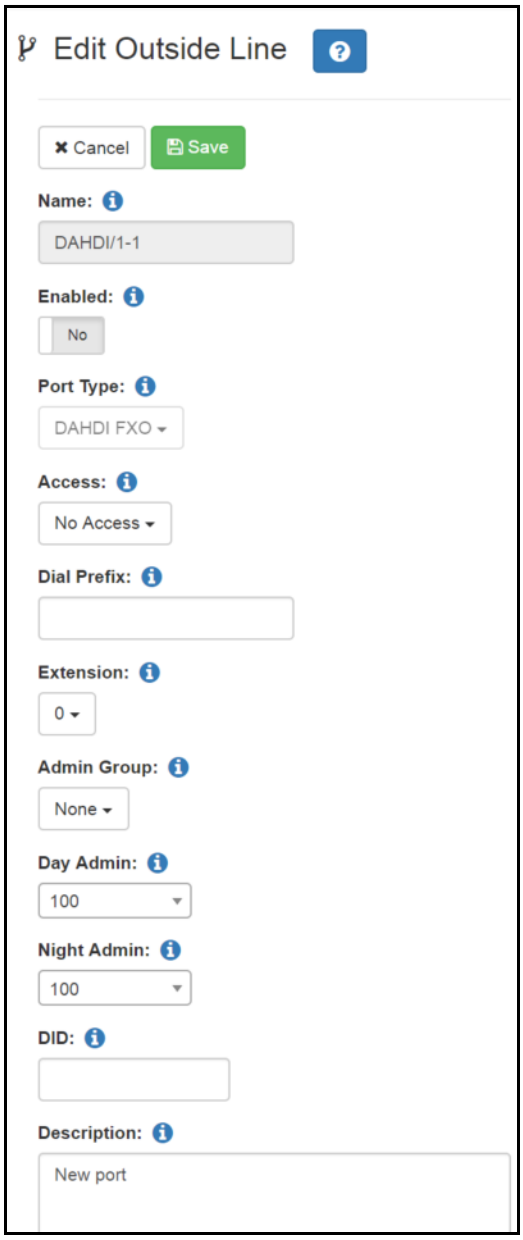


Figure 33. Edit Outside Line Page

Table 36. Edit Outside Line Page Parameters

Name	Identifies the system port name for the outside line. This parameter cannot be edited.
Enabled	Specifies if the outside line is enabled.
Port Type	Identifies system port type used for this line. This parameter cannot be edited.
Access	Identifies level of access allowed on this outside line. The available options are shown in *Table 29, "Incoming/Outgoing SIP calls by Access," on page 106*.
Dial Prefix	Identifies the digit or digits that must be dialed to obtain an outside line.
Extension	Identifies the station extension that is associated with the outside line (DISA station mapping and caller ID for incoming DISA).
Admin Group	Identifies the Admin Group to call if the Day or Night Admin Stations do not answer the call.
Day Admin	Identifies the Admin Station to call during daytime hours.
Night Admin	Identifies the Admin Station to call during nighttime hours.
DID	Identifies the DID telephone number associated with the outside line.
Description	Identifies the user-provided description of the outside line's purpose.

Discover Ports

The Discover Ports feature allows Nyquist to automatically discover a newly installed DAHDI PCI card and to automatically create entries for each port supported by the installed card. You can then edit each port with custom settings. The port name and port type are automatically set by Nyquist and cannot be changed.

Configuring Appliance Firmware

Firmware, computer software stored on a hardware device, can be updated for Nyquist appliances through the Nyquist Admin Web UI or through the appliance's web UI. For information about the appliance's web UI, refer to the device's configuration guide.

Note: Before configuring or using any Nyquist appliances, you should ensure that the appliance firmware is updated to the latest release. The latest firmware release can be obtained from the following website: https://www.bogen.com/c4000-resources

Through the Nyquist Admin Web UI, you can:

- upload a firmware file to the Nyquist system server (see *"Uploading New Firmware to the Server" on page 129*),
- check for firmware updates via the **Check for Updates** button (see *"Checking for Updates" on page 130*),
- download firmware to a station (see *"Downloading Firmware to a Device" on page 132*),
- view a list of stations that are linked to a firmware name (see *"Viewing Devices With a Specific Firmware Installed" on page 129*),
- set default firmware for any added stations (see *"Setting Default Firmware" on page 131*,
- configure automatic software download settings via the **Configure Automatic Software Download** button (see *"Configuring Automatic Software Download" on page 41*),
- check access to required Internet sites (including those from which firmware will be downloaded) via the **Check Internet Site Access** button (see *"Check Internet Site Access" on page 44*),
- and delete firmware entries (see *"Deleting Listed Firmware" on page 133*).

Viewing Firmware Stored on the Nyquist System Server

From the *Firmware* page, you can view a list of available firmware, bring up a list of devices that can be selected for updating firmware, set the file to the default firmware, check for updates, view release notes, select to edit information about or delete firmware files on the Nyquist system server, and configure automatic software downloads.

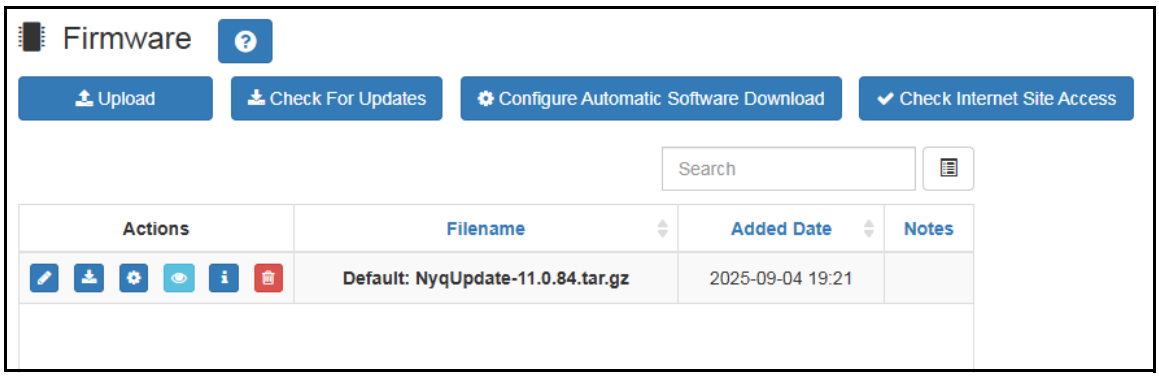


Figure 34. Firmware Page

To view firmware available for loading into Nyquist devices:

On the Navigation bar, select **Firmware**.

The following table describes the information provided for each available firmware file:

Table 37. Firmware Parameters Page

Upload	Uploads a specified firmware file to the Nyquist system server (see *"Uploading New Firmware to the Server" on page 129*).
Check for Updates	Checks Nyquist servers for firmware updates (see *"Checking for Updates" on page 130*).

Table 37. Firmware Parameters Page

Configure Automatic Software Download	Configures automatic software download settings (see *"Configuring Automatic Software Download" on page 41*).
Check Internet Site Access	Check network access to various Internet sites, including those from which firmware will be downloaded (see *"Check Internet Site Access" on page 44*).
Actions	Buttons for performing firmware file-specific actions: • **Edit** (see *"Editing Firmware" on page 132*) • **Device Selection** (see *"Selecting Devices for Firmware Update" on page 130*) • **Set as Default Firmware** (see *"Setting Default Firmware" on page 131*) • **View Selected Devices** (see *"Selecting Devices for Firmware Update" on page 130*) • **View Release Notes** (see *"Viewing Release Notes for Firmware" on page 132*) • **Delete** (see *"Deleting Listed Firmware" on page 133*)
Filename	Provides the name of firmware file that is ready for installing to a Nyquist device. The default firmware (see *"Setting Default Firmware" on page 131*) will be prefixed with "Default:".
Added Date	Provides the date that the firmware file was loaded to the Nyquist system server.
Notes	Provides notes entered by a user.

Viewing Devices With a Specific Firmware Installed

You can obtain a list of all devices in your Nyquist system that have a specific firmware version installed.

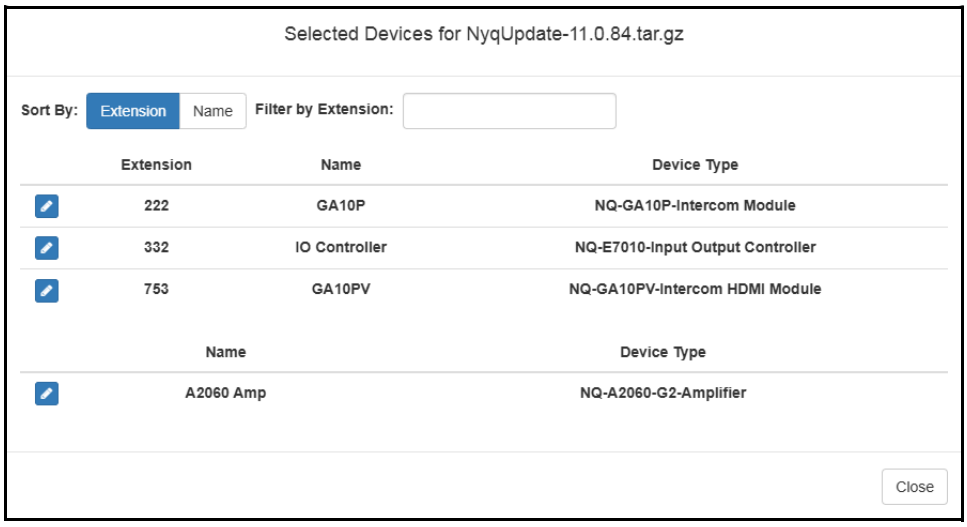


Figure 35. Selected Devices for Firmware Version

To obtain a list of devices with the same firmware version installed:

1. On the Navigation bar, select **Firmware**.
2. On the *Firmware* page, select the **View Selected Devices** icon next to a listed firmware version.

   A list of the devices that have the selected firmware version installed appears.
3. Select the **Edit** button next to a device to edit that device or station.
4. Select **Close** to return to the Firmware page.

Uploading New Firmware to the Server

The *Firmware* page contains an **Upload** button that allows you to upload new firmware files to your Nyquist server.

To upload new firmware to the server:

1. On the navigation bar, select **Firmware**.
2. On the Firmware page, select **Upload**.
3. Navigate to the file that you want to upload.
4. Select **Upload**.

Note: The upload could take as much as a couple minutes. The *Upload* dialog will automatically close when the upload has completed.

Checking for Updates

The *Firmware* page contains a **Check for Updates** button that allows you to check if new firmware is available and download updates that exist.

To check for firmware updates:

1. On the navigation bar, select **Firmware**.
2. On the Firmware page, select **Check For Updates**.
   A popup window appears with one of the following messages:
   - No firmware dates available
   - Can't check for updates, check Internet connection, and try again
   - Downloading firmware update

     If the system attempts to download a firmware update, you will receive a message that the firmware download was either successful or failed. In the case of a failure, you will be prompted to try again.
3. When prompted, select **OK**.

Selecting Devices for Firmware Update

You can select one or more devices to receive a firmware update.

To select devices for firmware update:

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

2 On the Firmware page, select the **Device Selection** icon next to the firmware version that you want to load.

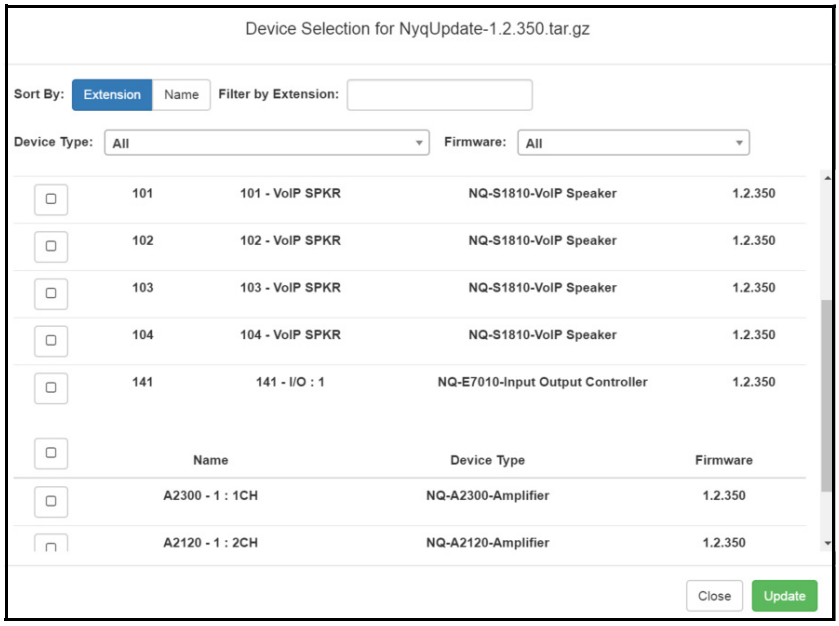


Figure 36. Device Selection for Firmware Update

3 Select the device or devices to which you want to install the firmware.

4 Select **Update**.

You can install firmware to one device at a time. **The Device Selection for <*firmware version*>** screen remains until you select **Close**.

Setting Default Firmware

Through the Firmware page, you can set a firmware file as the default firmware for any new stations added to your Nyquist system.

Important:	Selecting a new default does not change the firmware version currently configured and used by existing devices. It only applies to devices added after the default has been changed.

To set a default firmware file:

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

2 On the Firmware page, select the **Set as Default Firmware** icon next to a listed filename.

Warning	Completing this procedure will set the selected firmware file as the default firmware for all new devices, overriding the factory installed firmware. Ensure that the selected firmware version is compatible with your server's software version. To use some appliances, you may need to update your server software.

3 Select **Yes** to continue.

Downloading Firmware to a Device

To download firmware from the Nyquist system server to a station:

1 On the navigation bar, select **Firmware**.
2 On the Firmware page, select the **Device Selection** icon next to a listed filename.
3 Select the **Update** icon next to the device that you are updating firmware for.

Note: For stations that are attached to a Networked Power Amplifier, such as an NQ-A2300, the firmware is updated to the amplifier and not to each individual station.

Editing Firmware

You can edit **Notes** for firmware, but you cannot change the **Filename** or **Added Date** information.

To edit notes for firmware:

1 On the navigation bar, select **Firmware**.
2 Select the **Edit** icon next to the desired firmware file.
3 Make changes to the **Notes** parameter.
4 Select **Save**.

Viewing Release Notes for Firmware

Not all firmware versions have release notes. For those that do, you can view the release notes by selecting the appropriate icon in the Actions column.

To view release notes for a firmware version:

1 On the navigation bar, select **Firmware**.
2 On the Firmware page, select the **Information** icon.
3 After viewing the release notes, select **OK**.

Viewing Stations Linked to Firmware

To view stations linked to a specific firmware file:

1 On the navigation bar, select **Firmware**.
2 On the *Firmware* page, select the **View Selected Devices** icon next to a listed filename.

Deleting Listed Firmware

Note: Firmware cannot be deleted if it is associated with a device.

To delete a firmware file from the Nyquist system server:

1. On the navigation bar, select **Firmware**.
2. On the Firmware page, select the **Delete** icon next to the filename that you want to delete.
3. When prompted, select **Delete**.

Configuring Facilities

A *facility* is a site with one or more buildings managed by a single Nyquist system server.

With facilities, you can connect multiple Nyquist facilities (servers) to provide the following multi-site paging and calling features:

- Multi-Site Emergency-All-Call paging to all connected facilities in the Facilities list
- Multi-Site All-Call paging to all connected facilities in Facilities list
- Multi-Facility paging to one or more selected Facilities
- Facility Announcement to one or more selected Facilities
- Paging to a specific facility in the Facilities list
- Intercom calls to stations from facilities in the Facilities list
- Start Routines on one or more remote Facilities

These facility connections are unidirectional. A Nyquist system server can only initiate one of these actions toward a facility that is configured in that server's *Facilities* page. For the remote facility to initiate a multi-site call or page back, it must likewise define the first server as a facility.

For information about the facilities list, see *"Viewing Facilities" on page 134*.

Any connected facility can perform multi-site paging (i.e., paging to all facilities listed in the Facilities list), provided the facility has at least one station with the necessary CoS permissions enabled. If you are using an Admin Phone with the correct CoS permissions enabled, you can dial specific DTMF codes to perform various activities.

The following table provides a list of CoS permissions required and DTMF codes used for specific activities.

Table 38. Activities, CoS Permissions, and DTMF Codes

Activity	Required CoS Permissions	DTMF Syntax
Multi-Site Emergency-All-Call Page	Emergency All-Call, Multi-Site Paging	##0911
Multi-Site All-Call Page	All-Call Paging, Multi-Site Paging	##0
Facility All-Call Page	Inter-Facility Call/Page	##<Facility-Page-Number>
Multi-Facility Paging	Inter-Facility Call/Page	##<Facility-Page-Number>*<Facility-Page-Number>...
Facility Announcement	Multi-Site Paging, Inter-Facility Call/Page	*97<DTMF-Code>#<Facility-Page-Number>*<Facility-Page-Number>...
Intercom Call to Remote Facility	Inter-Facility Call/Page	##*<Facility-Page-Number>*<Station Extension Number>
Activate System Feature at Remote Facility	Inter-Facility Features	##*<Facility-Page-Number>*[900 – 999] ##*<Facility-Page-Number>*#<Feature Code> ##*<Facility-Page-Number>**<Feature Code> ##*<Facility-Page-Number>*00000<Feature Extension>

For information about Facility Error Conditions, see *"Facility Error Conditions" on page 370*.

Viewing Facilities

The *Facilities* page provides a quick view of the building or remote facilities (Nyquist servers) that are connected to this Nyquist server.

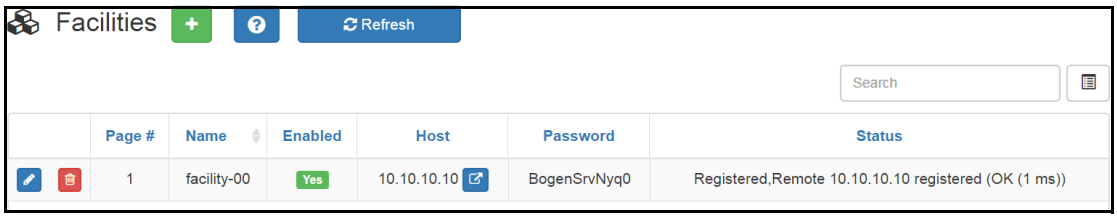


Figure 37. Facilities Page

To view facilities:

On the navigation bar, select **Facilities**.

Table 39 describes the *Facility* page parameters:

Table 39. Facilities Page Parameters

Page #	ID number that is used to page the facility.
Name	Displays the facility name of the remote server. Spaces in the name are replaced by dashes. The maximum facility name length is 30 characters.

Table 39. Facilities Page Parameters

Enabled	Specifies if the facility will register with the remote facility.
Host	Displays the host name or host IP address of the remote server.
Password	Displays the password that is used for the remote connection. Your Nyquist network can use multiple servers that all have the same password, or you can set different passwords for each server. The maximum password length is 12 characters.
Status	Displays the registration status of the local and remote facility peers. Some possible statuses are: • **Registration request sent; remote not registered**: Indicates that a connection is not established between the facilities. • **Registered; remote not registered**: Indicates that the local facility is registered with the remote facility but the remote facility is not registered with the local facility. This could be a temporary status captured during server startup, or it might result from the remote server not having the local facility properly configured. • **Timeout; remote not registered**: Indicates that a connection is not established between facilities. This is probably due to a network connection issue or the remote facility may be down. • **Timeout; remote 10.10.5.100 registered (OK (8 ms))**: Indicates that the remote facility has registered with the local facility and the connection is good, or OK, with 8 millisecond turnaround time (one-way connection). • **Registered; remote 10.10.5.100 registered (OK (3 ms))**: Indicates that the local facility has registered with the remote facility, the remote facility has registered with the local facility, and the connection is OK with 3 millisecond turnaround time. This is the desired state, and it's OK if the reported millisecond turnaround time is not 3. • **Rejected; remote not registered**: Probably indicates that the remote facility has disabled the local facility's configuration entry. • **Registered; remote 10.10.5.100 registered (UNREACHABLE)**: Indicates that both ends are (or were) registered but the local facility cannot reach the remote. This is probably due to a network issue or the remote Nyquist system server is down.

Editing a Facility

From the *Edit Facility* page, you can change parameters for a facility connected to your Nyquist system server.

Note: You cannot edit a facility linked to a **Facility-Page** routine action **Type** (see *"Understanding Action Parameters" on page 460*).

To edit a facility:

1. On the navigation bar, select **Facilities**.
2. Select the **Edit** icon next to the facility that you want to edit.
3. Make the desired changes. (See *Table 40, "Edit Facility Page Parameters," on page 136*.)
4. Select **Save**.

Table 40. Edit Facility Page Parameters

Page	ID number for facility that is used when paging the facility.
Name	Displays the facility name of the remote server. Spaces in the name are replaced by dashes.
Enabled	Specifies if the facility will register with the remote facility.
Host	Displays the host name or host IP address of the remote server.
Password	Displays the password that is used for the remote connection.

Deleting a Facility

Note: You cannot delete a facility linked to a **Facility-Page** routine action **Type** (see *"Understanding Action Parameters" on page 460*).

To delete a facility:

1. On the navigation bar, select **Facilities**.
2. On the Facilities page, select the **Delete** icon next to the facility that you want to delete.
3. When prompted, select **Delete**.

Adding a Facility

From the Add Facility page, you can add another Nyquist facility to the list of facilities connected to your Nyquist system server.

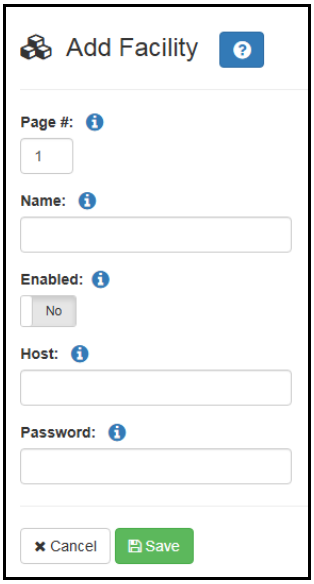


Figure 38. Add Facility Page

To add a facility:

1. On the navigation bar, select **Facilities**.
2. On the Facilities page, select the **Add** icon.
3. Complete the *Add Facility* parameters. (See *Table 41*.)
4. Select **Save**.

Table 41. Add Facility Page Parameters

Name	Enter the name of the remote facility. Spaces in the name are replaced by dashes. Maximum length is 30 characters.
Enabled	Specify if this facility will register with the remote facility.
Host	Enter the host name or host IP address of the remote server.
Password	Enter the password that is used for the remote connection. This is specified by the remote server as its **Facility Password** (see *"Passwords" on page 19*). Maximum length is 12 characters.

Important: If you're planning to link more than 45 facilities, you will need to use **Facility Names** and **Facility Passwords** that contain less than the maximum number of characters allowed. For example, if you're planning to link 78 facilities, the maximum **Facility Name** length should be 12 and the maximum **Facility Password** length should be 12. If you are going to link more than 45 facilities, ask Technical Support to recommend the maximum character lengths to use for **Facility Name** and **Password**.

Appliance Discovery Wizard

The **Nyquist Appliance Discovery and Network Settings Configuration Wizard** can be used at any time to discover Nyquist appliances on the network (via Port A and optionally Port B) and change the appliances' network settings. The available options for an appliance are:

- Enable or disable DHCP on the appliance.
- If DHCP is disabled, specify the appliance's static IP configuration, including a static IP address, subnet mask, and gateway IP address.
- Specify a TFTP server IP address or indicate that DHCP extended option 66 will be used to obtain it.

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

The wizard can be accessed via the **Device Discovery** button, which can be found on the *Stations*, *New Stations, Stations Status*, *Amplifier and Gateway Devices*, and *Appliance Status* pages or accessed directly via the following URLs:

```
https://<server>/setup/discovery
http://<server>/setup/discovery
```

The wizard will first ask if Nyquist appliances will be configured to receive IP addresses and (optionally) the TFTP server IP address from the DHCP server or if they will be explicitly configured.

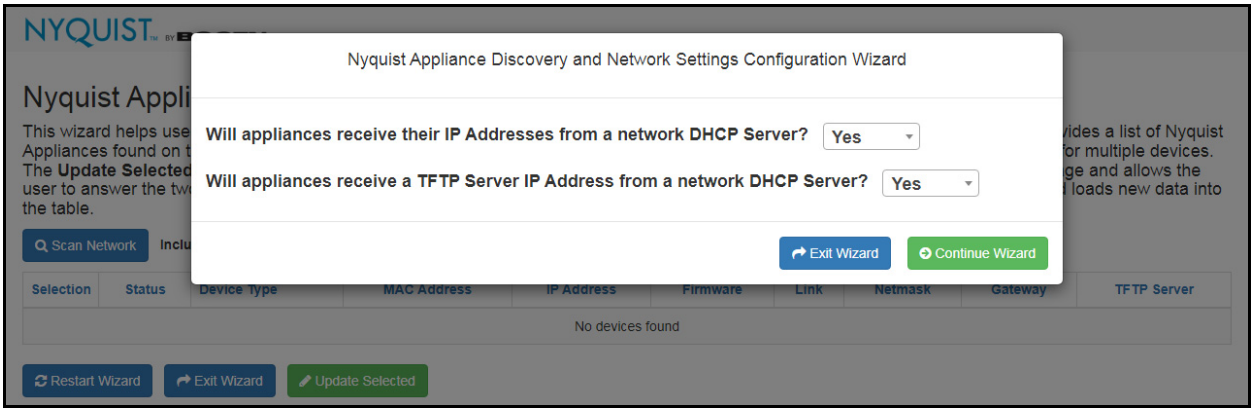


Figure 39. Network Appliance Discovery and Network Settings Configuration Wizard (start)

- *Will appliances receive their IP Addresses from a network DHCP Server?*

  No allows the user to configure the IP Address, Netmask, and Gateway settings for discovered Nyquist appliances.

  Yes indicates that these settings will be configured by the DHCP server.

  This option corresponds to the **DHCP Enabled** option on the *Network Settings* page of the appliance's web interface.

- *Will appliances receive a TFTP Server IP Address from a network DHCP Server?*

  No allows the user to configure the TFTP Server address for discovered Nyquist appliances.

Yes indicates that the TFTP server address will be specified by the DHCP server via extended option 66. This option is not available if *Will appliances receive IP Addresses from a DHCP Server?* is set to **No**.

This option corresponds to the **TFTP Server from DHCP** option on the *Network Settings* page of the appliance's web interface.

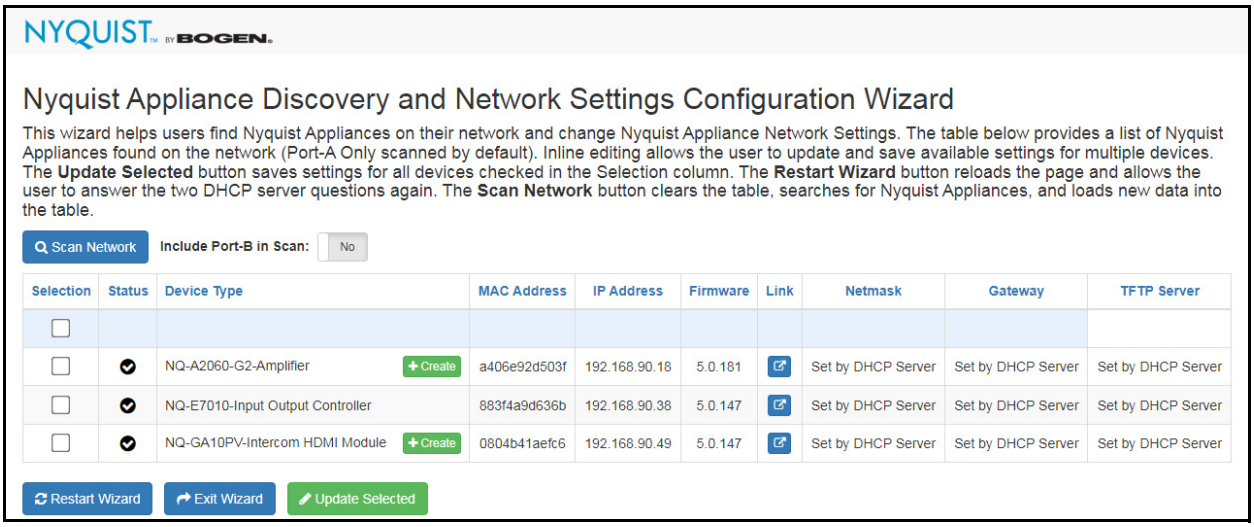


Figure 40. Network Appliance Discovery and Network Settings Configuration Wizard (appliances)

After scanning the network, the wizard will present a list of all Nyquist appliances found on the network(s). Depending on which options were selected at the beginning of the wizard, one or more settings may be available for each appliance.

Table 42. Nyquist Appliance Discovery and Network Setting Wizard Configuration Settings

Scan Network	Initiates a network scan to identify Nyquist appliances on the attached network(s). *Tip:* Due to the dynamic nature of networks and network devices, multiple scans may sometimes be needed to detect all devices and obtain their appropriate information.
Include Port-B in Scan	If set to **Yes**, both network ports (A and B) on the C4000 will be scanned for Nyquist appliances. If set to **No** (the default), only port A will be scanned. This takes effect the next time **Scan Network** is selected.
Selection	Select one or more appliances that will be updated when the **Update Selected** button is clicked.
Status	Indicates the status of the appliance. Possible values are: • Device Ready • Update Complete • Updating Device • Update Error
Device Type	The type of Nyquist appliance discovered.

Table 42. Nyquist Appliance Discovery and Network Setting Wizard Configuration Settings (continued)

Create	The **Create** button will be displayed next to the **Device Type** if the C4000 does not already have a station configured for this appliance. Selecting this button will create a new Station for the appliance. *Tip:* If a station had previously been defined for this appliance and then deleted, the **Create** button may not be displayed. Reboot the device (e.g., use the **Link** button to access the appliance's configuration pages and press the **Reboot Appliance** button on the **Firmware Update** page), wait 30 seconds, and press the **Scan Network** button to refresh the status.
MAC Address	Displays the MAC address of the appliance. This helps identity specific devices when installing multiple devices of the same type.
IP Address	Displays the current IP address of the appliance. If DHCP will not be used, selecting this value allows the IP address to be modified. IP addresses will not be changed until **Update Selected** is clicked. **Warning** Be careful to avoid specifying a currently used IP address (e.g., when swapping IP addresses) as this could result in IP address conflicts.
Firmware	Displays the current version of the appliance firmware running on the appliance.
Link	This provides a login window for the appliance. After you enter your **Username** and **Password**, the web UI for the device appears.
Netmask	If DHCP will not be used for this appliance, the IP subnet mask must be specified.
Gateway	If DHCP will not be used for this appliance, the gateway IP address must be specified.
TFTP Server	If the appliance will not receive the TFTP server IP address from the DHCP server using DHCP option 66 (see *"DHCP Server" on page 47*), the IP address of the TFTP server must be specified.
Restart Wizard	Selecting this button restarts the Appliance Discovery Wizard.
Skip Wizard	Exits the wizard and displays the C4000 Dashboard.
Update Selected	Updates any configurable values of the selected appliances (i.e., **IP Address**, **Netmask**, **Gateway**, and/or **TFTP Server**, if not specified via DHCP) with the provided values.

Managing Stations, Zones, and Queues

You can divide your facility into zones to control paging and audio activities or features.

For example, suppose you want to allow the use of an audio source—such as a flash drive—in a cafeteria, but prevent it from being played in a conference room. This feature, called *audio distribution*, can be turned on by zone, so the cafeteria could be placed in a zone that allows audio distribution, while the conference room would *not* be placed in that zone.

There is no limit to the number of stations that can be in a multicast zone, but performance limits do exist for unicast connections. The station limit for your system is determined by your Nyquist license. For licensing purposes, an I/O Controller is not counted as a station.

With the Page Queuing feature, you can record an unlimited number of pages or messages for queuing (stacking) for a specified zone or zones. A zone can only be added to a single queue, but a queue may have multiple zones associated with it. Zones must be created before a queue can be created.

Note: A station can be in multiple zones.

A Nyquist station can be:

- A device used to access the web interface
- A speaker
- A phone
- A Nyquist appliance

To manage stations and zones, first add stations and then create zones that contain one or more stations. You can add stations by allowing the Nyquist server to automatically discover the device type, MAC address, IP address, and serial number, or manually add these and other parameters. For more information about adding a station, see *"Adding a Station" on page 185*.

Speaker Extension Muting

When a station that is associated with a Speaker Extension initiates a page, the associated speaker will be muted during the page. This is to prevent the creation of an audio feedback loop.

All paging types are supported: Emergency-All-Call, All-Call, Zone-Page, Facility Pages that include the local facility, Multi-Site All-Call, and Multi-Site Emergency-All-Call. The associated speaker is muted for Facility Page to eliminate possible interference from local pages while the station is performing the Facility Page.

Viewing Station Configuration Settings

On the Stations page, you can:

- View all configured stations.
- Edit a station's configuration. (*See "Editing Station Configuration Settings" on page 155.*)
- Exclude a station from paging via the **Page Exclusion** button. (*See "Excluding Stations from Paging" on page 208.*)
- Initiate the *Appliance Discovery Wizard* via the **Device Discovery** button. (*See "Appliance Discovery Wizard" on page 138.*)
- Access the *Simplified Configuration* page via the **Simplified Configuration** button. (See *"Simplified Configuration" on page 220.*)
- View station status via the **Stations Status** button. (*See "Viewing Station Status" on page 210.*)
- Add new stations via the **New Stations** button. (*See "Adding a Station" on page 185.*)
- View the status of Nyquist appliances, such as the I/O controller, via the **Appliance Status** button. (See *"Viewing Appliance Status" on page 212.*)
- Edit a station. (See *"Editing Station Configuration Settings" on page 155.*)
- Delete a station. (*See "Deleting a Station" on page 184.*)
- View device status information for the station. (See *"Displaying Device Status" on page 221.*)

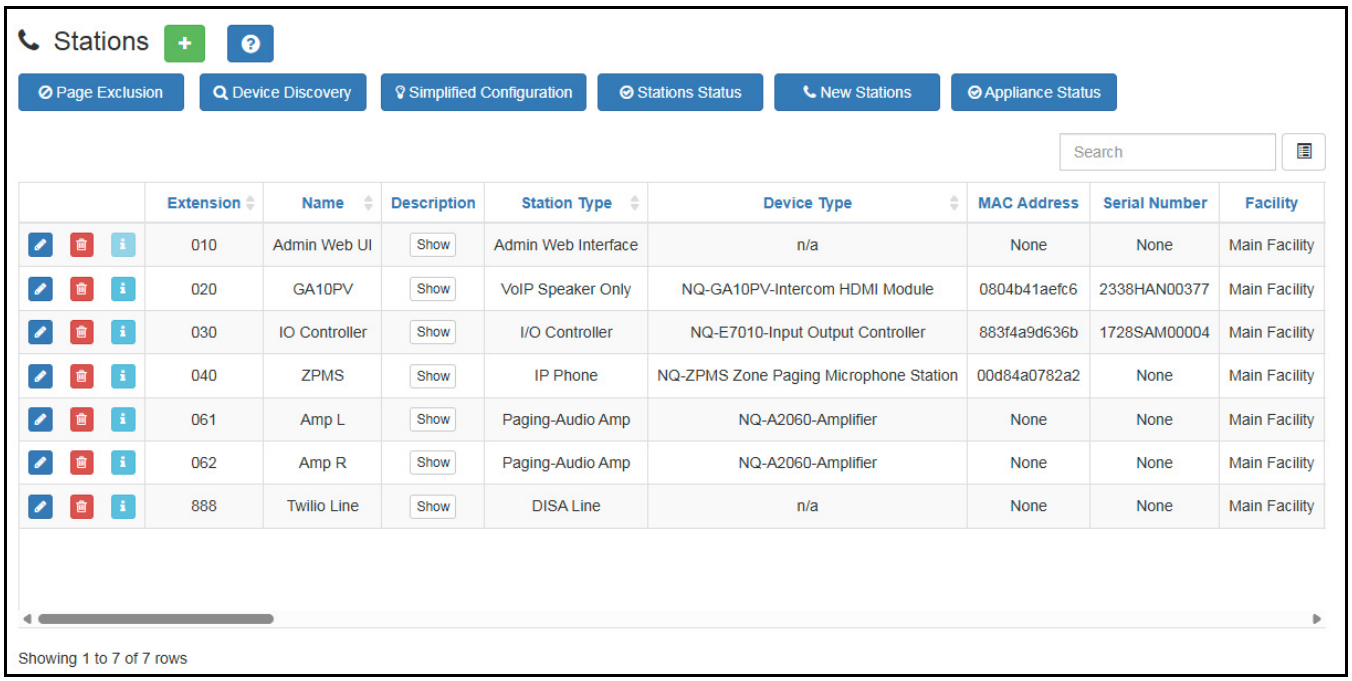


Figure 41. Stations Page

To view all stations:

On the navigation bar, select **Stations**.

The following table, *Table 43*, describes station configuration information:

Table 43. View, Add, or Edit Station Configuration Parameters

Note: Some of the following fields do not appear when adding or editing stations for specific device types.

Edit	Edit the station.
Delete	Delete the station.
Device Status	Display the device status for this station.
Extension	Specifies the unique multi-digit extension number for the station. Valid values range from 030 to 899 for three-digit dialing. The system can be configured to use three, four, five, or six-digit dialing. *Note:* Extensions 900 to 999 are reserved by Nyquist features; do not assign these extensions to stations.
Name	Specifies the name for the station. Names can contain up to 16 characters. *Note:* Valid characters include uppercase letters (A–Z), lowercase letters (a–z), numerals (0–9), space, and the following special characters: **! @ $ * ? - . ,** .
Description	Provides a description for this station. *Note:* Valid characters include uppercase letters (A–Z), lowercase letters (a–z), numerals (0–9), space, and the following special characters: **! @ $ * ? - . ,** .

Table 43. View, Add, or Edit Station Configuration Parameters (continued)

Device Type

Tip: The available **Device Type** options are affected by the selected **Station Type**, and the **Station Type** options are affected by the selected station **Device Type**. If the desired **Device Type** option (of the **Device Type** field itself) is not available, specify the appropriate **Station Type** first, which should enable the appropriate **Device Type** options.

Note: Nyquist does not display this field when adding or editing an Admin Web Interface, DISA Line, or Mobile Device.

Identifies the physical device used by the station.

Device types include:

- Cisco ATA191/192-3PW-K9
- Cisco SPA112
- DAHDI FXS
- Grandstream GXW4224 Analog Phone FXS Port
- Grandstream HT813 Analog Phone FXS Port
- n/a
- NQ-A2060[-G2]-Amplifier
- NQ-A2120[-G2]-Amplifier
- NQ-A2300[-G2]-Amplifier
- NQ-A4060[-G2]-Amplifier
- NQ-A4120[-G2]-Amplifier
- NQ-A4300[-G2]-Amplifier
- NQ-DSC01 Double-Sided Hallway Display Combo
- NQ-E7010-Input Output Controller
- NQ-EDP01-Entry Door Phone
- NQ-GA10P-Intercom Module
- NQ-GA10PV-Intercom HDMI Module
- NQ-GA20P2-Amplifier with Line Output
- NQ-GA400P-AoIP Gateway
- NQ-GA40P3-Amplifier with Line In/Out
- NQ-IPHRN01 IP Horn Speaker
- NQ-P0100-Matrix Mixer Pre Amp
- NQ-PA120 Public Address Mixer Amplifier
- NQ-PA240 Public Address Mixer Amplifier
- NQ-PA600 Public Address Mixer Amplifier
- NQ-S1810-E7020 VoIP Speaker CallSwitch
- NQ-S1810-VoIP Speaker
- NQ-S1810CT-G2 VoIP Ceiling Speaker Gen2
- NQ-S1810CT-T1 VoIP Ceiling Speaker with Transformer
- NQ-S1810WBC VoIP Wall Baffle Combo Spkr/Clock/Msg
- NQ-S1810WT-G2 VoIP Wall Baffle Speaker Gen2
- NQ-S1810WT-G3 VoIP Wall Baffle Speaker Gen3
- NQ-T1000 IP Phone - Basic LCD Display
- NQ-T1100 IP Phone - Color Touch Display
- NQ-T2000 IP Phone - Basic LCD Display
- NQ-ZPMS Zone Paging Microphone Station
- Yeastar-TA2400 Analog FXS Port

Table 43. View, Add, or Edit Station Configuration Parameters (continued)

Station Type

Specifies the station type. Available values include:

- Admin Phone
- Admin Web Interface

  Note: A station of type Admin Phone or Admin Web Interface is generally referred to as an "Admin Station." Although most capabilities of these station types can be explicitly granted to other station types, the typical usage is to specify one of these types for stations that will be used for administrative purposes.
- Admin PBX Extension
- IP Phone
- Mobile Device
- VoIP Speaker Only
- Analog Call Switch & Speaker
- Digital Call Switch & Speaker
- Analog Phone

  Note: An analog phone cannot be used as an Admin Phone destination (Day or Night Admin) even if it has the correct CoS set. An analog phone cannot be added to a zone, cannot be used as an emergency, cannot be monitored, and cannot be a call forwarding target from an Admin Phone.
- DISA Line
- 911 Line
- I/0 Controller

  Note: For licensing purposes, an I/O Controller is not counted as a station, so they do not subtract from the available station count set in the installed license.
- Matrix Mixer Pre-Amp
- Paging-Audio Amp
- Paging-Audio-Intercom Module
- Ambient Noise Sensor
- Push-To-Talk Microphone
- Audio Gateway
- Sound Masking

Tip: The available **Station Type** options are affected by the selected **Device Type**, and the **Device Type** options are affected by the selected **Station Type**. If the desired **Station Type** is not available, specify the appropriate **Device Type** first, which should enable the appropriate **Station Type** options.

Note: Once the station has been added, this setting cannot be modified.

Port

Nyquist only displays this field when adding or editing a **Station Type** of **Analog Phone** and a **Device Type** of **DAHDI FXS**.

Identifies the system port name for the analog line.

MAC Address

Specifies the Media Access Control (MAC) address, which is a unique identifier assigned to network interfaces for communications on the physical network segment.

Note: Nyquist does not display this field when adding or editing an Admin Web Interface, Admin PBX Extension, Analog Phone, Mobile Device, Paging-Audio Amp, or DISA Line.

Note: Valid values consist of twelve hexadecimal digits (0–9 and A–F). Optional colon (:) or hyphen (-) separators will be accepted and automatically removed.

Table 43. View, Add, or Edit Station Configuration Parameters (continued)

Serial Number	*Note:* Nyquist does not display this field when adding or editing an Admin Web Interface, Admin Phone, IP Phone, or DISA Line. Identifies the serial number for the device.
Facility	Identifies the facility where this station is installed.
Day CoS	Identifies CoS permissions that apply to this station during day time hours.
Night CoS	*Note:* Identifies CoS permissions that apply to this station during night time hours.
Day Admin	*Note:* Nyquist does not display this field when adding or editing an Admin PBX Extension, I/O Controller, Paging Audio Amp, or Matrix Mixer Pre-Amp. Identifies the Admin Station that covers this station during daytime hours. This is the station that will be called when the user dials zero (0, *0, or **0) or presses the call switch. *Note:* An analog phone cannot be used as an admin destination (day or night admin) even if it has the correct CoS set. If Admin Group is specified, all the Admin Stations of the caller's Admin Group will be called instead of a single Admin Station. If the Admin Group includes web interface stations, they will be called directly, receiving the call as an incoming call pop-up dialog. *Note:* If Admin Group is specified, the Emergency Link feature is not supported for this the station. See the Emergency Link description on page 73 for further details. For more information about CoS, *see "Using CoS Configuration" on page 100*.
Night Admin	*Note:* Nyquist does not display this field when adding or editing an Admin PBX Extension, I/O Controller, Paging Audio Amp, or Matrix Mixer Pre-Amp. Identifies the Admin Station that covers this station during nighttime hours. This is the station that will be called when the user dials zero (0, *0, or **0) or presses the call switch. *Note:* An analog phone cannot be used as an admin destination (day or night admin) even if it has the correct CoS set. If Admin Group is specified, all the Admin Stations of the caller's Admin Group will be called instead of a single Admin Station. If the Admin Group includes web interface stations, they will be called directly, receiving the call as an incoming call pop-up dialog. *Note:* If Admin Group is specified, the Emergency Link feature is not supported for this the station. See the Emergency Link description on page 73 for further details. For more information about CoS, *see "Using CoS Configuration" on page 100*.

Table 43. View, Add, or Edit Station Configuration Parameters (continued)

Admin Group	*Note:* Nyquist does not display this field when adding or editing an Admin Phone, Admin Web Interface, Admin PBX Extension, I/O Controller, Paging Audio Amp, or Matrix Mixer Pre-Amp. Identifies the Admin Group associated with the station. The Admin Group is called if the Day Admin or Night Admin does not answer within 30 seconds.
Registration Password **Registration Password Confirmation**	(Add and Edit only) Specify the password that this station will use when it registers with this Nyquist server as a SIP client. The Nyquist server will remember the registration password for each station. If **Registration Password** is unspecified, the **Default Registration Password** will be used (see *Table 23, "Edit System Parameters Page," on page 69*). If the **Default Registration Password** is not specified, **Registration Password** is required. The minimum length is five characters. For a description of the Registration Password, see *"Passwords" on page 19*.
Show Password **Show Saved Password** (Registration Password)	(Add and Edit only) Selecting this button shows the current password to the right of the button for four seconds. If at least one character is typed in the password field, the button label dynamically changes from **Show Saved Password** to **Show Password**.
Codecs Allowed	Identifies the list of codecs supported by the device that is associated with this station.
Voicemail Password	*Note:* Nyquist does not display this field when adding a VoIP Speaker Only, Call Switch & Speaker, I/O Controller, or Matrix Mixer Pre-Amp.
Voicemail Password Confirmation	(Add only) Provide the password used to access voicemail. This field can contain numeric characters only.
Show Password **Show Saved Password** (Voicemail Password)	(Add and Edit only) Selecting this button shows the current password to the right of the button for four seconds. If at least one character is typed in the password field, the button label dynamically changes from **Show Saved Password** to **Show Password**.
Force Name	*Note:* Nyquist does not display this field when adding or editing a VoIP Speaker Only, Call Switch & Speaker, I/O Controller, or Matrix Mixer Pre-Amp. Forces the user to record his name when setting up voicemail.
Force Greeting	*Note:* Nyquist does not display this field when adding or editing a VoIP Speaker Only, Call Switch & Speaker, I/O Controller, or Matrix Mixer Pre-Amp. Forces the user to record a greeting when setting up voicemail.
Call Recording	*Note:* Nyquist does not display this field when adding or editing an I/O Controller, Paging Audio Amp or Matrix Mixer Pre-Amp. Determines if all calls made and placed to this station are recorded.

Table 43. View, Add, or Edit Station Configuration Parameters (continued)

Paging	*Note:* Nyquist does not display this field when adding or editing an Admin Web Interface, Web Interface, DISA Line, I/O Controller, 911 Line, or Analog Phone. When set to **Off**, the station does not receive tones from the schedules, All-Call pages, or Zone pages. However, the station will receive Emergency All-Call pages unless the station is a NQ-T1000 or NQ-T2000 phone. If **Paging** is set to **On** for a NQ-T1000 or NQ-T2000 phone, then this device will receive Emergency All-Call pages even if the station is in the Paging Exclusion list. This device will receive All-Call and zone paging provided the station is not in the Paging Exclusion list. If **Paging** is set to **Off**, then the station will not receive Emergency All-Call, All-Call, or zone paging.
Audio Distribution to All Speakers	*Note:* Nyquist does not display this field when adding or editing an Admin Web Interface, Web Interface, DISA Line, I/O Controller, 911 Line, IP Phone, or Analog Phone. Determines if the station can receive audio distribution played to all stations. Audio distribution played to zones will still be received if the station is in the audio zone.
Intercom Cut Level (dB)	Specifies the volume cut level for intercom calls. The cut level can range from −42 to 0. The default level is −6.
Talkback Gain (dB)	*Note:* This field only applies if viewing, adding, or editing a station that is associated with an NQ-GA10P or an NQ-GA10PV Intercom Module. Indicates the gain that is to be applied to the talkback function for channels 1 and 2. Gain is the measure of the ability to increase the power or amplitude of a signal. The **Talkback Gain** can range from −12 to +20; default is set at 0.
Microphone Input Gain (dB)	*Note:* This field only applies if viewing, adding, or editing a station that is associated with an NQ-GA10P or an NQ-GA10PV Intercom Module and the **Station Type** is **Push-To-Talk Microphone**. Indicates the gain that is to be applied to the microphone function for channels 1 and 2. Gain is the measure of the ability to increase the power or amplitude of a signal. The **Microphone Input Gain** can range from −12 to +20; default is set at 0.
Outside Access	*Note:* Nyquist does not display this field when adding or editing an I/O Controller or Matrix Mixer Pre-Amp. Identifies permissions for this station to place outside calls. Parameters are: • No Access • Restricted • Restricted Day Only • Restricted Night Only • Unrestricted • Unrestricted Day Only • Unrestricted Night Only

Table 43. View, Add, or Edit Station Configuration Parameters (continued)

911 Route	*Note:* Nyquist does not display this field when adding or editing a VoIP Speaker Only, Call Switch & Speaker, I/O Controller, or Matrix Mixer Pre-Amp. Identifies where 911 calls placed by this station are routed, such as to a specific SIP trunk.
Auth Code	*Note:* Nyquist does not display this field when adding or editing an I/O Controller or Matrix Mixer Pre-Amp. Allows the user to enable the capabilities and features of this station if the Walking Class of Service CoS feature is enabled. The four-digit code activates features from the user's associated station to the station being used. If Auth Code is set to 0000, this feature is disabled.
Speaker Extension/Mute Speaker	*Note:* Nyquist does not display this field when adding or editing an I/O Controller or Matrix Mixer Pre-Amp. Identifies the extension of the speaker associated with the station for speaker drop-to-phone feature and the toggle audio distribution feature (*9). *Note:* Only one speaker extension can be associated with a station. *Note:* When a station that is associated with a Speaker Extension initiates a page, the associated speaker will be muted during the page to prevent feedback. For details, see *"Speaker Extension Muting" on page 141*.
VLAN Configuration	*Note:* Nyquist does not display this field when adding or editing an Admin Web Interface, 911 Line, or DISA Line unless the Admin Phone or IP Phone is connected to a Yeastar TA2400 or Grandstream GXW4224 port. Specifies how the station receives its Virtual Local Area Network (VLAN) configuration. Options are: • **Server**: Allows you to configure the VLAN settings via the Nyquist server web interface. The configured setting will then be sent to the Nyquist appliance by the Nyquist server. • **Network/Device**: The Nyquist devices will either listen for VLAN configuration from DHCP (Network) or the VLAN settings can be configured via the Nyquist device's web interface (Device). • **Disabled**: VLAN is disabled and not used.
VLAN ID	*Note:* Nyquist does not display this field when adding or editing an Admin Web Interface, 911 Line, or DISA Line unless the Admin Phone or IP Phone is connected to a Yeastar TA2400 or Grandstream GXW4224 port. Identifies the VLAN for this station. The VLAN ID parameters range from 2 through 4094 and pertain to the device's network interface (not to the ports or stations).
VLAN Priority	*Note:* Nyquist does not display this field when adding or editing an Admin Web Interface, 911 Line, or DISA Line unless the Admin Phone or IP Phone is connected to a Yeastar TA2400 or Grandstream GXW4224 port. Identifies the priority for the port. Values range from 0 through 7.

Table 43. View, Add, or Edit Station Configuration Parameters (continued)

Web Username	*Note:* Nyquist does not display this field when adding or editing an Admin Web Interface, Admin Phone, IP Phone, 911 Line, or DISA Line unless the Admin Phone or IP Phone is connected to a Yeastar TA2400 or Grandstream GXW4224 port. When applicable, provides a username for logging into the web interface of the device hosting the station.
Web Password **Web Password Confirmation**	*Note:* These fields appear only when adding or editing a station, provided the station is not an Admin Web Interface, Admin Phone, IP Phone, 911 Line, or DISA Line unless the Admin Phone or IP Phone is connected to a Yeastar TA2400 or Grandstream GXW4224 port. When applicable, provides a password for logging into the web interface of the device hosting the station. The minimum length is five characters. If **Web Password** is not specified, the **Default Web Password** system parameter value is used (see *Table 23, "Edit System Parameters Page," on page 69*). If **Default Web Password** is unspecified, this parameter is required. *Note:* Nyquist appliances have distinct web passwords for non-standalone and standalone modes. **Web Password** only applies to non-standalone mode.
Show Password **Show Saved Password** (Web Password)	(Add and Edit only) Selecting this button shows the current password to the right of the button for four seconds. If at least one character is typed into the password field, the button label dynamically changes from **Show Saved Password** to **Show Password**.
Load Impedance	*Note:* This field appears only when adding or editing a station where the **Device Type** is NQ-A2060-Amplifier, NQ-A2120-Amplifier, NQ-A2300-Amplifier, NQ-A4060-Amplifier, NQ-A4120-Amplifier, NQ-A4300-Amplifier, NQ-PA120 Public Address Mixer Amplifier, NQ-PA240 Public Address Mixer Amplifier, or NQ-PA600 Public Address Mixer Amplifier. This field is used to select the impedance of the attached load. Select **High** for devices that use 25V/70V and **Low** for devices that use 4 Ω or 8 Ω.

Table 43. View, Add, or Edit Station Configuration Parameters (continued)

Output Power (Watts)

Note: This field appears only when adding or editing a station for VoIP speakers, NQ-S1810WBC, NQ-GA10P, NQ-GA10PV, NQ-GA20P2, NQ-GA40P23, two- or four-channel amplifiers, or NQ-PAxxx amplifiers.

Selects the channel output power setting.

Defaults and settings vary depending on the appliance.

For example, VoIP speakers, NQ-GA10P, and NQ-GA10PV devices allow options of ⅛, ¼, ½, 1, 2, 4, and 8W, while NQ-GA20P2 devices also allow 16W and NQ-GA40P3 devices also allow 16W and 32W.

The default for these devices is ½.

For the other applicable devices, the available settings increment by 1 and range from −6 to +6 dB with the default being 0.

Firmware

Note: Nyquist does not display this field when adding or editing an Admin Web Interface, Admin Phone, IP Phone, Mobile Device, or when adding or editing a Networked Power Amplifier.

Provides information about firmware available for the station. 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 later than the one installed on the appliance, an automatic firmware update occurs. To prevent an automatic update, you must leave this **Firmware** parameter empty.

Sites

Note: The C4000 can be configured to use a different word or phrase in place of "Sites" in most places within the application (see the Schedule Site Settings settings in *Table 24, "System Tools," on page 78*).

Provides the sites that this station can view or edit on the Dashboard and in schedules.

For NQ-T1100 and NQ-ZPMS Admin Phones, this setting also specifies the site schedules that will be displayed on the phone's display and included in the phone's Schedules menu.

Maps

Note: This parameter is only displayed for Admin Web Interface stations, and only if the Map feature has been licensed for use.

Provides the maps that this station is authorized to view from the dashboard.

Queue Zone

Provides the default zone number for the station that will be used for page queuing (Record Page feature). If a zone number does not appear, the station user will be prompted to enter a zone number.

Table 43. View, Add, or Edit Station Configuration Parameters (continued)

Announcement Zone	*Note:* This parameter appears only when adding or editing a station if the **Station Type** is set to **Admin Web Interface**, **Admin Phone**, **IP Phone**, **Analog Phone**, or **Mobile Device**. **Announcement Zone** overrides the **Play to Zone** set when creating an announcement. Select a zone number to be used as this station's default zone when playing announcements. If an **Announcement Zone** is not set, you will be prompted for a zone number when playing an announcement. (See *"Using Announcements" on page 319*.)
Announcement Zone Configuration Type	*Note:* This parameter appears only when adding or editing a station if the **Station Type** is set to **Admin Web Interface**, **Admin Phone**, **IP Phone**, **Analog Phone**, or **Mobile Device**. Displays either **Fixed** or **Default**, depending on whether you can change the zone for announcements created by this station. If set to **Fixed**, the zone used to play announcements will always be the zone number provided for **Announcement Zone** and cannot be changed. If set to **Default**, the **Announcement Zone** value is used as the default zone, but you can set an announcement to play to another zone.
External Relay Trigger	*Note:* This parameter only applies to NQ-GA10P, NQ-GA10PV, NQ-GA400P, NQ-S1810CT-T1 Gen2 VoIP Speaker, and NQ-S1810WT-G3 VoIP Speakers. Specifies if the device should trigger an external relay when audio is present.
Dial Plan Type	*Note:* This parameter only appears when adding or editing a station with **Device Type** of **Cisco SPA112, Cisco ATA191/192-3PW-K9,** or **Grandstream HT813 Analog Phone FXS Port**. Specifies whether the station uses the default or a custom dial plan or if it will automatically dial an extension when the phone is taken off hook. The **Dial Plan Type** options are: • **Default**. When you select this option, the station has DTMF access to all Nyquist features. • **Auto Dial**. When you select this option, you must add the extension that will be automatically dialed when the phone is taken off hook. • **Custom**. When you select this option, the Dial Plan option appears and you can enter a custom dial plan string with a maximum of 255 characters.
Auto Dial Extension	*Note:* This parameter only appears when adding or editing a station with **Device Type** of **Cisco SPA112, Cisco ATA191/192-3PW-K9,** or **Grandstream HT813 Analog Phone FXS Port** and **Auto Dial** has been selected as the **Dial Plan Type**. Specifies the station extension that will be automatically dialed when the phone is taken off hook.

Table 43. View, Add, or Edit Station Configuration Parameters (continued)

Dial Plan	*Note:* This parameter only appears when adding or editing a station with **Device Type** of **Cisco SPA112, Cisco ATA191/192-3PW-K9,** or **Grandstream HT813 Analog Phone FXS Port**. This field will display **Nyquist Default** if the **Dial Plan Type** is set to **Default**. If the **Dial Plan Type** is set to **Auto Dial**, then **Dial Plan** is set to **S:1,(PO <:station extension>)**. For example, if you have entered **200** for the **Auto Dial Extension**, then this field displays **S:1,(PO <:200>)**. If **Dial Plan Type** is set to **Custom**, enter the custom dial plan string, which can contain up to 255 characters.
Description	Allows a user description for this station.
Annunciation Station	Specifies the speaker station at which a call-in announcement will be played ("Call from station <calling-extension>") when *this* station receives a call. Available options include stations of the following **Station Types**: • VoIP Speaker Only • Analog Call Switch & Speaker • Digital Call Switch & Speaker • Paging-Audio Amp • Paging-Audio-Intercom Module *Note:* If the annunciation station is already busy when a call is received, the announcement will not be played. **Important:** Emergency All Call pages will temporarily disable call-in announcements.
Add Phase Shift	Indicates whether the generated masking signal will be phase shifted (Yes) or not (No). *Note:* This parameter only appears when adding or editing a **Sound Masking** station. **Warning** If downward-facing speakers are installed and two amplifier stations are used within the same masking zone, it is critical that either the stations come from different amplifiers (preferable) or the Add Phase Shift setting for the two stations are configured differently (i.e., one Yes, one No). Otherwise, there will be phasing issues or uncontrollable variations in masking levels.

Table 43. View, Add, or Edit Station Configuration Parameters (continued)

Check-in as Station Extension

Specifies the check-in extension to use when this station performs a check-in. This allows the current station to perform a check-in on behalf of the specified station.

If set to **None**, the station's own extension will be tracked during check-in events.

Note: If specified, the current station will be added to the exclusion list to ensure it is not managed separately from the check-in station.

For further details about check-in, see *"Manage Check-In" on page 523*.

Tip: Configure all stations (including Web Interface stations) in a small physical area, like a room, to check-in as one area-specific station.

Use Uploaded Wallpaper Image

If set to **Yes**, the phone can use a custom wallpaper image uploaded via the phone's web interface and will not reset it to the default Bogen wallpaper each time the phone is provisioned.

If set to **No**, the phone can use a custom wallpaper image, but it will reset it to the default wallpaper each time the phone is provisioned.

Enable SIP TLS

Enables the use of TLS to secure SIP traffic for this station. This enables secure, encrypted call setup between the station and the Nyquist server.

If the **Firmware** version is 5.0.0 or higher, the default value is **Yes**. If not, the default value is **No**.

For stations associated with an amplifier or gateway, this value is determined by the amplifier or gateway configuration.See *"VoIP Security" on page 18* for further details.

Caution This setting may be inoperable when adding a new station. Do not assume the displayed value will be applied to the new station; edit the station after adding it to set the appropriate value.

Tip: To enable or disable SIP TLS and SRTP for all Nyquist stations at once, see the **Nyquist Appliance VoIP Security** option in *System Parameters* (see page 84).

Table 43. View, Add, or Edit Station Configuration Parameters (continued)

Enable SRTP	Enables encryption of voice traffic for this station. This enables secure, encrypted voice communication for intercom calls and calls between IP phones. If the **Firmware** version is 5.0.0 or higher, the default value is **Yes**. If not, the default value is **No**. *Note:* For stations associated with an amplifier or gateway, this value is determined by the amplifier or gateway configuration. See *"VoIP Security" on page 18* for further details. **Caution** This setting may be inoperable when adding a new station. Do not assume the displayed value will be applied to the new station; edit the station after adding it to set the appropriate value. *Tip:* To enable or disable SIP TLS and SRTP for all Nyquist stations at once, see the **Nyquist Appliance VoIP Security** option in *System Parameters* (see page 84).
Enable NQ-VCTRL–initiated Calls	Enables an attached NQ-VCTRL device to initiate calls for this station when the NQ-VCTRL device's button is pressed. When disabled, the NQ-VCTRL's LEDs always reflect the current volume. The default value is **Yes**.

Editing Station Configuration Settings

The *Edit Station* page allows you to change a station's configuration settings. For example, if you want to disable paging for a station or change a station's access to an outside line, you edit the station's configuration settings.

Note: You cannot change the extension for a station linked to a routine (see *"Using Routines" on page 425*).

Table 44. Station Type-specific Configuration Options

Station Type	Available Option(s)
• Admin Web Interface • Admin Phone • IP Phone • Analog Phone • Mobile Device	**Announcement Zone Configuration Type** and **Announcement Zone** If the **Announcement Zone Configuration Type** is set to **Fixed**, the zone used to play announcements will always be the zone number provided for **Announcement Zone** and cannot be changed. If set to **Default**, the **Announcement Zone** value is used as the default zone, but you can set an announcement to play to another zone.
• I/O Controller	**Configure Rules** (see *"Configuring I/O Controller Input Rules" on page 162* or *"Configuring I/O Controller Output Rules" on page 164*) **Configure Schedule** (see *"Adding an I/O Contacts Output Daily Schedule" on page 169*)
• MMPA (NQ-P0100)	**Configure PTT** (see *"Configuring Devices for Push-To-Talk" on page 172*)
• Intercom Module (NQ-GA10P, NQ-GA10PV)	**Configure Intercom Module** (see *"Push-To-Talk Configuration for GA10P or GA10PV Intercom Module" on page 174*)
• Intercom HDMI Module (NQ-GA10PV)	**Display Configuration** and options to configure how the message and clock appear on the monitor (see *"Configuring Intercom HDMI Module Display Options" on page 176*).
• NQ-WBC01 Dual-Sided Hallway Combo Display and NQ-S1810WBC VoIP Wall Baffle Combo Spkr/Clock/Msg	**Display Configuration** (see *"Configuring DSC and WBC Display Options" on page 182* and *"DSC01/WBC Flasher Configuration" on page 65*)

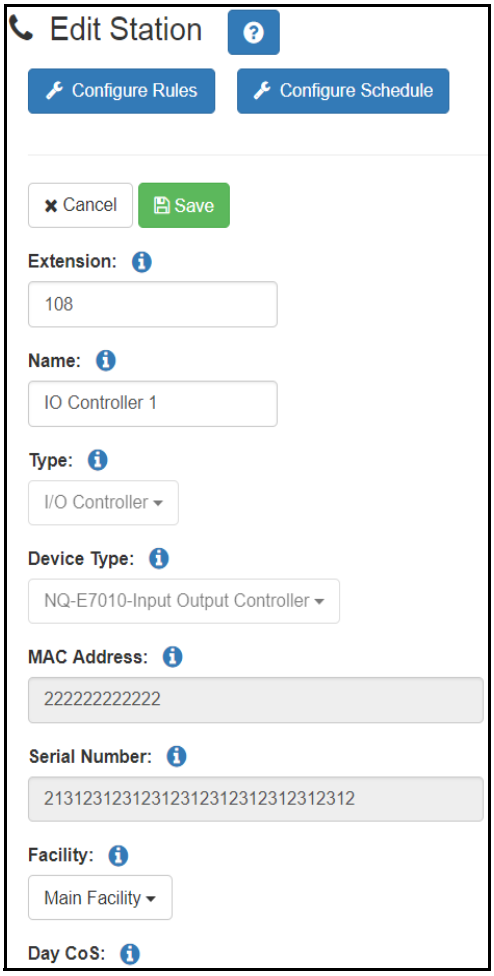


Figure 42. Edit Station Page

To edit a station's configuration settings:

1. From the navigation bar, select **Stations**.
2. Select the **Edit** icon for the station that you want to edit configuration settings.
3. Make desired changes. For information about the configuration settings, see *Table 43, "View, Add, or Edit Station Configuration Parameters," on page 143*.
4. Select **Save**.

Viewing I/O Controller Configuration Rules

The I/O Controller allows Nyquist to recognize third-party switch contact closures and to provide external circuits. Configuration rules can be set for each input and output port on an I/O Controller, so, for example, you can set a rule that if a contact is opened an alarm sounds, or set a rule that if a doorbell rings an Admin user can trigger another rule that opens the door.

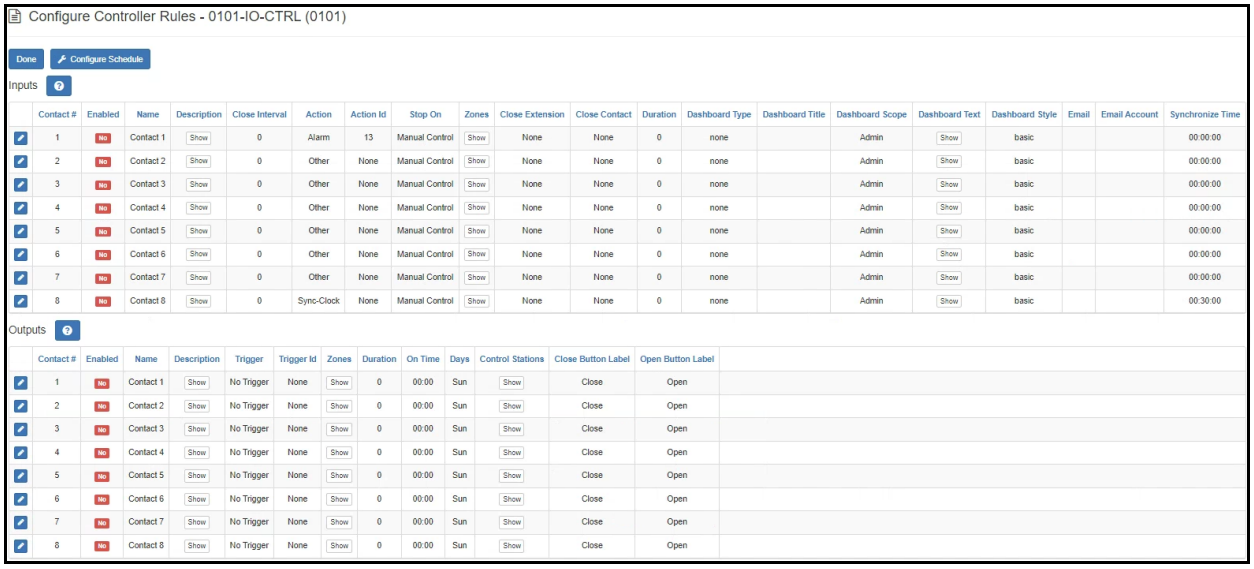


Figure 43. Configure Controller Rules Page

To view the configuration rules for an I/O Controller:

1. From the navigation bar, select **Stations**.
2. Select the **Edit** icon for the desired I/O Controller.
3. On the Edit Station page, select **Configure Rules**.
4. When finished viewing, select **Done**.

Table 45. Configure Controller Rules

Inputs	
Contact #	Displays the assigned number for this contact. This parameter is automatically set and cannot be edited.
Enabled	Indicates if a rule is enabled for this contact.
Name	Displays the user-provided name for the contact.
Description	Displays the user-provided description for the contact.
Close Interval	Displays how long the input contact must remain closed (in milliseconds) before the Action is started by the I/O Controller.

Table 45. Configure Controller Rules

Action	Displays the action, if any, that is to be taken when the contact is closed. Options are: • **Audio:** Starts the selected audio distribution specified by the Program Distribution field. *Note:* When an audio distribution is started, it can be set to stop when the input contact opens, or manually by using the Admin Web Interface or Admin Phone. • **Alarm:** Plays the alarm file selected by the **Action ID**. • **Announcement:** Plays the announcement file selected by the **Action ID**. • **Disable-Audio**: Disables all audio in the Nyquist system, performing the same action as when the **Disable Audio** button on the dashboard is selected. This action can be used by an external emergency system (for example, fire alarms) to disable all Nyquist audio, which includes: Audio Distribution, Tones, Alarms, Paging. *Note:* This contact closure action will only initiate the disabling of audio, it will not restore the audio. To restore audio, use a different contact with the action **Enable Audio**, or enable audio via an Admin Web Interface or Admin Phone. • **Other**: Used when you don't want to take one of the available actions, but you do want to close a contact, create a dashboard message, or send an email when the contact is closed. • **Tone**: Plays the tone file selected by the **Action ID**. • **Enable-Audio:** Enables all audio in the Nyquist system, performing the same action as when the **Enable Audio** button is selected on the dashboard. • **Sync-Clock**: Sets the Nyquist server's system time to the value specified in **Synchronize Time**.
Action ID	Displays identifier for action, such as an alarm or tone number. *Note:* This parameter is only available for Alarm, Announcement, and Tone actions.
Stop On	Specifies how the action is stopped. If set to **Manual Control**, you must manually stop the action. If set to **Contact Open**, the action automatically stops when the contact is opened.
Zones	Displays the zones that are affected by the action. *Note:* This parameter is only available for Alarm, Announcement, and Tone actions.
Close Extension	Specifies the target I/O Controller to use/operate.
Close Contact	Specifies contact number to close.
Duration	Displays duration of contact closure in milliseconds. A value of 0 means leave contact closed.
Dashboard Type	Specifies if the message appears in the dashboard message pane alone or also in a popup message.
Dashboard Title	Specifies the user-provided title that appears for the dashboard message.

Table 45. Configure Controller Rules

Dashboard Scope	Specifies which devices receive the message. Options are: • **All**: All web interface dashboards will receive the message. • **Admin**: Only Admin web interface dashboards will receive the message.
Dashboard Text	Specifies the user-provided text that appears for the dashboard message.
Dashboard Style	Specifies the icon and color coding that appear with the message. Options are: • Basic • Success • Info • Warning • Danger
Email	Specifies an email address for notification when an I/O contact is closed. *Tip:* To send a text message, use one of the email address formats described in *Table 135, "Email Address Formats for Cellular Carriers," on page 461*.
Email Account	Specifies the SMTP account to use for sending email.
Synchronize Time	If the Action is Sync-Clock, this field specifies the time to which the Nyquist clock should be set when the contact closes.

Outputs

Contact #	Displays the assigned number for this contact. This parameter is automatically set and cannot be edited.
Enabled	Indicates if a rule is enabled for this contact.
Name	Displays the user-provided name for the contact.
Description	Displays the user-provided description for the contact.

Table 45. Configure Controller Rules

Trigger	Displays the Nyquist system activity that will close the output contact when the activity starts, and will open the output contact when the activity stops. *Note:* If duration is greater than 0, the output contact opens after duration milliseconds even if the system activity is still ongoing. When a system activity is started, the output contact is closed; the contact is opened when the system activity ends. Options are: • **911**: A call to 911 has been initiated. • **Audio**: The selected Program Distribution has started playing. • **Alarm**: The selected Alarm has been activated. • **Announcement**: The selected Announcement has been started. • **All-Call**: An All-Call page has been started. • **Multi-Site-All-Call**: A Multi-Site All-Call page has been started. • **Multi-Site-Emergency-All-Call**: A Multi-Site Emergency All-Call page has been started. • **Emergency-Call**: An Emergency Call has been started. • **Emergency-All-Call**: An Emergency-All-Call page has been started. • **Hourly**: Close the contact hourly at the specified minute and second. • **Audio-Disabled**: Audio has been disabled. • **No Trigger**: This is the default trigger for outputs that have not yet been configured. • **Page**: A zone page has been started to the specified Zones. • **Tone**: The specified Tone has been started. • **Manual**: Creates a dashboard button that can be used to manually close or open specified output contact.
Trigger Id	Displays the Activity identifier for the output contact trigger (e.g., Alarm number).
Zones	Provides a list of paging zones that trigger an output. If blank, all zones are affected. *Note:* This field only appears when Trigger is set to **Page**.
Duration	Displays the duration of the contact closure in milliseconds. A value of 0 leaves the contact closed.
On Time	Specifies the minutes and seconds when the **Action** is set for **Hourly**. When set to 00:00, hourly closure is not enabled.
Days	Specifies the days of the week that the hourly closure of contact occurs.
Control Stations	Provides a list of stations that can manually control the output contact.
Close Button Label	Displays the user-provided label for the Dashboard button that is associated with the closing of an output contact. The duration for the contact must be set to 0 for this label to appear.
Open Button Label	Displays the user-provided label for the Dashboard button that is associated with the opening of an output contact. The duration for the contact must be set to 0 for this label to appear.

Configuring I/O Controller Input Rules

You can configure a unique input rule for each of the I/O Controller's eight inputs.

To configure an I/O Controller Input Rule:

1. From the navigation bar, select **Stations**.
2. Select the **Edit** icon for the desired I/O Controller.
3. On the Edit Station page, select **Configure Rules**.
4. Select the **Edit** icon for the input contact that you want to configure.
5. On the **Edit Controller Rule** page, complete the desired **Input Contact Rule Parameters** (see *Table 46, "Input Contact Rule Parameters," on page 162*).
6. Select **Save**.

Table 46. Input Contact Rule Parameters

Enabled	Indicates if a rule is enabled for this contact.
Contact Number	Displays the assigned number for this contact. This parameter is automatically set and cannot be edited.
Contact Type	Displays if the contact is an input or output contact. This parameter is automatically set and cannot be edited.
Extension	Displays the station extension. This parameter is automatically set and cannot be edited.
Name	Displays the user-provided name for the contact.
Description	Displays the user-provided description for the contact.
Close Interval	Specifies how long the input contact must remain closed (in milliseconds) before the Action is started by the I/O Controller.

Table 46. Input Contact Rule Parameters

Action	Specifies the action, if any, that is to be taken when the contact is closed. Options are: • **Audio:** Starts audio distribution to all stations (using previously selected playlist or matrix mixer input channel). *Note:* The I/O Controller can only be used to start audio distribution to all stations; it cannot stop the audio to all stations. Another method must be used to stop the audio such as selecting **Stop** from the Admin Web Interface or Admin Phone. • **Alarm:** Plays the alarm file selected as the **Action ID**. • **Announcement:** Plays the announcement file selected as the **Action ID**. • **Disable-Audio:** Disables all audio in the Nyquist system, performing the same action as when the **Disable Audio** button on the dashboard is selected. This action can be used by an external emergency system (for example, fire alarms) to disable all Nyquist audio, which includes: Audio Distribution, Tones, Alarms, Paging. *Note:* This contact closure action will only initiate the disabling of audio, it will not restore the audio. To restore audio, use a different contact with the action **Enable Audio**, or manually enable audio via an Admin Web Interface or Admin Phone. • **Other:** Used when you don't want to take one of the available actions, but you do want to close a contact, create a dashboard message, or send an email when the contact is closed. • **Tone:** Plays the tone file selected as the **Action ID**. • **Enable-Audio:** Enables all audio in the Nyquist system, performing the same action as when the **Enable Audio** button is selected on the dashboard. • **Sync-Clock:** Sets the Nyquist server's system time to the value specified in **Synchronize Time**.
Alarms	Specifies the alarm file that plays. *Note:* This parameter is only available for an Alarm **Action**.
Announcements	Specifies the announcement that plays. *Note:* This parameter is only available for an Announcement **Action**.
Tones	Displays the tone that plays. *Note:* This parameter is only available for a Tone **Action**.
Program Distribution	Specifies which audio distribution to play. *Note:* This parameter is only available if the **Action** is set to **Audio**.
Stop On	Sets how the **Action** is stopped. Options are: • **Manual Control:** You must manually stop the action. • **Contact Open:** Action automatically stops when the relevant input contact is opened.

Table 46. Input Contact Rule Parameters

Zones	Specifies the zone that is affected by the action. *Note:* This parameter is only available for Alarm, Announcement, and Tone actions, and only a single zone can be added for an input rule.
Synchronize Time	Specifies the time to which the Nyquist clock should be set when the relevant input contact closes.
Close Extension	Specifies which target I/O Controller to use/operate.
Close Contact	Specifies which contact number to close on the target I/O Controller.
Duration	Specifies duration of target output contact closure in milliseconds. A value of zero (0) means leave contact closed.
Dashboard Type	Specifies if the message appears in the dashboard message pane alone or also in a popup message.
Dashboard Title	Specifies the user-provided title that appears for the dashboard message.
Dashboard Scope	Specifies which devices receive the message. Options are: • **All:** All web interface dashboards will receive the message. • **Admin:** Only Admin web interface dashboards will receive the message.
Dashboard Text	Specifies the user-provided text that appears for the dashboard message.
Dashboard Style	Specifies the icon and color coding that appear with the message. Options are: • Basic • Success • Info • Warning • Danger
Email	Specifies an email address for notification when an input contact is closed. *Tip:* To send a text message, use one of the email address formats described in *Table 135, "Email Address Formats for Cellular Carriers," on page 461*.
Email Account	Specifies the SMTP account to use for sending email.

Configuring I/O Controller Output Rules

You can configure a unique output rule for each of the I/O Controller's eight outputs.

To configure an I/O Controller Output Rule:

1. From the navigation bar, select **Stations**.
2. Select the **Edit** icon for the desired I/O Controller.
3. On the Edit Station page, select **Configure Rules**.
4. Select the Edit icon for the output contact that you want to configure.
5. On the Edit Controller Rule page, complete the desired Output Contact Rule Parameters (see *Table 47, "Output Contact Rule Parameters," on page 165*).
6. Select **Save**.

Table 47. Output Contact Rule Parameters

Enabled	Select if a rule is to be enabled for this contact.
Contact Number	Displays the assigned number for this contact. This parameter is automatically set and cannot be edited.
Contact Type	Displays that the contact is an output contact. This parameter is automatically set and cannot be edited.
Extension	Displays the station extension. This parameter is automatically set and cannot be edited.
Name	Provide a name for the contact.
Description	Provide a description for the contact.

Table 47. Output Contact Rule Parameters

Trigger	Select the Nyquist system activity that will close the output contact when the activity starts, and will open the output contact when the activity stops. *Note:* If duration is greater than 0, the output contact opens after the specified number of milliseconds even if the system activity is still ongoing. When a system activity is started, the output contact is closed; the contact is opened when the system activity ends. Options are: • **911**: A call to 911 has been initiated. • **Audio**: The selected Program Distribution has started playing. • **Alarm**: The selected Alarm has been activated. • **Announcement**: The selected Announcement has been started. • **All-Call**: An All-Call page has been started. • **Multi-Site-All-Call**: A Multi-Site All-Call page has been started. • **Multi-Site-Emergency-All-Call**: A Multi-Site Emergency All-Call page has been started. • **Emergency-Call**: An Emergency Call has been started. • **Emergency-All-Call**: An Emergency-All-Call page has been started. • **Hourly**: Close the contact hourly at the specified minute and second. • **Audio-Disabled**: Audio has been disabled. • **No Trigger**: This is the default trigger for outputs that have not yet been configured. • **Page:** A zone page has been started to the specified Zones. • **Tone**: The specified Tone has been started. • **Manual**: Creates a dashboard button that can be used to manually close or open specified output contact.
On Time	Use the down arrows to select the **Minute** and **Second** if the **Trigger** is set for **Hourly**. When set to 00:00, hourly closure is not enabled.
Days	Specifies the days of the week that the hourly closure of contact occurs. This parameter appears only if the **Trigger** is set to **Hourly**.
Zones	Specifies which paging zones trigger the output contact closure if the **Trigger** is set to **Page**. If left blank, any zones started trigger the output contact closure.
Tones	Specifies which tone triggers the output contact closure when the **Trigger** is set to **Tone**.
Announcements	Specifies which announcement triggers the output contact closure when the Trigger is set to **Announcement**.
Alarms	Specifies which alarm triggers the output contact closure when the Trigger is set to **Alarm**.
Program Distribution	Specifies which audio distribution triggers the output closure when the Trigger is set to **Audio**.
Duration	Provide the duration of the contact closure in milliseconds. A value of 0 leaves the contact closed until the triggering event ends.

Table 47. Output Contact Rule Parameters

Control Stations	Select the stations that can manually control the output contact. A button for manually setting the output contact appears on the dashboard.
Close Button Label	Provide a label for the Dashboard button that is associated with the closing of an output contact. The duration for the contact must be set to 0 for this label to appear.
Open Button Label	Provide a label for the Dashboard button that is associated with the opening of an output contact. The duration for the contact must be set to 0 for this label to appear.

Sample I/O Controller Configuration Rules

The following sections describe scenarios that can be achieved using I/O Controller Configuration Rules.

Using Nyquist to Open a Secured Door

One example of the configuration and use of the I/O Controller is the opening of a secured, or locked, door. The I/O Controller can be connected to a doorbell that, when pressed, sends a dashboard message to Admin Stations that someone wants to gain access through a secured door. You or other Admin users can then select an **Activate** button that unlocks the door and allows entry to the secured area.

In this example, the dry contact connection of the doorbell would be wired to an I/O Controller input terminal and the secured door's relay driver would be wired to an I/O Controller's output terminal. (Refer to NYQUIST Input/Output Controller NQ-E7010 Installation and Use.)

Follow the steps for configuring an I/O Controller Input Configure Rule (see *"Configuring I/O Controller Input Rules" on page 162*) using the following parameters:

- For **Close Interval**, enter how long (in milliseconds) the input contact must remain closed before the input action is triggered.
- For **Action**, select **Other**.
- For **Close Extension**, select that extension, or station number, for the I/O Controller connected to the output contact that, when closed, will open the door.
- For **Close Contact**, select the **Output Contact #** that is to be closed when Activate is pressed on the dashboard message.
- For **Duration**, enter the number of milliseconds required for the door open circuit to open the door.
- For **Dashboard Type**, select **io-contact**.
- For **Dashboard Title**, enter a title for the dashboard popup message (for example, **Front Door**).
- For **Dashboard Text**, enter the message that you want displayed on the dashboard popup message (for example, **Front doorbell activated; press "Activate" to open the front door**.
- For **Dashboard Style**, select **basic**.

When configured properly, the doorbell sounds and a message appears when the doorbell is pressed.

Figure 44. Example of Dashboard Message

If you select **Activate**, the door opens. If you select **Ignore**, the door remains closed and the popup message disappears.

Synchronizing Nyquist Server Time to an I/O Input Contact Closure

An I/O Controller Input Contact can be used to synchronize the Nyquist server's clock to a specified time whenever the I/O Input Contact is closed.

You can create an I/O Controller Input Rule using action **Sync-Clock**, defining the **Synchronize Time** property as the value (i.e., time) to which the Nyquist system clock should be set when the I/O Contact closes. The **Synchronize Time** field is expressed in 24-hour military time format: HH:MM:SS.

For example, if the **Synchronize Time** is defined as "23:00:00", when the I/O Contact closes, the Nyquist server's system clock will be set to 23:00:00 (or 11:00:00 p.m.).

Caution	Only the time will be set on the Nyquist server, not the date. This could cause issues if the contact closure occurs shortly before or after 00:00:00 (server time), as clock drift may result in a different date than intended. For best results, set the **Synchronize Time** at least several minutes before or after midnight.

Important:	Set the Input Contact's **Close Interval** to at least 1000 (1 second) to compensate for the 1-second delay when setting the **Synchronize Time** field. Setting the clock happens very fast, the only delay you should see is the Close Interval delay.

Viewing an I/O Controller Schedule

You can view all contact closures set for specific dates and times using the Configure Schedule button on the I/O Controller's Edit Station page. For information about scheduling a output contact event, *see "Adding an I/O Contacts Output Daily Schedule" on page 169*.

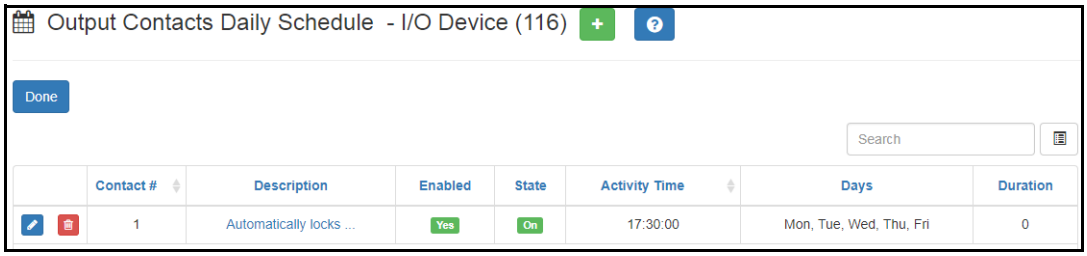


Figure 45. Output Contacts Daily Schedule – I/O Device Page

To view contact closure schedules for an I/O Controller:

1. On the navigation bar, select **Stations**.
2. Select the **Edit** icon for the desired I/O Controller.
3. On the Edit Station page, select **Configure Schedule**.
   The I/O Contacts Output Daily Schedule page appears.

Table 48. I/O Contacts Output Daily Schedule Page

Contact #	Displays the assigned number for the contact. This parameter is automatically set and cannot be edited.
Description	Displays the user-provided description for the contact.
Enabled	Indicates if a contact activity event is enabled.
State	Displays if the closure is open or closed.
Activity Time	Displays the time to change the contact event in HH:MM:SS format.
Days	Displays the day or days of the week that the event is to be executed.
Duration	Displays the duration of the contact closure in milliseconds. A value of 0 means that the contact remains closed until an open event occurs.

Adding an I/O Contacts Output Daily Schedule

Contact closures can be set for specific dates and times using the **Configure Schedule** button on the I/O Controller's Edit Station page. For example, suppose you want to schedule an output that unlocks a door at 7:30 each weekday morning. You can set up an output contact closure schedule for 7:30 a.m. Monday through Friday. When the Activity Time occurs, the contact is closed, which in turn triggers a third-party contact switch that unlocks the door.

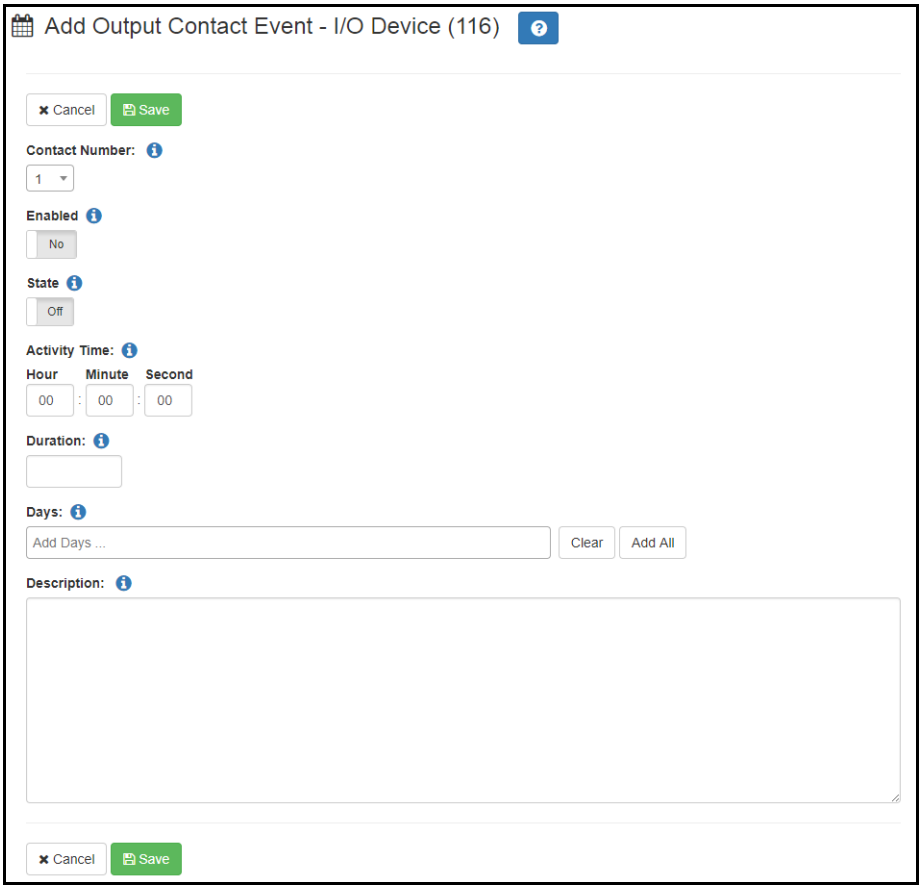


Figure 46. Add Output Contact Event Page

To add an output daily schedule for an I/O contact:

1. On the navigation bar, select **Stations**.
2. Select the **Edit** icon for the desired I/O Controller.
3. On the Edit Station page, select **Configure Schedule**.
4. On the I/O Contacts Output Daily Schedule page, select the **Add** icon.
5. Complete the parameters on the Add I/O Contact Output Event page (*Table 49, "Add or Edit I/O Contact Output Event Parameters," on page 170*).
6. Select **Save**.

Table 49. Add or Edit I/O Contact Output Event Parameters

Contact #	Select the contact number for this contact.
Enabled	Select to enable the contact activity event.
State	Select the state for this new output event from the drop-down menu. Options are: • On: The contact is closed. • Off: The contact is open.

Table 49. Add or Edit I/O Contact Output Event Parameters (continued)

Activity Time	Enter the time to change the contact event, using the down arrows to make the appropriate selections in the **Hour**, **Minute**, and **Second** fields.
Duration	Enter the duration of the contact closure in milliseconds. A value of 0 means that the contact remains closed until an open event occurs.
Days	Enter the day or days of the week that the event is to be executed.
Description	Enter a description for the contact event. This field is required.

Editing the Daily Schedule for an I/O Contact

The Edit Output Contact Event - I/O Controller page allows you to change the parameters, such as duration, for an I/O contact's daily schedule.

To edit an output daily schedule for an I/O contact:

1. On the navigation bar, select **Stations**.
2. Select the **Edit** icon for the desired I/O Controller.
3. On the Edit Station page, select **Configure Schedule**.
4. On the I/O Contacts Output Daily Schedule page, select the **Edit** icon next to the contact that you want to edit.
5. Make desired changes to the Edit I/O Contact Output Event page. (For information about the parameters for this page, see *Table 49, "Add or Edit I/O Contact Output Event Parameters," on page 170*.)
6. Select **Save** to return to the I/O Contact Output Daily Schedule page.

Deleting an I/O Contacts Output Daily Schedule

You can delete an output contacts daily schedule that is no longer needed from the station's Output Contacts Daily Schedule page.

To delete an output daily schedule for an I/O contact:

1. On the navigation bar, select **Stations**.
2. Select the **Edit** icon for the desired I/O Controller.
3. On the Edit Station page, select **Configure Schedule**.
4. On the I/O Contacts Output Daily Schedule page, select the **Delete** icon next to the contact that you want to delete.
5. When prompted, select **Delete**.

Configuring Devices for Push-To-Talk

Push-To-Talk (PTT) functionality can be configured for the Matrix Mixer Pre-Amp and the GA10P/GA10PV Intercom Modules.

Push-To-Talk Configuration for a Matrix Mixer Pre-Amp (MMPA)

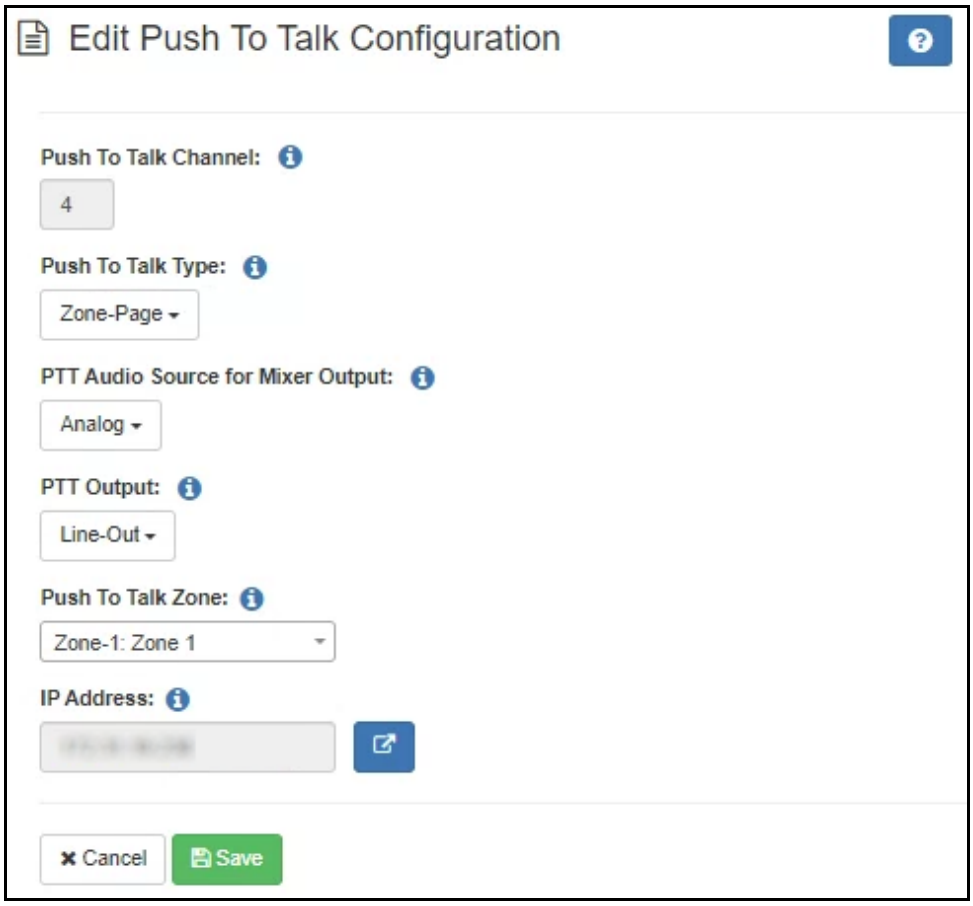


Figure 47. Push-To-Talk Configuration Page (MMPA)

To edit Push-To-Talk configuration for a Matrix Mixer Pre-Amp:

1. On the navigation bar, select **Stations**.
2. Select the **Edit** icon for the Matrix Mixer Pre-Amp that you want to configure.
3. Select **Configure PTT**.
4. Specify parameters from the Edit Push To Talk Configuration page. For details, see *Table 50, "MMPA Push-To-Talk Configuration Parameters," on page 173*.
5. Select **Save**.

Table 50. MMPA Push-To-Talk Configuration Parameters

Push To Talk Channel	Channel 4 is the only available PTT channel.
Push To Talk Type	Select the type of activity that is performed when the button is pressed on the microphone. Options are: • Disabled • Analog-Output • All-Call-Page • Emergency-All-Call-Page • Zone-Page • Record-Zone-Page • Multi-Site-All-Call-Page • Multi-Site-Emergency-All-Call-Page *Note:* For all selections other than **Disabled**, the DSP Router settings of the device are overridden to route the PTT microphone input signal (**Analog 4**) to the output channel (**Analog 1**). *Tip:* To prevent the PTT microphone signal from being sent to the network, select Analog-Output. All other settings (other than Disabled) will send the PTT microphone signal over the network.
PTT Audio Source for Mixer Output	*Note:* This field does not appear if **Push To Talk Type** is set to **Disabled** or **Analog-Output**. Specifies whether the PTT microphone signal is sent to the network output or both the analog and network outputs. If **Analog** is selected, the PTT microphone input is routed as specified in the **PTT Output** setting as well as being sent over the network. If **Network** is selected, the PTT microphone input is routed only through the network. Note that this could create a small but noticeable delay.
PTT Output	Selects the output used for locally playing PTT-initiated paging if either **Push To Talk Type** is Analog-Output or **PTT Audio Source for Mixer Output** is Analog. Options are: • Disabled • Line-Out
Push To Talk Zone	*Note:* This field appears only if **Push To Talk Type** is set to **Zone-Page**. Select the zone to receive the page.
IP Address	Displays the IP address of the device, if known, and a **Link** button that allows you to start the device's UI. If the Nyquist server has not discovered the device's IP address, the **Link** button does not appear.

Push-To-Talk Configuration for GA10P or GA10PV Intercom Module

If you have added an NQ-GA10P or NQ-GA10PV Intercom Module with a station type of Push-To-Talk Microphone, you can select the type of page that can be made when the PTT microphone is active.

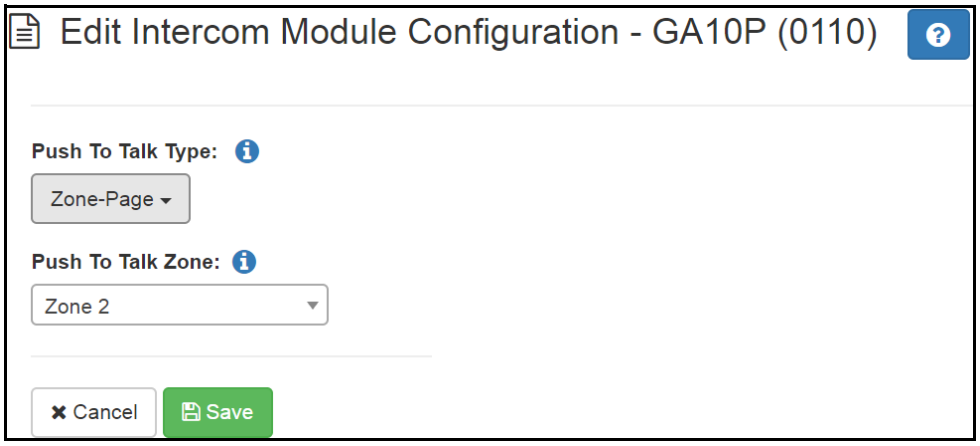


Figure 48. Edit Intercom Module Configuration

To edit an intercom module:

1. On the navigation bar, select **Stations**.
2. Select the **Edit** icon for the intercom module that you want to configure.
3. Select **Configure Intercom Module**.
4. Specify parameters from the Edit Intercom Module Configuration page (see *Figure 51, "Edit Intercom Module Configuration Parameters," on page 174*).
5. After making your edits on the Edit Intercom Module Configuration page, select **Save**.

Table 51. Edit Intercom Module Configuration Parameters

Push To Talk Type	Select the type of pages that can be made from the microphone. The available options are: • All-Call-Page • Emergency-All-Call-Page • Zone-Page • Record-Zone-Page • Multi-Site-All-Call-Page • Multi-Site-Emergency-All-Call-Page
Push To Talk Zone	Use the drop-down arrow to select a zone to receive the page. Only one zone can be selected. *Note:* This option is only available when **Push To Talk Type** is Zone-Page or Record-Zone-Page.

Configuring Ambient Noise Sensor

The Ambient Noise Sensor (ANS) ensures that page announcements and music are audible even during periods of high noise levels by continuously monitoring the ambient noise level through a microphone module and adjusting the paging signal level for that area's amplifier channel.

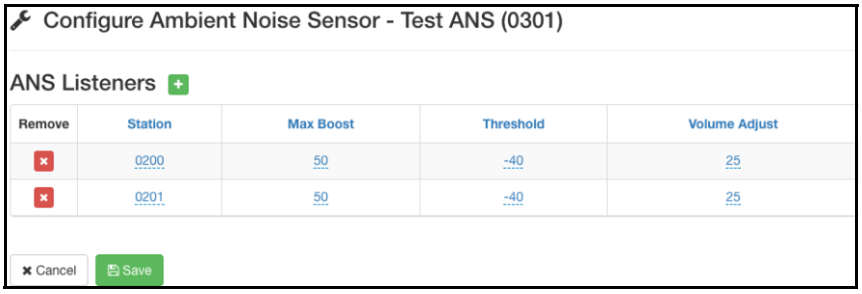


Figure 49. Configure Ambient Noise Sensor

This feature requires that an ANS500M Ambient Sound Microphone be attached to an intercom module station type. For installation instructions, refer to the NQ-GA10P, NQ-GA10PV VoIP Intercom Module Installation and Use manual.

You must set the **Ambient Noise Sensor Multicast IP Address** and **Ambient Noise Sensor Multicast Port** system parameters (see *"Setting System Parameters" on page 67*).

Then, create a station with **Station Type** as Ambient Noise Sensor and **Device Type** as **NQ**-GA10P-Intercom Module or NQ-GA10PV-Intercom HDMI Module (see *"Adding a Station" on page 185*).

To configure ANS parameters:

1. On the navigation bar, select **Stations**.
2. Select the **Edit** icon for the Ambient Noise Sensor station.
3. Select **Configure**.
4. Select the **Add** icon to add an ANS Listener.

   An ANS Listener is a station that will receive Sound Pressure Level (SPL) reports from the ANS. For example, suppose you have speakers in a warehouse area that you want the volume to automatically adjust when noisy machines are operating. You would add the speaker stations as ANS Listeners. When the SPL in the warehouse increases, the ANS reports the increase to the ANS Listeners and the speakers' volumes are adjusted automatically.
5. Set the ANS parameters for the ANS Listener.
6. If you want to remove a station from the ANS Listener list, select the **Remove** icon on the station's row.

7 When all edits are made, select **Save**.

Table 52. Configure Ambient Noise Sensor Parameters

Station	Displays the extension number of the station that is an ANS Listener. A station can only listen to one ANS.
Max Boost (dB)	Displays the maximum dB gain adjustment allowed. Setting this parameter to –42 disables any volume adjustments from the ambient noise sensor. The default value is 0 dB.
Threshold (dBFS)	Displays the *decibels relative to full scale* (dBFS) value at which the device will adjust the volume to compensate for the increased ambient noise volume. This value should be between –42 and 0 dBFS. A fairly noisy environment is approximately –20 dBFS. Quiet environments are approximately –42 dBFS. The default value is –24 dBFS.
Volume Adjust (dB)	Displays the amount of decibels to stay above the ambient noise level. Setting this to 0 disables any volume adjustments from the ANS. The default value is 12 dB.
Sample Length(s)	Displays the ambient noise sampling length, which can range from 1 to 20 seconds. Short lengths provide quicker response to changes in the ambient noise; longer lengths will ignore sudden, short fluctuations in the ambient noise.

Configuring Intercom HDMI Module Display Options

Note: When a NQ-GA10PV boots up, it queries the attached display and sets the display mode settings to the highest compatible setting (1080@30Hz or 1080@24Hz). If the display does not support either of those settings, the attached display is set to the highest non-compatible setting and a message appears that lists this unsupported resolution and the resolutions that are supported.

If you have a NQ-GA10PV Intercom HDMI Module **Device Type**, you can set display types for the connected monitor, including the type of clock and display colors that appear.

Options configured for the station affect the overall appearance of the display, such as the background color for the display and fonts used to display date and event. Options for specific messages are set through the **Display Message** option on the dashboard (see *"Creating a Display Message via the Dashboard" on page 501*).

You can also configure it to automatically display the check-in status map during an active check-in process (e.g., a lockdown), allowing staff and emergency personnel to quickly and easily view check-in status information. To enable the check-in status map, set **Check-In Enabled** to **Yes** on the GA10PV's *Display Configuration* page. You can also select what will be displayed during the check-in process; the available configuration settings are similar to those available on the Manage Check-In page (see *"Manage Check-In" on page 523*).

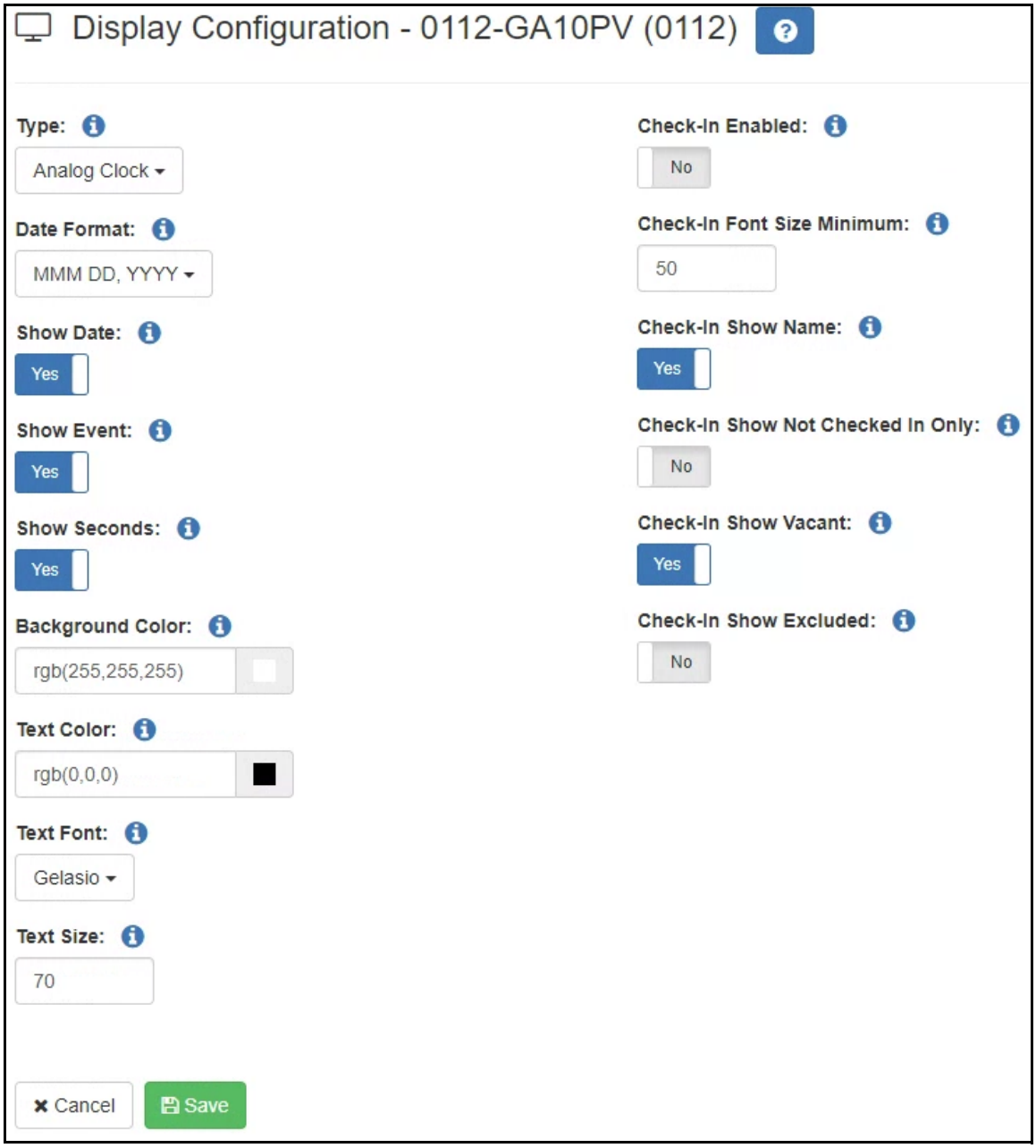


Figure 50. Display Configuration for GA10PV Station

To configure display options:

1. On the navigation bar, select **Stations**.
2. Select the **Edit** icon for the intercom HDMI module that you want to configure.
3. Select **Display Configuration**.
4. After making your edits on the Display Configuration page, select **Save**.

Table 53. Display Configuration

Type	Select one of the five layouts available: • **Analog Clock**. Displays an analog clock on the left side of the display screen. • **Digital Clock**. Displays a digital clock on the top of the screen. • **Messages 1 Column**. Displays messages only in a single column. • **Messages 2 Columns**. Displays messages only in two columns. • **Messages 3 Columns**. Displays messages only in three columns.
Date Format	Select the format for displaying the date. Available formats are: • DDD, MMM DD • MMM DD, YYYY • DD MMM YY • DD MMM YYYY • DD/MM/YY • DD/MM/YYYY • MM/DD/YY • MM/DD/YYYY
Show Date	Use the slider to select if the date will be displayed.
Show Event	Use the slider to select if the scheduled events will be displayed. (See *"Understanding Event Settings" on page 271*.)
Show Seconds	Use the slider to select if seconds will be displayed on the clock.
Background Color	Select a background color for the display. You can select a color by: • Using the color picker • Entering a hex color (for example: #000000, for black) • Entering an RGB color (for example: rgb(0,0,0) for black) • Entering a color alias name (for example: red, blue, etc.) For more information, see *"Using Color in Display Messages" on page 505*.
Text Color	Select a color for the text. You can select a color by: • Using the color picker • Entering a hex color (for example: #000000, for black) • Entering an RGB color (for example: rgb(0,0,0) for black) • Entering a color alias name (for example: red, blue, etc.) For more information, see *"Using Color in Display Messages" on page 505*.

Table 53. Display Configuration

Text Font	Select a font for the text from the drop-down list. Available fonts are: Comic-Relief Courier-Prime Gelasio Liberation Sans Linux Libertine
Text Size	Enter the text size. This value is based on font points, with 72 points being an inch.
Time Format	Select whether the time is to appear in 12 or 24 hour format.
Time Color	Select the color for the time display. You can select a color by: • Using the color picker • Entering a hex color (for example: #000000, for black) • Entering an RGB color (for example: rgb(0,0,0) for black) • Entering a color alias name (for example: red, blue, etc.) For more information, see *"Using Color in Display Messages" on page 505*.
Time Font	Select a font for the time from the drop-down list. Available fonts are: Comic-Relief Courier-Prime Gelasio Liberation Sans Linux Libertine
Time Size	Select the font size for the time. This value is based on font points, with 72 points being an inch.
Check-In Enabled	If set to **Yes**, the GA10PV will automatically display check-in status during an active check-in procedure while disabling the display of clock and messages.
Check-In Font Size Minimum	The Minimum Font Size specifies the minimum font size to use during scaling (do not scale below the minimum specified value). Stations displayed on the check-in status screen will automatically be scaled in an attempt to fit as many stations on the available screen space as possible. The minimum font size can help ensure that the font is large enough to read the station list from the anticipated viewing distance while attempting to fit as many stations on the display as possible. This value is based on font points, with 72 points being an inch.

Table 53. Display Configuration

Check-In Show Name	If set to **Yes**, station names will be displayed under the station extension. Hiding station names may allow you to fit more stations on the screen.
Check-In Show Not Checked In Only	If set to **Yes**, stations that have not checked in will be displayed, while stations that have checked in will not be displayed. This option can help fit more stations on the screen.
Check-In Show Vacant	If set to **Yes**, stations that are marked as vacant will also be displayed. If a vacant station checks in, it will be displayed as checked-in (green) instead of vacant.
Check-In Show Excluded	If set to **Yes**, stations that are excluded from the check-in process will also be displayed.

If you select to use an analog clock, the clock appears on the left side of the HDMI connected display and messages appear on the right side. If you select to use a digital clock, the time appears on the top of the display and the messages appear beneath.

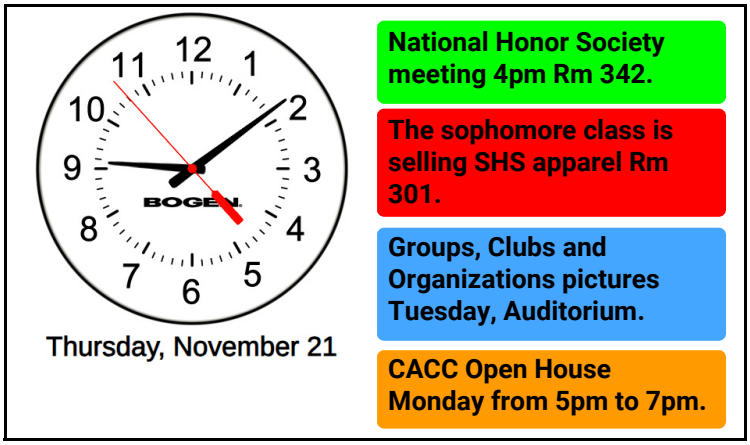


Figure 51. Example of Display with Type *Analog Clock*

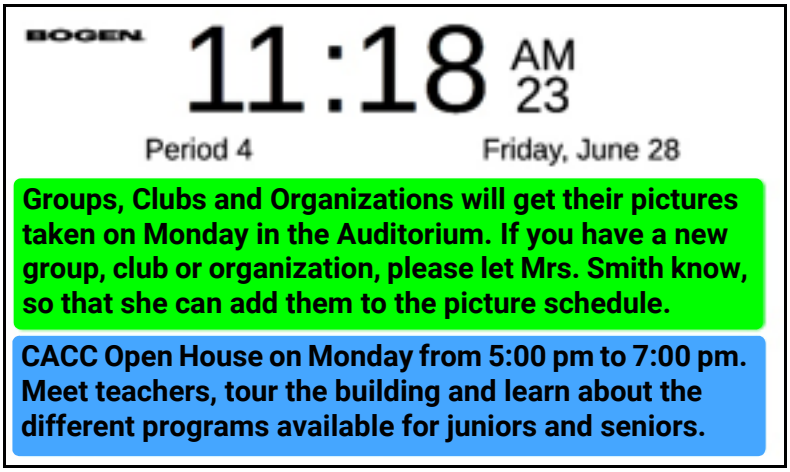


Figure 52. Example of Display with Type *Digital Clock*

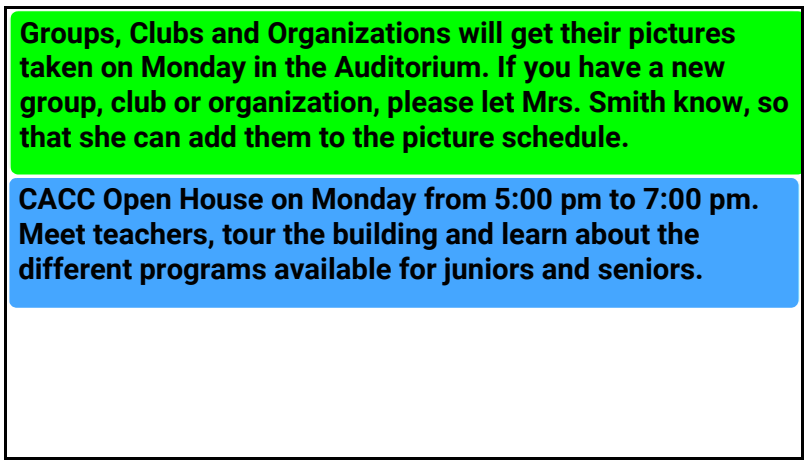


Figure 53. Example of Display with Type *Messages 1 Column*

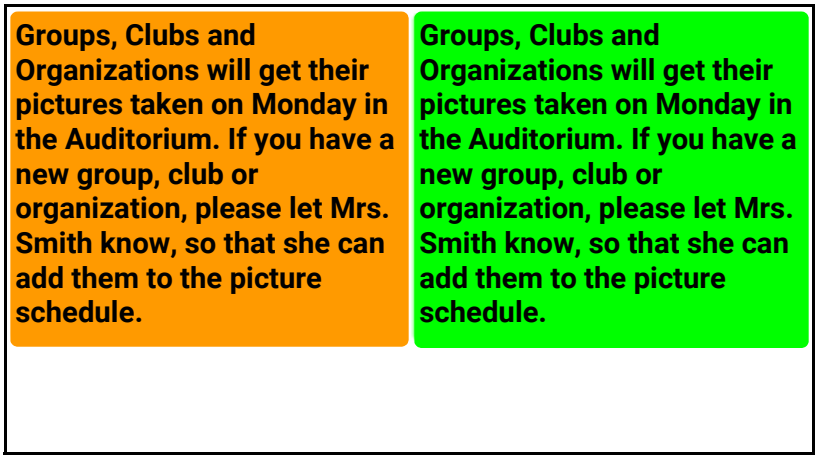


Figure 54. Example of Display with Type *Messages 2 Columns*

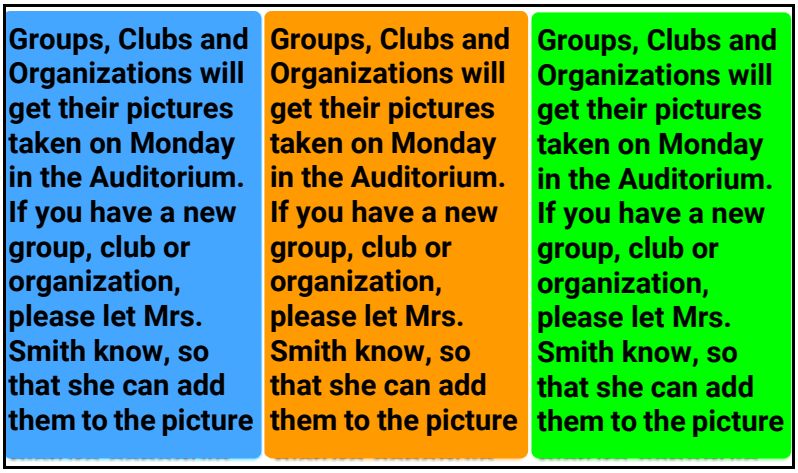


Figure 55. Example of Display with Type *Messages 3 Columns*

If **Check-In Enabled** is set to **Yes**, the check-in status of the relevant stations will be displayed on GA10PV devices during active Check-In processes. For details, see *"Managing Check-In Status" on page 523*.

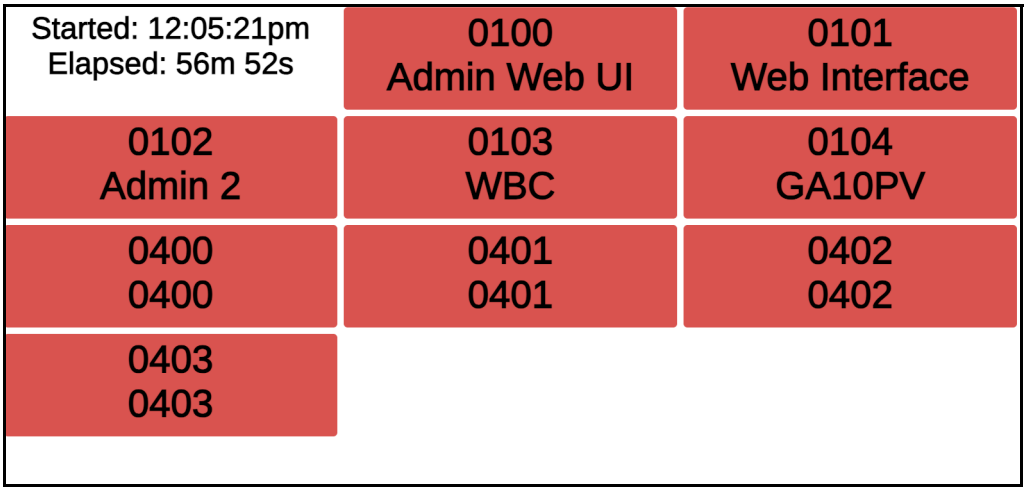


Figure 56. Example of Check-In Status (Check-In Enabled set to Yes, during Check-In process)

Configuring DSC and WBC Display Options

The NQ-DSC01 and NQ-S1810WBC include an LED display and flasher (as well as a clock for the NQ-DSC01), each of which have several configurable settings. These settings can be configured via the *Display Configuration* page or via a Routine, which might be executed in response to a System Event (e.g., Emergency All-Call, etc.) or as part of a calendar schedule (see *"Adding a Schedule" on page 264*) or as a scheduled routine (see *"Add a Scheduled Routine" on page 285*).

Important:	Be aware that both the NQ-DSC01's and NQ-S1810WBC's LED displays can only display uppercase characters. Lowercase characters are allowed as input, but will display as uppercase.

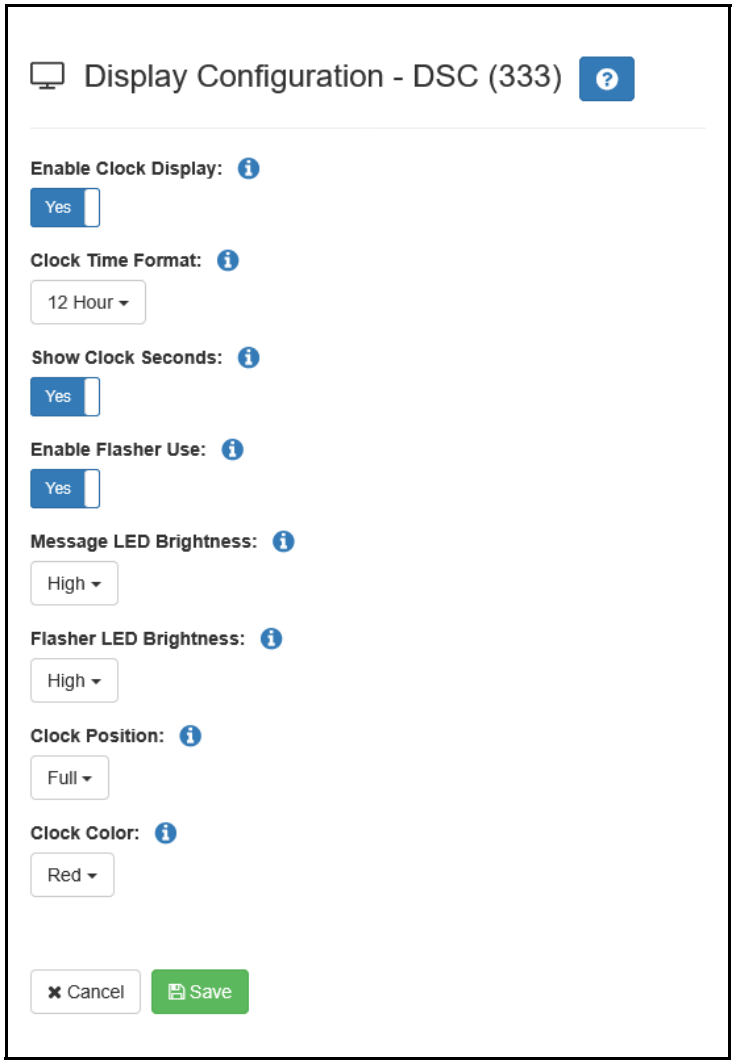


Figure 57. Display Configuration

To configure the LED display and flasher:

1. On the navigation bar, select **Stations**.
2. Select the **Edit** icon for the NQ-DSC01 or NQ-S1810WBC device that you want to configure.
3. Select **Display Configuration**.
4. Complete the configuration parameters for the station. Parameters are described in *Table 54, "Display Configuration," on page 183*.

Table 54. Display Configuration

Enable Clock Display	Specify **Yes** if the clock will be enabled (i.e., displayed) or **No** if it will be disabled (i.e., hidden). When the clock is disabled, the WBC can still be used to display messages and LED flashers.
Clock Time Format	Specify **12 Hour** to display the clock in AM/PM format or **24 Hour** to display the clock in 24-hour (i.e., military time) format.

Table 54. Display Configuration

Show Clock Seconds	Specify **Yes** to display seconds or **No** to hide them.
Enable Flasher Use	Select **Yes** to enable the LED flasher or **No** to disable it. If disabled, the LED flasher will never be illuminated, even if requested.
Message LED Brightness	Specify the brightness level of the red message LEDs on the display. Valid values are: • Off • Low • Medium • High
Flasher LED Brightness	Specify the brightness level of the message LEDs. Valid values are: • Low • Medium • High
Clock Position (NQ-DSC01 only)	Specify the screen position of the displayed clock. The available options are: • Top • Full • Bottom
Clock Color (NQ-DSC01 only)	The color of the displayed clock. The available options are: • Amber • Blue • Blue Violet • Cyan • Deep Pink • Green • Indigo • Lime • Magenta • Ocean • Orange • Pink • Red • Spring Green • Turquoise • Violet • White • Yellow • Yellow Green

Deleting a Station

Note: You cannot delete a station that is used in a routine action (see *"Understanding Action Parameters" on page 460*).

When you delete a station, all of its settings are deleted and the station will not be able to register with the Nyquist system server. If it is an Admin Station, you may not be able to delete it until you delete all

associations that the Admin Station has (for example, member of Day Admin, Night Admin, Night Ring, or Admin Group).

After you delete a second station from an SPA112 or ATA191/192-3PW-K9 Analog Telephone Adapter (ATA), the Nyquist system server reboots the ATA device. If the Nyquist system server does not know the ATA device's IP address, you must reboot the device for the changes to take effect on that device.

When a station is deleted from an ATA device, it can take several minutes for the changes to show up on the device's web interface. When the second station is deleted from the device, the remaining station is set up on the first port (Phone 1) even if that station was previously set up on the second port (Phone 2). If this situation occurs, move the attached phone cable from Phone 2 to Phone 1.

To delete a station's configurations:

1. On the navigation bar, select **Stations**.
2. Select the **Delete** icon for the station that you want to delete configuration settings.
3. When prompted, select **Delete**.

Adding a Station

Using the Nyquist system server's TFTP-based automatic discovery and configuration feature is the preferred method of adding a station. If you manually add a station, you risk having the MAC address entered incorrectly, which would prevent the station from functioning properly.

Important: If TFTP-based discovery is not possible, we recommend that stations be added using the "*Appliance Discovery Wizard*", as described on page 138.

To view and add discovered stations:

1. On the navigation bar, select **Stations**.
2. On the *Stations* page, select **New Stations**.
3. From the *New Stations* page, select the **Add** icon next to the newly detected appliance that you want to configure.

Tip: If the new appliance is not shown, make sure the appliance has an IP address and is configured to use this C4000 (e.g., by enabling the C4000's DHCP server or configuring option 66 of the DHCP server with the IP address of the C4000), then try rebooting it.

Important: Non-Nyquist devices, such as phones, do not appear under **New Stations**. Stations can be manually added and configured for these devices by specifying the MAC address of each. Once added, the phone can be connected to the network, where it can use the TFTP auto-configuration feature to download the configured Station settings.

4 Complete the configuration parameters that are not automatically configured. Parameters are described in *Table 43, "View, Add, or Edit Station Configuration Parameters," on page 143*.

Note: If this new appliance is replacing an existing one, see *"Swapping a Nyquist Device" on page 186*.

5 When prompted, enter the Web Interface password.

6 Select **Save**.

To manually add a station:

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

2 Select the **Add** icon.

3 Complete the configuration parameters for the new station. Parameters are described in *Table 43, "View, Add, or Edit Station Configuration Parameters," on page 143*.

Important: Make sure to select the correct **Station Type** and **Device Type**, as these cannot be modified for most appliance types once the station has been created.

Tip: Some **Device Type**-specific options are not available while adding the device (see *Table 44, "Station Type-specific Configuration Options," on page 156*). To access these options, add the new device, then edit its settings (see *"Editing Station Configuration Settings" on page 155*).

4 Select **Save**.

Swapping a Nyquist Device

Through the **New Stations** option, you can replace an existing device with an identical replacement device. This option allows you to replace a device, such as VoIP speaker, with a new device of the same type and maintain the original device's extension and configuration.

Note: You can replace a VoIP speaker with a VoIP speaker G2 and replace a VoIP speaker G2 with a VoIP speaker G2, but you cannot swap a VoIP speaker G2 with an earlier generation VoIP speaker.

You can also use the **New Stations** option to replace an audio power amplifier with another amplifier, regardless of type. For example, you can replace an NQ-A2060 amplifier with an NQ-A2300 amplifier. You can also replace an earlier generation 2- or 4-channel amplifier with a later generation amplifier, assuming the number of channels is the same. For example, you can replace an NQ-A2060 with an NQ-A2300 G2.

Select **Swap** under the **Action** column to switch a discovered appliance for an appliance that was previously added to the database but now needs to be removed. For example, the old device may have stopped working and new hardware is replacing the broken device.

Tip: If possible, upgrade both the original and replacement devices' firmware to the latest version before swapping in the new device. This will improve compatibility and help ensure the conversion will be successful. This is particularly important for pre-1.2.1647 firmware releases, for which the configuration will not be preserved.

Using a Cisco SPA112 or ATA191/192 Analog Telephone Adapter

The Cisco SPA112 and ATA191/192-3PW-K9 Analog Telephone Adapters (ATAs) allow an analog phone to access IP phone services through two standard telephone RJ-11 phone ports.

The following limitations exist when a Cisco ATA is used as a Nyquist Admin Phone station:

- Call queuing is not supported.
- Call waiting is limited to one call. If the Admin Phone is associated with an Admin Group, a call made to the Admin Phone when the phone is already on a call will automatically ring the Admin Group. If the Admin Phone is not associated with an Admin Group and receives a call when already on a call, a beep sounds on the Admin Phone to indicate a call is on call waiting.
- When you add two stations to an ATA device, you must enter the same MAC address for both ports.
- The station number with the lowest numerical value will be set up on the first port (Phone 1) of the SPA112.
- After you add or delete a second station to or from the ATA device, the Nyquist system server reboots the device. If the Nyquist system server does not know the device's IP address, you must manually reboot the device for the changes to take effect on that device.
- When a station is added to the ATA device, the web password is changed to **bogen**. You can change the web password when adding or editing the station.
- If you configure two stations on the same ATA device, the web password is set to the station with the highest station number, even if the other station has a different web password defined. Ensure that the same web password is entered for both stations on the ATA device.
- When you delete the second station from the ATA device, the remaining station is set up on the first port (Phone 1) even if that station was previously set up on the second port (Phone 2). If this situation occurs, move the attached phone cable from Phone 2 to Phone 1.
- When you configure two stations on the same ATA device, the second station (Phone 2) uses port 5061.
- It can take several minutes for changes to show up on the ATA device's web interface when adding, modifying, or deleting stations to or from the device.
- When you add a station to an ATA device for the first time, you must reboot the device after adding the station with the Nyquist web UI before the device will retrieve its configuration information.
- If station VLAN settings are provided and two stations are defined on the ATA device, the VLAN settings from the station with the lowest station number are used. The best practice is to ensure that both stations on the SPA112 use the same VLAN settings.

Tip: Refer to the *Cisco Small Business SPA100 Series Phone Adapters Administration Guide* or the *Cisco ATA 191 and ATA 192 Analog Telephone Adapter Administration Guide for Multiplatform Firmware* for instructions on connecting the ATA.

To add a Cisco SPA112 or Cisco ATA191/192-3PW-K9 station:

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

2 Select the **Add** icon.

Note: If **Use Network Time Server defined by DHCP** is set to Yes on the Nyquist system server, the Cisco ATA device's NTP server configuration is not changed; otherwise the device's NTP server is set to the Nyquist system server's defined NTP server.

---

3 Complete the configuration parameters for the new station:

a) For **Type**, select **Admin Phone** or **IP Phone**.

b) For **Device Type**, select **Cisco SPA112** or **Cisco ATA191/192-3PW-K9**.

c) For **MAC Address**, enter the MAC address of the Cisco SPA112 or Cisco ATA191/192-3PW-K9.

Note: The MAC address can be found on the Voice → Information tab of the device's Phone Adapter Configuration Utility (see subsequent steps).

---

d) For **Dial Plan Type**, select **Custom**, and for **Dial Plan**, specify the following value:

```
S:5,(911|91x.|*92x.|*94x.|*96x.|##0911S0|#0911S0|#x.|*xxx|#xxx|987*x.|98x.|*x.|*990|*991x.|
7*x.|971x.|972x.|973x.|974x.|978x.|xxx|##x.#x.|##*x.x.|904x.|904x.|3*xxxx*xxx.|942#x.#x.|94
3#x.#x)
```

For all other parameters, see *Table 43, "View, Add, or Edit Station Configuration Parameters," on page 143*.

4 If you would like to create a second station for this ATA device (it supports up to two lines), repeat the previous steps, providing the same MAC address but a different extension.

5 Select **Save**.

6 From your web browser, enter the IP address of the Cisco SPA112 or Cisco ATA191/192-3PW-K9 device.

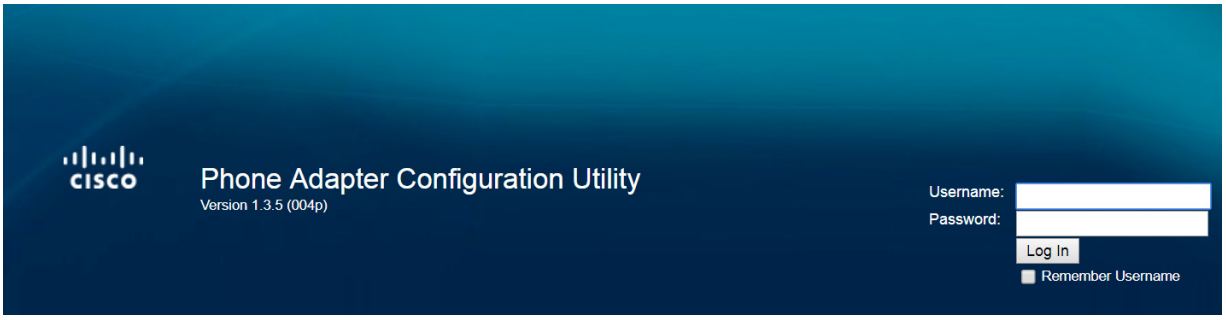


Figure 58. Cisco SPA112 or Cisco ATA191/192-3PW-K9 Login Window

7 Log into the device.

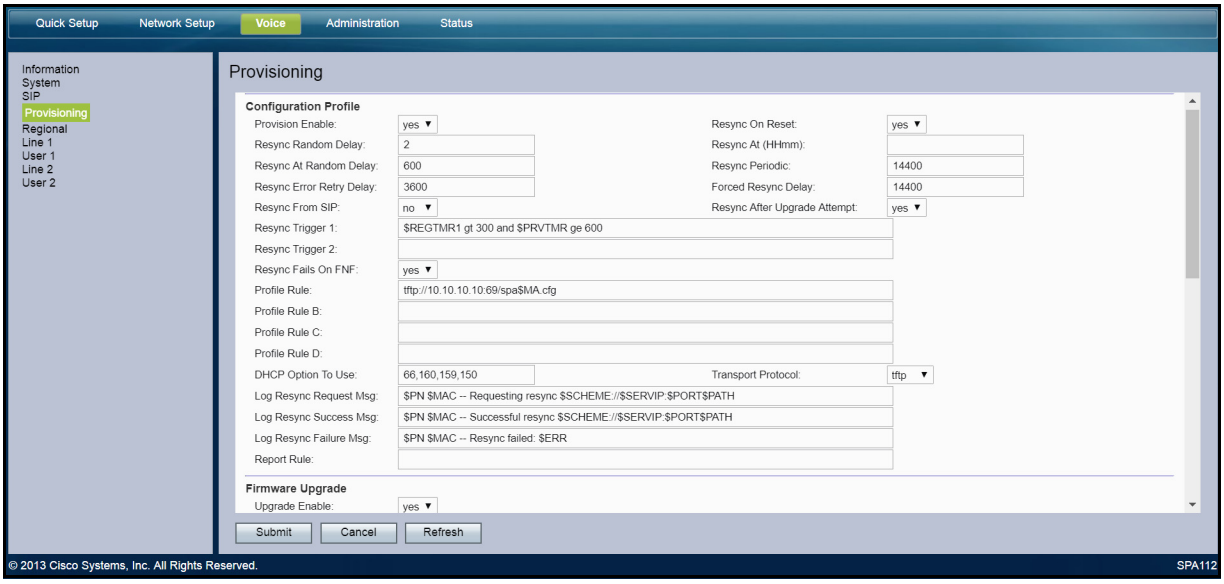


Figure 59. Provisioning Settings

8 Select the **Voice** tab, and then select **Provisioning**.

9 Set the **Profile Rule** value to `tftp://<nyquist-sysctrl-ip>:69/spa$MA.cfg`, replacing `<nyquist-sysctrl-ip>` with the IP address of the C4000 System Controller.

10 Set **Transport Protocol** to **tftp**, and then select **Submit** to reboot the device.

11 Verify that the device has been provisioned.

- On the device, select the **Voice** tab and then select **Information**. Scroll to the bottom of the page and verify that **Provisioning Status** is set to *Successful*. Verify that **Registration State** under **Line 1 Status** (and **Line 2 Status**, if two stations are being added) indicates *Registered*.
- On the System Controller, navigate to the **Stations** tab and press the **Stations Status** button. On the *Stations Status* page, find the device. Ensure its Status says “Not in use” in green.

12 Log back into the device. The C4000 system server will have set the following parameters:

- Quick Setup → Line 1 (and optionally Line 2) → Proxy
- Quick Setup → Line 1 (and optionally Line 2) → Display Name
- Quick Setup → Line 1 (and optionally Line 2) → User ID
- Quick Setup → Line 1 (and optionally Line 2) → Password
- Quick Setup → Line 1 (and optionally Line 2) → Dial Plan
- Network Setup → Basic Settings → Connection Settings → Host Name
- Network Setup → Time Settings → Time Server → Manual
- Network Setup → Time Settings → Time Server (IP or Hostname)
- Network Setup → Auto Recovery After Reboot → Yes (checked)
- Network Setup → Advanced Settings → VLAN → Enable VLAN
- Network Setup → Advanced Settings → VLAN → VLAN ID
- Voice → Provisioning → Resync Trigger 1
- Voice → Provisioning → Profile Rule → "`tftp://<nyquist-sysctrl-ip>:69/spa$MA.cfg`"
- Voice → Provisioning → Resync From SIP → "no"

- Voice → Line 1 (and optionally Line 2) → Mailbox ID → `<nyquist-station-extension-number>`
- Voice → Line 1 (and optionally Line 2) → Mailbox Subscribe URL → `<nyquist-server-ip-address>`
- Voice → Line 1 (and optionally Line 2) → Proxy → `<nyquist-server-ip-address>`
- Voice → Line 1 (and optionally Line 2) → Subscriber Information → Display Name, User ID, Password
- Voice → Line 1 (and optionally Line 2) → Dial Plan
- Administration → Management → User List → password for username = `admin`

13 Log out of the device.

Note: Each time the ATA device is rebooted, it will retrieve the configuration settings from the Nyquist System Controller.

Using a Grandstream HT813 Adapter

The Grandstream HT813 Analog Telephone Adapter (ATA) provides one analog telephone FXS port and one PSTN line FXO port.

> For details about this product, refer to the following product documentation provided by Grandstream:
>
> - https://www.grandstream.com/hubfs/Product_Documentation/HT813_User_Guide.pdf
> - https://www.grandstream.com/hubfs/Product_Documentation/HT813_Administration_Guide.pdf
> - https://www.grandstream.com/products/gateways-and-atas/analog-telephone-adaptors/product/ht813
> - https://www.grandstream.com/support/resources?title=HT813

Setting up the HT813 for use by the Nyquist system

Users can choose to use the FXS port, the FXO port, or both ports (FXS and FXO).

1 Start with basic device setup using the HT813 web interface
(see *"Basic HT813 Setup" on page 190*)

2 Configure a Nyquist Station to use the HT813 FXS port
(see *"Configure station to use HT813 FXS port" on page 191*)

3 Configure a Nyquist SIP Trunk to use the HT813 FXO port
(see *"Configure SIP Trunk to use HT813 FXO port" on page 193*)

Basic HT813 Setup

1 Plug an Ethernet cable into the HT813's WAN Port. The cable should be connected to a switch that is connected to your Nyquist server network.

2 Power up the HT813 by plugging it in.

By default, the HT813 will request an IP address from a DHCP server over the WAN port.

3 Upgrade the HT813 firmware to version 1.0.5.2 or greater.
https://www.grandstream.com/support/firmware

Note: Upgrading to this version or greater is very important, the Nyquist system will not be able to properly configure the device if it is not using this firmware version or greater.

---

4 If DHCP is used in the Nyquist network, and the DHCP server provides the Nyquist server's TFTP IP address via option 66, skip to step 7.

5 On the HT813 *Basic Settings* page, configure the HT813's static IP address.

6 On the HT813 *Advanced Settings* page, select **TFTP for Firmware Upgrade and Provisioning** and then enter the Nyquist server's IP address in the **Config Server Path:** field (see *"Grandstream Device Configuration Advanced Settings" on page 191*).

7 You are now ready to configure the FXS and FXO ports by using the Nyquist server web interface. See *"Configure station to use HT813 FXS port" on page 191* and *"Configure SIP Trunk to use HT813 FXO port" on page 193* for details.

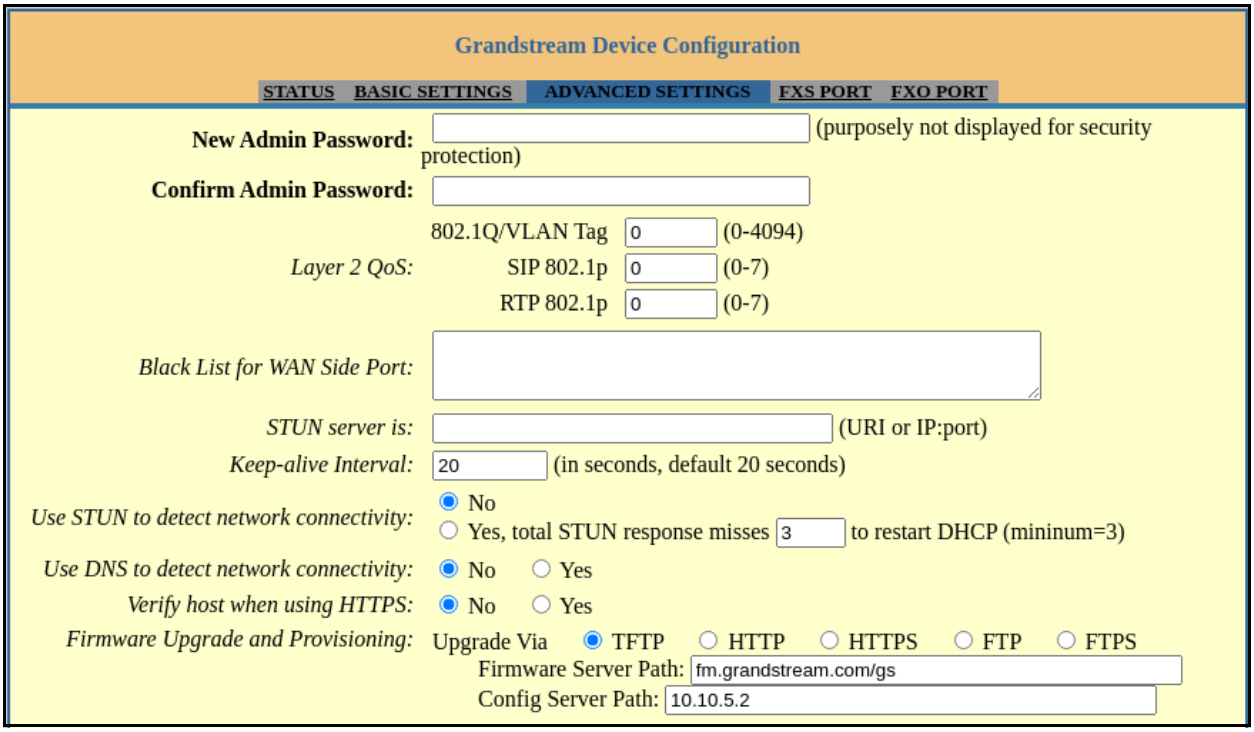


Figure 60. Grandstream Device Configuration Advanced Settings

Configure station to use HT813 FXS port

1 From the navigation bar, select **Stations**.

2 From the *Station* page, select the **Add** icon.

3 Add a new Station for the FXS port using the station settings specified in *Table 55, "Add Station Properties to use HT813 FXS port," on page 192* (which only details HT813-specific fields).

4 Press the **Save** button.

5 Reboot the HT813 device (see *"HT813 Device Reboot Required after making changes" on page 195*).

Table 55. Add Station Properties to use HT813 FXS port

Device Type	Select **Grandstream HT813 Analog Phone FXS Port**.
Station Type	Select either **Admin Phone** or **IP Phone**.
MAC Address	Enter the HT813's LAN MAC Address. This address can be obtained by viewing the HT813's Status page (see *"Grandstream Device Configuration Status Page" on page 193*). **Important:** Make sure you enter the LAN MAC Address, not the WAN MAC Address. *Note:* The HT813 uses the LAN MAC Address for configuration file names, even when the WAN Port is used to connect it to the network.
VLAN Configuration (optional)	If a VLAN is going to be used, you can enter the VLAN information.
Registration Password	Enter a password that the HT813 will use to register with the Nyquist server as a SIP client. The Nyquist server will remember the registration password for each station.
Web Password	Enter a new password to be used by the HT813's web interface.
Web Password Confirmation	Since the default password for the HT813 web interface is *admin*, we strongly recommend that you change it for security reasons. *Note:* Changing the **Web Username** is not supported. Any value you enter in the **Web Username** field that differs from *admin* will be ignored.
Dial Plan Type	You may change the dial plan type to meet your requirements. If you choose **Auto Dial**, you can then select an **Auto Dial Extension**. If you select **Auto Dial** and select an **Auto Dial Extension**, do not change the data that is automatically entered into the **Dial Plan** field. If you select **Custom** to create a custom dial plan, refer to the *Grandstream HT813 Administration Guide* (https://www.grandstream.com/hubfs/Product_Documentation/HT813_Administration_Guide.pdf) for details on the Dial plan format used by the HT813. You will also need to understand the DTMF codes used by the Nyquist system to create a valid dial plan (see *"Nyquist DTMF Feature Dialing Codes" on page 574*).

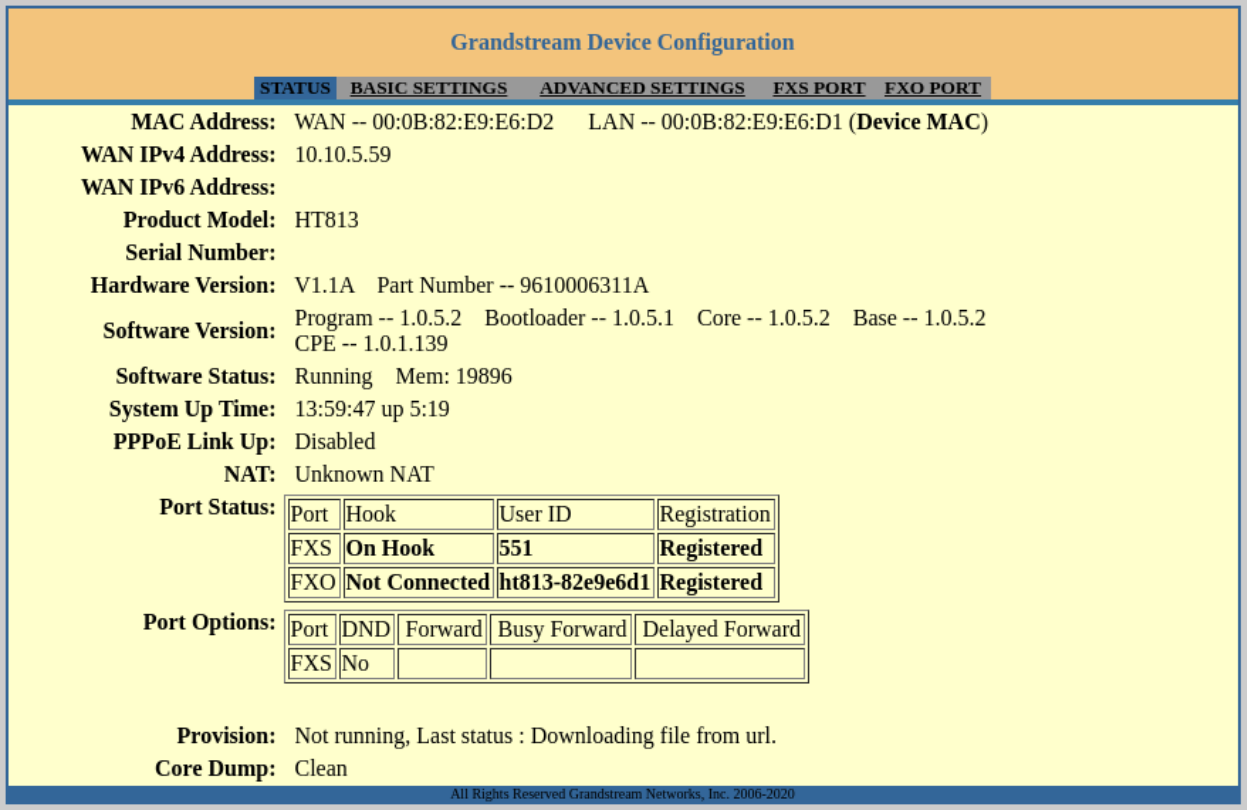


Figure 61. Grandstream Device Configuration Status Page

Configure SIP Trunk to use HT813 FXO port

1. From the navigation bar, select **SIP Trunks**.
2. From the *SIP Trunks* page, select the **Create New Trunk > HT813 SIP Trunk** button.
3. Add a new SIP Trunk for the FXO port, using the SIP Trunk settings specified in *Table 56, "Add SIP Trunk Properties to use HT813 FXO port," on page 194*.
4. Press the **Save** button.
5. Reboot the HT813 device (see *"HT813 Device Reboot Required after making changes" on page 195*).

Tip: The HT813 cannot be rebooted via the Nyquist system. You can reboot the HT813 by performing a power cycle, or you can initiate a reboot via the HT813's Advanced Settings page of the web interface (see *"Grandstream Device Configuration Advanced Settings" on page 191*).

Table 56. Add SIP Trunk Properties to use HT813 FXO port

Name	The name must match the following format:
	`ht813-<last-8-digits-of-HT813-LAN-MAC-Address>`
	For example, if the HT813's LAN MAC address is `000b82e9e6d1`, the name must be:
	`ht813-82e9e6d1`
	Note: Lowercase characters must be used in the MAC address portion, and a dash must be included between the ht813 portion and the MAC address portion.

Extension	Select a previously created DISA Station extension.
Host	Set this to the IP address of the HT813 WAN Port IP Address. The WAN port IP address can be obtained by viewing the HT813's web interface Status page (see *"Grandstream Device Configuration Status Page" on page 193*).
DID	For a PSTN-based POTS line connection (assuming the FXO port is plugged into a standard POTS line), set this value to match the POTS line phone number, including area code. Whenever a standard POTS line is used, this value will not change the outbound Caller-ID, because it is already assigned by the POTS line. If the FXO is connected to a PBX system, the DID may affect the Caller-ID seen by the PBX.
Custom Settings	While displaying the HT813's Status page, copy the MAC address information from the HT813's Status page into the "Custom Settings" field. Sample MAC address information copied from HT813 Status page: `WAN – 00:0B:82:E9:E6:D2 LAN – 00:0B:82:E9:E6:D1` **Caution** If you forget to add the MAC address information into the Custom Settings field, the configuration will not properly create a valid SIP Trunk for the FXO port.

Custom Settings (for SIP Trunk - FXO Port)

First, make sure that the HT813's MAC address information is the first information included in the Custom Settings field. This is mandatory. You can use copy/paste to transfer this information directly from the HT813's Status page into the custom settings field; the extra spaces and dashes are automatically handled by the custom settings parser.

Example MAC address information taken from HT813 web interface Status page:

```
WAN – 00:0B:82:E9:E6:D2 LAN – 00:0B:82:E9:E6:D1
```

Custom P-Value Parameters

In addition, with consultation from Bogen Technical Support, custom parameters for configuring the HT813 can be included in the custom settings field after the MAC Address information.

Example one:

```
WAN – 00:0B:82:E9:E6:D2 LAN – 00:0B:82:E9:E6:D1
:PVALS:(P100]0(/P100]:PVALS:
```

Example one will set P100 to 0 on the HT813 device.

Example two:

```
WAN – 00:0B:82:E9:E6:D2 LAN – 00:0B:82:E9:E6:D1
:PVALS:
(P100]1(/P100]
(P200]10.10.5.2(/P200]
:PVALS:
```

Example two will set P100 to **1** and P200 to **10.10.5.2** on the HT813 device.

The use of P-value custom parameters is not required by the Nyquist system when the FXS and FXO ports are used as designed to integrate with the Nyquist system.

For further details about custom parameters, contact Bogen Technical Support (see *"Getting Help" on page 15*).

HT813 Device Reboot Required after making changes

After making any changes to a SIP Trunk or Station related to an HT813 device, the HT813 device must be manually rebooted by power cycling the device (Nyquist has no way to instruct the device to reboot). To power cycle the device, unplug it, wait a few seconds, then plug it back in. While powering up, the HT813 device will read the configuration file from the Nyquist server and apply any changes that were made to SIP Trunks that affect the FXO port, and apply any changes that were made to a Nyquist Station that affect the FXS port.

You can also initiate a reboot by using the HT813's web interface, Advanced Settings page (*"Grandstream Device Configuration Advanced Settings" on page 191*). Press the "Reboot" button at the bottom of the configuration menu to reboot the ATA remotely. The web browser will then display a message window to confirm that reboot is underway. Wait 30 seconds to log in again.

HT813 Firmware Updates

The Nyquist system is not responsible for maintaining available firmware for the HT813 or responsible for upgrading the HT813 firmware. The customer has sole responsibility for maintaining and upgrading the HT813 firmware. Customers can use the HT813 user interface to upgrade the firmware and to initiate automatic upgrade using Grandstream's servers.

Using the Yeastar TA2400

The Nyquist system supports the use of the Yeastar TA2400 FXS VoIP Gateway to integrate 24 standard analog phones into your IP communications system.

Note: Quantum/Multicom MCESS and MCWESS phones are not supported by this device.

To install the gateway, refer to the Yeastar TA2400 installation guide at:

http://help.yeastar.com/download/docs/ta1600-ta2400-ta3200-v3-v4-installation-guide-en.pdf

To configure the Yeastar TA2400 for use with the Nyquist system, you first set up the Yeastar TA2400 to retrieve configuration from the Nyquist server. (See *"Connect the Yeastar TA2400 to the Nyquist Server" on page 196*.) You then add a station that uses a port on the TA2400 via the Nyquist Admin UI. (See *"Adding a Station that Uses a Yeastar TA2400 Port" on page 197*.)

You can also use the Yeastar TA2400 web interface to view port status. (See *"Viewing Yeastar TA2400 Status" on page 197*.)

Connect the Yeastar TA2400 to the Nyquist Server

Setting up the Yeastar TA2400 to retrieve information from the Nyquist server is done through the Yeastar TA2400 web interface.

Follow instructions in the Yeastar TA Series Analog VoIP Gateway Installation Guide for getting an IP address for the Yeastar TA2400 and for logging into the Yeastar TA2400 web interface.

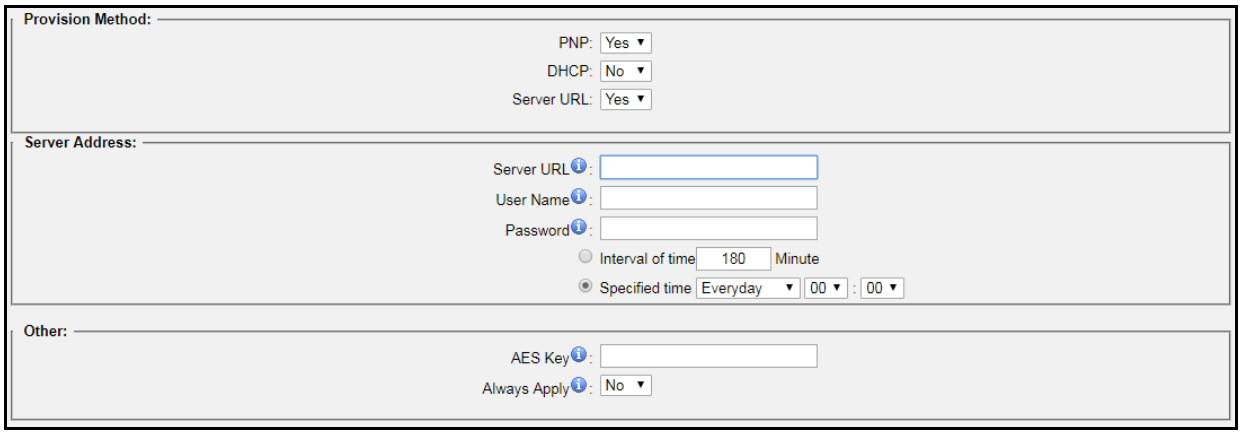


Figure 62. Yeastar Auto Provisioning Settings

To set up the Yeastar TA2400:

1. From the Yeastar TA2400 web interface, select **System**.
2. Under **System Preferences**, select **Auto Provision Settings**.
3. In **Provision Method**, change **Server URL** to **Yes**.
4. In **Server Address**, select the **Server URL** field and type `tftp://` followed by the IP address of the Nyquist server and /. For example: `tftp://10.10.5.2/`.
5. Leave **User Name** and **Password** blank.
6. In the **Interval of time** field, enter `60`.
7. Select **Save**.
8. Select **Apply Changes**.
9. Under **System Preferences**, select **Reset and Reboot**.
10. If prompted, select **OK**.

Adding a Station that Uses a Yeastar TA2400 Port

To add a station that uses a Yeastar TA2400 port to your Nyquist system, follow the procedures for adding a station (See *"Adding a Station" on page 185*).

When you select **Yeastar-TA2400 Analog FXS Port** as the **Device Type**, you must select the **Port Number** that the station is attached to from the drop-down list. Valid values are 1 through 24.

Note: Port number 1 must always be used.

If you have only one phone attached to the TA2400, it must be attached to port 1. If you have multiple phones attached to the TA2400, one must be attached to port 1 but the use of the other ports can be random. For example, you can have phones attached to port 1, 2, 5, and 10. However, you cannot attach phones to just ports 2, 5, and 10 since that combination does not include phone 1.

The following rules apply when adding a station to a Yeastar TA2400 port:

- **Device Type** is **Yeastar-TA2400 Analog FXS Port**.
- You can select **Admin Phone** or **IP Phone** for **Station Type**.
- **MAC Address** is a required field. If you are adding the first station for this **MAC Address**, the **Port Number** is automatically set to **1**.
- **Paging** is set to **No** and cannot be changed.
- **Multicast Audio Distribution** is set to **No** but does not appear on the *Add Station* or *Edit Station* pages.
- Volume controls do not appear.
- **Codecs Allowed** is set to **g722** and cannot be changed.
- If you enter **1** for **Port Number**, the Admin Web UI displays the **VLAN settings**, **Web Username**, and **Web Password** fields.
- Stations attached to the Yeastar TA2400 are not available for ringing during Night Ring operations.
- You can associate an external speaker to a TA2400 port by selecting a **Speaker Extension**.
- After adding a station, the Yeastar TA2400 must be manually rebooted via the Yeastar TA2400's web interface.
- The Nyquist **Appliances Network Time Server Source** will be used to configure the Network Time Service on the Yeastar TA2400. (See *"Using the Yeastar TA2400" on page 195*.)
- The Yeastar TA2400 time zone will be set to match the Nyquist server's time zone.

Viewing Yeastar TA2400 Status

You can use the Nyquist Station Status feature to view overall status of the Yeastar TA2400 device. (See *"Viewing Station Status" on page 210*.)

You can obtain status of the individual ports through the Yeastar TA2400 UI.

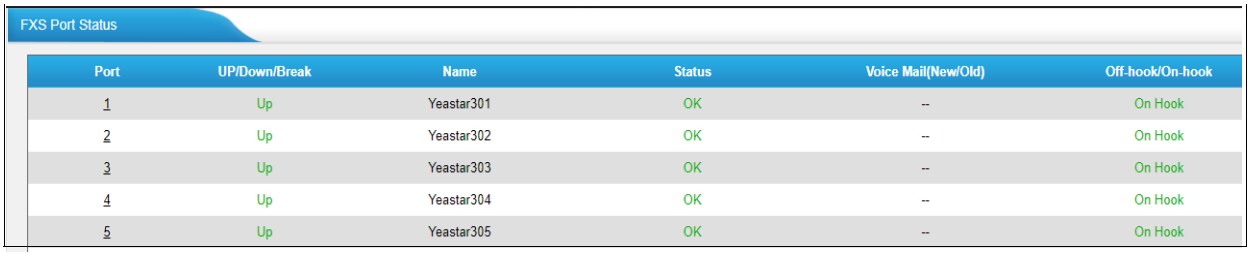


Figure 63. FXS Port Status

To view port status:

1. From the Yeastar TA2400 web interface, select **Status**.
2. Select **Port Status**.
   Parameters that can be viewed and a description of the possible statuses are described in *Table 57 on page 198*.

Table 57. Port Status Parameters

Port	Provides the port number for the associated station.
Up/Down	Displays **Up** if the FXS module is working. Otherwise, displays **Down**.
Name	Provides the name of the station.
Status	Shows the state of the port Possible statuses are: • **OK**. Registration is successful, and the port is ready for use. • **Unreachable**. The FXS module cannot determine the status of the port. • **Request Sent**. A request for registering the port has been transmitted to the FXS module. • **Waiting for authentication**. The FXS module is verifying that the correct password and user name have been entered. • **Failed**. The port registration has failed.
Voice Mail (New/Old)	This field is not used.
Off hook/On hook	**On Hook** appears if the FXS port is idle. **Off Hook** appears if the FXS port is busy.

Using the Grandstream GXW4224

The Nyquist system supports the use of the Grandstream GXW4224 FXS VoIP Gateway to integrate 24 standard analog phones into your IP communications system.

Note: Quantum/Multicom MCESS and MCWESS phones are not supported by this device.

To install the gateway, refer to the Grandstream GXW4224 installation guide at:

https://documentation.grandstream.com/article-categories/gxw4200-series

To configure the Grandstream GXW4224 for use with the Nyquist system, you first set up the Grandstream GXW4224 to retrieve configuration from the Nyquist server (see *"Connect the Grandstream GXW4224 to the Nyquist Server" on page 199*). You then add a station that uses a port on the GXW4224 via the Nyquist Admin UI (see *"Adding a Station that Uses a Grandstream GXW4224 Port" on page 200*).

You can also use the Grandstream GXW4224 web interface to view port status (see *"Viewing Grandstream GXW4224 Status" on page 201*).

Connect the Grandstream GXW4224 to the Nyquist Server

Setting up the Grandstream GXW4224 to retrieve information from the Nyquist server is done through the Grandstream GXW4224 web interface.

Follow instructions in the *GXW42XX series Analog IP Gateway User Manual* for getting an IP address for the Grandstream GXW4224 and for logging into the Grandstream GXW4224 web interface.

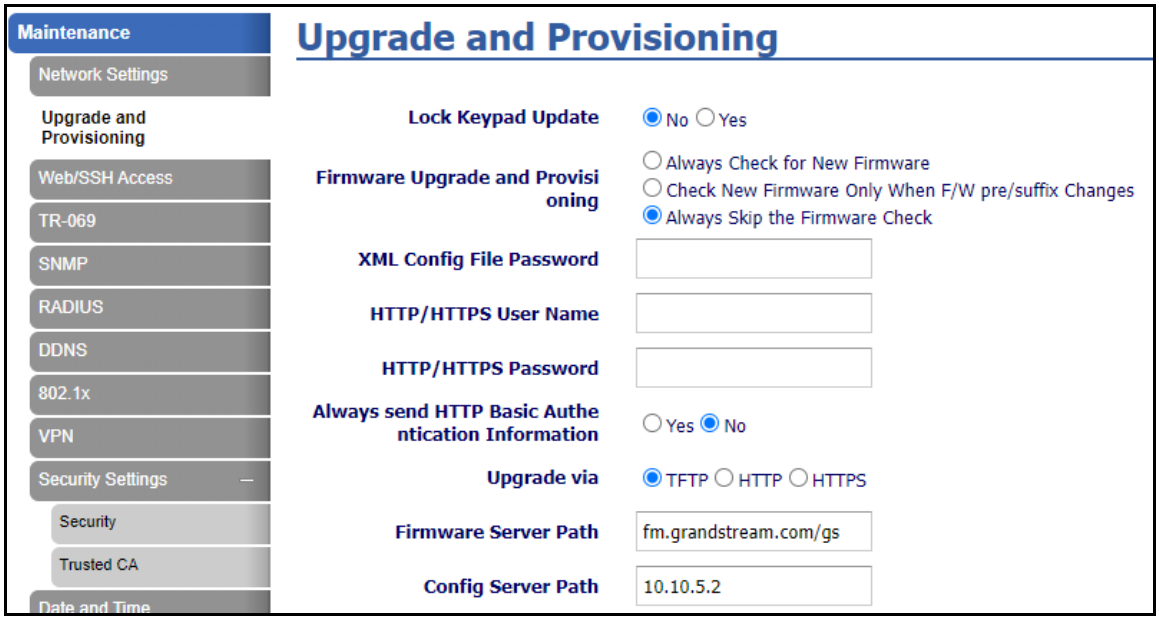


Figure 64. Grandstream GXW4224 Upgrade and Provisioning

To set up the Grandstream GXW4224:

1. Log into the Grandstream GXW4224 web interface. The default username is **admin** and default password is **admin**.
2. From the Grandstream GXW4224 web interface, select **Maintenance** tab.
3. Select **Upgrade and Provisioning**.
4. In the **Config Server Path** field type the IP address of the Nyquist server.
5. Select **Save and Apply**.
6. From the Grandstream GXW4224 web interface, select **Maintenance** tab.

7 Select **Date and Time**

8 Select desired Time Zone from the **Time Zone** field.

9 Select **Save and Apply**.

10 Manually reboot the GXW4224 by pressing **Reboot** located on the upper-right corner of the GXW4224's web interface. You will also need to reboot the device after adding associated stations to the Nyquist server.

Adding a Station that Uses a Grandstream GXW4224 Port

To add a station that uses a Grandstream GXW4224 port to your Nyquist system, follow the procedures for adding a station (see *"Adding a Station" on page 185*).

When you select **Grandstream GXW4224 Analog Phone FXS Port** as the **Device Type**, you must select the Port Number that the station is attached to from the drop-down list. Valid values are 1 through 24.

Note: Port number 1 must always be used. If you have only one phone attached to the GXW4224, it must be attached to port 1. If you have multiple phones attached to the GXW4224, one must be attached to port 1, but the use of the other ports can be random. For example, you can have phones attached to port 1, 2, 5, and 10. However, you cannot attach phones to just ports 2, 5, and 10 since that combination does not include port 1.

The following rules apply when adding a Nyquist station for a Grandstream GXW4224 port:

- **Device Type** is **Grandstream GXW4224 Analog Phone FXS Port**.
- You can select **Admin Phone** or **IP Phone** for **Station Type**.
- **MAC Address** is a required field. If you are adding the first station for this MAC Address, the Port Number is automatically set to 1.
- All stations configured for a Grandstream GXW4224 instance must have the same **MAC Address** configured.
- **Transmit/Receive Volume Gain** fields are settable on Port 1 only, and apply to all ports.
- **Paging** is set to No but does not appear on the *Add Station* or *Edit Station* pages..
- **Multicast Audio Distribution** is set to **No** but does not appear on the *Add Station* or *Edit Station* pages.
- **Codecs Allowed** is set to **g722** and cannot be changed.
- If you enter 1 for **Port Number**, the Admin Web UI displays the **VLAN settings**, **Web Username**, and **Web Password** fields. The **Web Username** is always **admin** and can't be changed.
- You can associate an external speaker to a GXW4224 port by selecting a **Speaker Extension**.
- The **Nyquist Appliances Network Time Server Source** will be used to configure the Network Time Service on the Grandstream GXW4224.
- The Grandstream GXW4224 time zone must be set via the Grandstream GXW4224 web interface.
- Stations attached to the Grandstream GXW4224 are not available for ringing during Night Ring operations.

- After adding/editing a station, the Grandstream GXW4224 must be manually rebooted.

Important:	After you make changes to stations associated with a Grandstream GXW4224, you must reboot the GXW4224 to force it to fetch the configuration file from the Nyquist server and update its settings.

Viewing Grandstream GXW4224 Status

You can use the Nyquist *Station Status* feature to view overall status of the Grandstream GXW4224 device via the station status of related stations (see *"Viewing Station Status" on page 210*). Nyquist stations associated with GXW4224 devices will show the IP address of the device.

You can obtain status of the individual ports through the Grandstream GXW4224 UI by selecting **Port Status** under the Status tab.

The Grandstream GXW4224 locally uses ports in the range 5061 through 5107. If the use of these port numbers causes network issues (e.g., firewall or diagnostics), you can instead setup the Grandstream GXW4224 to use ephemeral port numbers by making the following change via the Grandstream GXW4224 web interface:

1. Under *Profiles*, select **Profile 1** → **SIP Settings** → **Basic Settings**
2. Change **Use Actual Ephemeral Port in Contact with TCP/TLS** to Yes
3. Select **Save and Apply**
4. Select **Reboot**, located on the top-right of the web page.

Grandstream GXW4224 Security

- Consider enabling HTTPS for secure web access.
  Select **Maintenance** tab, then select HTTPS for **Web Access Mode**.
- Consider disabling SSH.
  Select **Maintenance** tab, then select Yes for **Disable SSH**.
- Consider disabling user-level and viewer-level web access.
  Select **Maintenance** tab, then select Yes for **Disable User Level Web Access** and **Disable Viewer Level Web Access**.
- Consider updating GXW4224 firmware to 1.0.23.8 or later (optional).

Customizing an NQ-T1100 IP Phone – Color Touch Display

Once a NQ-T1100 IP Phone - Color Touch Display has been added as a Station (see *"Adding a Station" on page 185*), the placement and labels of keys on the NQ-T1100 admin phone can be customized.

To edit the line keys of the NQ-T1100 IP phone:

1. Select **Stations** from the navigation bar.

2 Select the **Edit** button next to the NQ-T1100 station, which will have a **Device Type** of **NQ-T1100 IP Phone - Color Touch Display**.

3 Press the **Edit Line Keys** button.

4 The *Edit Line Keys* view will be displayed (see *"NQ-T1100 - IP Phone - Color Display Edit Line Keys" on page 204*).

5 Click on each key to be customized to display and edit the **Edit Line Key** properties for that key, as described in *Table 58, "Edit Line Key # Properties," on page 202*.

Note: The existing settings for a key will not always be displayed in the **Edit Line Key** properties window.

---

6 When all keys have been defined, click **Update Phone Settings** to update the settings on the NQ-T1100 device. After pressing **Update Phone Settings**, it will take a couple of minutes for the NQ-T1100 Admin phone to reboot and update the touch-screen keypad to match the edits performed via the web interface.

7 Press the **Done** key.

Table 58. Edit Line Key # Properties

Type	The type of action to be initiated by this key. The listed types are fairly self-explanatory, but there are several special values: • **Custom Speed Dial**: The key's label and value (DTMF dialing digits) can be configured by the user. • **Empty**: The key will be inoperable with no label. • **Reserved**: The Nyquist system will not configure the key, allowing the user to manually configure it via the Admin Phone's touch screen interface. The Nyquist web interface will label the key "Reserved" as a reminder that Nyquist will reserve the key for user customization via the Admin Phone.
Label	A string of characters that will be displayed on the line key. Maximum length is 30 characters. *Tip:* You may want to use extra spaces to align text that spans multiple lines.

Table 58. Edit Line Key # Properties

Value	Only available when **Type** is **Custom Speed Dial**. A string of characters that will be used to place a call when the specified line key is pressed on the Admin phone. Any valid Nyquist DTMF sequence can be used. See *"Nyquist DTMF Feature Dialing Codes" on page 574* for further details. Maximum length is 99 characters.
Format String	Only available when **Type** is **Zone**. A string of characters that are used to format the label for a line key that represents a Paging Zone speed dial. It may contain the following variables, which will be replaced with the appropriate value when the line key label is created for a Paging Zone: • `$name`: Paging Zone name • `$number`: Paging Zone number For example, the following format string: `Z$number: $name` when used for a zone with zone number 5 and a zone name of "Outdoor," would show up on the line key as "Z5: Outdoor". This is the default format for Zone line keys, which is used if a value is not specified for the Format String field. Maximum length is 30 characters. *Note:* The buttons will not display the label defined by the **Format String** during the customization process, but instead simply display "Zone" (as shown in *"NQ-T1100 - IP Phone - Color Display Edit Line Keys" on page 204*).

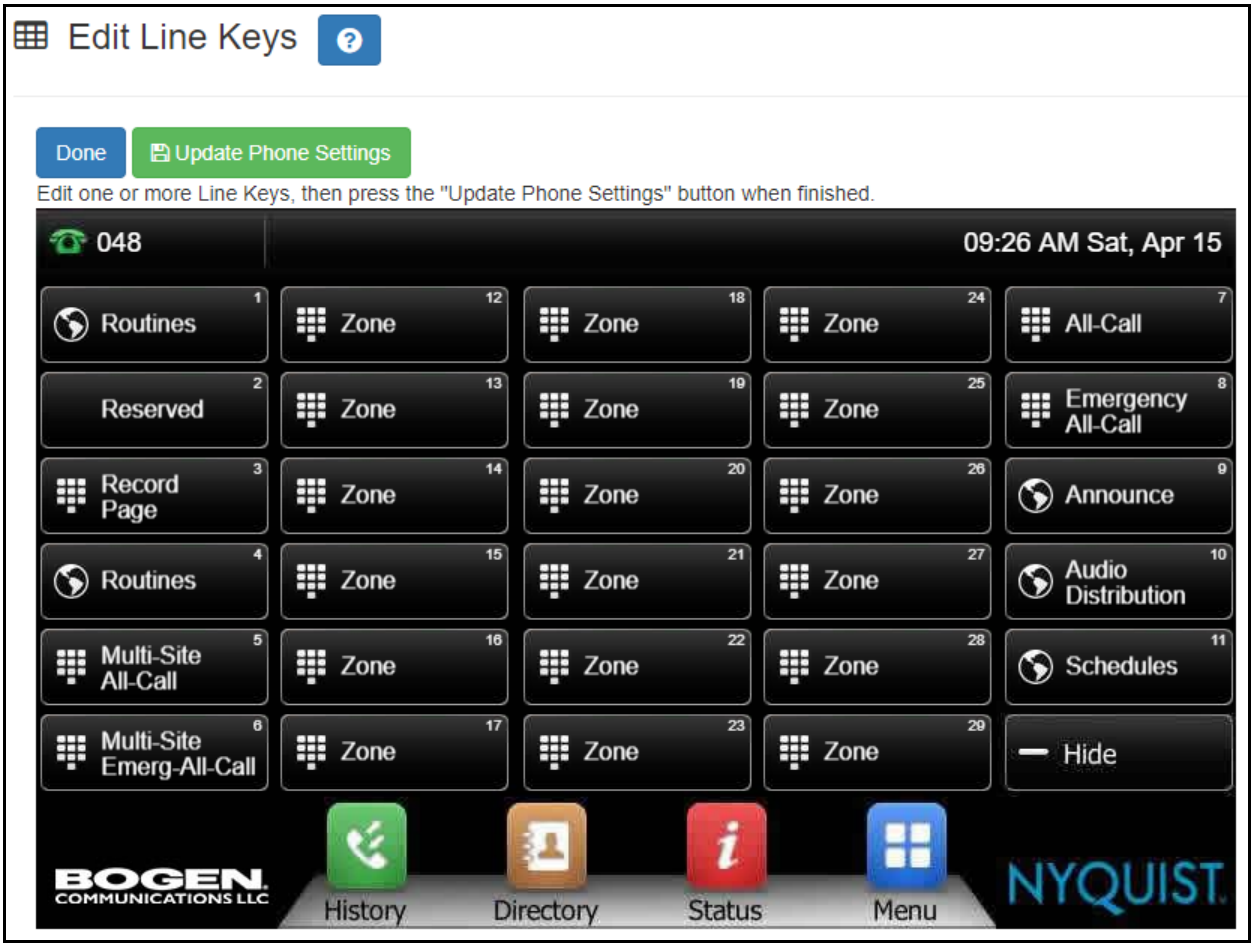


Figure 65. NQ-T1100 - IP Phone - Color Display Edit Line Keys

Customizing an NQ-ZPMS Zone Paging Microphone Station

Once an NQ-ZPMS Zone Paging Microphone Station has been added as a station (see *"Adding a Station" on page 185*), the placement and labels of keys on the NQ-ZPMS phone can be customized.

To edit the line keys of the NQ-ZPMS IP phone:

1. Select **Stations** from the navigation bar.
2. Select the **Edit** button next to the NQ-ZPMS station, which will have a **Device Type** of **NQ-ZPMS Zone Paging Microphone Station**.
3. Press the **Edit Line Keys** button.
4. The *Edit Line Keys* view will be displayed (see *Figure 66, "NQ-ZPMS Zone Paging Microphone Station – Edit Line Keys," on page 207*).
5. Click on each key to be customized to display and edit the *Edit Line Key* properties for that key, as described in *"Edit Line Keys Properties" on page 205*. All keys are customizable except the top-left key, which displays the station name, and the rightmost column of keys.

Tip: This view provides access to four pages of keys that can be viewed and edited. Click on one of the black dots shown above the first row of keys to view a different page.

Note: The existing settings for a key will not always be displayed in the *Edit Line Key* properties window.

6 When all keys have been defined, click **Update Phone Settings** to update the settings on the NQ-ZPMS device. After pressing **Update Phone Settings**, it will take a couple of minutes for the NQ-ZPMS phone to reboot and update the touchscreen keypad to match the edits performed via the web interface.

7 Press the **Done** key.

Table 59. Edit Line Keys Properties

Type	The type of action to be initiated by this key. The listed types are fairly self-explanatory, but there are several special values: • **Custom Speed Dial**: The key's label and value (DTMF dialing digits) can be configured by the user. • **Empty**: The key will be inoperable with no label. • **Reserved**: The Nyquist system will not configure the key, allowing the user to manually configure it via the phone's touch screen interface. The Nyquist web interface will label the key "Reserved" as a reminder that Nyquist will reserve the key for user customization via the phone. • **SIP Line**: If you have configured additional SIP Lines on the phone, this line key **Type** can be used to associate the line key with a specified SIP Line. If the SIP Line is registered, a green indicator will show on the line key. Pressing this line key will initiate dialing using the defined SIP line.
Label	A string of characters that will be displayed on the line key. If the text does not fit in the space provided, it will scroll. Maximum length is 30 characters.

Table 59. Edit Line Keys Properties (continued)

Value	Only available when **Type** is **Custom Speed Dial**. A string of characters that will be used to place a call when the specified line key is pressed on the phone. Any valid Nyquist DTMF sequence can be used. See *"Nyquist DTMF Feature Dialing Codes" on page 574* for further details. Maximum length is 99 characters.
Format String	Only available when **Type** is **Zone**. A string of characters that are used to format the label for a line key that represents a Paging Zone speed dial. It may contain the following variables, which will be replaced with the appropriate value when the line key label is created for a Paging Zone: • `$name`: Paging Zone name • `$number`: Paging Zone number For example, the following format string: `Z$number: $name` when used for a zone with zone number 5 and a zone name of "Outdoor" would show up on the line key as "Z5: Outdoor". This is the default format for Zone line keys, which is used if a value is not specified for the Format String field. Maximum label length is 30 characters. *Note:* The buttons will not display the label defined by the Format String during the customization process, but instead simply display "Zone".

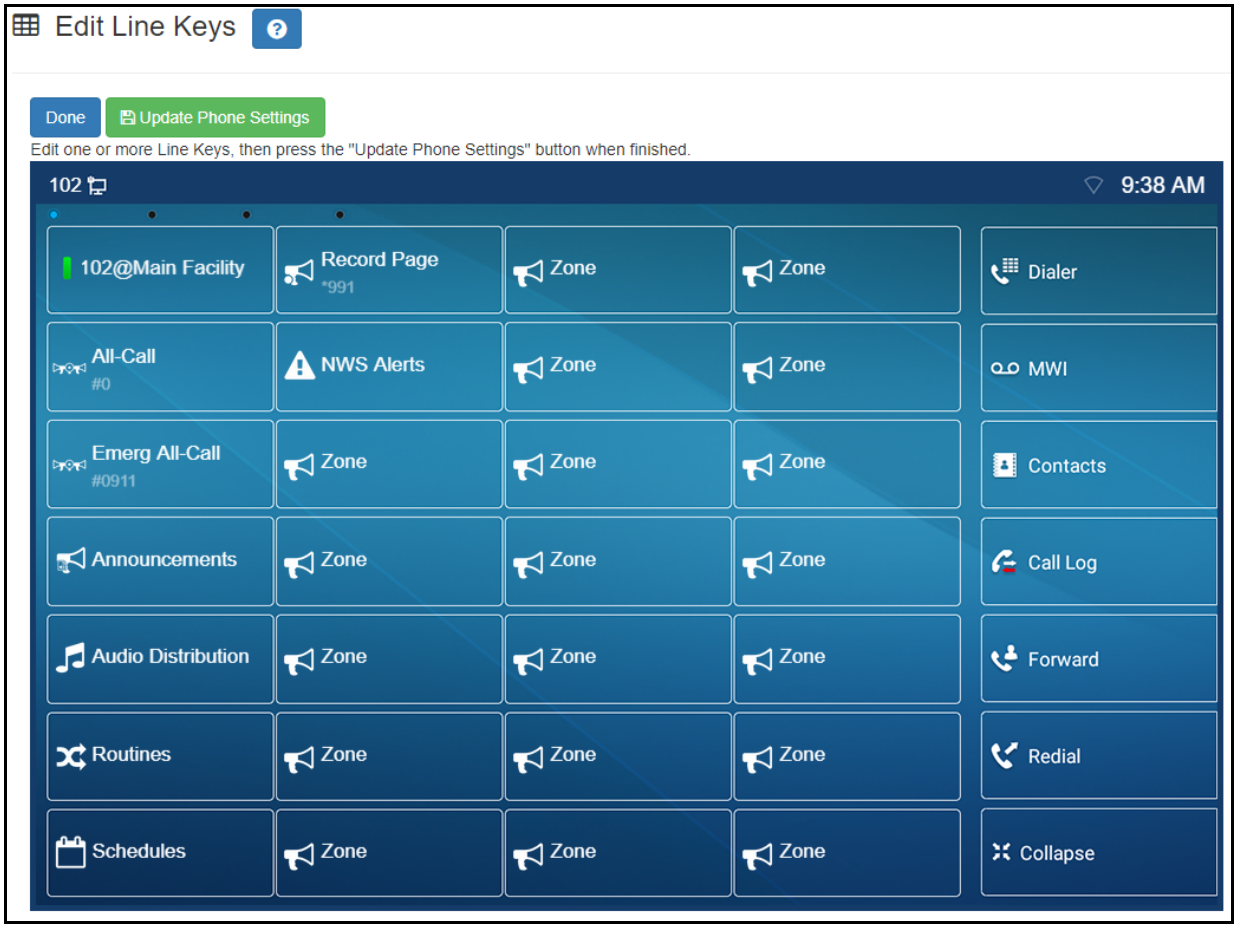


Figure 66. NQ-ZPMS Zone Paging Microphone Station – Edit Line Keys

Routing Intercom Calls to PBX Extensions via SIP Trunk

The Nyquist system can be configured to route call-switch–initiated intercom calls to Admin extensions on PBX systems by using a SIP Trunk and one or more *Admin PBX Extension* stations.

Nyquist stations that include Day/Night Admin configuration but do not have a call-switch can also place Admin intercom calls to Admin PBX extensions by dialing 0, *0, or *00:

0 = Normal intercom call to Day/Night Admin

*0 = Emergency intercom call to Day/Night Admin

*00 = Urgent intercom call to Day/Night Admin

Regarding this feature, the term *intercom call* does not include calls placed by dialing a station's extension. This feature requires call-switch–based initiated calls to an Admin station or the use of 0, *0, *00 to place a call to an Admin station. The Admin station called is defined by the caller's Day/Night Admin setting.

The following steps outline configuration for using this feature.

1 Configure a SIP Trunk with **Allow Outbound Intercom Calls** enabled.

   Set **Allow Outbound Intercom Calls** to *Yes* to allow call-switch–based stations to place calls to PBX-based Admin extensions via the SIP Trunk, using Day/Night Admin-PBX-Extension.

2 Add one or more stations with **Station Type** equal to *Admin PBX Extension*.

   The Admin PBX Extension stations are used as Day/Night Admin stations to route intercom calls to PBX-based Extensions via a SIP Trunk.

Note: When adding an Admin PBX Extension station, the length of the Extension field is not restricted to the Dialing Length set on the Nyquist system. For example if the Nyquist Dialing Length is set to three, you can still use any dialing length in the Extension field of the Admin PBX Extension station. For example, suppose your Nyquist system's Dialing Length is set to three, but your PBX extensions all use four digits. In this case, if your PBX extension is 1001, you can enter 1001 into the Extension field of the Admin PBX Extension, even though it exceeds the three-digit Dialing Length currently set on the Nyquist system.

---

3 Configure **Day/Night Admin** extensions for call-switch–based station.

   To send call-switch–based intercom calls to Admin PBX Extension stations, specify Day/Night Admin extensions that have the following format:

   `<Admin-PBX-Extension>@<SIP-Trunk-Name>`

   where `<Admin-PBX-Extension>` represents the station extension of an existing station of type *Admin PBX Extension* and `<SIP-Trunk-Name>` represents the name of the SIP Trunk to use for placing the intercom call to the Admin PBX Extension station.

   Day Admin:`<Admin-PBX-Extension>@<SIP-Trunk-Name>`

   Night Admin:`<Admin-PBX-Extension>@<SIP-Trunk-Name>`

   For example, if the Day/Night Admin is using PBX extension 100 and SIP Trunk with name equal to "UHS":

   `100@UHS`

   This would cause call-switch–based intercom calls to ring PBX extension 100 over SIP Trunk with name "UHS."

Excluding Stations from Paging

Stations can be excluded from paging except for Emergency All Call pages. Emergency All Call pages will be sent and heard at the station even if that station is set to exclude paging.

Stations excluded from paging are also excluded from receiving audio distribution, even if the station's **Multicast Audio Distribution** parameter is enabled, the station is a member of a zone being used for Audio Distribution, or both.

If you exclude a station from paging and the station is included in a **Time** or **Paging+Time** zone, the station does not receive tones either.

Tip: There is no need to exclude the Speaker Extension associated with a station to avoid feedback, as the associated speaker of a station is automatically muted while paging from that station. For details, see *"Speaker Extension Muting" on page 141*.

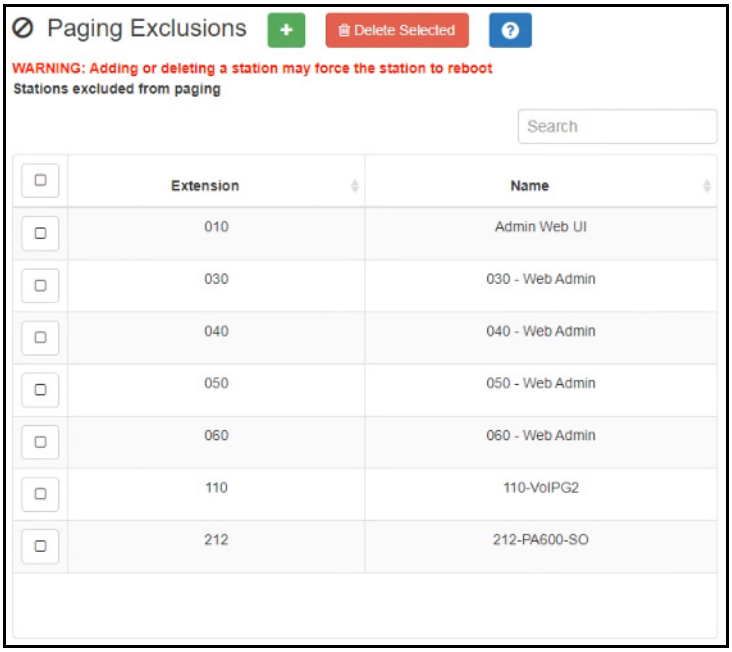


Figure 67. Paging Exclusions Page

To add a station to the Page Exclusions list (i.e., exclude it from paging):

1. Select **Paging Exclusions** from the navigation bar.
   a) Alternatively, select **Dashboard** from the navigation bar and select **Page Exclusion** in the **Calling/Paging** area.
2. Select the **Add** (+) button to display the **Add Paging Exclusions** popup.
3. Optionally, filter the displayed list of stations by extension or name.
4. Select one or more stations.
   - Click **Toggle All** to select (or deselect) the entire list of stations.
5. Select the **Add Exclusions** button to add the selected stations to the Page Exclusions list.

Warning Adding or deleting a station from the page exclusions list may force the station to reboot.

To remove a station from the Page Exclusions list:

1. Select **Paging Exclusions** from the navigation bar.
   - Alternatively, select **Dashboard** from the navigation bar and select **Page Exclusion** in the **Calling/Paging** area.
2. Select one or more extensions to be deleted from the exclusion list.
   - Optionally, toggle the checkbox in the header row above the selection checkboxes to select (or deselect) the entire list of stations.

3 When all selections are ready, click **Delete Selected** to remove the selected extensions from the list.

Note: You can also use the Page-Exclusion Routine Action (see *Table 2, "Routine Action Type-Specific Parameters," on page 588*) to add or remove stations from Paging Exclusions.

Viewing Station Status

The Station Status feature allows you to quickly assess the status of all stations.

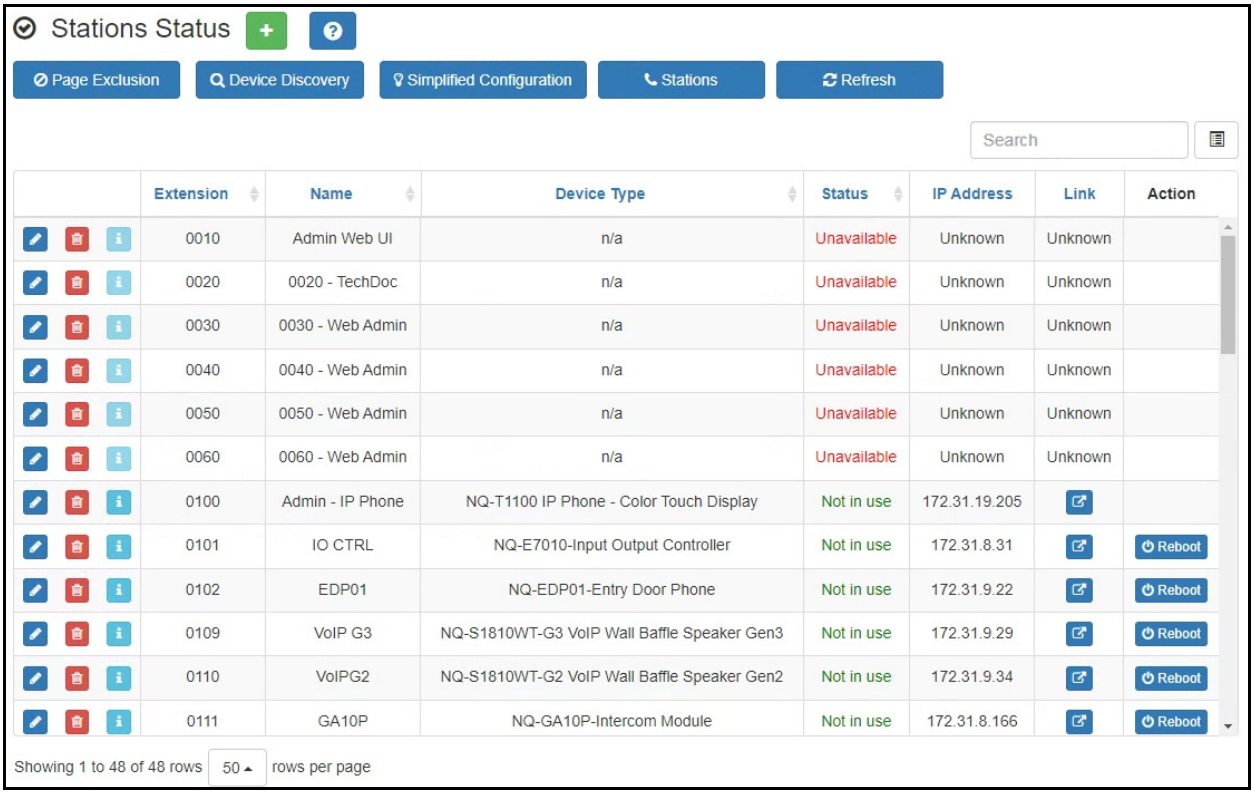


Figure 68. Station Status Page

To view station status:

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

2 Select **Stations Status**.

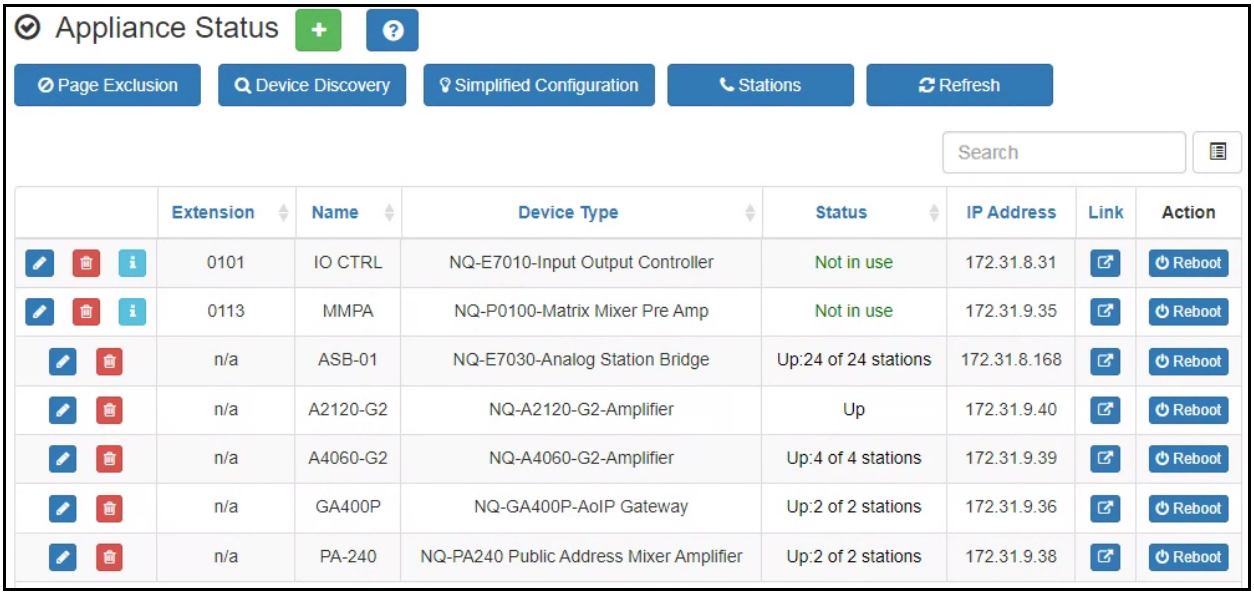
The following information appears for all stations:

Table 60. Station Status Page Parameters

Extension	Specifies the unique multi-digit extension number for this station. Valid values range from 001 to 899 for three-digit dialing. The system can be configured to use three-, four-, five-, or six-digit dialing. *Note:* For Sound Masking stations, **None** will be displayed.
Name	Specifies the name for the station. Names can be up to 16 characters in length.
Device Type	Specifies the **Device Type**, such as **NQ-P0100 Matrix Mixer Pre Amp**.
Status	Shows the current state of the station. Possible statuses are: • **Not in use**. This status indicates that the station is registered with the Nyquist system server and is not on a call. • **In use**. This status indicates that the station is off hook and either placing a call or in a call, such as an intercom call, page, or using a Nyquist feature. • **Ring+Inuse**. Indicates that the station is off hook, on a call, and ringing (at least one incoming call is ringing the station). • **Ringing**. Indicates that the station is on hook and ringing (at least one incoming call is ringing the station). • **Unavailable**. Indicates that the station is not registered with the Nyquist system server and is unavailable. A station in this status is unable to receive calls and most likely cannot place calls.
IP Address	Provides the IP address of the station.
Link	If the device can be configured or managed via an appliance web UI, this provides a login window for the device. After you enter your **Username** and **Password**, the web UI for the device appears.
Action	Provides a **Reboot** button for Nyquist devices that have an IP address. Selecting this button reboots the device.

Viewing Appliance Status

The Appliance Status feature allows you to quickly view the status of appliances such as I/O controllers and Matrix Mixer Pre-Amps without having to set a filter or manually search for each appliance.



	Extension	Name	Device Type	Status	IP Address	Link	Action
	0101	IO CTRL	NQ-E7010-Input Output Controller	Not in use	172.31.8.31		Reboot
	0113	MMPA	NQ-P0100-Matrix Mixer Pre Amp	Not in use	172.31.9.35		Reboot
	n/a	ASB-01	NQ-E7030-Analog Station Bridge	Up:24 of 24 stations	172.31.8.168		Reboot
	n/a	A2120-G2	NQ-A2120-G2-Amplifier	Up	172.31.9.40		Reboot
	n/a	A4060-G2	NQ-A4060-G2-Amplifier	Up:4 of 4 stations	172.31.9.39		Reboot
	n/a	GA400P	NQ-GA400P-AoIP Gateway	Up:2 of 2 stations	172.31.9.36		Reboot
	n/a	PA-240	NQ-PA240 Public Address Mixer Amplifier	Up:2 of 2 stations	172.31.9.38		Reboot

Figure 69. Appliance Status Page

To view appliance status:

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

2 Select **Appliance Status**.

The following information appears for each appliance recognized by the Nyquist system server:

Table 61. Appliance Status Page Parameters

Extension	Specifies the unique multi-digit extension number for this station. Valid values range from 001 to 899 for three-digit dialing. The system can be configured to use three, four, five, or six-digit dialing. *Note:* For appliances that can have more than one station associated with them, **n/a** will be displayed. If the appliance is being used for Sound Masking, **n/a** will be displayed.
Name	Specifies the name for the station. Names can be up to 16-characters in length.
Device Type	Identifies the type of appliance such as **NQ-E7010-Input Output Controller**.

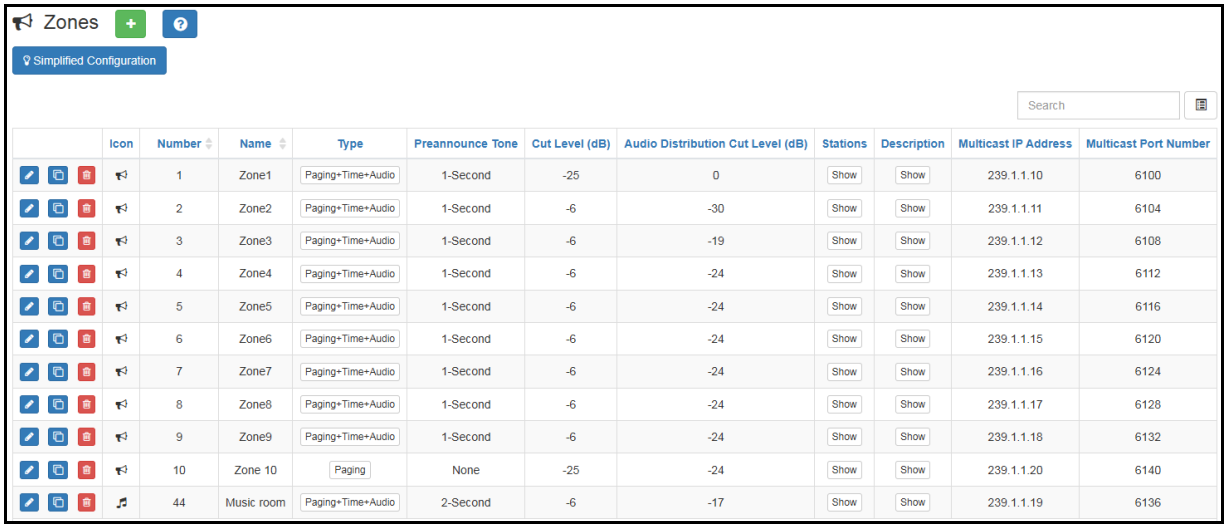
Table 61. Appliance Status Page Parameters (continued)

Status	Shows the current state of the appliance. Possible statuses are: • **Not in use**. This status indicates that the station is registered with the Nyquist system server and is not on a call. • **In use**. This status indicates that the station is off hook and either placing a call or in a call, such as an intercom call, page, or using a Nyquist feature. • **Unavailable**. Indicates that the station is not registered with the Nyquist system server and is unavailable. • **Unknown**. The server is unable to determine the state of the device. • **Unreachable**. Indicates that the appliance is currently unreachable (which usually means that a ping test failed). • **Up**. Indicates that the device is reachable and operational. This status may also include the number of stations that are currently registered with the Nyquist server.
IP Address	Provides the IP address of the appliance. If **Status** is currently **Unreachable**, this indicates the last known IP address of the appliance.
Link	If the device can be configured or managed via an appliance web UI, this provides a login window for the device. After you enter your **Username** and **Password**, the web UI for the device appears.
Action	Provides a **Reboot** button for Nyquist devices that have an IP address. Selecting this button reboots the device.

You can return to the Stations page by selecting **Stations**.

Viewing Zone Information

From the Zones page you can select to add, edit, or delete zones and view parameters for all existing zones.



	Icon	Number	Name	Type	Preannounce Tone	Cut Level (dB)	Audio Distribution Cut Level (dB)	Stations	Description	Multicast IP Address	Multicast Port Number
		1	Zone1	Paging+Time+Audio	1-Second	-25	0	Show	Show	239.1.1.10	6100
		2	Zone2	Paging+Time+Audio	1-Second	-6	-30	Show	Show	239.1.1.11	6104
		3	Zone3	Paging+Time+Audio	1-Second	-6	-19	Show	Show	239.1.1.12	6108
		4	Zone4	Paging+Time+Audio	1-Second	-6	-24	Show	Show	239.1.1.13	6112
		5	Zone5	Paging+Time+Audio	1-Second	-6	-24	Show	Show	239.1.1.14	6116
		6	Zone6	Paging+Time+Audio	1-Second	-6	-24	Show	Show	239.1.1.15	6120
		7	Zone7	Paging+Time+Audio	1-Second	-6	-24	Show	Show	239.1.1.16	6124
		8	Zone8	Paging+Time+Audio	1-Second	-6	-24	Show	Show	239.1.1.17	6128
		9	Zone9	Paging+Time+Audio	1-Second	-6	-24	Show	Show	239.1.1.18	6132
		10	Zone 10	Paging	None	-25	-24	Show	Show	239.1.1.20	6140
		44	Music room	Paging+Time+Audio	2-Second	-6	-17	Show	Show	239.1.1.19	6136

Figure 70. Zones Page

To view existing zones:

1. On the navigation bar, expand **Zones and Queues**.
2. Select **Zones**.
   Zone information is described in *Table 62*.
   Details about each zone can be viewed in either table format or in a card view by zone format.
3. To change the format used for the view, select the **Filter** icon.

Table 62. Zone Page Parameters

Simplified Configuration	Displays the *Simplified Configuration* page, which presents an alternate method for configuring zones (see *"Simplified Configuration" on page 220*).
Icon	Displays a visual icon that represents the zone or zone type. For example, the **Cutlery** icon can be used for a zone that contains the cafeteria, while a **Briefcase** icon can be used for a zone that contains executive offices.
Number	Displays a number associated with the zone. This number can have up to five digits.
Name	Identifies the zone by the user-created name. The name can be alphanumeric (such as *Bldg 1*) and contain up to 30 characters.
Type	Identifies the zone as being able to receive paging, time, audio, or a combination of paging, time, or audio.
Preannounce Tone	Identifies what, if any, tone should play before a paging announcement.

Table 62. Zone Page Parameters

Cut Level (dB)	Sets the device volume cut level to be used when devices included in the zone receive pages, time-scheduled tones, manually activated tones, and announcements. The cut level can range from –42 to 0.
Audio Distribution Cut Level (dB)	Sets the volume cut level to be used when devices in the zone receive audio distribution and scheduled audio (see *"Using Audio Distribution" on page 402*). The cut level can range from –42 to 0.
Stations	Displays the extensions included in the zone when **Show** is selected.
Description	Provides a description of the zone when **Show** is selected.
Multicast IP Address	Identifies the IP address for multicast calls to the zone.
Multicast Port Number	Identifies the port number for multicast calls to the zone.

Adding a Zone

To perform this procedure, you must have permission to add zones.

Note: The maximum number of zones that a Nyquist appliance can be enrolled in is 24; Admin Phones can be enrolled in a maximum of seven zones. An error displays if you attempt to add a Nyquist station to a zone and it is already enrolled in the maximum number of zones.

The number of zones that your Nyquist system can have depends on your license. (See *"Paging Zone License Expansion Package (NQ-C4000PZX)" on page 624*.)

When you create a zone, you select whether the zone will allow manual paging (Paging zone), scheduled tones (Time zone), audio distribution (Audio zone), or any combination of manual paging, scheduled tones, and audio distribution.

Table 63. Audio Activities by Zone Type

Zone Type	Type of Audio	Audio Activities
Paging	Caller speaking (optionally after a preannouncement audio clip) Announcements (prerecorded)	One-way calls that allow the caller to speak an announcement to all stations (i.e., speakers) of Paging-type zones. Announcements are also played to Paging-type zones.

Table 63. Audio Activities by Zone Type

Zone Type	Type of Audio	Audio Activities
Time	Tones	Scheduled events, routines, I/O contact closures, and manually initiated tones play to stations of Time-type zones. *Note:* These are known as "Time" zones because most Tones are played by scheduled events.
Audio	Audio distribution (usually music)	Scheduled events, routines, I/O contact closures, and manually initiated audio distributions play to stations of Audio-type zones.

If you want tones to play during active pages, you must create separate Paging and Time zones, and the Time zones must be created first. Creating Time zones first sets the priority of Time zones over Paging zones.

Warning Although a station can be assigned to more than one zone, be aware that this can cause problems if a scheduled event is assigned to two or more zones that include the same station.

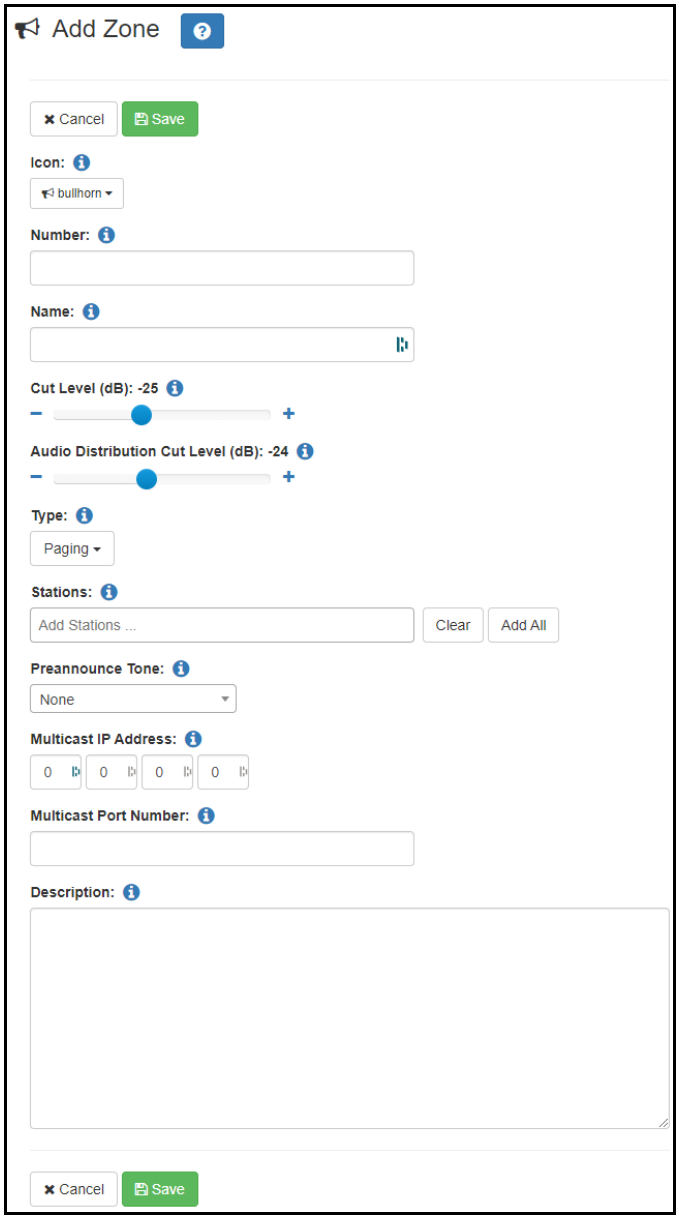


Figure 71. Add Zone Page

To add a zone:

1. On the navigation bar, expand **Zones and Queues**.
2. Select **Zones**.
3. Select the **Add** icon.
4. Complete all parameters for the zone. Parameters are described in*Table 64*.
5. Select **Save**.

Table 64. Add/Edit Zone Page Parameters

Icon	Use the drop-down menu to select a visual icon that represents the zone or zone type. For example, the **Cutlery** icon can be used for a zone that contains the cafeteria, while an **Eraser** icon can be used for a zone that contains only classrooms.
Number	Enter a number associated with the zone. A zone number can contain a maximum of five digits.
Name	Enter a name for the zone. The name can be alphanumeric (such as Bldg 1) and contain up to 30 characters.
Cut Level (dB)	Set the device volume cut level to be used when devices included in the zone receive pages, time scheduled tones, manually activated tones, and announcements. The cut level can range from −42 to 0.
Audio Distribution Cut Level (dB)	Set the volume cut level to be used when devices in the zone receive audio distributions and scheduled audio (see *"Using Audio Distribution" on page 402*). The cut level can range from −42 to 0.
Type	Identifies the zone as being able to receive some combination of paging, tones, and audio (see *Figure 63, "Audio Activities by Zone Type"*). Options are: • **Paging** • **Time** • **Audio** • **Paging+Time** • **Paging+Audio** • **Paging+Time+Audio** • **Audio+Time** *Note:* If you want tones to play during active pages, you must create separate paging and time zones and the time zones must be created first. Creating time zones first sets the priority of time zones over page zones. Stations can be in multiple zones, and you can create a paging zone (or a Paging+Audio zone) and a time zone (or Audio+Time zone) that contain the same stations.
Stations (optional)	Add extensions for the stations to be included in the zone. If scheduled events or audio distributions are using this zone and the specified stations would result in a *zone overlap* condition (see *"Zone Overlap Messages" on page 372*), this change will not be allowed. *Note:* An analog phone station cannot be added to a zone.
Preannounce Tone	Use the drop-down menu to select what, if any, tone should play before a paging announcement.
Multicast IP Address (optional)	Specify the IP address for multicast calls to the zone. Bogen suggests an address in the range 239.0.0.0–239.255.255.255, but recommends consulting with your IT department to avoid conflicts.

Table 64. Add/Edit Zone Page Parameters

Multicast Port Number (optional)	Specify the first of four port numbers used for multicast calls to this zone. Recommended range: 6000 to 7499 *Note:* This field is required if a Multicast IP Address is specified. The port number must be an even number and are assigned in increments of four. For example, if a zone was created with the Multicast Port Number of 6004, the next available Multicast Port Number would be 6008. **Caution** Not using multicast when a zone has many stations can cause performance issues.
Description	Provide a description of the zone.

Editing Zone Configuration

The Edit Zone page allows you to change zone parameters, including adding or deleting stations from the zone. You must be logged in with a role that has permission to edit a zone before completing this procedure.

Note: You cannot edit a zone number for a zone that is linked to a routine.

To edit a zone:

1. On the navigation bar, expand **Zones and Queues**.
2. Select **Zones**.
3. Select the **Edit** icon for the zone.
4. Complete all parameters for the zone.
   Parameters are described in *Table 64, "Add/Edit Zone Page Parameters," on page 218*.
5. Select **Save**.

Cloning a Zone

You can clone a source zone to a target zone, which essentially copies the list of stations of the cloned zone to the target zone. This can be very helpful for creating zones that have the same or similar list of stations as another zone. It can also be used to create a zone that encompasses the stations of multiple existing zones by cloning multiple source zones to one target zone.

To clone a zone:

1. On the navigation bar, expand **Zones and Queues**.

2 Select **Zones**.

1 If the target zone does not already exist, create it (see *"Adding a Zone" on page 215*). Cloning a zone does not create a new zone.

2 Select the **Copy Stations** icon for the source zone.

3 In the **To** combo box, specify the target zone to which all source zone Stations will be copied.

4 Select **Copy Stations**.

5 The *Edit Zone* page of the target zone is displayed with the Stations from the source zone added to this target zone.

6 Select **Save**.

Important: The stations from the source zone are not actually added to the target zone until the updated target zone is saved.

Deleting a Zone

You can delete a zone that is no longer being used.

Note: You cannot delete a zone that is linked to a routine.

To delete a zone:

1 On the navigation bar, expand **Zones and Queues**.

2 Select **Zones**.

3 Select the **Delete** icon for the zone.

4 When the confirmation page appears, select **Delete**.

Simplified Configuration

The *Simplified Configuration* page provides an alternative interface for viewing and configuring Zones.

To display the Simplified Configuration view:

1 Ensure the *Simplified Configuration* role permission is enabled.

2 On the navigation bar, expand **Zones and Queues**, then select **Zones**.

   a) Alternatively, expand **Stations** or **Amplifier and Gateway Devices**.

3 Select the **Simplified Configuration** button.

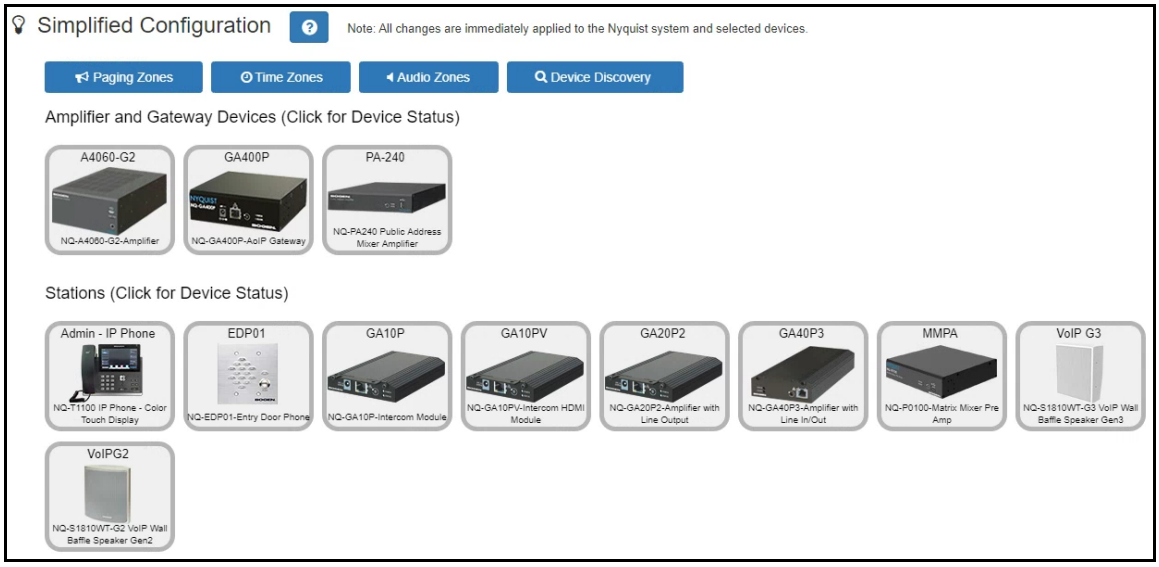


Figure 72. Simplified Configuration: Main Screen

The **Simplified Configuration** view displays an image of each appliance in the Nyquist system. The appliances are divided into lists of *Amplifier and Gateway Devices* and *Stations*.

Hovering the mouse over an appliance image displays a tooltip indicating the appliance's configured extensions.

Displaying Device Status

Clicking an appliance image displays information about the device and its configuration.

Figure 73. Simplified Configuration Device Status

The C4000 will ping the device, displaying the results in the Device Status. The other information displayed is determined by the device's type and configuration. The properties displayed correspond to the device and stations configuration settings described in the following:

- *Table 43, "View, Add, or Edit Station Configuration Parameters," on page 143*
- *Table 44, "Station Type-specific Configuration Options," on page 156*
- *Table 68, "Add/Edit Amplifier and Gateway Devices Parameters," on page 240*

Paging Zones, Time Zones, and Audio Zones

The Simplified Configuration page includes three buttons—**Paging Zones**, **Time Zones**, and **Audio Zones**—that allow you to assign appliances to zones and configure zone cut levels. Select any one of these buttons to view and edit the zones of the selected type.

To configure Paging, Time, or Audio Zones:

1. On the navigation bar, expand **Zones and Queues**, then select **Zones**.
   a) Alternatively, expand **Stations** or **Amplifier and Gateway Devices**.
2. Select the **Simplified Configuration** button.
3. Select the **Paging Zones**, **Time Zones**, or **Audio Zones** button, depending on which zone type you want to configure.

4 Select the zone to be edited using one of the following mechanisms:

   a) select the left or right arrow buttons to iterate through the currently defined zones until the target zone is displayed, or

   b) select the down-arrow button to display a list of all defined zones of the current type, then select the target zone.

5 The zone being edited is displayed at the top of the page as "**<zone type> Zones - Zone-#: <zone name>**." Appliances that are assigned to the current zone will be displayed with a green border.

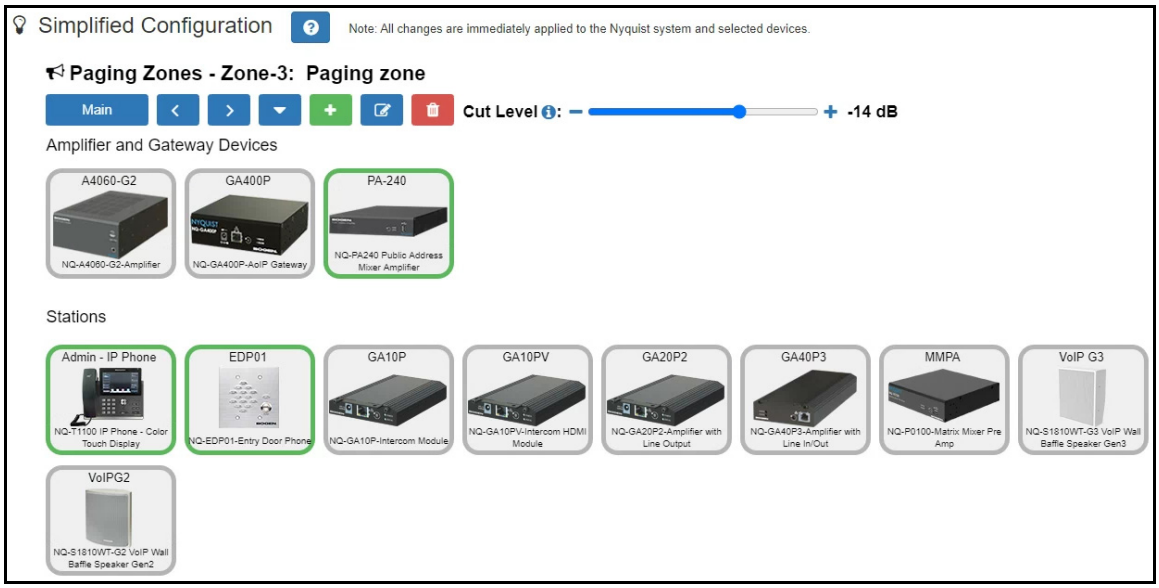


Figure 74. Simplified Configuration: Paging Zones

From the **Paging Zones**, **Time Zones**, or **Audio Zones** page, stations can be added or removed from a zone and zones can be created, edited, and deleted.

To return to the Simplified Configuration Main Page, select the **Main** button.

Add or Remove a Station to or from a Zone

To add or remove a station to or from a zone:

1 Select the target zone.

2 Click on the corresponding appliance image.

   a) If prompted whether or not to enable **Paging** for this appliance, select **Yes** or **No**.

3 An image of the appliance will be displayed with a button for each extension associated with this station (see *Figure 75, "Simplified Configuration Add or Remove Station," on page 224*). Toggle the extension button(s) to include or exclude the extension(s) from the current zone.

Important:	Keep in mind that if the zone has multiple Zone Types (i.e., Paging+Time, Paging+Audio, Audio+Time, or Paging+Time+Audio), adding or removing a station while viewing one Zone Type will add or remove the station to or from the corresponding Zone Type pages.

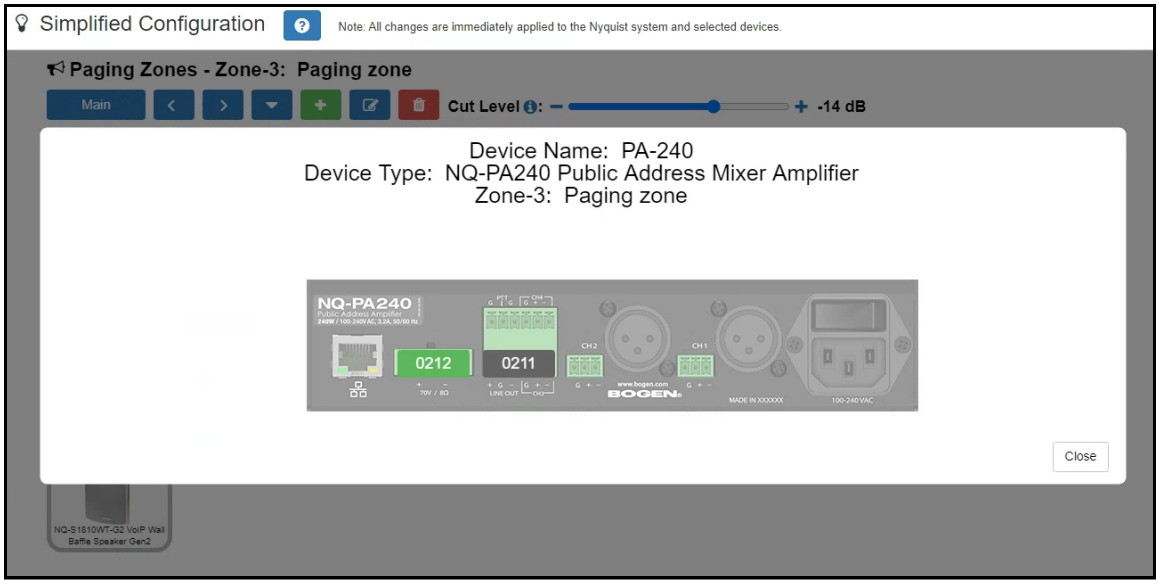


Figure 75. Simplified Configuration Add or Remove Station

Create a Zone

To create a new zone:

1. Select the add button.
2. Follow the screens of the **Create Zone** wizard. For details, see *"Adding a Zone" on page 215*.

Edit a Zone

To edit a zone:

1. Select the zone to be edited.
2. Select the edit button.
3. Follow the screens of the **Edit Zone** wizard. For details, see *"Editing Zone Configuration" on page 219*.

Delete a Zone

To delete a zone:

1. Select the zone to be deleted.
2. Select the delete button.
3. Select **Delete** to confirm.

Changing the Cut Level

To change the cut level for a zone:

1. Select the zone to be configured using one of the following mechanisms:
   a) select the left or right arrow buttons to iterate through the currently defined zones until the target zone is displayed, or
   b) select the down-arrow button to display a list of all defined zones of the current type, then select the target zone.
2. Adjust the **Cut Level** slider to adjust the level.

   For the *Audio Zones* view, the slider adjusts the zone's **Audio Distribution Cut Level**; for the *Time Zones* and *Paging Zones* views, it adjusts the zone's **Cut Level**.

Device Discovery

The **Device Discovery** button launches the *Appliance Discovery Wizard*. For details, see *"Appliance Discovery Wizard" on page 138*.

Page Queuing

Warning Changes to queues—including adding a queue, modifying an existing queue, or deleting a queue—will result in the deletion of all recorded pages that have not yet played. Changes should only be done after business hours or during a small maintenance window that does not exceed five minutes.

If you have the appropriate license, you can use the Page Queuing feature. To determine the maximum queues allowed by your system, view your **Maximum Page Stacking Queues** on the Product License page (see *"Product License" on page 24*).

The Page Queuing feature allows you to record an unlimited number of pages or messages for queuing (aka, stacking) to one or more specified zones.

Note: A zone can only be added to a single queue, but a queue may have multiple zones associated with it. Zones must be created before a queue can be created.

Page Queuing is designed to eliminate feedback that can occur if a page is made in an area where a microphone and speaker are in close proximity. With Page Queuing, the page does not start until the user recording the page has indicated that the recording is completed. It also prevents page overlapping because pages sent to a queue play one at a time.

Though similar, the Page Queuing feature differs from the Schedule Announcement (see *"Using the Schedule Announcements Feature" on page 278*) and Record Announcement (see *"Recording Announcements" on page 322*) features. The Schedule Announcement feature allows you to specify a date and time when the announcement is to be played, and the Record Announcement (DTMF code *990) fea-

ture allows you to use the admin phone to record an announcement, which is played immediately after it is recorded.

With the Page Queuing feature, the recorded page is placed in a zone's queue. The pages in the zone's queue are played in the order that they are placed in the queue.

A live page started on a zone that is playing a recorded page will cause the recorded page to be terminated and sent back to the queue. The interrupted message will play again, from the beginning of the message, when the zone becomes idle. Multi-Site Emergency-All-Call, Multi-Site All-Call, Emergency All-Call, All-Call, Alarm, Tone, and Emergency Announcement will also interrupt any playing recorded zone messages. All re-queued interrupted messages will play again, from the beginning of the message, when the zones becomes idle.

If **Enable Queue All-Call Page** is set to **Yes** in the *System Parameters*, All-Call pages will also be queued. Queued All-Call pages have a higher priority than queued zone pages and will interrupt any that are playing, which will later be replayed upon completion of the All-Call page. To start a real-time All-Call page, without queuing, dial `#0*` (`#0*#` when using DISA, or `0000001` if the PBX is not able to pass hashtags).

Important: Multi-Site All-Call pages are not queued. Similarly, All-Call pages initiated by remote facilities are not queued. These will be played in real time.

Note: Unlike queued zone pages, queued All-Call pages do not support the Message Plays parameter. They are always played once.

Selecting **Disable Audio** will cause all recorded messages to stop. The messages will resume play from the beginning when audio is re-enabled.

For information about recording pages, see *"Record Page" on page 379*.

Viewing Queues

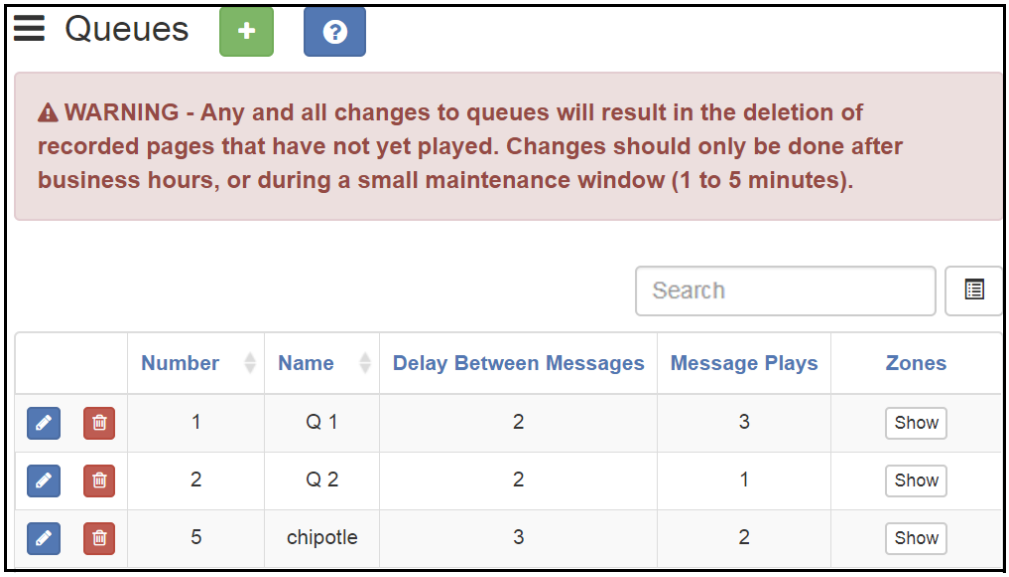


Figure 76. Queues

Using DTMF codes *991 or *991*{zone} or selecting **Record Page** from the Admin Phone or the Admin web UI allows you to initiate a queued page.

When DTMF code #{zone} is used to initiate a zone page, Nyquist will start a queued page if the zone belongs to a queue. If you want to start a real-time page instead, dial #{zone}*.

To view existing queues:

1. On the navigation bar, expand **Zones and Queues**.
2. Select **Queues**.
   Table 65 describes the Queue information:

Table 65. Queues Page Parameters

Number	Number that the user assigns to the queue.
Name	Name that the user assigns to the queue.
Delay Between Messages	Number of seconds to pause between pages. The delay can range between 1 and 10 seconds. The default is 2 seconds.
Message Plays	How many times each page in the queue will play. The number can range between 1 and 3. The default is 1, which means that the message plays only one time.
Zones	Select **Show** when viewing a queue to see the list of zones assigned to the queue. When adding a queue, only zones not already assigned to a queue and that are **Paging**, **Paging+Time**, **Paging+Audio**, and **Paging+Time+Audio** type appear in the drop-down menu. *Note:* A zone can only be associated to a single queue.

Adding a Queue

Depending upon your license, you can create multiple queues for stacking pages, and a queue may have one or more zones. However, a zone can only be associated with a single queue.

Warning Changes to queues—including adding a queue, modifying an existing queue, or deleting a queue—will result in the deletion of all recorded pages that have not yet played. Changes should only be done after business hours or during a small maintenance window that does not exceed 5 minutes.

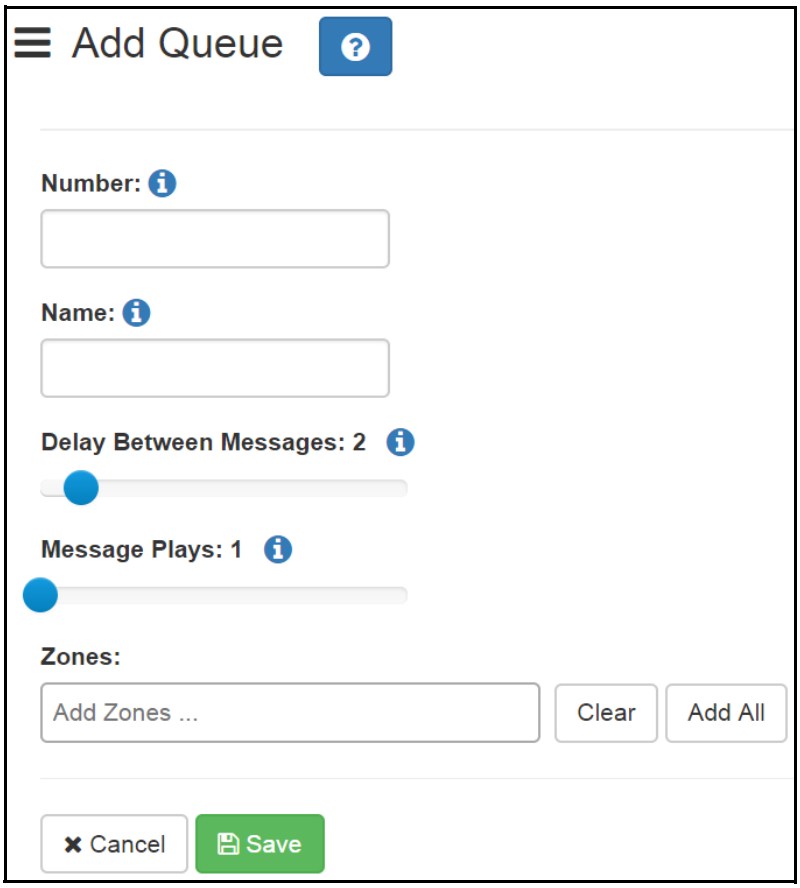


Figure 77. Add Queue

To create a queue:

1. On the navigation bar, expand **Zones and Queues**.
2. Select **Queues**.
3. Select the **Add** icon.
4. Complete the Add Queue parameters. (See *Table 65, "Queues Page Parameters," on page 227*.)
5. Select **Save**.

Editing a Queue

You can edit a queue to change any of its parameters.

Warning Changes to queues—including adding a queue, modifying an existing queue, or deleting a queue—will result in the deletion of all recorded pages that have not yet played. Changes should only be done after business hours or during a small maintenance window that does not exceed 5 minutes.

To edit a queue:

1. On the navigation bar, expand **Zones and Queues**.
2. Select **Queues**.
3. Select the **Edit** icon next to the queue that you want to modify.
4. Make desired changes to the queue parameters. (See *Table 65, "Queues Page Parameters," on page 227*.)
5. Select **Save**.

Deleting a Queue

You can delete a queue that is no longer needed.

Warning Changes to queues—including adding a queue, modifying an existing queue, or deleting a queue—will result in the deletion of all recorded pages that have not yet played. Changes should only be done after business hours or during a small maintenance window that does not exceed 5 minutes.

To delete a queue:

1. On the navigation bar, expand **Zones and Queues**.
2. Select **Queues**.
3. Select the **Delete** icon next to the queue that you want to delete.
4. When prompted, select **Delete**.

Sound Masking Zones

A sound masking zone consists of one or more sound masking stations, each one corresponding to an amplifier channel attached to one or more speakers. Each sound masking station, however, can be associated with only one sound masking zone and cannot be used for any other purpose (e.g., announcements, paging, etc.).

The speakers associated with the stations within a sound masking zone will play generated noise designed to mask unwanted sound. This can reduce or eliminate the perception of sound, usually to minimize distracting noise and/or increase privacy.

Upon initial exposure, people may require time to acclimate to the masking sound. *Ramping* facilitates this process by playing the masking sound at a lower level (−10 dB relative to the final level) and gradually increasing the level to the final level over a masking zone-specific number of days (20 or 30 days), giving people time to slowly get used to the masking sound.

For similar reasons, it may be helpful, even after the initial ramping period, to gradually increase and decrease the masking sound levels, such as at the beginning and ending of each exposure period. For example, you may want to gradually increase the level by +10 dB at the beginning of each day and gradually decrease it by −10 dB at the end of each day. This can be accomplished by using scheduled routines (see *"Using Routines" on page 425*) that include the SM-Scheduled-Ramp action, which can gradually increase or decrease the masking sound volume over a period of one to two hours.

Tip: There are several Routine actions that are available for controlling sound masking operations: SM-Enable-Zone, SM-Disable-Zone, SM-Scheduled-Ramp, and SM-Set-Output-Gain. For more details, see *"Using Routines" on page 425*.

When a masking zone amplifier detects an Emergency-All-Call announcement, an Alarm tone or Emergency announcement that plays to all speakers, or the Disable-Audio routine action or dashboard control, the masking sound is immediately muted to allow important notifications to be heard. Once the announcement has completed, the masking sound will be automatically ramped up to its configured level over a period of five minutes. This also occurs whenever the masking zone signal has been disabled and re-enabled or when the appliance is restarted, such as a reboot, power cycle, or firmware update.

Note: Sound masking is *not* muted for an Emergency Announcement or Alarm that is being played to a specific zone.

Privacy needs often vary throughout the day and week. Several routine actions—SM-Disable-Zone, SM-Enable-Zone, and SM-Set-Output-Gain—allow you to enable, disable, and adjust the masking sound levels of your sound masking zones via scheduled and/or triggered routines (see *"Using Routines" on page 425*).

Viewing Sound Masking Zones

To view existing Sound Masking Zones:

1. On the navigation bar, expand **Zones and Queues**.
2. Select **Sound Masking Zones**. See *Table 66, "Sound Masking Zones Parameters," on page 231* for details.

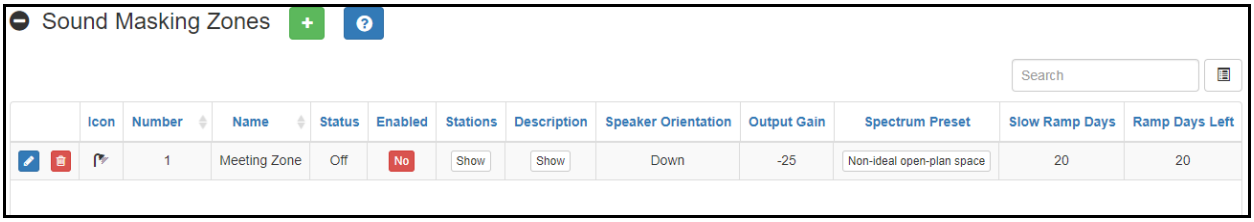


Figure 78. Sound Masking Zones

Table 66. *Sound Masking Zones* Parameters

Edit button Edit this sound masking zone.

Delete button Delete this sound masking zone.

Note: An active sound masking zone must be disabled before it can be deleted.

Start Ramping button Start ramping up the sound masking noise for this zone.

Note: Only available when the sound masking zone is enabled.

Stop Ramping button Stop ramping up the sound masking noise for this zone.

Note: Only available when the sound masking zone is enabled.

Note: Stopping the ramping up process does not stop the sound masking; it sets the level to the defined, non-ramping gain level.

Icon Displays the icon configured for this zone.

Number Displays the unique number configured for this zone.

Name Displays the name configured for this zone.

Status Indicates the current sound masking status.

Valid values are:

- **On**: Sound masking is currently active.
- **Off**: Sound masking is currently inactive.
- **Pause**: Sound masking has been temporarily paused, such as when audio is disabled.
- **Ramping**: Sound masking is currently active and slowly ramping to full volume.

Enabled Indicates whether or not this sound masking zone is enabled (i.e., **Yes** indicates signal is being played).

Tip:	On the Sound Masking Zones page, this is a button that can be used to enable or disable the sound masking noise.

Stations Displays which Sound Masking stations are included in this sound masking zone.

Description Displays the configured description of this sound masking zone.

Table 66. *Sound Masking Zones* Parameters (continued)

Speaker Orientation	Indicates the configured orientation of the speakers. Valid values are **Up** and **Down**.
Output Gain	Indicates the configured output gain (in dB) of the sound masking noise. The default value is −35 dB.
Spectrum Preset	Indicates the preset frequency spectrum to be played for sound masking. The available options are described below.

Important: To change the Spectrum Preset for an active masking zone, disable the zone, change the preset, then re-enable the zone.

Closed-plan space	Recommended for private office or small conference room with some reflective surfaces, absorptive ceiling, and furnishings.
Good open-plan space	Suitable for open office with 4- to 5-foot high cubical panels, some reflective surfaces, and moderate furniture absorption.
Ideal open-plan space	Suitable for open offices with 5-foot or higher cubical panels, absorptive ceilings and furnishings, and proper layout.
NCB Contour	Noise Criterion Balanced (NCB) Contour may be used to evaluate the acceptability of masking sound in various non-industrial environments.
Non-ideal open-plan space	Recommended for open office with no cubical panels or with cubical panels under 4-foot high, reflective surfaces, and moderate furniture absorption.
NRC Canada Contour	A cost-effective open-plan environment masking spectrum published by the National Research Council, Canada.
NC40 Contour	Noise Criterion (NC) 40 Contour may be used to evaluate the acceptability of masking sound in an open office environment.

Slow Ramp Days	Indicates the number of days over which the masking noise will gradually increase from −10 dB below the specified Output Gain level to the specified level. Valid values are 20 and 30 days. Gradually ramping up the sound levels this way helps listeners to slowly acclimate to the masking noise over time to avoid or minimize discomfort.
Ramp Days Left	The number of days remaining before the masking noise will reach the specified Output Gain level when ramping up the sound level.

Adding and Editing a Sound Masking Zone

Before you can create a Sound Masking Zone, you must first create one or more Sound Masking stations. Unlike a standard station, however, a Sound Masking station is created via the *Station Manage-*

ment view of the amplifier to be used as a Sound Masking station (see *"Using Station Management for Amplifiers and Gateway Devices" on page 244*). Edit each amplifier channel to be included in the Sound Masking Zone (see *"Editing Station Configuration Settings" on page 155* for details) and set its **Station Type** to **Sound Masking**.

Warning	If downward-facing speakers are installed and two amplifier stations are used within the same masking zone, it is critical that either the stations come from different amplifiers (preferable) or the In-Phase setting for the two stations are configured differently (i.e., one Yes, one No). Otherwise, there will be phasing issues or uncontrollable variations in masking levels.

Once one or more Sound Masking stations have been defined, a Sound Masking Zone can be created.

Important:	When adding a new Sound Masking station, always use the **Station Management** button of an amplifier listed in the *Amplifiers and Gateway Devices* view and select a channel of an existing amplifier. Adding a station from the *Stations* view and assigning a **Station Type** of **Sound Masking** will not associate the station with an actual device.

Warning	Sound masking amplifiers and stations are not monitored by Station Supervision.

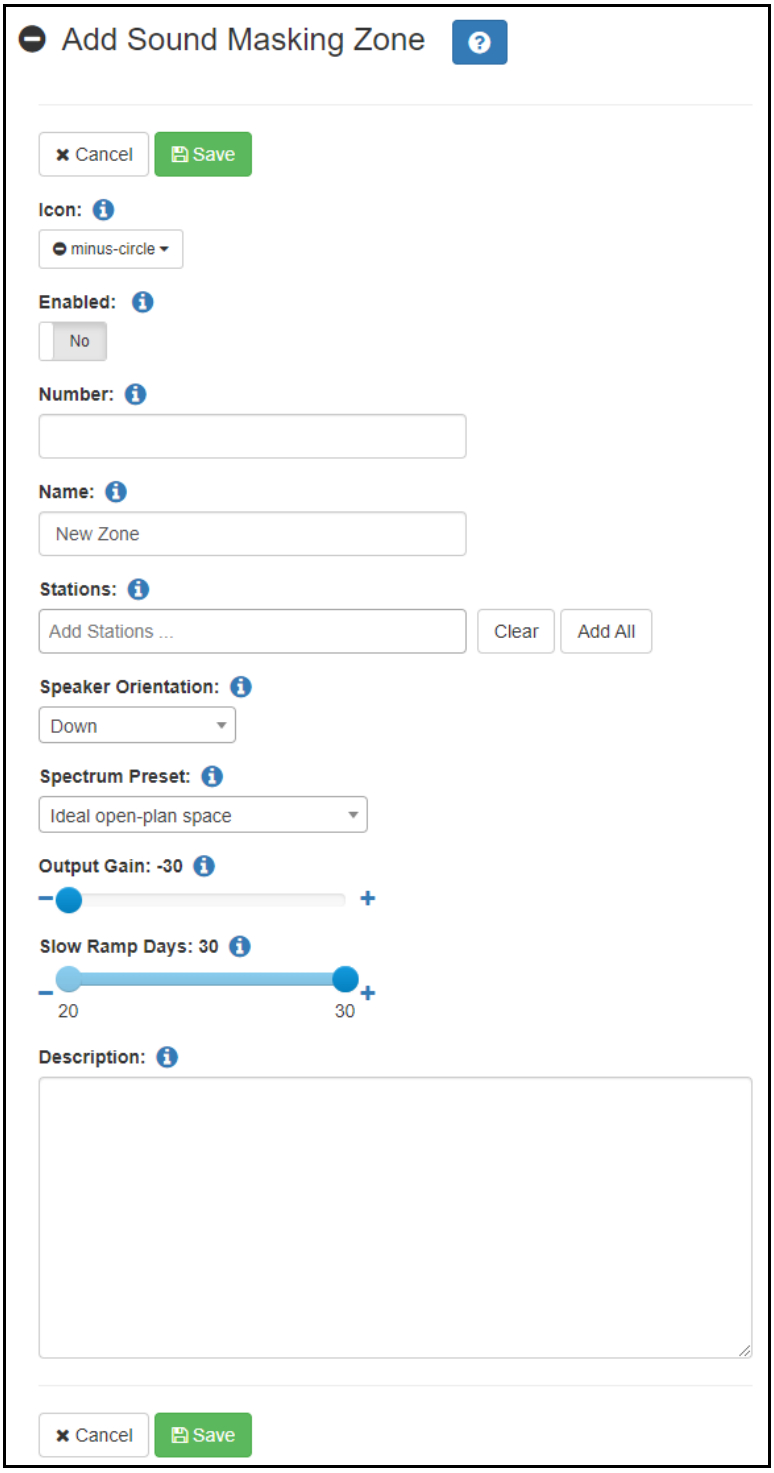


Figure 79. Add Sound Masking Zone page

To create or edit a sound masking zone:

1. On the navigation bar, expand **Zones and Queues**.
2. Select **Sound Masking Zones**.
3. Select the Add icon.
4. Complete the parameters to the Add Sound Masking Zone page (see *Table 66, "Sound Masking Zones Parameters," on page 231*).

5 Select **Save**.

Managing Amplifiers and Gateway Devices

You can assign stations to an audio power amplifier or a public address/mixer amplifier provided the amplifier has an available port. The station must be assigned manually but the amplifier itself can be automatically discovered by your Nyquist system.

Viewing Amplifier and Gateway Devices

Through the *Amplifier and Gateway Devices* page, you can view information about all audio power amplifiers and public address/mixer amplifiers configured for your Nyquist system; select to add, edit, or delete these devices; select to manage stations for an amplifier; and select to configure Push-To-Talk parameters for an amplifier.

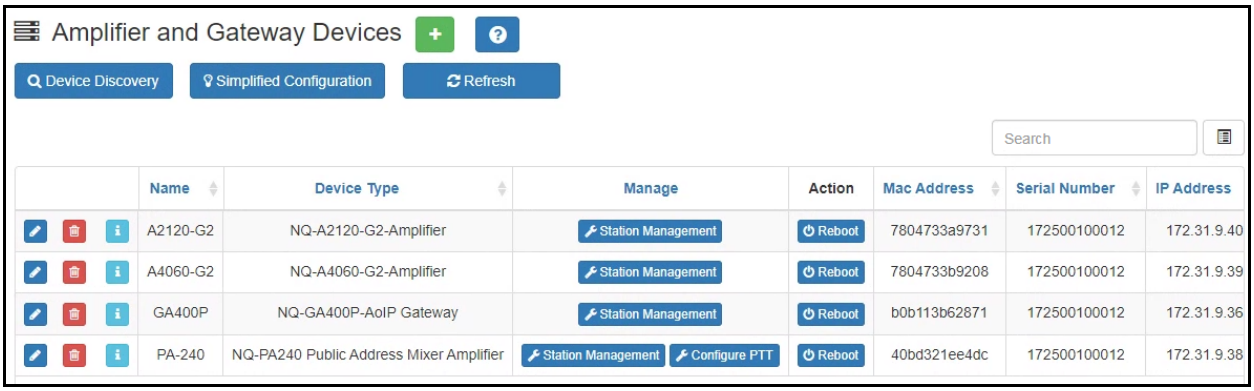


Figure 80. Amplifier and Gateway Devices

To view amplifiers and gateway devices attached to your network:

On the navigation bar, select **Amplifier and Gateway Devices**.

Table 67 describes the parameters for each amplifier or gateway device:

Table 67. Amplifier and Gateway Devices Page

Edit	Edit the amplifier or gateway device.
Delete	Delete the amplifier or gateway device.
Device Status	Display the device status for this amplifier or gateway device.
Name	Provides a name for the amplifier or gateway device.
Device Type	Provides the type of device, such as *NQ-A2120-Amplifier*.
Manage	Provides a link to the **Station Management** and, if applicable, **Configure PTT** tools for the amplifier or gateway device.
Action	Provides a **Reboot** button to select the if amplifier or gateway device needs to be rebooted.
MAC Address	Provides the MAC address for the amplifier or gateway device.

Table 67. Amplifier and Gateway Devices Page (continued)

Serial Number	Provides the serial number of the amplifier or gateway device.
IP Address	Provides the IP address of the amplifier or gateway device.
Link	Provides link to the amplifier or gateway device's UI.
Status	Provides the status of the amplifier or gateway device. Possible statuses include: • **Unknown**: The server is unable to determine the state of the amplifier or gateway device. • **Unreachable**: The server is unable to ping the amplifier or gateway device. • **Registering**: More than one IP address has been found. Stations may still be registering with new IP addresses. • **Up: # of # stations**: Indicates the number of registered available stations attached to the amplifier or gateway device. If the numbers do not match, then one or more stations attached to the amplifier or gateway device are not available for service. The station or stations may be in the process of registering, or if the condition persists, there may be a configuration error. *Note:* When an amplifier is used for Sound Masking, the Up status indicator will not include a station count. *Note:* After an amplifier or gateway device is rebooted, it can take a few minutes for all associated stations to register with the Nyquist server (usually less than three minutes).
Description	Select **Show** to view the user-provided description of the amplifier or gateway device.
VLAN Configuration	Provides how the VLAN configuration is set. Options are: • **Server**: Allows you to configure the VLAN settings via the Nyquist server web interface. The configured setting will then be sent to the Nyquist appliance by the Nyquist server. • **Network/Device**: The Nyquist devices will either listen for VLAN configuration from DHCP (Network) or the VLAN settings can be configured via the Nyquist device's web interface (Device). • **Disabled**: VLAN is disabled and not used.
VLAN ID	Provides the VLAN for the amplifier or gateway device. The LAN ID parameters range from 2 through 4094 and pertain to the amplifier or gateway device's network interface (not to the ports or stations). *Note:* This field can only be changed when the **Server** option is used for **VLAN Configuration**.
VLAN Priority	Provides the priority for the port. Values range from 0 through 7. *Note:* This field can only be changed when the **Server** option is used for **VLAN Configuration**.
Web Username	Provides the username for logging into the amplifier or gateway device's web UI.
Firmware	Provides information about firmware that is loaded onto the amplifier or gateway device.

Table 67. Amplifier and Gateway Devices Page (continued)

Number of Stations	Provides the number of stations associated to the amplifier. This number limits the number of associated stations that can be added to the amplifier. The number is usually provided by the amplifier during device discovery so changing the number is not necessary. Do not change this number unless you are manually adding the amplifier (i.e., not using device discovery) or have been instructed to change it.
Channels	Displays the channels configured on the amplifier via bridge switch positions.
Enable SIP TLS	Enables the use of TLS to secure SIP traffic for this amplifier or gateway device. See *"VoIP Security" on page 18* for further details.
Enable SRTP	Enables encryption of voice traffic for this amplifier or gateway device. See *"VoIP Security" on page 18* for further details.

Adding Amplifier and Gateway Devices

From the Add Amplifier and Gateway Devices page, you can add a new audio power amplifier to your Nyquist system.

Tip: Amplifiers and gateway devices can also be added using the "*Appliance Discovery Wizard*", as described on page 138.

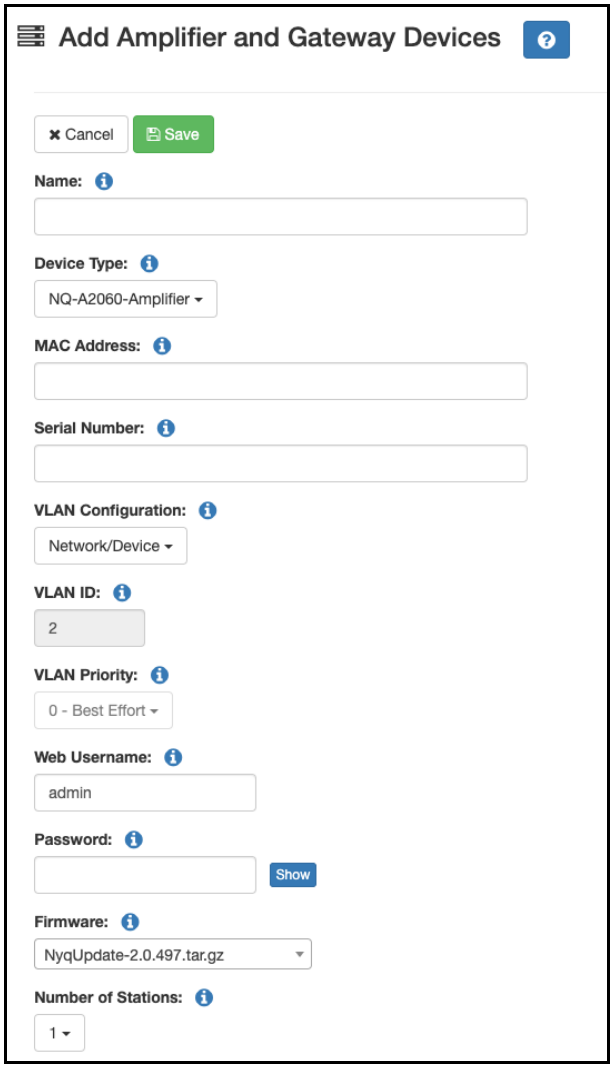


Figure 81. Add Amplifier and Gateway Devices

To add an amplifier:

1. On the navigation bar, select **Amplifier and Gateway Devices**.
2. On the *Amplifier and Gateway Devices* page, select the **Add** icon.
3. Complete the parameters on the *Add Amplifier and Gateway Devices* page (see *Table 68*).
4. Select **Save**.

After you save the information, the Station Management page appears so that you can add stations and select the settings to be applied to them (see *"Using Station Management for Amplifiers and Gateway Devices" on page 244*).

Table 68. Add/Edit Amplifier and Gateway Devices Parameters

Name	Enter a name for the amplifier or gateway device.
Device Type	Select the type of device. Options are: • NQ-A2060[-G2]-Amplifier • NQ-A2120[-G2]-Amplifier • NQ-A2300[-G2]-Amplifier • NQ-A4060[-G2]-Amplifier • NQ-A4120[-G2]-Amplifier • NQ-A4300[-G2]-Amplifier • NQ-GA400P-AoIP Gateway • NQ-PA120 Public Address Mixer Amplifier • NQ-PA240 Public Address Mixer Amplifier • NQ-PA600 Public Address Mixer Amplifier
MAC Address	Enter the MAC address for the amplifier or gateway device.
Serial Number	Enter the serial number of the amplifier or gateway device.
VLAN Configuration	Select how the VLAN configuration is set. Options are: • **Server**: Allows you to configure the VLAN settings via the Nyquist server web interface. The configured setting will then be sent to the Nyquist appliance by the Nyquist server. • **Network/Device**: The Nyquist devices will either listen for VLAN configuration from DHCP (Network) or the VLAN settings can be configured via the Nyquist device's web interface (Device). • **Disabled**: VLAN is disabled and not used.
VLAN ID	Select the VLAN for the amplifier or gateway device. The LAN ID parameters range from 2 through 4094 and pertain to the amplifier's network interface (not to the ports or stations). *Note:* This field can only be changed when the **Server** option is used for **VLAN Configuration**.
VLAN Priority	Select the priority for the port. Values range from 0 through 7. *Note:* This field can only be changed when the **Server** option is used for **VLAN Configuration**.
Web Username	*Note:* When applicable, provides a username for logging into the web interface of the device hosting the station.
Web Password	Provide a password for logging into the device's web UI. Select **Show** to reveal a previously set password.
Web Password Confirmation	If **Web Password** is not specified, the **Default Web Password** system parameter value is used (see *Table 23, "Edit System Parameters Page," on page 69*). If **Default Web Password** is unspecified, this parameter is required. *Note:* Nyquist appliances have distinct web passwords for non-standalone and standalone modes. **Web Password** only applies to non-standalone mode.

Table 68. Add/Edit Amplifier and Gateway Devices Parameters (continued)

Firmware	Provides information about firmware that is loaded onto the amplifier or gateway device. 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 later than the one installed on the appliance, an automatic firmware update occurs. To prevent an automatic update, leave this **Firmware** parameter empty.
Number of Stations	Select how many stations are associated with the device based on the number of ports.
Channels	Select the channels configured on the amplifier via the switch position.
Enable SIP TLS	Enables the use of TLS to secure SIP traffic for this amplifier or gateway. This is disabled by default. See *"VoIP Security" on page 18* for further details.
Enable SRTP	Enables encryption of voice traffic for this amplifier or gateway. This is disabled by default. See *"VoIP Security" on page 18* for further details.
Description	Provide a description of the device.

Editing Amplifier and Gateway Devices

The Edit Amplifier and Gateway Devices page allows you to change parameters for an amplifier or gateway device. You can also select the **Station Management** button to associate stations to the amplifier or gateway device.

To edit an amplifier or gateway device:

1. On the navigation bar, select **Amplifier and Gateway Devices**.
2. On the *Amplifier and Gateway Devices* page, select the **Edit** icon.
3. Complete the parameters on the *Edit Amplifier and Gateway Devices* page. (See *Table 68, "Add/Edit Amplifier and Gateway Devices Parameters," on page 240*.)
4. Select **Save**.

Configuring Push-To-Talk for a Public Address Mixer Amplifier

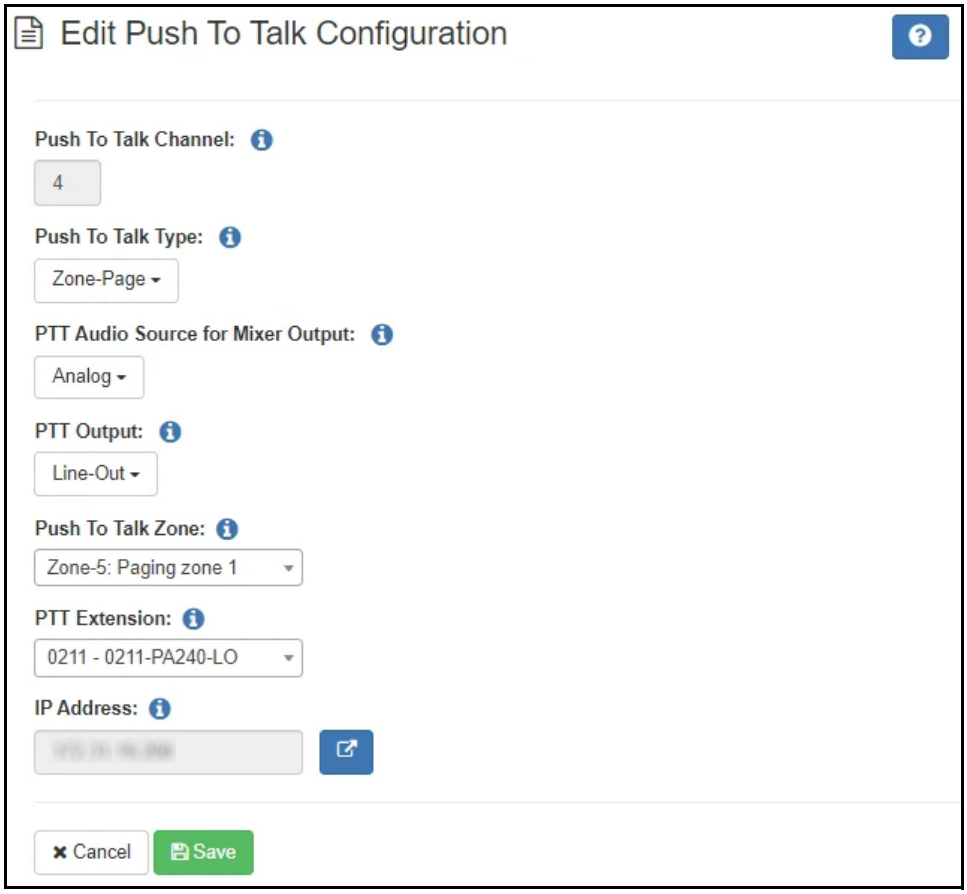


Figure 82. Push-To-Talk Configuration Page (PAMA)

To edit Push-To-Talk configuration for a Public Address Mixer/Amplifier:

1. On the navigation bar, select **Amplifier and Gateway Devices**.
2. For the public address mixer amplifier that you want to configure, in the **Manage** column, select **Configure PTT**.
3. Specify parameters from the Edit Push To Talk Configuration page. For details, see *Table 69, "PAMA Push-To-Talk Configuration Parameters," on page 243*.
4. Select **Save**.

Table 69. PAMA Push-To-Talk Configuration Parameters

Push To Talk Channel	Channel 4 is the only available PTT channel.
Push To Talk Type	Select the type of activity that is performed when the button is pressed on the microphone. Options are: • Disabled • Analog-Output • All-Call-Page • Emergency-All-Call-Page • Zone-Page • Record-Zone-Page • Multi-Site-All-Call-Page • Multi-Site-Emergency-All-Call-Page *Note:* For all selections other than **Disabled**, the DSP Router settings of the device are overridden to route the PTT microphone input signal (**Analog 4**) to the line output and speaker output channels (**Line Out** and **Speaker Out**). *Tip:* To prevent the PTT microphone signal from being sent to the network, select Analog-Output. All other settings (other than Disabled) will send the PTT microphone signal over the network.
PTT Audio Source for Mixer Output	*Note:* This field does not appear if **Push To Talk Type** is set to **Disabled** or **Analog-Output**. Specifies whether the PTT microphone signal is sent to the network output or both the analog and network outputs. If **Analog** is selected, the PTT microphone input is routed as specified in the **PTT Output** setting as well as being sent over the network. If **Network** is selected, the PTT microphone input is routed only through the network. Note that this could create a small but noticeable delay.
PTT Output	Specifies the amplifier output used for the PTT microphone signal if **Push To Talk Type** is Analog-Output or **PTT Audio Source for Mixer Output** is **Analog**. Options are: • Disabled • Line-Out • Speaker-Out • Both
Push To Talk Zone	*Note:* This field appears only if **Push To Talk Type** is set to **Zone-Page or Record-Zone-Page**. Select the zone to receive the page.

Table 69. PAMA Push-To-Talk Configuration Parameters (continued)

PTT Extension	The station extension to be displayed to call recipients for PTT calls from this station.
IP Address	Displays the IP address of the device, if known, and a **Link** button that allows you to start the device's UI. If the Nyquist server has not discovered the device's IP address, the **Link** button does not appear.

Using Station Management for Amplifiers and Gateway Devices

Depending on the **Device Type**, the *Station Management* screen for **Amplifier and Gateway Devices** can show Ports listed as **Channel A** to **Channel D** (e.g., NQ-A2xxx/A4xxx Amplifiers), **Speaker Out** and **Line Out** (e.g., NQ-PAxxx Amplifiers), or **Output 1** and **Output 2** (e.g., NQ-GA400P AoIP Gateway).

The number of ports that appear for an amplifier in the *Station Management* page depends on the number of ports allowed by the device type. For example, the A2120 Audio Power Amplifier will have only two ports appear on the *Station Management* page while the four-channel A4120 Audio Power Amplifier, will have four ports.

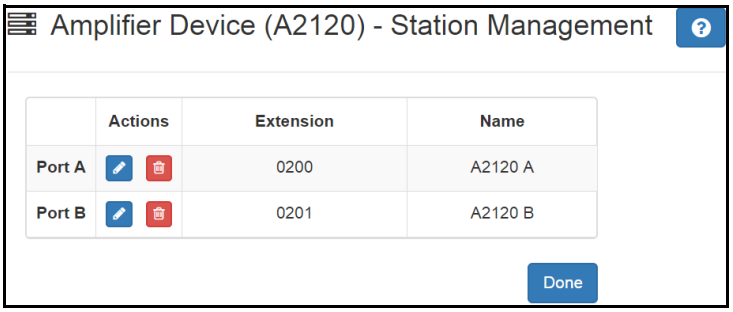


Figure 83. Station Management for Two-Channel Amplifier

If you select *Station Management* for a Public Address/Mixer Amplifier (NQ-PA120, NQ-PA240, or NQ-PA600), the **Speaker Out** and **Line Out** appear.

To use Station Management for amplifiers:

1. On the navigation bar, select **Amplifier and Gateway Devices**.
2. Select **Station Management** for the desired amplifier.

Note: The Station Management page for amplifiers automatically appears when you create a new amplifier. See *"Adding Amplifier and Gateway Devices" on page 238*.

---

3. If you want to delete a port:
   a) Select the **Delete** icon next to the port.
   b) When prompted, select **Delete**.

4 If you want to edit the station associated with a port, select the **Edit** icon next to the port and follow the steps for editing a station (see *"Editing Station Configuration Settings" on page 155*).

Warning If an amplifier has one station defined as type **Sound Masking**, then all stations for that amplifier should be defined as **Sound Masking**. For more information, see *"Sound Masking Zones" on page 229*.

5 Select **Done**.

Deleting Amplifier and Gateway Devices

You can delete an amplifier device through the Amplifier and Gateway Devices page.

To delete an amplifier:

1 On the navigation bar, select **Amplifier and Gateway Devices**.

2 On the *Amplifier and Gateway Devices* page, select the **Delete** icon next to the amplifier or gateway device that you want to delete.

3 When prompted, select **Delete**.

Managing Roles and Users

Nyquist uses roles to control system configuration, access, and use. When you create a user, you assign a role that determines what the user sees from the dashboard and what tasks the user can perform.

Nyquist provides four default roles. These roles can be edited or deleted by anyone assigned permissions to do so. Of the default roles, only the Admin role has the ability to add users and to add, edit, and delete roles.

Table 70. Default Roles

Admin	Has access to the entire system and can perform all tasks.
OpTech	Can operate the system and can view, but not change, system configurations.
Operator	Can operate the system, but cannot view or change system configurations.
User	Can only operate specific parts of the system.

Viewing Roles

The default roles of Admin and OpTech can view existing roles. If you are assigned one of these roles or a user-created role that allows it, you can assign View Roles permissions to other roles.

To view roles:

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

The Roles page appears. *Table 71 on page 246* describes the parameters that appear on this page.

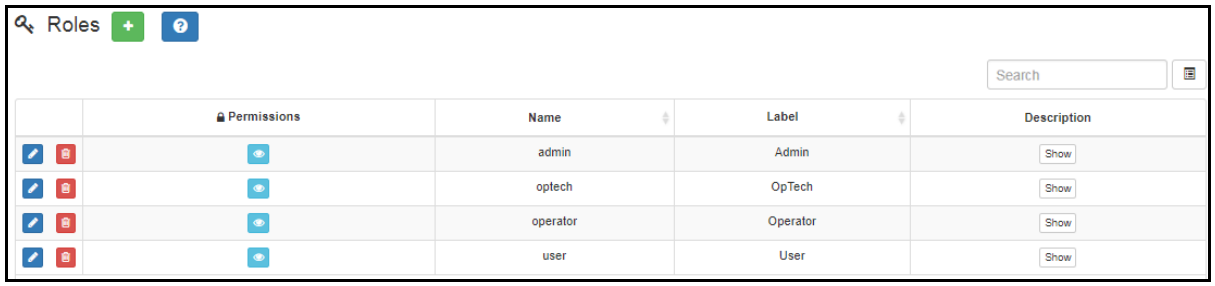


Figure 84. Roles Page

Table 71. Roles Page Parameters

Permissions	When the icon is selected, displays the Edit Admin Permissions page where the permissions assigned to this role can be viewed or changed.
Name	Displays the nomenclature created for the role. *Note:* Valid characters include uppercase letters (A–Z), lowercase letters (a–z), numerals (0–9), space, and the following special characters: **! @ $ * ? - . , .**

Table 71. Roles Page Parameters

Label	Displays the role name that is used when creating a user. *Note:* Valid characters include uppercase letters (A–Z), lowercase letters (a–z), numerals (0–9), space, and the following special characters: **! @ $ * ? - . , .**
Description	When the **Show** button is selected, displays a brief description of the role. *Note:* Valid characters include uppercase letters (A–Z), lowercase letters (a–z), numerals (0–9), space, and the following special characters: **! @ $ * ? - . , .**

Adding a Role

If none of the default roles have the exact permissions that you want for a role, you can edit the permissions for a default role or create a new role. For example, only the Admin default role has the ability to create a new station and to add a new user. You could edit the permissions for an existing role or create a new role specifically for use when adding stations or users. (For information about adding stations, *see "Adding a Station" on page 185*.)

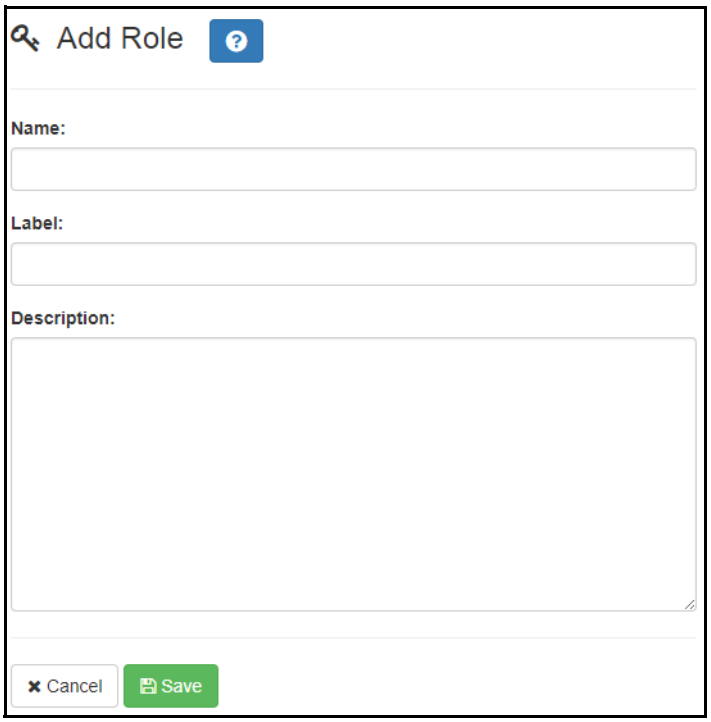


Figure 85. Add Role Page

Note: To perform this task, you must be logged in with a role that has permission to add other roles.

To add a role:

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

2 On the *Roles* page, select the **Add** icon.

3 On the *Add Role* page, add the name, label, and description for this role. (See *Table 71, "Roles Page Parameters," on page 246*.)

4 Select **Save**.

5 On the *Roles* page, select the **Permissions** icon for the role just added.

6 Set permissions for this role. (*See "Assigning and Editing Permissions" on page 248*.)

7 Select **Save**.

Editing a Role

You may want to change the names, labels, and descriptions assigned to a role for clarity purposes. For example, you could rename the default role "User" to "Agent." In some cases, you may want to change the permissions assigned to an existing role. In both of these scenarios, you would edit a role.

Note: To perform this task, you must be logged in with a role that has permission to edit other roles.

To edit a role:

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

2 On the *Roles* page, select the **Edit** icon next to the role that you want to edit.

3 On the *Edit Role* page, make any desired changes to the **Name**, **Label**, and **Description** fields. (See *Table 71, "Roles Page Parameters," on page 246*.)

4 Select **Save**.

5 On the *Roles* page, select the **Permissions** icon.

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

7 Select **Save**.

Assigning and Editing Permissions

Selecting the **Permissions** icon for a role displays the *Edit Permissions* page, which allows you to set permissions, for example, the ability to edit or view Schedule Settings. Permission parameters differ depending upon the option. For example, permissions for the Dashboard (and for most Dashboard features) are limited to **View**, while available permissions for Schedule Announcements include **Create**, **Delete**, **Edit**, and **View**.

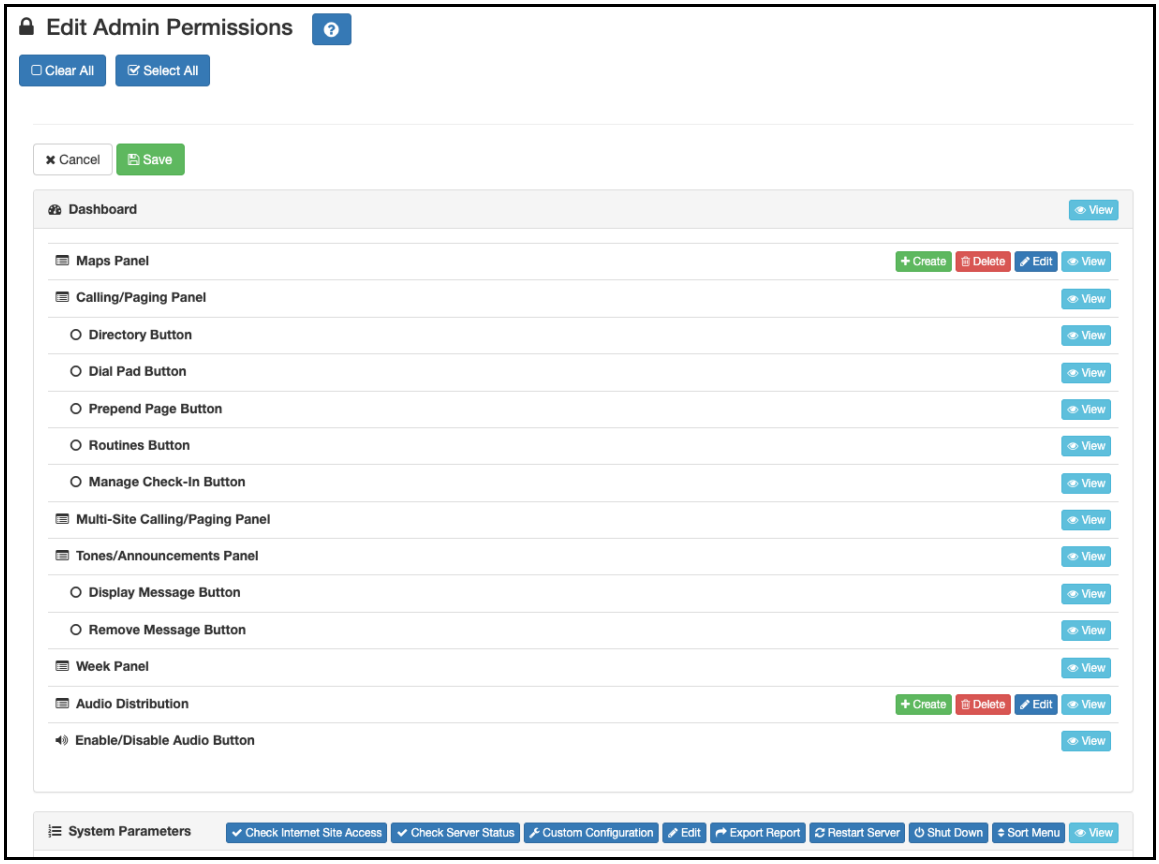


Figure 86. Edit Permissions Page

Table 72. Descriptions of Permission Buttons

+ Create	Allows user to create a new item, such as a new user.
Delete	Allows user to delete an item.
Edit	Allows user to edit an item.
View	Allows user to view an item.
Manage	Allows user to manage items. This option pertains only to playlists.
Import/Export	Allows user to import or export a system backup file.
Settings	Allows user to set parameters for system backup jobs.
Restore	Allows user to restore a system backup.
Sort Menu	Allows user to change the order of the navigation bar menu.

Table 72. Descriptions of Permission Buttons

	Allows user to import a system update.
	Allows user to verify Nyquist server can access URLs required to run properly. For details, see *"Check Internet Site Access" on page 44*.
	Allows user to check and display the status of the Nyquist server. For details, see *"Check Server Status" on page 44*.
	Allows user to update Actions and Custom Variables, SNMP Configuration, and Syslog Configuration.
	Allows user to export an Excel spreadsheet with configuration information. For details, see *"Exporting a Report" on page 23*.
	Allows user to restart the Nyquist server. For details, see *"Restarting the Server" on page 29*.
	Allows user to shut down the Nyquist server. For details, see *"Shutting Down the Server" on page 43*.

Note: To perform this task, you must be logged in with a role that has permission to assign or edit permissions.

To assign or edit permissions:

1. On the navigation bar, select **Roles**.
2. On the *Roles* page, select the **Permissions** icon next to the role for which you are assigning or editing permissions.
3. On the *Edit Permissions* page, select the appropriate buttons to assign permissions to the role.
4. Select **Save**.

Note: The C4000 will not allow the minimum administrative permissions to be revoked from the current user's role if they are the only administrator, as this could result in a system with no administrators.

Deleting a Role

If a role is not being used by your organization or the Nyquist system, you can delete the role, provided that role is not associated with a user.

Note: A warning appears if you attempt to delete a role that is associated with a user.

To delete a role:

1. On the navigation bar, select **Roles**.
2. On the *Roles* page, select the **Delete** icon next to the role that you want to delete.

3 When prompted, select **Delete**.

Viewing Users

Users are personnel who are authorized to use Nyquist. When you create a user, you assign the user a role that determines what the user sees from the Dashboard of their web interface station and what tasks the user can perform on the Nyquist system. You can only create a user if you have been assigned the default Admin role or a custom role that provides permissions to create a user.

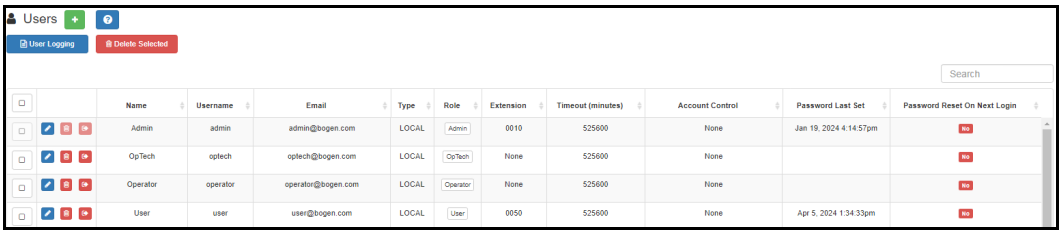


Figure 87. Users Page

Tip: It can often be useful to create virtual users. For example, create a virtual user to represent a room or location, particularly if the location is used by more than one person. Or create one or more virtual users with which to execute Routines (see *"Using Routines" on page 425*), restricting the CoS permissions to only those necessary to execute the relevant Routines.

To view users:

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

2 To filter the list of users, enter the desired text into the **Search** field. All fields will be searched for the specified text value. For example, enter "Bogen" to find each user that contains the (case-insensitive) text "Bogen" within the displayed listing.

The following table describes the information displayed for each user.

Table 73. User Page Parameters

Edit	Opens the Edit User view for the user.
Delete	Deletes the user.
Logout	Logs this user out of any active web sessions on this C4000.
Name	Displays the name of the user.
Username	Displays the username used by this user to log onto the system.
Email	Displays the email address for the user.
Type	Indicates whether the user account was created on the C4000 (LOCAL) or imported from an LDAP service (LDAP).

Table 73. User Page Parameters

Role	Displays the role assigned to the user.
Extension	Displays the extension used by the user.
Timeout (minutes)	Displays the number of minutes of inactivity after which a session will be automatically logged out.
Account Control	Displays the LDAP account's UserAccountControl status. *Note:* This indicates the enabled status of the account as well as password expiration information.
Password Last Set	The date and time when the password was last modified.
Password Reset on Next Login	Displays **Yes** if the user will be forced to change their password the next time they login; otherwise displays **No**.
User Logging	Opens the *User Logging* view (see *"User Logging" on page 256*).
Delete Selected	Deletes all selected users.

Adding a User

When you add a user, you assign a role, which provides a set of permissions for the user. (See *"Viewing Roles" on page 246*.)

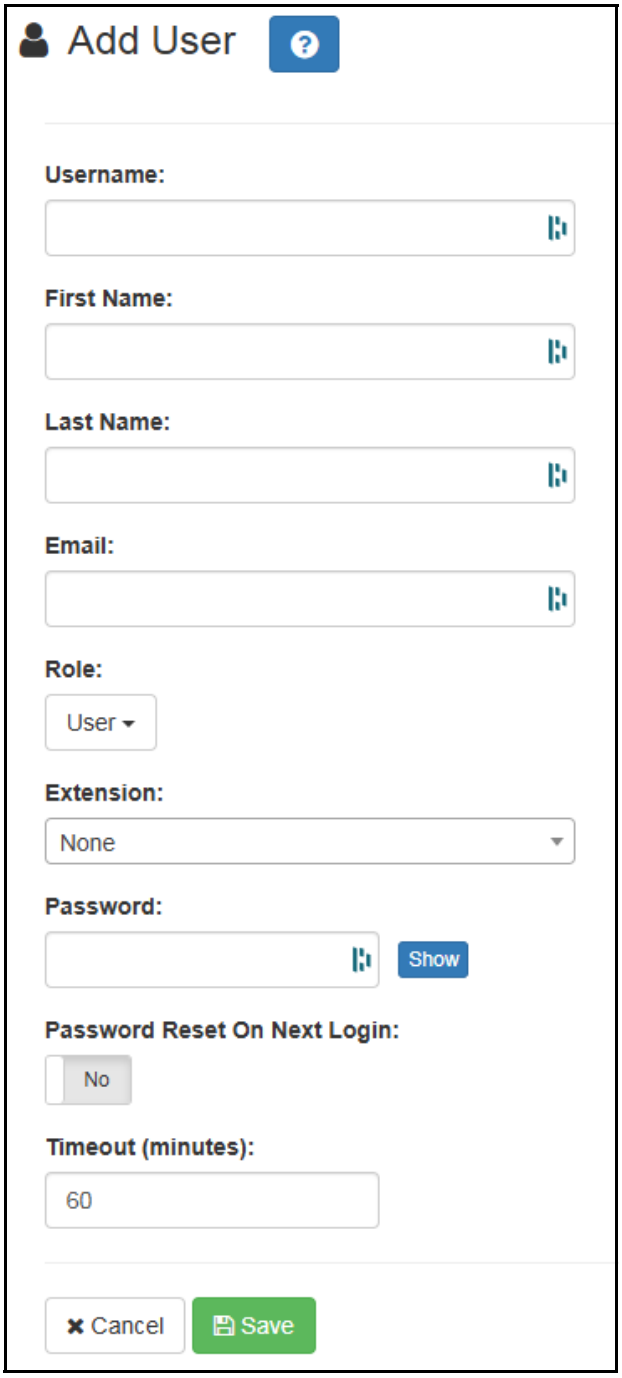


Figure 88. Add User Page

Note: You must have permissions to create a user before performing this procedure. (See *"Assigning and Editing Permissions" on page 248*.)

To add a user:

1. On the navigation bar, select **Users**.
2. On the Users page, select the **Add** icon.
3. Complete the parameters on the Add User page.
4. Select **Save**.

Understanding User Information

The following information parameters appear when adding or editing user information.

Table 74. Add or Edit User Page Parameters

Username	Provide the username used by this user to log onto the system. *Note:* This value is read-only when editing an LDAP user account. *Note:* The username field is case sensitive.
First Name	Provide the first name of the user. *Note:* This value is read-only when editing an LDAP user account.
Last Name	Provide the last name of the user. *Note:* This value is read-only when editing an LDAP user account.
Email	Provide the email address of the user. This value must be unique among all users. *Note:* This value is read-only when editing an LDAP user account.
Type (Edit User only)	Displays whether the user account was created on the C4000 (LOCAL) or imported from an LDAP service (LDAP). *Note:* This value is read-only.
Access Control (LDAP users only)	Displays the current access control settings for this user. Possible values are: • Enabled • Enabled, password never expires • Disabled • Disabled, password never expires *Note:* This value is read-only.
Password Last Set (Edit User only)	Displays the date and time when the password was last modified. *Note:* This value is read-only.
Role	Select the user's role from the drop-down menu.
Extension	Select the Admin Web Interface station extension to be associated with this user from the drop-down menu.

Caution	Users' extension associations must be unique. If multiple users are associated with the same extension, system behavior will be unpredictable.

Table 74. Add or Edit User Page Parameters (continued)

Password or **Change Password** (LOCAL users only)	Enter the new password. All entered characters will be hidden for security purposes. Press the **Show** button to view the characters. *Note:* The password is case-sensitive and must contain uppercase letters, lowercase letters, digits, symbols, and a minimum of five characters.
Password Reset on Next Login	If set to **Yes**, the user will be forced to reset their password the next time they login. The default value is **No**.
Timeout (minutes)	Specify the number of minutes of inactivity after which the user will be automatically logged off a web session (known as a *forced logout*). Valid values are 4 to 525600 (i.e., 365 days) or zero (0), which means never perform a forced logout. The default value is 60 minutes. *Note:* The manner in which a User account will be used can have a significant impact on the timeout value to be specified. For example, a short timeout might be best for an admin account used primarily for configuration purposes, while a long timeout (or no timeout) might be best for an account used to receive incoming intercom calls. If the User will be used for multiple purposes, it may be helpful to create a different User account for each purpose, particularly as only one active session is allowed per User account.

Tip: Moving the mouse while the two-minute timeout warning modal is displayed will reset the timeout.

Deleting a User

You should delete a user when they are no longer authorized to use the Nyquist system. For example, if a receptionist accepts a position at another site, the receptionist's user account should be deleted from your Nyquist system.

To delete a user:

1. On the navigation bar, select **Users**.
2. On the Users page, select the **Delete** icon next to the user that you want to delete.
3. When prompted to confirm, select **Delete**.

To delete multiple users:

1. On the navigation bar, select **Users**.
2. On the users page, select the check box for each user that you want to delete.
3. Select the **Delete Selected** button.
4. When prompted to confirm, select **Delete Selected**.

Note: You cannot delete your own user account.

Editing User Information

If you have Admin permissions, you can change a user's information, including email address, password, and role.

To edit a user's information:

1. On the navigation bar, select **Users**.
2. On the Users page, select the **Edit** icon next to the user whose information you want to change.
3. On the Edit User page, make the desired changes. (See *Table 74, "Add or Edit User Page Parameters," on page 254*.)
4. Select **Save**.

User Logging

Each time a user logs into or out of the C4000, an event is logged, including failed login attempts and automatic logouts.

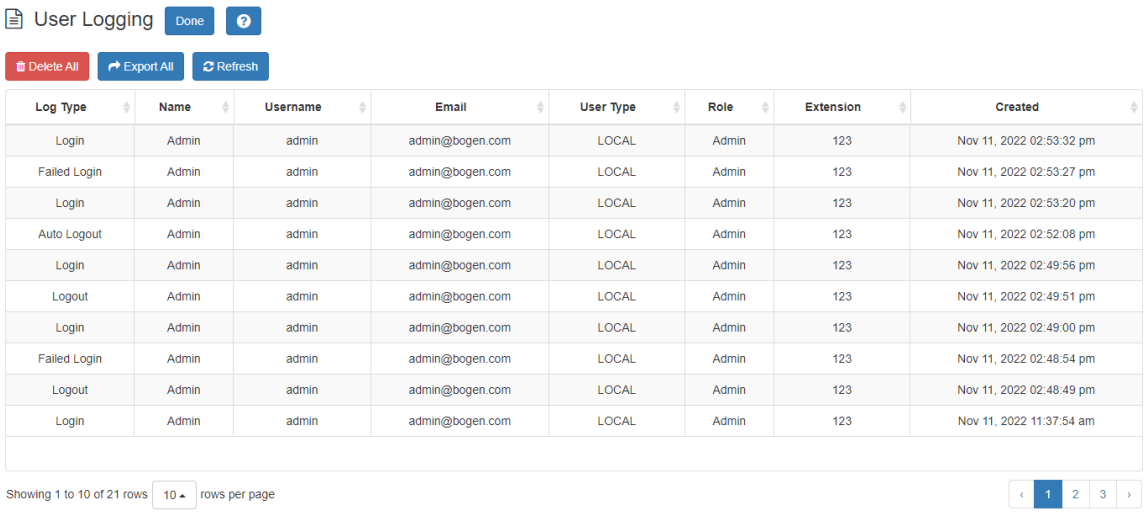


Figure 89. User Logging Page

To view the user log:

1. On the navigation bar, select **Users**.
2. Select the **User Logging** button.

The following table describes the information displayed for each logging event.

Table 75. User Logging Page Properties

Log Type	Displays the type of event. Valid values are: • **Login** • **Failed Login** • **Logout** • **Auto Logout** (i.e., session timeout) • **Forced Logout** (i.e., **Logout** button on *Users* page)
Name	Displays the name of the user.
Username	Displays the username of the user.
Email	Displays the email address of the user.
User Type	Indicates whether the user account was created on the C4000 (**LOCAL**) or imported from an LDAP service (**LDAP**).
Role	Displays the user's assigned Role.
Extension	Displays the user's assigned extension.
Created	Displays the date and time of the event.
Delete All	Deletes all User Logging events.
Export All	Generates and downloads a comma-separated CSV file containing all User Logging events. The column names, as provided in the first row of the file, are: • `log_type` • `user_type` • `user_id` • `role` • `username` • `email` • `first_name` • `last_name` • `extension` • `created`
Refresh	Updates the page to show the latest logging events.

Note: The information logged reflects the state of the user at the time of the event, such as the user's role, extension, email address, etc. Changes to these attributes will not be reflected in events prior to those changes.

Using Admin Groups

You can place Admin Stations into Admin Groups, which are used if incoming calls are not answered by the assigned Admin Station or the Day or Night Admin associated with the Admin Station. Admin Groups act as an always-answer feature by providing an alternate list of Admin Stations. If an incoming call is not answered by the assigned Admin Station within 30 seconds for normal calls or 15 seconds for emergency calls, all Admin Stations in the Admin Group will ring.

If Call Forwarding is enabled at the Admin Station, Nyquist tries the forwarded extension. If that station is busy or does not answer within 15 seconds, the call rolls over to the Admin Group.

In addition, if an emergency-level call receives no answer, the Admin Group will ring if the Day Admin or Night Admin does not answer.

You can assign Admin Stations to multiple Admin Groups. A Day or Night Admin can also be assigned to one or more Admin Groups.

Viewing Admin Groups

Through the *Admin Groups* page, you can view, add, edit, or delete Admin Groups.

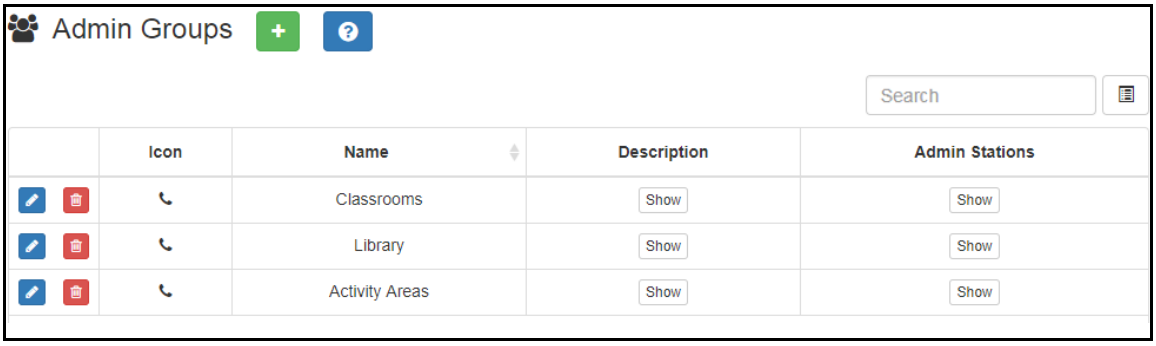


Figure 90. Admin Groups Page

To view Admin Groups:

On the navigation bar, select **Admin Groups**.

The following table describes the information that appears on the Admin Groups page:

Table 76. Admin Groups Page Parameters

Icon	Displays the icon that is associated with the Admin Group.
Name	Identifies the name of the Admin Group. *Note:* Valid characters include uppercase letters (A–Z), lowercase letters (a–z), numerals (0–9), space, and the following special characters: **! @ $ * ? - . , .**

Table 76. Admin Groups Page Parameters (continued)

Description	Provides a description of the Admin Group when the **Show** icon is selected. *Note:* Valid characters include uppercase letters (A–Z), lowercase letters (a–z), numerals (0–9), space, and the following special characters: **! @ $ * ? - . , .**
Admin Stations	Provides a list of the Admin Stations in the group when the **Show** icon is selected.

Editing an Admin Group

You can use the Edit Admin Group page to change the name, icon, and description of an Admin Group. You can also use this page to add or delete Admin Stations from the Admin Group.

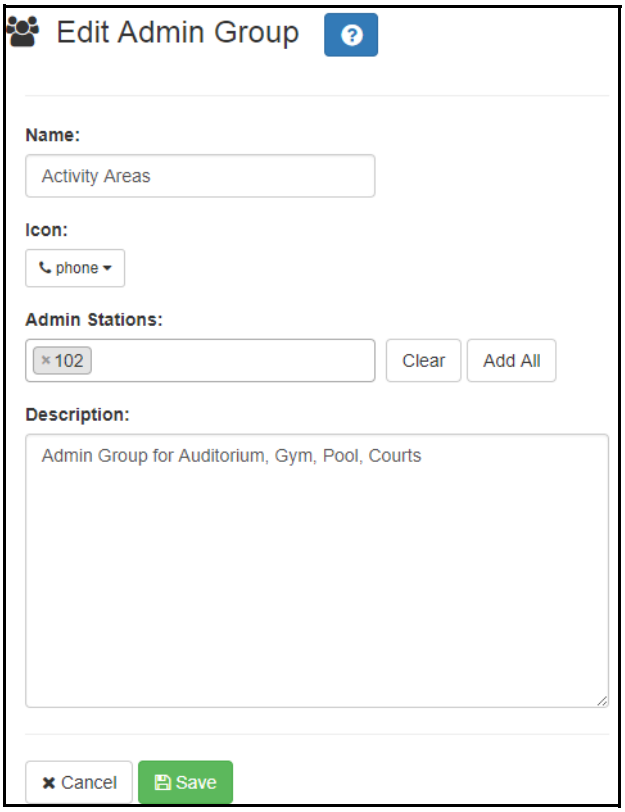


Figure 91. Edit Admin Group Page

You can also add an Admin Station to an Admin Group when adding or editing a station. (*See "Adding a Station" on page 185* and *"Editing Station Configuration Settings" on page 155*.)

Note: Nyquist does not display the Admin Group parameter when adding or editing an I/O Controller or Matrix Mixer Pre-Amp as a station.

To edit an Admin Group:

1. Select the **Edit** icon next to the group that you want to edit.
2. On the *Edit Admin Group* page, make desired changes.
3. After all changes have been made, select **Save**.

Table 77. Edit Admin Group Page Parameters

Name	Type the name of the Admin Group. *Note:* Valid characters include uppercase letters (A–Z), lowercase letters (a–z), numerals (0–9), space, and the following special characters: **! @ $ * ? - . ,** .
Icon	Use the drop-down menu to select the icon that you want associated with the Admin Group.
Admin Stations	Provide a list of the Admin Stations you want to have in this group. You can select **Add All** to select all Admin Stations, or you can select the Admin Stations list to view all available Admin Stations and select the ones you want to include in this group.
Description	Provide a description of the Admin Group. *Note:* Valid characters include uppercase letters (A–Z), lowercase letters (a–z), numerals (0–9), space, and the following special characters: **! @ $ * ? - . ,** .

Deleting an Admin Group

You cannot delete an Admin Group if it is associated with a station, an outside line, or a Day or Night Admin. If necessary, first edit a station, an outside line, or a Day or Night Admin to delete the station before attempting to delete the Admin Group. (*See "Editing Outside Lines" on page 125, "Setting System Parameters" on page 67*, or *"Editing Station Configuration Settings" on page 155*.)

To delete an Admin Group:

1. Select the **Delete** icon next to the group that you want to delete.
2. When prompted, select **Delete**.

Adding an Admin Group

You can create an Admin Group and assign Admin Stations to it. No limit exists for the number of Admin Groups that you can create, and an Admin Station can belong to multiple Admin Groups.

If you want to route 911 calls from an extension (station) to an Emergency Group, create an Admin Group called Emergency. Then, configure the station to use this group for its **911 Route**. (See *"Editing Station Configuration Settings" on page 155*.)

To add an Admin Group:

1. On the navigation bar, select **Admin Groups**.
2. On the *Admin Groups* page, select the **Add** icon.
3. Enter the parameters on the *Add Admin Groups* page.
4. Select **Save**.

Table 78. Add Admin Groups Page Parameters

Name	Enter the name of the Admin Group. *Note:* Valid characters include uppercase letters (A–Z), lowercase letters (a–z), numerals (0–9), space, and the following special characters: **! @ $ * ? - . ,** .
Icon	Select an icon associated with an Admin Group. Associating an icon to an Admin Group offers a visual key to the type of group.
Admin Stations	Provide a list of Admin Stations that are to be included in this Admin Group. Only Admin Station types, such as a Web Admin UI or an Admin Phone, can be selected.
Description	Provide a description of the Admin Group. *Note:* Valid characters include uppercase letters (A–Z), lowercase letters (a–z), numerals (0–9), space, and the following special characters: **! @ $ * ? - . ,** .

Managing Schedules

The Schedules feature allows you to set tones, announcements, and audio distribution to be played at specific times and in specific zones, set up holiday schedules, maintain calendar features, and schedule announcements, including recurring announcements. The Schedules feature also allows you to schedule the execution of Routines at specific dates and times and on recurring schedules.

Through the web-based UI, you can associate events (such as a tone that signals the end of visiting hours) to a schedule, select how a schedule appears on your dashboard, and edit event settings, which include:

- Event name
- Signal time
- Zone
- Tone
- Scheduled Audio
- Routines

Understanding the Site Page

Through the Site page, you can select start and end dates for a schedule or choose to create a non-ending schedule, select a name for the site, and select a color that appears for the site schedule on the dashboard.

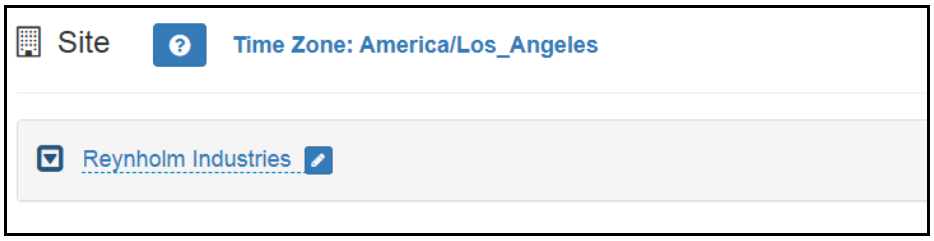


Figure 92. Site Page

You can then create one or more schedules and select the appropriate schedule for specific days of the week.

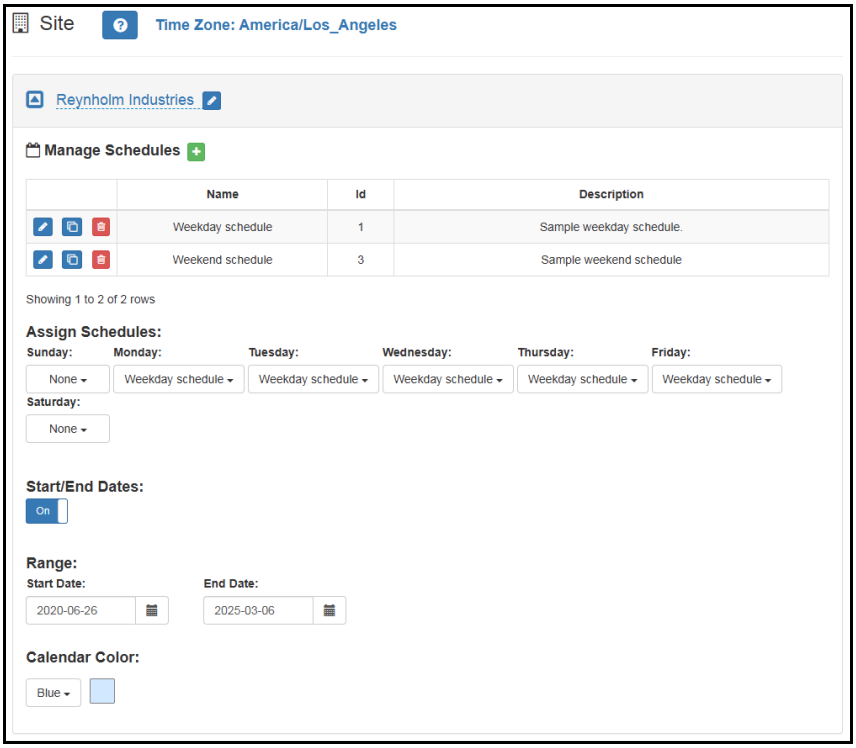


Figure 93. Creating a Schedule

Using Site Settings

The *Site* page provides parameters that can be added, viewed, and changed for a schedule. The following table describes these parameters:

Table 79. Site Settings Page Parameters

Time Zone	Displays the time zone specified via the **Time Zone** setting of the *System Settings* page (see *Table 24, "System Tools," on page 78*).
Manage Schedules	Create or edit one or more daily schedules, which can then be assigned to specific days of the week. *Note:* Each schedule is automatically assigned an identifier (Id), which can be referenced via the `$scheduleid` variable from various actions and conditional statements.
Assign Schedules	For each day of the week, select the schedule that is to be used for that day from the drop-down menu.
Start/End Dates	Use the slider to set to **On** if you want to enter start and end dates. If set to **Off**, the schedule continues indefinitely.
Range Start Date	*Note:* This option appears only if **Start/End Dates** is set to **On**. Use the calendar to select the start date for this schedule. By default, today's date appears. When selecting a new **Start Date**, the date cannot be before the **End Date**.

Table 79. Site Settings Page Parameters

Range End Date	*Note:* This option appears only if **Start/End Dates** is set to **On**. Use the calendar to select the end date for this schedule. By default, today's date appears. The **End Date** must be after the **Start Date**.
Calendar Color	Use the drop-down menu to select the color for this schedule that is used when the schedule appears on the dashboard's calendar view.

From the Site page, you can also view, add, edit, or delete a schedule for a facility or view events for a schedule.

Renaming a Site

You can rename a site to quickly identify the facility or site that the schedule is for.

Figure 94. Edit Site Name

To rename a site:

1. On the navigation bar, expand **Schedules**.
2. Select **Site**.
3. Select the **Edit** icon next to the name of the site that you want to rename.
4. In the Edit Site Name popup box, type the new name.

Note: Valid characters include uppercase letters (A–Z), lowercase letters (a–z), numerals (0–9), space, and the following special characters: **! @ $ * ? - . ,** .

---

5. When done, select the **Check** icon.

Adding a Schedule

You can add multiple schedules for a site. For example, you may have different schedules set up for Tuesday and Thursday than you have for the rest of the week.

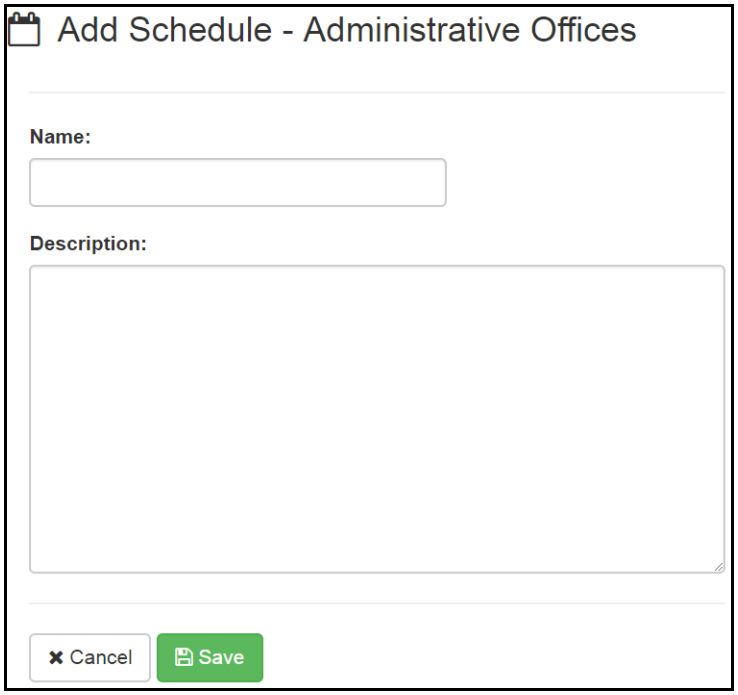


Figure 95. Add Schedule Page

To add a schedule:

1. On the navigation bar, expand **Schedules**.
2. Select **Site**.
3. Select the down arrow next to the site name.
4. Select the **Add** icon next to **Manage Schedules**.
5. On the Add Schedule page, enter the **Name** and **Description** for the schedule.

Note: Valid characters include uppercase letters (A–Z), lowercase letters (a–z), numerals (0–9), space, and the following special characters: **! @ $ * ? - . ,** .

---

6. Select **Save**.

Copying a Schedule

If you need to create a schedule that is similar to an existing schedule, whether from the same or different site, it may be easier to copy an existing schedule than to create one from scratch.

To copy a schedule:

1. On the navigation bar, expand Schedules.
2. Select **Site**.
3. Select the down arrow next to the site name to expand it (if it is not already expanded).
4. Select the **Copy Schedule** icon for the schedule to be copied.

5 A popup is displayed. Specify the site to which the schedule will be copied.

6 Select **Copy Schedule**.

7 Select the **Edit** icon for the newly created schedule and modify as desired.

Replacing a Schedule

If you attempt to delete a schedule that is in use, you are provided a chance to replace the schedule with another. If you select to delete rather than replace, then all matching default schedules and calendar exceptions are set to **None**. (*See "Deleting a Schedule" on page 272*.)

To replace a schedule:

1 On the navigation bar, expand **Schedules**.

2 Select **Site**.

3 Select the down arrow next to the site name.

4 Select the **Delete** icon for the schedule.

5 When prompted, select **Replace**.

6 When prompted, use the drop-down menu to select the replacement schedule.

7 Select **Confirm Replace**.

Reviewing and Editing a Schedule

Through the Site page, you can select the start and end dates for the schedules, a name for the site, and a color that appears for the site schedule on the dashboard. You can then create one or more schedules and select the appropriate schedule for specific days of the week.

Any changes made to the Site page affect the schedule going forward. For example, if you change the schedule for Tuesday and Thursday from Regular Day to Early Day, all Tuesdays and Thursdays until the End Date will use the Early Day schedule. If you want to change the schedule for days in a specific week, then you use the Calendars feature to create an exception. (*See "Using the Calendars Feature" on page 273*.)

To review and edit a schedule:

1 On the navigation bar, expand **Schedules**.

2 Select **Site**.

3 Select the down arrow next to the site name.

4 Make desired changes to the Site settings. (*See "Using Site Settings" on page 263*.)

Viewing Events for a Schedule

An event is the scheduled sounding of a tone or the playing of Scheduled Audio. You add events to a schedule. For example, you can schedule a tone to sound at 8 a.m. as an event, such as the start of a shift. You can add a second event that has the tone sound at 10 a.m. for a scheduled break.

Tip: This view allows you to view scheduled events, not past events that have already occurred. To view past events, look for entries with the Scheduler source and/or Scheduled Event type in the *Call Details* view (see *"Using the Call Details Feature" on page 362*). Each scheduled event's Source will be Scheduler, Type will be Scheduled Event, Status will be Start or Played, and Destination will indicate the scheduled event ID, event name, and target zone(s).

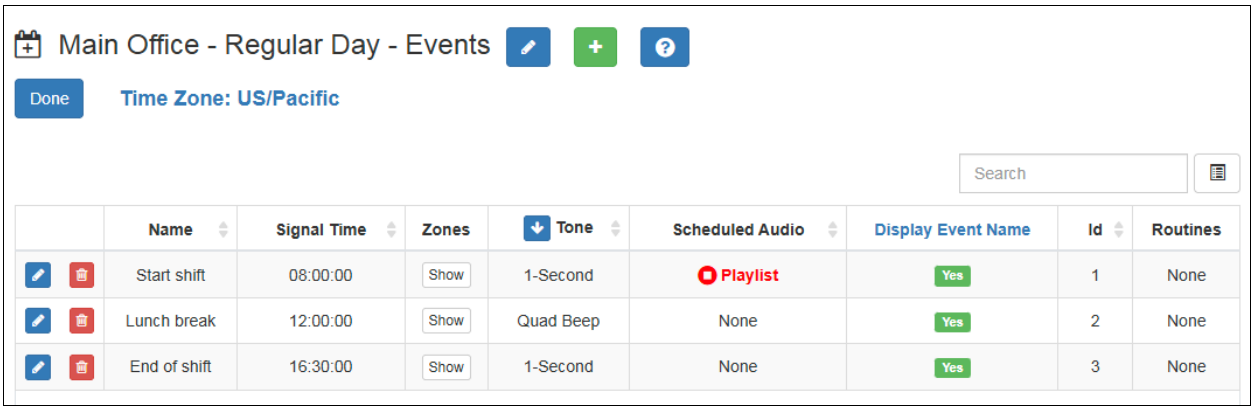


Figure 96. Events Page

To review events for a schedule:

1. On the navigation bar, expand **Schedules**.
2. Select **Site**.
3. Select the down arrow next to the site name to see site details.

   Schedules that are associated with the site appear on the *Edit Settings* page.
4. To view the events for a schedule, select the **Edit** icon for a schedule.

   The *Events* page appears. *Table 80* describes the parameters for this page:

Table 80. Events Page Parameters

Name	Displays the name for the event. *Note:* Valid characters include uppercase letters (A–Z), lowercase letters (a–z), numerals (0–9), space, and the following special characters: **! @ $ * ? - . , .**
Signal Time	Displays the time for this event to start using the HH:MM:SS format.
Zones	Upon hovering the mouse over the Show button, the zones to be included in this event are shown.

Table 80. Events Page Parameters

Tone	Displays the desired tone for this event. Select the arrow button to update the tone for all events, regardless of filter settings. A popup will be displayed where a tone can be selected.
Scheduled Audio	Displays if the event includes Scheduled Audio, and if so, what playlist, Matrix Mixer Pre-Amp channel, or amplifier is used for this event.
Display Event Name	Displays if the event name will appear on the GA10PV displays associated to the event zone or zones.
Id	The identifier for this event. *Note:* This value is accessible as $eventid in Routines and GA10PV Display Messages.
Routines	Specifies the routine(s) that will start when the event starts.

Editing Name and Description for a Schedule

You may want to edit a schedule's name and description to make it more descriptive. For example, if you originally created a schedule called Wednesday for an early release day, you may want to rename it Early Release.

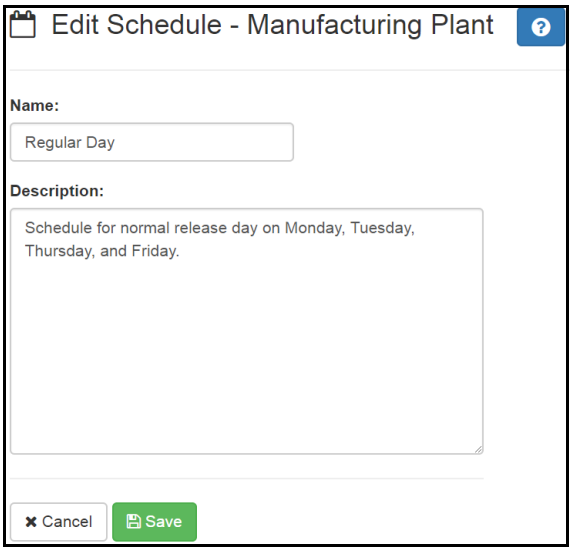


Figure 97. Edit Schedule Page

To edit a schedule's name and description:

1. On the navigation bar, expand **Schedules**.
2. Select **Site**.
3. Select the down arrow next to the site name.
4. Under Manage Schedules, select the **Edit** icon for the schedule.

5 On the Events page, select the **Edit** icon for the schedule.

6 On the Edit Schedule page, make the desired changes to the **Name** and **Description** fields.

Note: Valid characters include uppercase letters (A–Z), lowercase letters (a–z), numerals (0–9), space, and the following special characters: **! @ $ * ? - . , .**

---

7 Select **Save**.

Editing an Event

The Edit Event page allows you to change the parameters for events. For example, you may want to change the playlist for Scheduled Audio for the lunch period. Or, you might want to add or remove zones affected by an event.

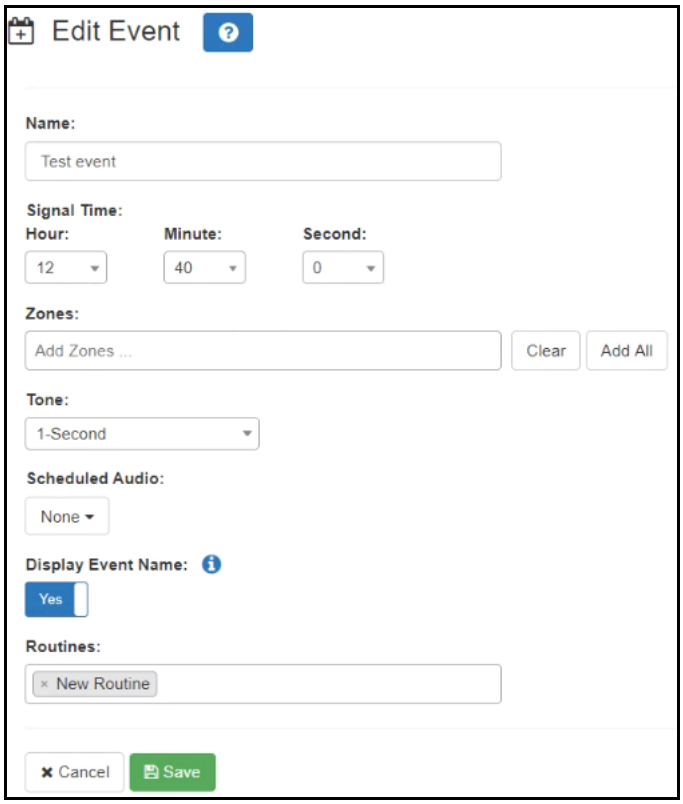


Figure 98. Edit Event Page

To edit an event:

1 On the navigation bar, expand **Schedules**.

2 Select **Site**.

3 Select the down arrow next to the site name.

4 Select the **Edit** icon for the schedule.

5 On the Events page for the schedule, select the **Edit** icon for the event that you want to edit.

6 On the Edit Event page, make the desired changes. (See *Table 81, "Event Settings Page Parameters," on page 271*.)

7 Select **Save**.

Deleting an Event

You can delete an event from a schedule when the event is no longer needed or wanted. For example, suppose your site's schedule was set up to have warning bells that ring five minutes before a shift starts. If you decide to end the use of warning bells, you would delete each warning bell event from the schedule.

To delete an event:

1 On the navigation bar, expand **Schedules**.

2 Select **Site**.

3 Select the down arrow next to the site name.

4 Select the **Edit** icon for the schedule.
Events that are associated with the schedule appear on the Events page.

5 Select the **Delete** icon for the event that you want to delete from the schedule.

6 When prompted, select **Delete**.

Adding an Event

When a schedule is created, it has no events, which are specific times when tones play. After you create a schedule, you add events through the Add Event page.

To add an event to a schedule:

1 On the navigation bar, expand **Schedules**.

2 Select **Site**.

3 Select the down arrow next to the site name.

4 Select the **Edit** icon for the schedule you want to add an event to.

5 Select the **Add** icon.

6 Complete the parameters on the *Add Event* page. (See *Table 81 on page 271*.)

7 When completed, select **Save**, or if you want to add another event to this schedule, select **Save and Create Another** and return to Step 6.

Understanding Event Settings

Event settings appear when adding or editing an event.

Table 81. Event Settings Page Parameters

Name	Specifies the name for the event. *Note:* Valid characters include uppercase letters (A–Z), lowercase letters (a–z), numerals (0–9), space, and the following special characters: **! @ $ * ? - . ,** .
Signal Time	Specifies the time for this event to start using the HH:MM:SS format. For example, if you want the event to start at 08:15:15, type or use the down arrows to make the appropriate selections in the **Hour**, **Minute**, and **Second** fields.
Zones	Specifies the zones to be included in this event. *Note:* You can select **Add All** to have all zones appear in the zone field, and then remove a zone by selecting the **X** for a zone. You can also delete zones by placing your cursor in the Zones field and pressing the **Delete** key. **Caution** It is possible for multiple zones to have one or more stations in common. If you schedule an event for zones that share one or more stations, a condition known as a *zone overlap* (see *"Zone Overlap Messages" on page 372*), there may be issues.
Tone	Select the desired tone for this event. If an audio distribution entry from the **Scheduled Audio** menu is selected, this field is not required. *Note:* If a tone is specified for this setting and the devices in the specified zones are unable to communicate with the Nyquist server at the scheduled time, the devices will still trigger this event for up to 72 hours after the last successful synchronization with the Nyquist server (which occurs at midnight). Instead of the specified Tone, however, it will play the **Appliance Backup Scheduled Tone** (see *"Edit System Parameters Page" on page 69*).
Scheduled Audio	Specifies if the event includes Scheduled Audio, and if so, what playlist, Matrix Mixer Pre-Amp channel, or amplifier is used for this event. You can also select to stop the Scheduled Audio by selecting **Stop Playlist** or **Stop Line-Input**. *Note:* When **Stop Playlist** is specified, the last playlist(s) that were started on the specified zone(s) will be stopped. If a playlist was started on multiple zones, all of those zones must be specified to stop the playlist. If an airable/SoundMachine source is selected, the Scheduled Audio list includes selections to start or stop the audio stream. This list only includes airable/SoundMachine selections that apply to the specific time zone. If the Audio Distribution zone selected includes a time zone and another zone type, such as Paging, that is not for time, the audio distribution does not appear in this **Scheduled Audio** list.

Table 81. Event Settings Page Parameters (continued)

Display Event Name	Specifies if the event name will appear on the GA10PV displays associated to the event zone or zones. *Note:* If you schedule an event with **Display Event Name** enabled, the event remains on the display connected to the NQ-GA10PV until the next scheduled event replaces it. To clear the event name from the display, create another scheduled event with the **Name** set to **No-Event**.
Amplifiers/Matrix Mixers	Specifies the amplifiers or Matrix Mixer Pre-Amp and its associated station number. *Note:* This parameter appears only if **Scheduled Audio** is set to **Start Line-Input**.
Input Channel	Specifies the matrix channel being used for input. *Note:* This parameter appears only if **Scheduled Audio** is set to **Start Line-Input**.
Routines	Specifies one or more routines to be executed when this event starts. *Note:* If a specified routine is disabled, it will not execute, but will not be removed from the trigger.

An event with **Scheduled Audio** set to **Stop Playlist**, **Stop Line-Input**, or **Stop <airable/SoundMachine source>** should be created for each Scheduled Audio start command to ensure the Scheduled Audio stops when you want. If an associated **Stop** event is not in the schedule, Scheduled Audio started by a scheduled event will not stop playing.

If you want to start Scheduled Audio without also playing a tone, set **Tone** to **No Tone**.

You can use the scheduling feature to schedule audio distribution using Scheduled Audio; when using Scheduled Audio in a scheduled event to schedule audio distribution, set **Tone** to **No Tone**. Zone numbers are not required.

If several overlapping scheduled events use Scheduled Audio and have overlapping zones defined, a scheduled Scheduled Audio event will not start the audio if an existing Scheduled Audio event is already playing to a zone defined in the scheduled event. Error messages will be displayed on the dashboard whenever overlapping zones prevent Scheduled Audio from starting. Ensure that scheduled events with Scheduled Audio do not use the same zones during the same time frames.

Deleting a Schedule

If you have the correct permissions, you can delete a schedule that is no longer being used. When you delete a schedule, you delete all associated schedules, scheduled events, and schedule exceptions.

To delete a schedule:

1. On the navigation bar, expand **Schedules**.
2. Select **Site**.
3. Select the **Delete** icon next to the schedule that you want to delete.
4. When prompted, select **Delete**.

Using the Calendars Feature

Nyquist provides a calendar view of the schedule used for past days, the schedule for the current and future days, and the scheduled holidays. The view is for the current month, but you can use the **<Prev>** and **<Next>** buttons to display other months.

The Calendar view also provides access to the calendars of Facilities that are defined in the Facilities view (see *"Configuring Facilities" on page 133*). You can view and modify calendars of any Facilities that are configured to allow access via the Remote Calendar Control settings (see *Table 23, "Edit System Parameters Page," on page 69*).

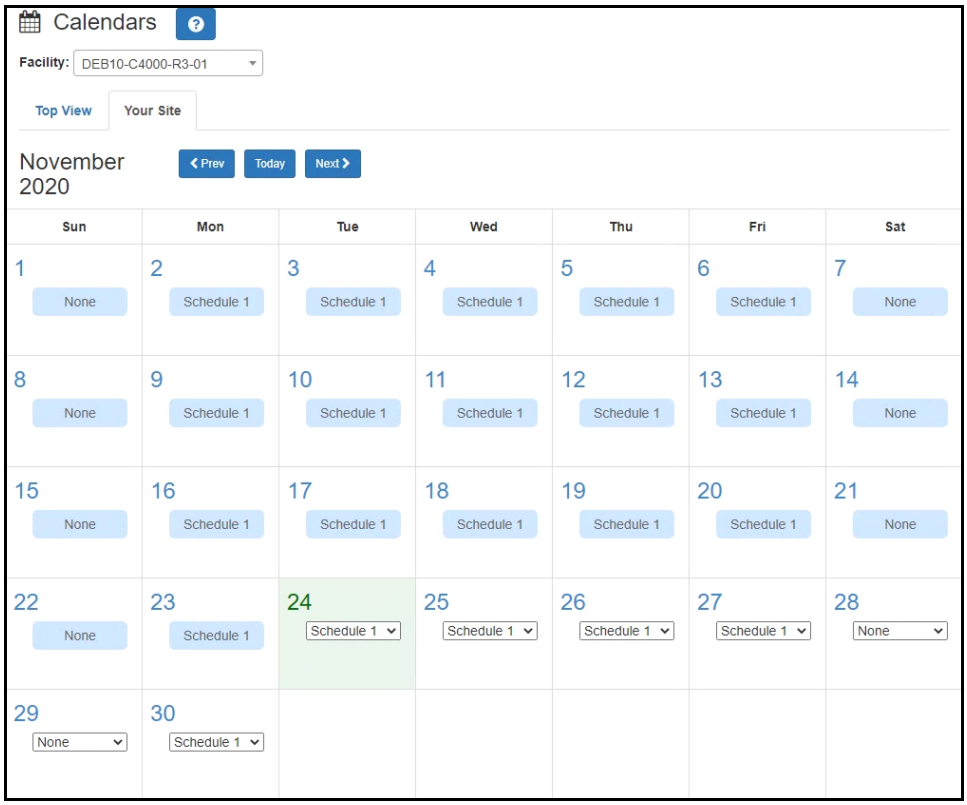


Figure 99. Calendars Page

The Calendars feature also provides a quick way to change the schedule. For example, if you normally use an *Early Release* schedule for Wednesdays but want to use this schedule for Monday through Friday for the last week of the year, you can use the Calendars feature to create exceptions for your schedule.

To view or change a monthly calendar:

1. On the navigation bar, expand **Schedules**.
2. Under Schedules, select **Calendars**.
3. Select the **Facility** whose calendar you wish to view.

Note: If the **Remote Calendar Control** setting for the selected Facility does not allow access to your Nyquist server, an error will be displayed and your Facility selection will be rejected.

---

4 Select either **Top View** or the tab that displays your site's name.

5 To change the schedule for the current or future dates, make sure you are the tab for your site and use the drop-down menu for the date or dates to select the replacement schedule.

6 To view events scheduled for a date, make sure you are on the **Top View** tab and select the date. Events for the schedule are detailed in the Schedule popup window that appears.

7 When done viewing events, select **Close**.

Schedule Popup Window Parameters

The Schedule popup window appears when viewing events for a date from either the monthly view (*see "Using the Calendars Feature" on page 273)* or from the dashboard's Weekly Schedule panel (*see "Viewing the Schedule for the Week" on page 401*).

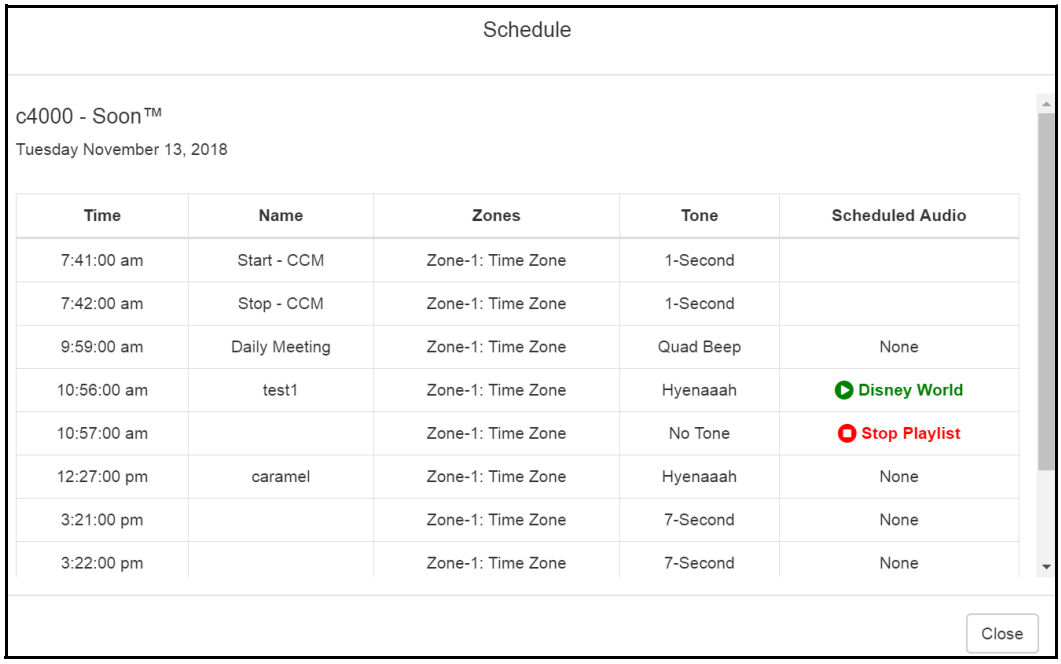


Figure 100. Schedule Popup Window

The Schedule popup window displays the name, the day, and the date of the schedule. It also contains the following parameters:

Table 82. Schedule Popup Window Parameters

Time	Identifies the time of the event start in HH:MM:SS format.
Name	Identifies the user-provided name for the event. *Note:* Valid characters include uppercase letters (A–Z), lowercase letters (a–z), numerals (0–9), space, and the following special characters: **! @ $ * ? - . ,** .
Zones	Identifies the zones and types of zones that are specified for this event.

Table 82. Schedule Popup Window Parameters (continued)

Tone	Identifies the name of the tone used for this event.
Scheduled Audio	Identifies a playlist, Matrix Mixer Pre-Amp channel, amplifier, or airable/SoundMachine source to use if the Scheduled Audio feature is used for this event. Otherwise, the option appears as **None**.

Using the Holidays Management Tool

Holidays, which can be a single day or a range of dates, often require changes in schedule assignments. The holidays management tool allows you to enter ranges of days when all schedules are turned off and to add these holidays to the calendar via the Schedules feature. You can also export a holiday schedule as a .csv file and import the holiday schedule file to another Nyquist server.

Holidays override other schedules that are set for a date range.

Viewing Holidays

Holidays affect the schedule of each facility managed by your Nyquist server. The Holidays page displays a list of all holidays that have been set up for the Nyquist system. Holidays take precedent over regular schedules. For example, suppose you configure Mondays to use a schedule called Regular that has tones sounding throughout the day to mark the ending and beginning of shift changes. If you set a holiday for Monday, May 28, then the holiday "overrules" the Regular schedule and tones do not sound during that day.

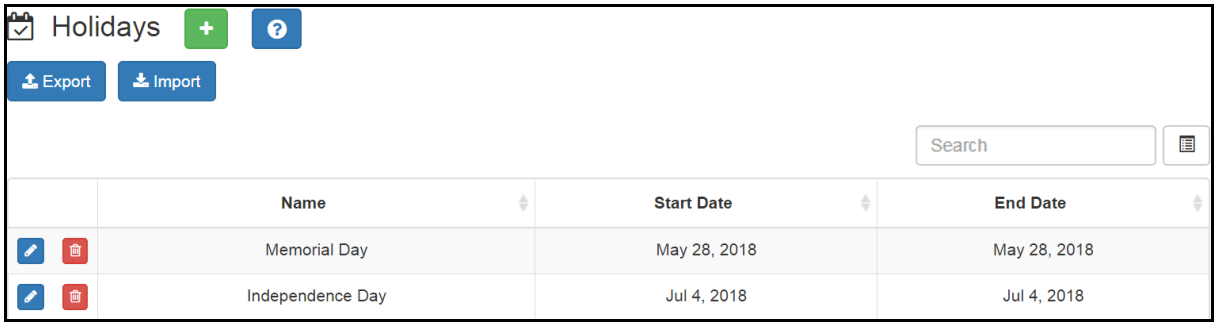


Figure 101. Holidays Page

To view holidays:

1. On the navigation bar, expand **Schedules**.
2. Select **Holidays**.
   A listing of holidays and the parameters associated with these holidays appears.

The following table describes these parameters:

Table 83. Holiday Parameters

Name	Provides the name of the holiday.
Multiple Days	*Note:* Appears only when adding or editing a holiday. Indicates if the holiday includes multiple days (such as spring break). If No is selected, then the **Start Date** appears as **Date** and **End Date** does not appear.
Start Date	Provides the start date of the holiday. *Note:* For holidays that do not involve multiple days, this field appears as **Date**.
End Date	Provides the end date of the holiday. *Note:* For holidays that do not involve multiple days, this field does not appear.

The Holidays page also contains **Export** and **Import** buttons that allows you to easily capture holiday settings and import them to other Nyquist servers.

Adding a Holiday

You can create a holiday for any day that the schedule should be turned off, including state and federal holidays. Holidays automatically appear on the dashboard and on the Calendar views.

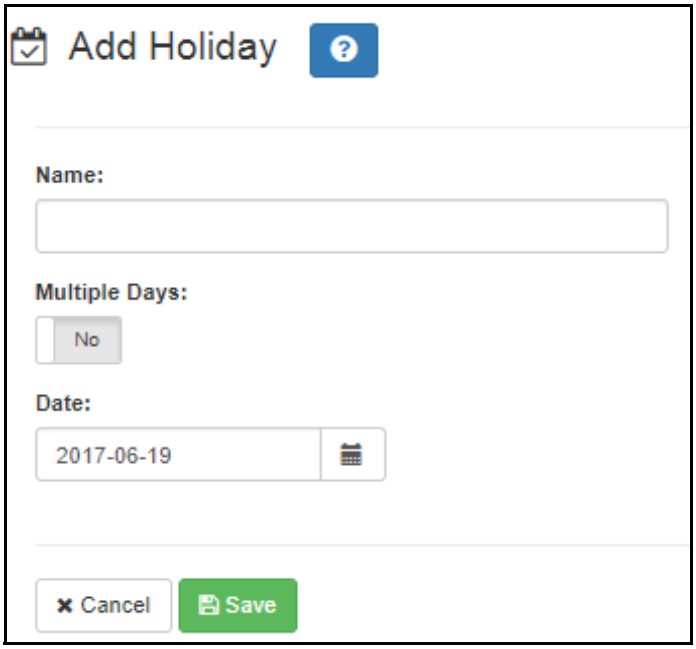


Figure 102. Add Holiday Page

To add a holiday:

1. On the navigation bar, expand **Schedules**.
2. Select **Holidays**.

3 On the Holidays page, select the **Add** icon.

4 Enter the parameters for the holiday. (See *Table 83, "Holiday Parameters," on page 276*.)

5 Select **Save**.

Deleting a Holiday

You may need to delete a holiday in cases such as when a manager's workday is rescheduled to a regular day to make up for an earlier site closure due to inclement weather.

To delete a holiday:

1 On the navigation bar, expand **Schedules**.

2 Select **Holidays**.

3 On the Holidays page, select the **Delete** icon next to the holiday that you want to delete.

4 When prompted, select **Delete**.

Editing a Holiday

You can edit a holiday if you need to change the name or start or end dates for the holiday.

To edit a holiday:

1 On the navigation bar, expand **Schedules**.

2 Select **Holidays**.

3 On the Holidays page, select the **Edit** icon next to the holiday that you want to edit.

4 On the Edit Holiday page, make the desired changes. Parameters for the holiday are described in *Table 83, "Holiday Parameters," on page 276*.

5 After all changes have been made, select **Save**.

Exporting Holidays

To aid in configuring multiple Nyquist servers or System Controllers that share the same holiday schedule, Nyquist allows you to export the holiday schedule to a CSV file.

To export the holiday schedule:

1 On the navigation bar, expand **Schedules**.

2 Select **Holidays**.

3 Select **Export**.
The holidays.csv file will be sent to your Downloads folder.

Importing Holidays

If you have exported a holiday schedule created at one Nyquist server or System Controller, you can import that schedule to another Nyquist server or System Controller.

You can also create a custom holiday CSV file using the following conventions:

- Create four columns with each column separated by commas.
- Insert a line return at the end of each row.
- Set the first column 0 because it will be replaced by an autogenerated value when the file is imported into the database.
- For first, second, and third columns, enclose the entries in double-quotation marks (").
- In the second column, provide the holiday name.
- Enter the start date in the third column using the format YYYY-MM-DD.
- Enter the end date in the fourth column using the format YYYY-MM-DD. For a one day holiday, the start and end dates will be the same.

To import a holiday schedule:

1. On the navigation bar, expand **Schedules**.
2. Select **Holidays**.
3. Select **Import**.
4. Select **Choose file** and navigate to select the CSV file that you want to import.
5. If you want to delete all existing holidays before importing the file, use the slider to select **Yes**.
6. Select **Import**.

Using the Schedule Announcements Feature

After an announcement has been created via the Audio feature, you can schedule it to play via the Schedules feature. For information about the Audio feature, refer to *"Managing Audio" on page 290*.

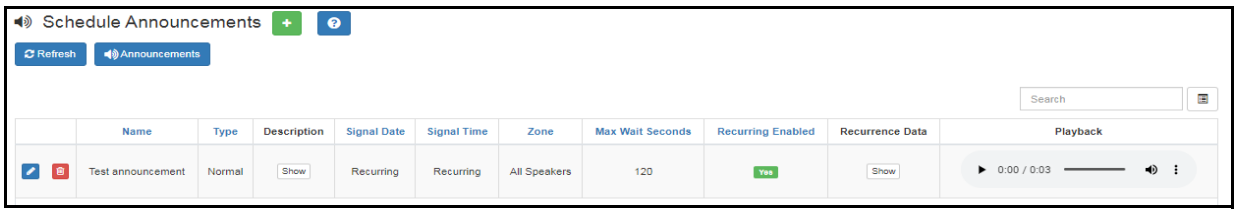


Figure 103. Schedule Announcements Page

To view schedule announcements:

1. On the navigation bar, expand **Schedules**.

2 Select **Schedule Announcements**.

The Schedule Announcements page appears. This page displays the following information about all scheduled announcements:

Table 84. Schedule Announcements Page Parameters

Refresh button	Refreshes the list of scheduled Announcements.
Announcements button	Browses to the *Announcements* page (see *"Viewing Announcements" on page 328*).
Name	Displays the name of the announcement. *Note:* Valid characters include uppercase letters (A–Z), lowercase letters (a–z), numerals (0–9), space, and the following special characters: **! @ $ * ? - . ,** .
Type	The type of announcement; either **Normal** or **Emergency**.
Description	Displays the description of the announcement. *Note:* Valid characters include uppercase letters (A–Z), lowercase letters (a–z), numerals (0–9), space, and the following special characters: **! @ $ * ? - . ,** .
Signal Date	Displays the date that the announcement is to play.
Signal Time	Displays the time the announcement is to play in HH:MM:SS format.
Zone	Displays the zone that is to receive this announcement.
Maximum Wait Seconds	Specifies the maximum number of seconds to wait for an active page or announcement to complete so the scheduled announcement can be played. The default is 120 seconds. If an Emergency All-Call is in progress at the time that a scheduled announcement should be played, the scheduled announcement will not be played due to the active Emergency All-Call. In this case, the scheduled announcement will not wait for the Emergency All-Call to end and will be canceled. *Note:* Scheduled Announcements will not play during an active check-in process.
Recurring Enabled	*Note:* If an announcement is already playing, a recurring announcement will not play until its next scheduled occurrence. Indicates if the announcement is scheduled to reoccur.
Recurrence Data	Displays data for the recurring announcement, such as the start and end dates, when you roll over or select the **Show** button.
Playback	Allows you to manually play the announcement. Selecting the down arrow in this field also allows you to download and save the announcement.
Refresh	Press the Refresh button to refresh the list of Scheduled Announcements.

Adding a Schedule Announcement

On the Schedule Announcements page you can create a schedule announcement. When you schedule an announcement, you select the date and time the announcement plays, how many times it plays, and the zone that it plays in. Instead of selecting a single zone, you can select **All Speakers**.

Note: You must create an announcement before you can create a schedule announcement. (See *"Adding an Announcement" on page 322*.)

To add a schedule announcement:

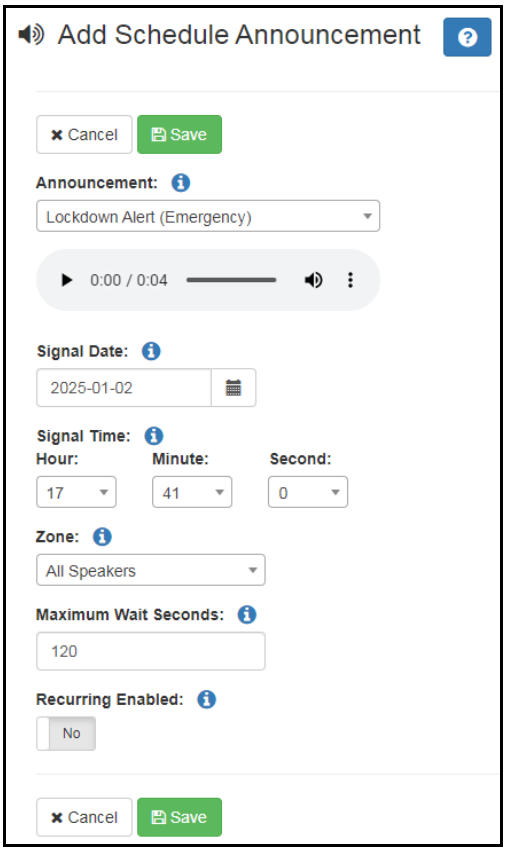


Figure 104. Add Schedule Announcement Page

1. On the navigation bar, expand **Schedules**.
2. Select **Schedule Announcements**.
3. On the Schedule Announcements page, select the **Plus** icon.
4. On the Add Schedule Announcement page, complete the parameters.
5. Select **Save**.

Table 85. Add Schedule Announcement Parameters

Announcement	Use the drop-down menu to select the announcement that you want to schedule.
Signal Date	*Note:* This field only appears if **Recurring** has been set to **No**. Use the calendar or type to select the date that the announcement is to play.
Signal Time	*Note:* This field only appears if **Recurring** has been set to **No**. Select the **Hour**, **Minute,** and Second from the corresponding dropdown menus.
Zone	Select either **All Speakers** or a specific zone that is to receive this announcement.
Maximum Wait Seconds	The maximum number of seconds to wait if there is already an active page preventing the scheduled announcement from playing. Valid values range from 0 to 86400. The default value is 120 seconds.
Recurring Enabled	Use the slider to indicate if the announcement will be scheduled to recur. *Note:* Disabling this setting erases any schedule settings. To temporarily disable a schedule, disable **Recurring Schedule Enabled** instead.

If **Recurring Enabled** is set to Yes, the following parameters will be displayed:

Table 86. Recurring Schedule Parameters (only if **Recurring Enabled** is set to Yes)

Recurrence Start Date	Use the calendar to select the start date for this recurring announcement.
Recurrence End Date	Use the calendar to select the end date for this recurring announcement. *Note:* This field only appears if **No End Date** is disabled.
No End Date	Use the slider to select **Yes** if you want this announcement to recur indefinitely.
Recurrence Second	Specify at which second of the **Recurrence Minutes** to play the Announcement.
Recurrence Minutes	Specify one or more values to indicate at which minutes of the specified **Recurrence Hours** the Announcement will play. If unspecified, the Announcement will play every minute of the hour.
Recurrence Hours	Specify one or more values to indicate at which hours of the specified **Recurrence Days** and **Recurrence Days of Week** the Announcement will play. If unspecified, the Announcement will play every hour of the day.

Table 86. Recurring Schedule Parameters (only if **Recurring Enabled** is set to Yes)

Recurrence Days	Specify one or more values to indicate on which days of the specified **Recurrence Months** the Announcement will play. If this and **Recurrence Days of Week** are both unspecified, the Announcement will play every day of the month.
Recurrence Months	Specify one or more values to indicate on which months of the year the Announcement will play. If unspecified, the Announcement will play every month.
Recurrence Days of Week	Specify one or more values to indicate on which days of the week the Announcement will play. If this and **Recurrence Days** are both unspecified, the Announcement will play every day of the week.

Deleting a Schedule Announcement

To delete a schedule announcement:

1. On the navigation bar, expand **Schedules**.
2. Select **Schedule Announcements**.

   The Schedule Announcements page appears. This page displays information about all scheduled announcements.
3. Select the **Delete** icon next to the schedule that you want to delete.
4. When prompted, select **Delete**.

Editing a Schedule Announcement

From the Edit Schedule Announcement page, you can change the selected announcement, the date and time the announcement is set to play, and the zones in which the announcement is scheduled to play.

Note that if you change the zone for a Schedule Announcement that is currently playing, the announcement will play to both the original zone and to the new zone. To stop the announcement from playing to the original zone, you must use the stop announcement feature (see *"Managing Announcements via the Dashboard" on page 390*).

To edit an announcement:

1. On the navigation bar, expand **Schedules**.
2. Select **Schedule Announcements**.
3. Select the **Edit** icon next to the schedule that you want to edit.
4. Make the desired changes. (See *Table 85, "Add Schedule Announcement Parameters," on page 281*.)

5 After making the desired changes, select **Save**.

Using the Schedule Routines Feature

Routines can be scheduled to execute at a future date/time, and can be scheduled to repeatedly execute using a recurring schedule.

Routines that will be scheduled for execution must have an **Extension** defined and must have **Use Caller's Extension** set to No.

Tip: Make sure that none of the routine's Actions or Conditions attempt to access variables that are only defined for API-initiated routines (e.g., $apiParam1 or other Routines API-specific variables [see *"Using the Routines API" on page 428*]) or DTMF-initiated routines (e.g., $cmdParam1 [see *"Starting and Stopping a Routine from the Admin Phone" on page 426*]). Routine database variables, however, can be accessed (see *"Managing Routine Database Variables" on page 495*).

To view Schedule Routines, and to schedule a Routine:

1 On the navigation bar, expand **Schedules**.

2 Select **Schedule Routines**.

3 To schedule a Routine for execution, select the Add icon.

The *Schedule Routines* page appears.

Figure 105. Schedule Routines

This page displays the following information for each scheduled routine:

Table 87. Schedule Routines Properties

Name	Name of the Routine to be executed.
Refresh button	Refreshes the list of scheduled Routines.
Routines button	Browses to the *Routines* page (see *"Viewing Routines" on page 448*).
Description	Displays the description of the routine. *Note:* Valid characters include uppercase letters (A–Z), lowercase letters (a–z), numerals (0–9), space, and the following special characters: **! @ $ * ? - . , .**
Execute Date	Date on which Routine will execute.

Table 87. Schedule Routines Properties

Execute Time	Time at which Routine will execute.
Parameter 1	Value to be passed to the Routine as $schedParam1.
Parameter 2	Value to be passed to the Routine as $schedParam2.
Zone	Either **All Speakers** or the specific zone associated with the Routine.
Recurring Enabled	If the Routine can be scheduled to recur, **Yes**, otherwise **No**. *Note:* Disabling this setting erases any schedule settings. To temporarily disable a schedule, disable **Recurring Schedule Enabled** instead.
Recurring Schedule Enabled	Indicates if the Recurring Schedule is enabled. Click this button to enable or disable the Recurring Schedule.
Recurrence Data	Displays data for the recurring routine, such as the start and end dates, when you roll over or select the **Show** button.

Add a Scheduled Routine

To schedule a Routine execution, select the Plus icon.

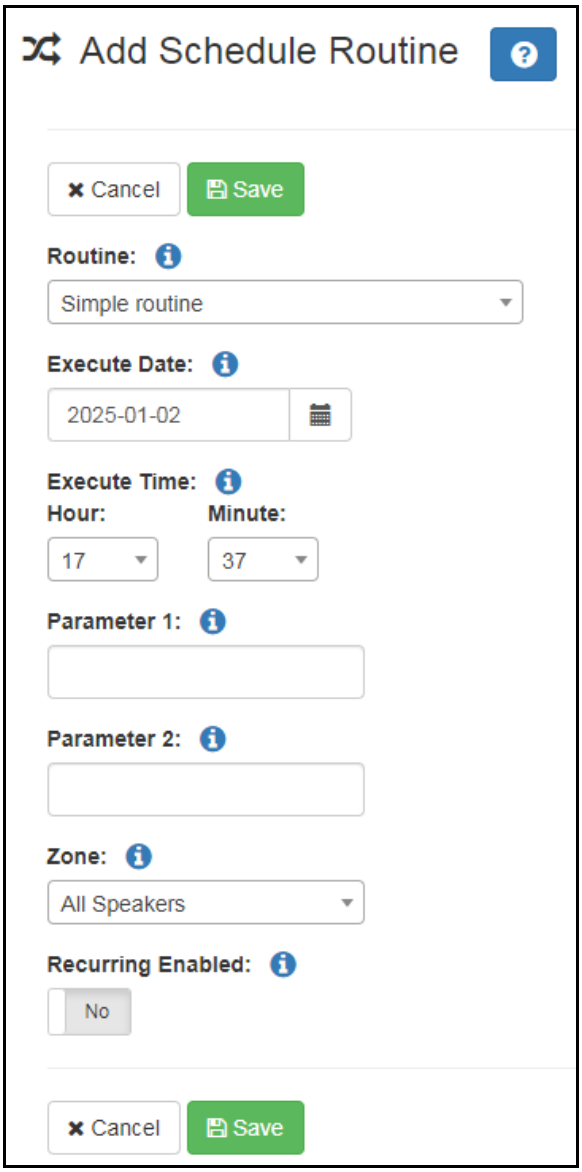


Figure 106. Add Schedule Routine

Table 88. Add Schedule Routine Parameters

Routine	Use the drop-down menu to select the Routine that you want to schedule. *Note:* Only Routines that have Extension set and have Use Caller's Extension set to No will be displayed.
Execute Date	*Note:* This field only appears if **Recurring Enabled** has been set to No. Use the calendar to select the date on which the Routine is to execute.

Table 88. Add Schedule Routine Parameters (continued)

Execute Time	*Note:* This field only appears if **Recurring Enabled** has been set to No. Select the Hour and Minute from the corresponding drop-down menus to specify the time at which the Routine is to execute. *Note:* Scheduled Routines will start at the beginning of the selected minute. If you want the actions in a Routine to start a few seconds after the beginning of the selected minute, you can insert a Pause action in the Routine to delay the execution of actions until the second that you want them to execute. For example, if you want the actions in a Routine to start at 12h:05m:15s, add a Pause action with Seconds equal to 15.
Parameter 1 **Parameter 2**	The Parameter 1 and Parameter 2 values are made available to Routine Conditions and the following Routine actions via the `$schedParam1` and `$schedParam2` variables (see *Table 2, "Routine Action Type-Specific Parameters," on page 588* for details): • Add-Announcement-Audio • Dash-Text • Dash-Text-Delete • Display-Msg • Display-Msg-Delete • Email
Zone	Select either **All Speakers** or a specific zone to associate with the Routine. The zone number is used by the following: • Dash-Text and Dash-Delete actions for Text field and Identifier field via `$zone` variable. • Display-Msg and Display-Msg-Delete actions for Text field and Identifier field via `$zone` variable. • Email action subject field and text field via the `$zone` variable. • The zone number is also passed to Routines that are executed by the scheduled Routine, which is useful if the subsequently executed Routine includes a Feature-Wait action or other actions that use the `$zone` variable.
Recurring Enabled	Use the slider to indicate if the Routine can be scheduled to recur. If **Recurring Enabled** is set to **Yes**, further parameters will be displayed to configure the recurring Routines, as described in *Table 89, "Recurring Scheduled Routine Parameters," on page 287*. If set to **No**, all current recurrence-related settings (see *Table 89, "Recurring Scheduled Routine Parameters," on page 287*) will be deleted.

If **Recurring Enabled** is set to Yes, the following parameters will be displayed:

Table 89. Recurring Scheduled Routine Parameters

Recurring Schedule Enabled	If Yes, the scheduled Routine will execute at the scheduled time(s). If No, the Routine will not execute at the scheduled time(s).
Recurrence Start Date	Use the calendar to select the start date for this recurring Routine.
Recurrence End Date	Use the calendar to select the end date for this recurring Routine. *Note:* This field only appears if **No End Date** is disabled.
No End Date	Use the slider to select **Yes** if you want this Routine to recur indefinitely.
Recurrence Second	Specify which second of the **Recurrence Minutes** at which to execute the Routine.
Recurrence Minutes	Specify one or more values to indicate at which minutes of the specified **Recurrence Hours** the Routine will execute. If unspecified, the default will be every minute of the hour.
Recurrence Hours	Specify one or more values to indicate at which hours of the specified **Recurrence Days** the Routine will execute. If unspecified, the default will be every hour of the day.
Recurrence Days	Specify one or more values to indicate on which days of the specified **Recurrence Months** the Routine will execute. If this and **Recurrence Days of Week** are both unspecified, the Routine will execute every day of the month.
Recurrence Months	Specify one or more values to indicate on which months of the year the Routine will execute. If unspecified, the default will be every month.
Recurrence Days of Week	Specify one or more values to indicate on which days of the week the Routine will execute. If this and **Recurrence Days** are both unspecified, the Routine will execute every day of the week.

Edit a Schedule Routine

To edit a Scheduled Routine:

1. On the navigation bar, expand **Schedules**.
2. Select **Schedule Routines**.
3. Select the **Edit** icon for the Schedule Routine.

4 On the Edit Schedule Routine page, make the desired changes. (See *Table 87, "Schedule Routines Properties," on page 283* and *Table 86, "Recurring Schedule Parameters (only if Recurring Enabled is set to Yes)," on page 281*).

5 Select **Save**.

Schedule Routine Call Details Records

When a scheduled routine is executed, a Call Detail Record (CDR) (see *"Using the Call Details Feature" on page 362*) is created using the following format:

Table 90. Scheduled Routine Call Detail Record

Source	Destination	Type	Status
<extension>	Routine (<routine DTMF code>)	Scheduled Routine	Executed

Call Detail Records are created for Routines executed on a specific scheduled date/time and for each execution of a recurring schedule.

Retrieving First and Last Scheduled Events

You can retrieve XML from the C4000 that either provides the first and last events for today's schedule or shows that the active schedule for the day is a holiday. This information could be used to schedule the opening of facility doors before the first scheduled event and the closing of facility doors after the last scheduled event.

To retrieve this information:

1 In your browser, type the following:

```
http://<server>:8088/static/schedules-boundary.xml
```

2 Press **Enter**.

Alternatively, you can retrieve the XML programmatically or from a command prompt or script. Here are a couple simple examples:

Curl example:

```
curl.exe http://<server>:8088/static/schedules-boundary.xml
```

PowerShell example:

```
(Invoke-WebRequest -Uri http://<server>:8088/static/schedules-boundary.xml).Content
```

The XML returned will contain the schedule name, as well as the start and end event times, for the site. If the day has been scheduled as a holiday, the word "Holiday" appears in the XML file (see *Figure 108, "XML Output for a Holiday," on page 289*).

```
<?xml version="1.0" encoding="UTF-8"?>
<Schedules>
  <Site>
    <Name>Manufacturing Plant</Name>
    <Schedule>
      <Name>Regular Day</Name>
      <First-Event>8:40:00</First-Event>
      <Last-Event>14:50:00</Last-Event>
    </Schedule>
  </Site>
</Schedules>
```

Figure 107. Schedule Information for a Site

```
<Schedules>
  <Holiday>
    <Name>New Year’s Day</Name>
    <Start-Date>2022-01-01</Start-Date>
    <End-Date>2022-01-01</End-Date>
  </Holiday>
</Schedules>
```

Figure 108. XML Output for a Holiday

Managing Audio

With Nyquist's audio file management feature, you can:

- Specify an audio program for distribution to stations or zones.
- Record and play tones and announcements to stations or zones.
- Manage recordings of telephone calls made to and from stations.

Audio programs for distribution to stations or zones can include line-input from the MMPA, Nyquist 2-channel or 4-channel amplifiers, user-supplied songs or playlists, and Internet Radio Services. The Audio Distribution, tones, and announcement files added through the audio file management feature can be set through the Schedules feature to automatically play during specified times. (*See "Managing Schedules" on page 262*.) Through the Internet Radio Services, you can listen to live radio stations and add media catalogs and music services without updating devices or software.

Default tone and song files include white noise and pink noise that allows you to tune paging and audio distribution volumes.

Note: Before using the audio file management feature, make sure that stations and zones have been configured (see *"Managing Stations, Zones, and Queues" on page 141*) and that the station you are using to start announcements, tones, or Audio Distribution has the appropriate CoS parameters set (see *"Using CoS Configuration" on page 100*).

Audio Distribution

Suppose you want to use an audio source, such as a radio station accessed via the Internet, in a cafeteria but prevent that source from being played in a conference room. This feature, called Audio Distribution, can be turned on by zone (an area or group of stations) or stations (group of devices such as VoIP speakers). You can add the speakers, or stations, in the cafeteria to a zone that allows Audio Distribution while the speakers in a conference room would not be placed into that zone.

Audio Distribution involves creating a playlist or selecting an input source and specifying which zones hear the playlist or input source. Through the Scheduled Audio feature, Audio Distribution can be tied to a specific event in a schedule (see *"Adding an Event" on page 270*).

The following steps will guide you through setting up Audio Distribution:

1. Define audio sources by:
   - Adding songs and creating playlists (see *"Managing Songs" on page 294* and *"Managing Playlists" on page 299*)
   - Adding airable Radio Station sources (see *"Using Internet Radio Services" on page 304*)
   - Adding SoundMachine sources (see *"Adding a Source" on page 305*)
   - Setting up appliances that will provide audio sources (see *"Managing Line-Input Sources" on page 292*)

2 On the Dashboard, add Audio Distributions that can be used by the system. Each Audio Distribution defines the audio source to use and the destinations (i.e., zones and/or stations) for the audio when played (see *"Creating an Audio Distribution" on page 311*).

3 Setup your Audio Distributions to play by:

- Scheduling Audio Distribution via Schedules (see *"Using the Schedule Announcements Feature" on page 278*)
- Starting Audio Distribution via Routines (see *"Using Routines to Start Audio Distribution" on page 316*)
- Starting Audio Distribution via I/O Controller contact closure (see *"Configuring I/O Controller Input Rules" on page 162*)
- Starting Audio Distribution manually using one of the following:
  - •Web Interface Dashboard (see *"Using Audio Distribution" on page 402*)
  - •NQ-T1100 or NQ-ZPMS Admin Phone (see *"Customizing an NQ-T1100 IP Phone – Color Touch Display" on page 201*, *"Customizing an NQ-ZPMS Zone Paging Microphone Station" on page 204*, and *"Using the Admin Phone" on page 319*)

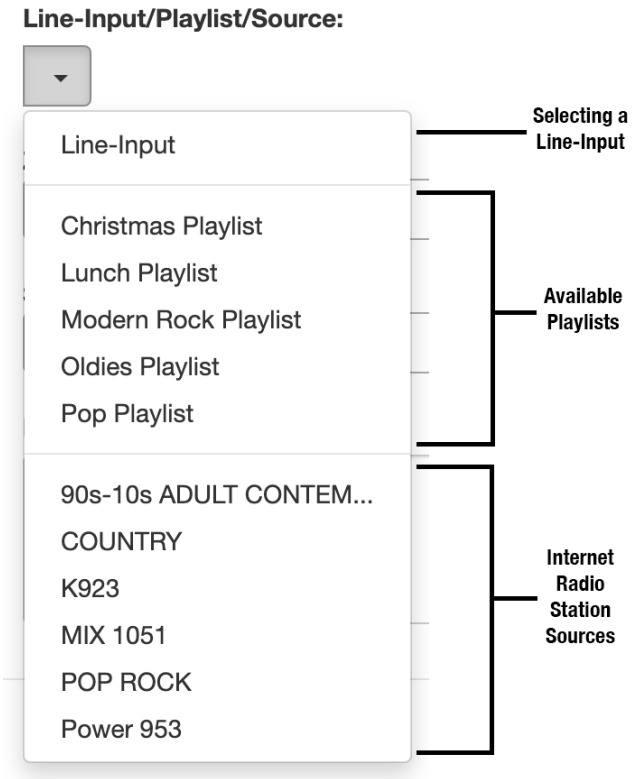


Figure 109. Audio Distribution Sources

Audio Distribution sources can include:

- Audio from two- or four-channel audio power amplifier's or MMPA's Line Inputs
- User-supplied music (songs and playlists)
- Internet Radio Services
  - airable stations
  - SoundMachine stations

Managing Line-Input Sources

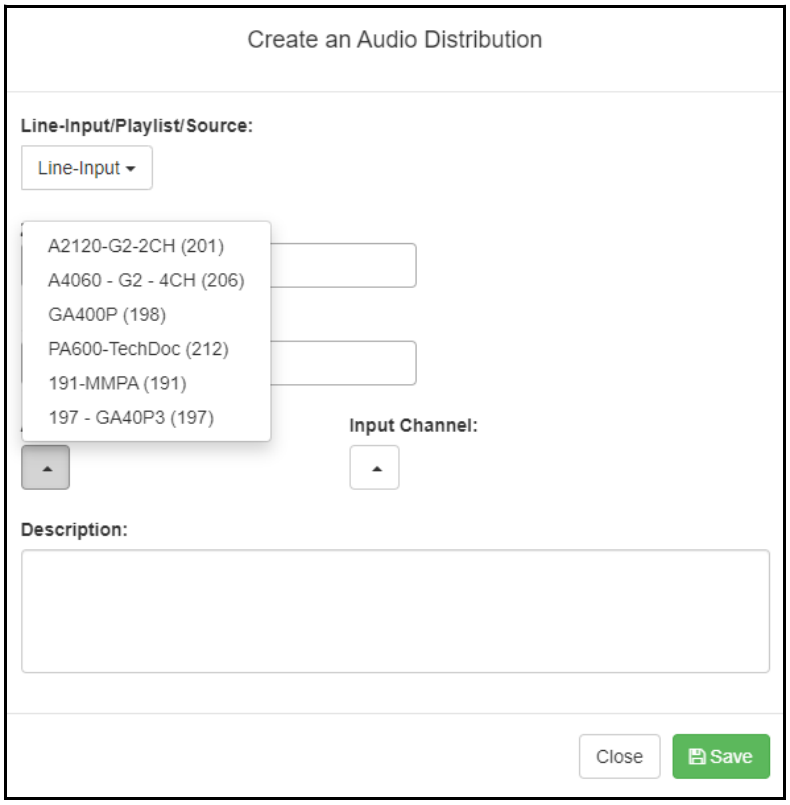


Figure 110. Line-Input Sources

If your Nyquist system uses two-channel or four-channel audio power amplifiers or MMPAs, these stations will appear as sources for Line-Input when creating Audio Distribution.

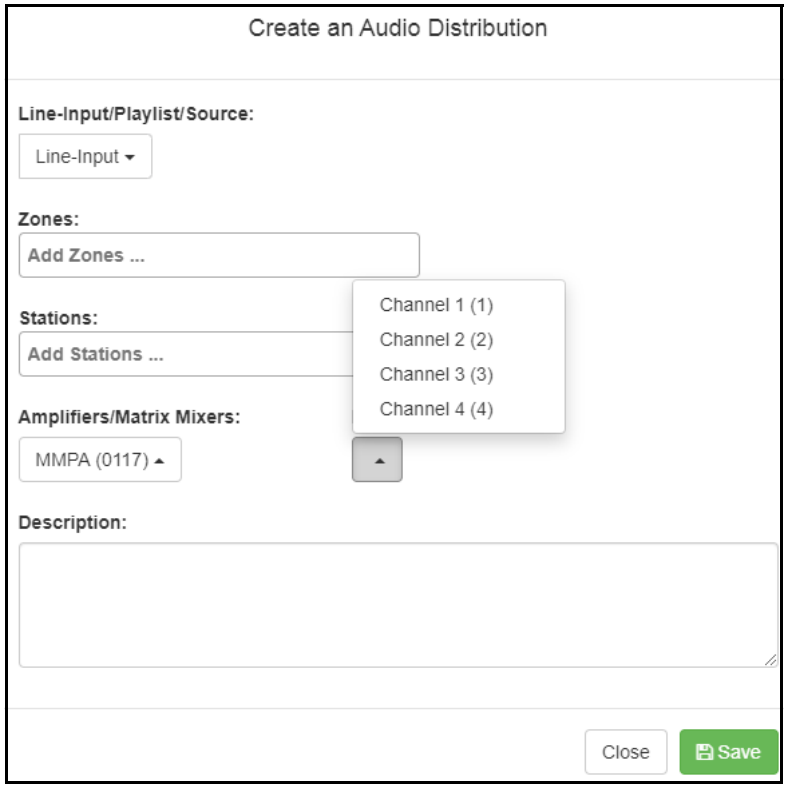


Figure 111. Available Channels for an MMPA

The available Input Channel selections can range from 1 or 2 for an amplifier or 1 to 4 for an MMPA.

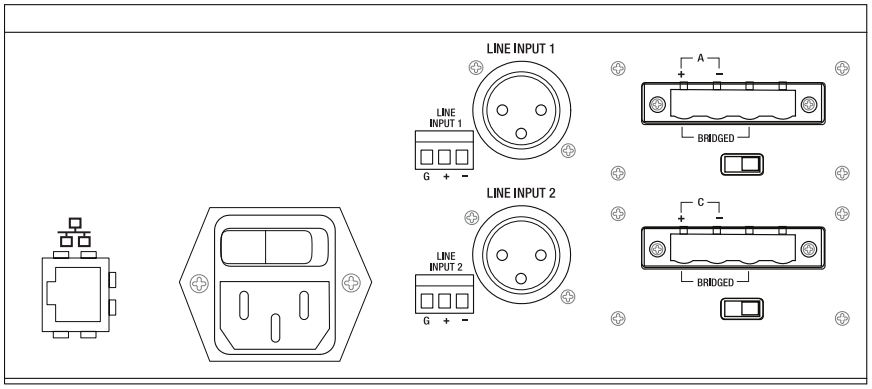


Figure 112. Line Input for NQ-A4300 Audio Power Amplifier

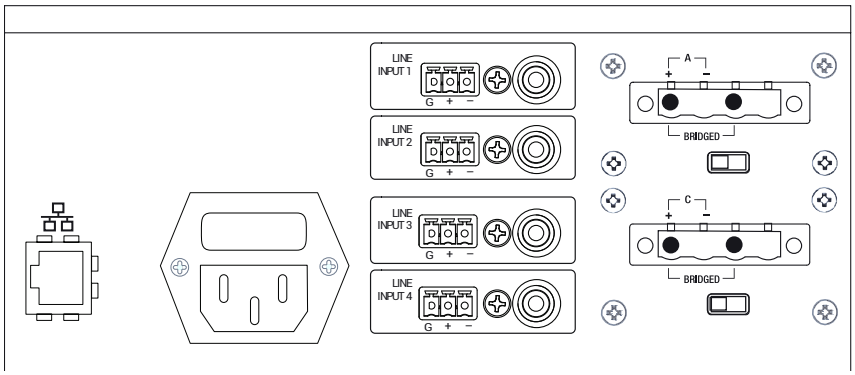


Figure 113. Line Input for NQ-A4300-G2 Audio Power Amplifier

The first generation amplifiers and MMPAs must be configured at the device, using either XLR or Phoenix (but not both) as the input. The G2 amplifiers must be configured at the device, using either RCA or Phoenix (but not both) as the input.

The Amplifiers/Matrix Mixers and Input Channel selections are made when creating an audio distribution.

Managing Songs

The songs feature allows you to select songs that can be added to a playlist; the playlist can then be selected to play manually or during scheduled events such as lunch time. You upload a song similarly to how you upload an announcement file or tone. You can store songs on a USB flash drive; these songs can then be played via the playlists feature (see *"Playing Songs Directly from a USB Flash Drive" on page 296*).

By default, white noise and pink noise songs are provided to help tune the volume of an Audio Distribution zone. (See *"Tuning Volume with White or Pink Noise" on page 364*.)

Viewing the Song List

From the Songs page, you can add, edit, or delete a song. If you delete a song that is in a Playlist, the song is automatically removed from the Playlist.

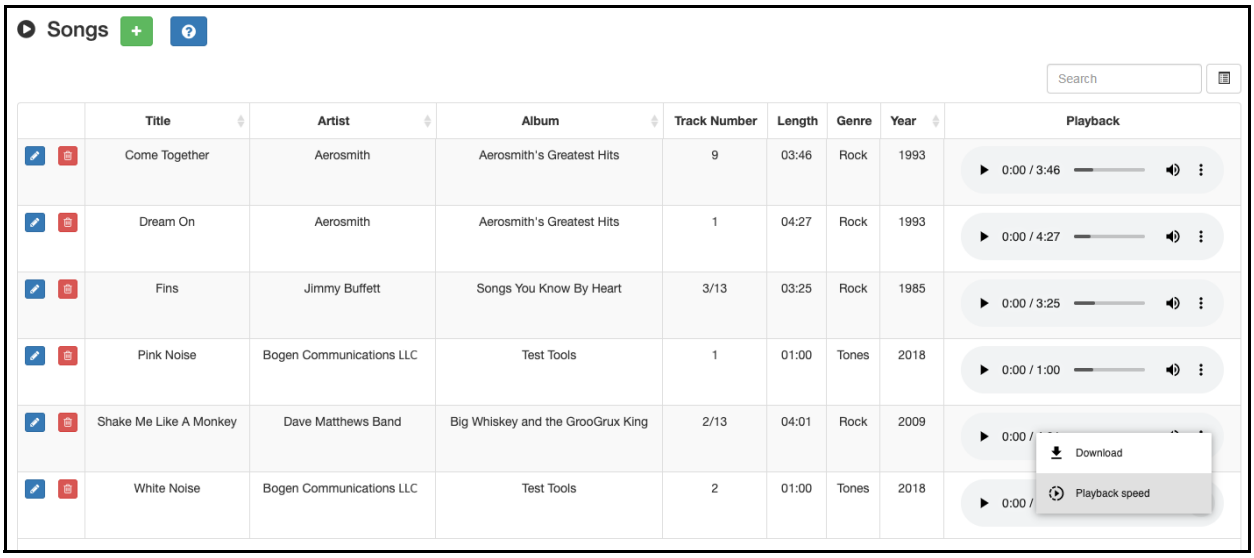


Figure 114. Songs Page

To view the song list:

1. On the navigation bar, expand **Audio**.
2. Select **Songs**.

The following table describes the information provided about each song:

Table 91. Songs Page Parameters

Title	Displays the user-provided song title.
Artist	Displays the name of the musician performing the song.
Album	Displays the name of the album the song is from.
Track Number	Displays the track on the album for the song.
Length	Provides the length of the song in seconds.
Genre	Displays the music genre, or category, for the song.
Year	Displays the year the song was recorded.
Playback	Allows you to manually play the song. Selecting the **Menu** icon in this field also allows you to download and save the song, as well as specify the song's playback speed.

Playing Songs Directly from a USB Flash Drive

You can use a USB flash drive as storage for songs that can be played via the playlists feature.

To add songs and create a playlist for a USB flash drive, create a root file on the USB flash drive called `MusicLibrary.txt`. This file can contain the following entries:

```
playlistname=<text entered by customer>
createplaylist=no
useexistingplaylist=yes
```

If `createplaylist=no` is found in MusicLibrary.txt, a playlist is not created for the imported files.

If `useexistingplaylist=yes` is used, new songs will be added to the playlist defined by the `playlistname` option.

The music files must be in the root directory of the USB flash drive. Valid formats for these files are mp3, wav, and aac.

The Nyquist server automatically mounts the USB flash drive, adds all songs found in the root directory to the songs list, and creates a playlist for the added songs. The default name for the playlist is *USB Music Library*.

If you want to see if a USB flash drive is plugged into the System Controller and mounted for use, you can use the **Check Server Status** feature from *System Parameters* to view a list of mounted USB drives (search for "USB Drives" in the "Disk Space" section of the *Check Server Status* report).

Note: If you use a USB flash drive as storage for songs on a playlist and the USB flash drive is removed from the USB drive, the metadata for the songs and the playlist still resides in the Nyquist song list and playlist, but Audio Distribution cannot play. For this reason, we recommend never removing the flash drive from the computer.

Warning After you have inserted a USB flash drive into the System Controller, removing it may damage the contents stored on the USB flash drive. If you need to remove the USB flash drive from the System Controller, use **Shut Down**, found in *System Parameters*, to shutdown the Nyquist System Controller before removing the USB flash drive.

Adding Songs

You can add songs from your local computer or from removable media, such as a flash drive. You can add a song to playlists as part of the Add Song process or you can add a song to a playlist later through the **Playlists** menu.

You can select to add one song or multiple songs.

Nyquist can use any ID3 tag data and save that automatically. An ID3 tag acts as a container file within an MP3 audio file and commonly contains the title, artist name, album, track data, year, and genre.

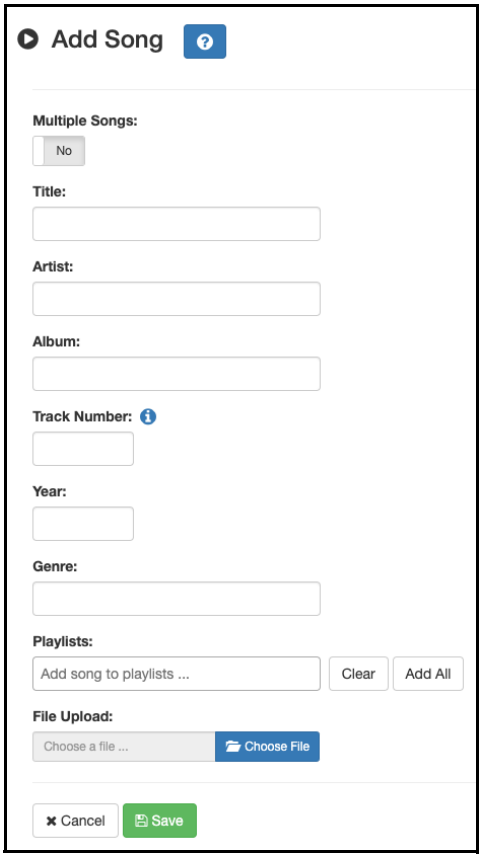


Figure 115. Add Song Page

To add a song file:

1. On the navigation bar, expand **Audio**.
2. Select **Songs**.
3. On the Songs page, select the **Add** icon.

Note: If the imported song file contains metadata, Nyquist automatically fills in the Title, Artist, Album, Track Number, Year, and Genre after you press the **Save** button. If no metadata exists, the song **Title** is set to **Untitled** and the other parameters are left blank. Most MP3 files do contain metadata. You also can choose to not fill in the parameters.

---

4. On the *Add Song* page, complete the parameters. If you want to add multiple songs, ensure that you select **Yes** for **Multiple Songs**. Then, use the *Shift* or *Control* keys when selecting multiple files. Parameters do not appear when using the **Multiple Songs** option.
5. After completing all changes, select **Save**. The song or songs will be copied onto the Nyquist system.

Table 92. Add Song Page Parameters

Multiple Songs	Allows you to select multiple songs.
Title	Displays the user-provided song title.

Table 92. Add Song Page Parameters (continued)

Artist	Displays the name of the musician performing the song.
Album	Displays the name of the album the song is from.
Track Number	Displays the track on the album for the song.
Year	Displays the year the song was recorded.
Genre	Displays the music genre, or category, for the song.
File Upload	Allows you to select the song that you want to upload.
Playlists	Select the playlists that you want to add the song to. You can select multiple playlists, select all playlists by selecting **Add All**, or use the **Clear** button to remove the playlists.
File Upload	Select **Choose file** and navigate to select the file to upload. This option allows you to select files not only from your computer but also from a USB flash drive inserted in your computer.

Editing Song Information

Through the Edit Song page, you can edit the information that appears on the Songs page for a particular song or replace the downloaded file with another.

To edit the information associated with the song file:

1. On the navigation bar, expand **Audio**.
2. Select **Songs**.
3. On the *Songs* page, select the **Edit** icon next to the song that you want to edit information for.
4. On the *Edit Song* page, make changes to the parameters (see *Table 93 on page 298*).
5. After completing all changes, select **Save**.

Table 93. Edit Song Page Parameters

Title	Displays the user-provided song title.
Artist	Displays the name of the musician performing the song.
Album	Displays the name of the album the song is from.
Track Number	Displays the track on the album for the song.
Year	Displays the year the song was recorded.
Genre	Displays the music genre, or category, for the song.
File Upload	Allows you to select the song that you want to upload.
Playlists	Allows you to add or remove the song from playlists.

Deleting a Song

Through the Songs page, you can delete a song from your Nyquist system. If you delete a song that is in a Playlist, the song is automatically removed from the Playlist.

To delete a song:

1. On the navigation bar, expand **Audio**.
2. Select **Songs**.
3. On the Songs page, select the **Delete** icon next to the song that you want to delete.
4. When prompted, select **Delete**.

Managing Playlists

You can create and manage playlists that contain multiple songs to use for scheduled events and dashboard Audio Distribution entries. You can select a playlist when creating an event. (See section *"Adding an Event" on page 270.)* Specifying the audio program for stations or zones is known as audio distribution.

Viewing Playlists

Through the Playlists page, you can view all playlists available to your Nyquist system and create, delete, and manage a playlist. With the Manage Playlist feature, you can add, delete, or change the order of a playlist's songs.

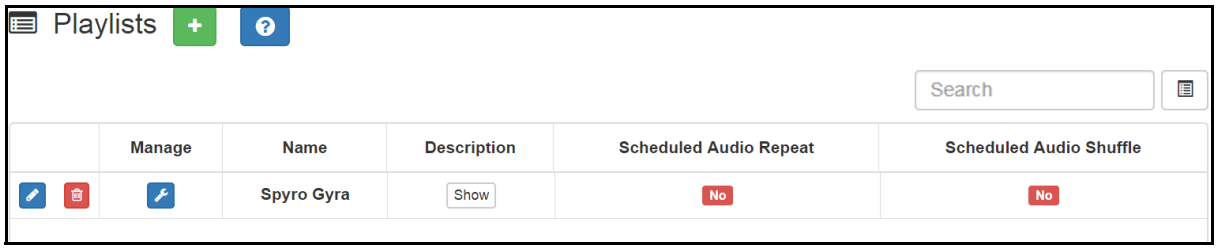


Figure 116. Playlists Page

To view playlists:

1. On the navigation bar, expand **Audio**.
2. Select **Playlists**.

The Playlists page appears. The following table describes the information that appears on this page:

Table 94. Playlists Page Parameters

Manage	When selected, this option displays the songs that can be dragged and dropped to and from the playlist.
Name	Displays the user-provided name for the playlist. This field can contain a maximum of 40 characters. *Note:* Valid characters include uppercase letters (A–Z), lowercase letters (a–z), numerals (0–9), space, and the following special characters: **! @ $ * ? - . ,** .
Description	When **Show** is selected, the user-provided description of the play list appears. This field can contain a maximum of 256 characters. *Note:* Valid characters include uppercase letters (A–Z), lowercase letters (a–z), numerals (0–9), space, and the following special characters: **! @ $ * ? - . ,** .
Scheduled Audio Repeat	When enabled, the playlist audio will be repeated after all songs have been played. When disabled, Scheduled Audio will automatically stop after the last song has been played from the playlist. When disabled, a corresponding stop event is not needed when Scheduled Audio is started via the schedule. *Note:* When playlists are being used by the Audio Distribution feature, the Scheduled Audio options are ignored.
Scheduled Audio Shuffle	When enabled, the order in which the songs are played is shuffled. When disabled, the playlist songs will be played in the order that they appear in the playlist. *Note:* When playlists are being used by the Audio Distribution feature, the Scheduled Audio options are ignored.

Creating a Playlist

When you add a playlist, you first create the playlist container and then you use the Manage tool to add songs to the playlist. To add songs to a playlist, you must have access to songs that have been uploaded to your Nyquist server or are available on a USB flash drive inserted into the Nyquist server.

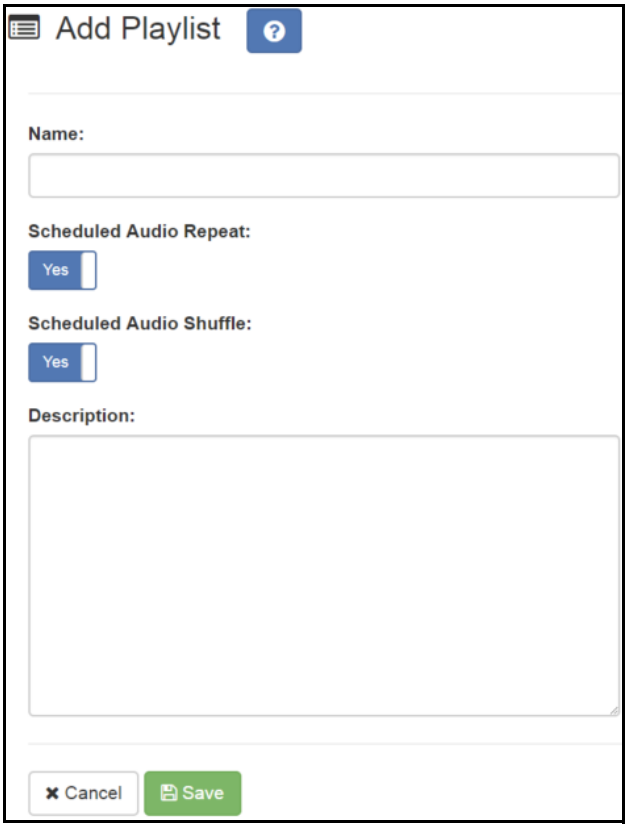


Figure 117. Add Playlist Page

To add a playlist:

1. On the navigation bar, expand **Audio**.
2. Select **Playlists**.
3. Select the **Add** icon.
4. On the *Add Playlist* page, complete parameters for this playlist. (See *Table 95, "Add Playlist Parameters," on page 301*.)
5. Select **Save**.

Table 95. Add Playlist Parameters

Name	Displays the user-provided name for the playlist. This field can contain a maximum of 40 characters. *Note:* Valid characters include uppercase letters (A–Z), lowercase letters (a–z), numerals (0–9), space, and the following special characters: ! @ $ * ? - . , .
Scheduled Audio Repeat	When enabled, the playlist audio will be repeated after all songs have been played. When disabled, Scheduled Audio will automatically stop after the last song has been played from the playlist. When disabled, a corresponding stop event is not needed when Scheduled Audio is started via the schedule. *Note:* When playlists are being used by the Audio Distribution feature, the Scheduled Audio options are ignored.

Table 95. Add Playlist Parameters (continued)

Scheduled Audio Shuffle	When enabled, the order in which the songs are played is shuffled. When disabled, the playlist songs will be played in the order that they appear in the playlist. *Note:* When playlists are being used by the Audio Distribution feature, the Scheduled Audio options are ignored.
Description	When **Show** is selected, the user-provided description of the playlist appears. This field can contain a maximum of 256 characters. *Note:* Valid characters include uppercase letters (A–Z), lowercase letters (a–z), numerals (0–9), space, and the following special characters: ! @ $ * ? - . , .

Adding Songs to a Playlist

After you create a playlist, use the Manage tool to add songs to the playlist.

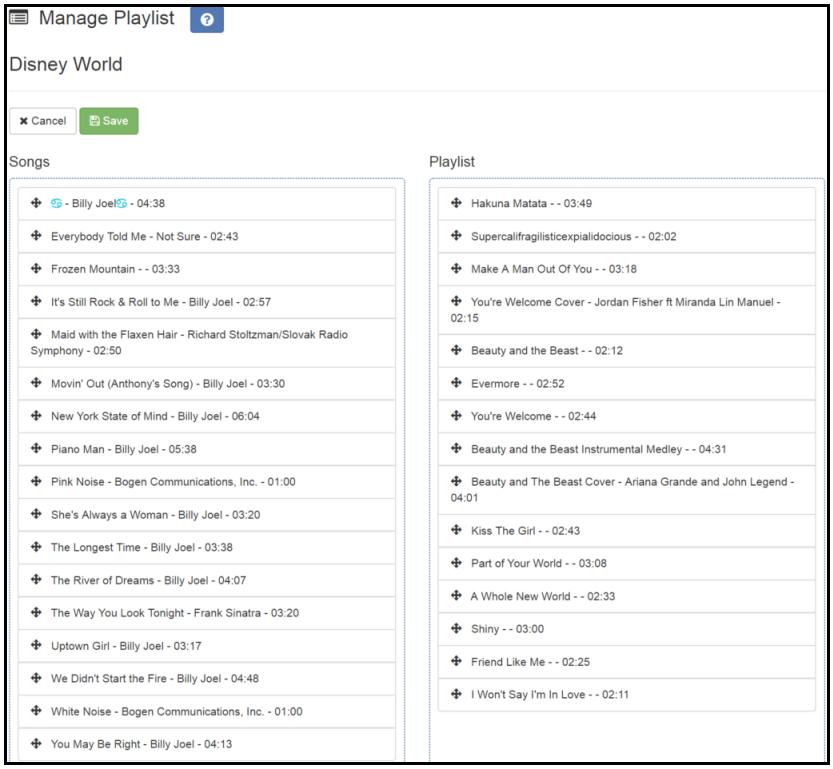


Figure 118. Manage Playlist Page

To add songs to a playlist:

1. On the navigation bar, expand **Audio**.
2. Select **Playlists**.
3. On the Playlists page, select the **Manage** icon next to the playlist that you want to add songs to.
4. On the *Manage Playlist* page, drag and drop the song you want to add from the **Songs** field to the Playlist field.
5. After all desired songs have been added to the Playlist, select **Save**.

Changing Song Order in a Playlist

You can use the Manage tool to change the order of songs in a playlist.

To change the song order:

1. On the navigation bar, expand **Audio**.
2. Select **Playlists**.
3. On the Playlists page, select the **Manage** icon next to the playlist for which you want to change song order.
4. On the *Manage Playlist* page, drag and drop the songs into the order that you want.
5. Select **Save**.

Deleting a Song from a Playlist

You can use the Manage tool to remove a song from a playlist.

To delete a song from a playlist:

1. On the navigation bar, expand **Audio**.
2. Select **Playlists**.
3. On the Playlists page, select the **Manage** icon next to the playlist.
4. Drag and drop the song from the **Playlist** field to the **Songs** field.
5. After all desired changes are completed, select **Save**.

Editing a Playlist

The **Edit** icon allows you to edit the parameters for a playlist. To change the order of songs in a playlist, see *"Adding Songs to a Playlist" on page 302*. To delete a song from a song list, see *"Deleting a Song from a Playlist" on page 303*.

To edit a playlist:

1. On the navigation bar, expand **Audio**.
2. Select **Playlists**.
3. Select the **Edit** icon next to the playlist.
4. On the *Edit Playlist* page, make desired changes to the parameters. (For more information about the parameters, see *Table 95, "Add Playlist Parameters," on page 301*.)
5. Select **Save**.

Deleting a Playlist

You can delete a playlist provided the playlist is not being used with an I/O Controller Input or Output Rule.

To delete a playlist:

1. On the navigation bar, expand **Audio**.
2. Select **Playlists**.
3. Select the **Delete** icon next to the playlist.
4. When prompted, select **Delete**.

Using Internet Radio Services

Through the Internet Radio Services, you can access online content, such as music services and Internet radio, using airable and SoundMachine. With this service, you can listen to live radio stations and add media catalogs and music services without updating devices or software.

You can navigate through the catalog of radio stations by:

- Genre
- Language
- Location
- Quality
- Popularity

You can also search the catalog for particular artists or songs.

Use of the Internet Radio Services feature requires the Nyquist server to have Internet access. It also depends on the permissions assigned to the role with which you are associated.

Figure 119. Internet Radio Services Permissions

For information about assigning permissions to roles, see *"Assigning and Editing Permissions" on page 248*.

Viewing Internet Radio Services

If you have **View** permission for the Internet Radio Services, you can view a list of Internet radio stations that can be accessed through your system as well as information about each station. Through the Internet Radio Services page, you can also select to manage credentials for services such as SoundMachine. (See *"Managing Credentials" on page 308*.)

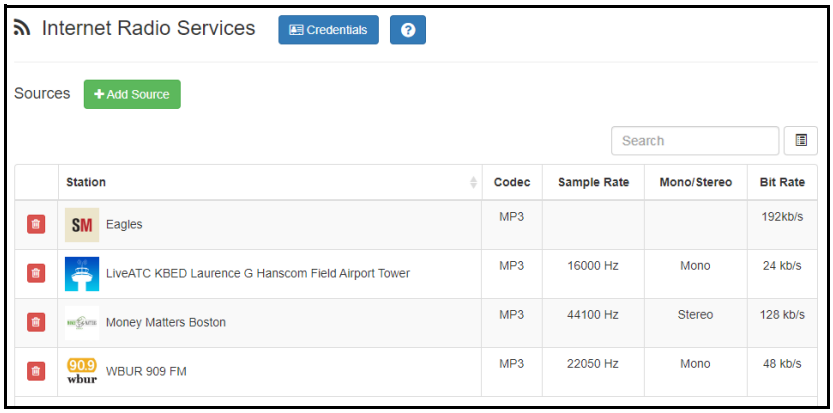


Figure 120. Internet Radio Services View

To view Internet Radio Services added to your system:

1. On the navigation bar, expand **Audio**.
2. Select **Internet Radio Services**.

The following parameters appear for each source configured for your Nyquist system:

Table 96. Internet Radio Services

Station	Displays the icon, name, and description of the radio station.
Codec	Displays how the streaming media is compressed and decompressed.
Sample Rate	Displays the number of samples of audio carried per second.
Mono/Stereo	Displays if the signal is being transmitted by a single channel (mono) or by two channels (stereo).
Bit Rate	Displays the bit rate used to transmit the streaming media.

Adding a Source

You can select to add an Internet radio source or a service, such as SoundMachine. The screen that appears when you select **Add Source** also allows you to manage credentials or sign up for SoundMachine.

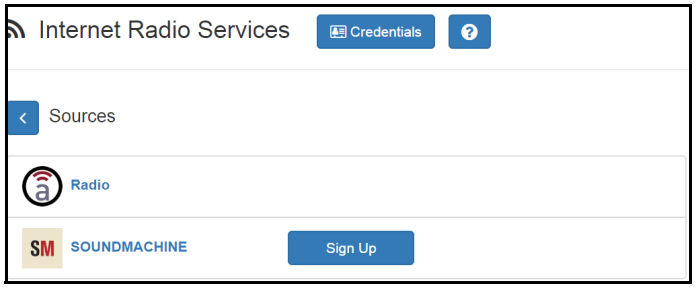


Figure 121. Add Source Page

To add a source:

1. On the navigation bar, expand **Audio**.
2. Select **Internet Radio Services**.
3. On the *Internet Radio Services* page, select **Add Source**.
4. Select from the list of **Sources**.
5. If you select **Radio**, do the following:
   a) Select how you want to select a source. Options are:

Table 97. Radio Source Parameters

Local stations	Select to view a list of stations near your location.
Popular stations	Select to view stations considered to be the most popular.
Trending	Select to view the stations that are gaining momentum.
High quality	Select to view the stations with a high sound quality.
New stations	Select to filter the list of stations by new stations added to Internet Radio Services.
Filter	Select to filter the list of stations by **Location**, **Language**, or **Genre**.
Search	Select to enter a search term.

   b) When the list of stations that meet the selected criteria appears, select the station that you want.
   c) Select **Add Source** for each source (aac or mp3) that you want.
6. If you select **SoundMachine**, do the following:
   a) Select how you want to open a source. Selections are:

Table 98. SoundMachine Parameters

Genres	Displays a list of genres, such as **Blues** and **Pop**, which you can select to drill down genre choice even further.
Stations	Displays categories for stations, such as **Country**, which you can select to drill down to select a specific album or song.
My Stations	Displays radio stations that you added through the SoundMachine website.
Mixes	Displays categories of stations that combine, or mix, music genres. Mixes can be created using your SoundMachine account and SoundMachine user interface. All Mixes that you create in your SoundMachine account will be available in the Mixes list. Mixes allow you to select albums and songs to include in the Mix.
Music Selection Schedules	Displays the Schedules that have been created through SoundMachine. (See *"Using SoundMachine Music Selection Schedules" on page 310*.) Schedules allow the playing of specific stations or mixes during specific times of the day. For example, you can play soft jazz music during morning hours and select a different genre mix for mid-day. When you create a Music Selection Schedule, you cannot have any empty time periods or Audio Distribution will stop when the empty time period is encountered. The Music Selection Schedules that you create appear as **Line-Input/Playlist/Source** selections for Audio Distribution. (See *"Using Audio Distribution" on page 402*.)
Logout	Select to log out of SoundMachine.

b) Drill down until you can select a specific album or song.

c) Select **Add Source**.

Deleting a Source

To delete a source:

1 On the navigation bar, expand **Audio**.

2 Select **Internet Radio Services**.

3 On the Internet Radio Services window, select the **Delete** icon next to the source that you want to delete.

4 When prompted, select **Delete**.

Managing Credentials

If you have been assigned permissions, you can view, add, edit, and delete login credentials needed to access the SoundMachine service.

For information about roles and permissions, see *"Assigning and Editing Permissions" on page 248*.

Viewing Credentials

The Credentials list allows a quick view of the users who have login credentials.

To view the Credentials list:

1. On the navigation bar, expand **Audio**.
2. Select **Internet Radio Services**.
3. Select **Credentials**.

The Credentials list displays the following information:

Table 99. Credentials Parameters

Name	Displays the name of the service, such as SoundMachine.
Enabled	Indicates if the account is enabled for this service.
Username	Provides the **Username** for the account.

Adding Credentials

You can create a user account that allows a user to use an Internet Radio Service, such as SoundMachine. You can also use the Add Credential page to sign up for SoundMachine.

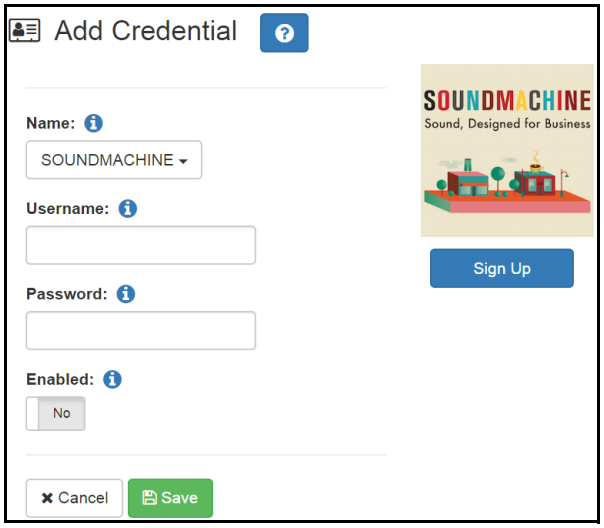


Figure 122. Add Credential

To create an account:

1. On the navigation bar, expand **Audio**.
2. Select **Internet Radio Services**.
3. Select **Credentials**.
4. Select the **Add** icon.
5. Complete the following parameters:

Table 100. Add Credential Parameters

Name	Use the drop-down arrow to select the name of the service.
Username	Enter the username for this account.
Password	Enter the password for this account.
Enabled	Select **Yes** to enable this account.

Edit Credential

If you have the appropriate permissions, you can edit a user's credentials for accessing SoundMachine, including viewing or changing a user's password and enabling or disabling their use of the service.

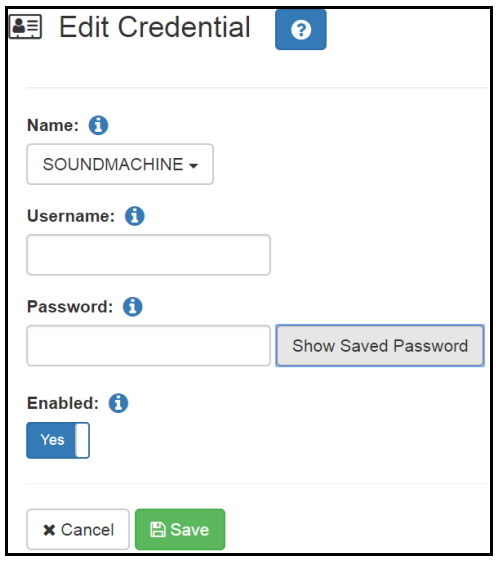


Figure 123. Edit Credential

To edit an account:

1. On the navigation bar, expand **Audio**.
2. Select **Internet Radio Services**.
3. Select **Credentials**.
4. Select the **Edit** icon next to the account that you want to edit.
5. Make the desired changes. (See *Table 101*.)

6 Select **Save**.

Table 101. Edit Credentials Parameters

Name	Use the drop-down arrow to select the name of the service.
Username	Enter the username for this account.
Password	Enter the password for this account. Select **Show Saved Password** to view an existing password for the account being edited.
Enabled	Select **Yes** to enable this account.

Delete Credentials

You can delete a user's credentials to access SoundMachine.

To delete an account:

1 On the navigation bar, expand **Audio**.
2 Select **Internet Radio Services**.
3 Select **Credentials**.
4 Select the **Delete** icon next to the account that you want to edit.
5 When prompted, select **Delete**.

SoundMachine Sign Up

You can sign up for SoundMachine via the Add Source (see *"Adding a Source" on page 305*) or Add Credential (see *"Adding Credentials" on page 308*) windows.

To sign up for SoundMachine:

1 On the navigation bar, expand **Audio**.
2 Select **Internet Radio Services**.
3 Do one of the following:
   - Select **Add Source**.
   - Select **Credentials** and then select the **Add** icon.
4 Select **Sign Up**.
5 When the SoundMachine and BOGEN page appears, follow the on-screen instructions.

Using SoundMachine Music Selection Schedules

Schedules that you create using the SoundMachine web-based user interface appear as **Music Selection Schedules** in the Nyquist Admin Web UI. You can select a Music Selection Schedule to play as Audio Distribution. (See *"Using Audio Distribution" on page 402*.)

When you create a Music Selection Schedule, you cannot have any empty time periods or Audio Distribution will stop when the empty time period is encountered.

You cannot name a Music Selection Schedule using all special characters; the name must contain at least one alpha or numeric character or the Music Selection Schedule will not appear.

Scheduled Audio takes priority over a Music Selection Schedule. For information about Scheduled Audio, refer to *"Understanding Event Settings" on page 271*.

Creating an Audio Distribution

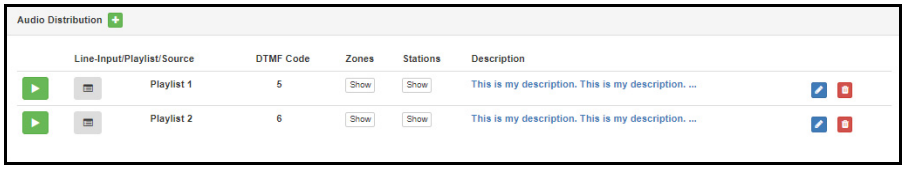


Figure 124. Audio Distribution Portion of Dashboard

To use the Audio Distribution feature, you must have the proper CoS configuration on your station. See *"Editing CoS Parameters for a Station" on page 104* if you need to change your station's CoS.

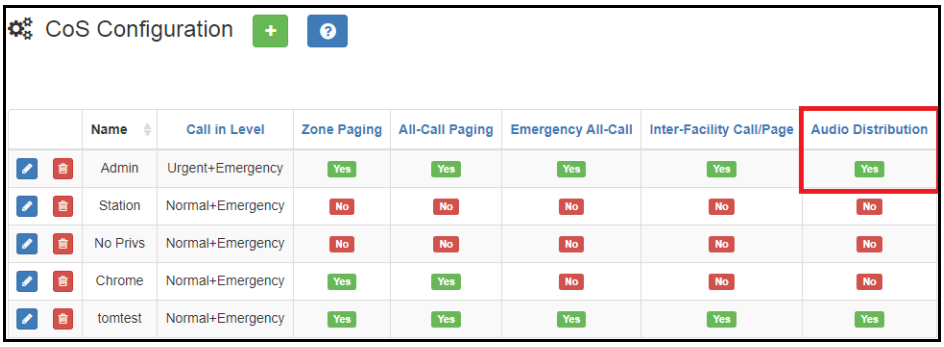


Figure 125. Audio Distribution Set in CoS

You must also be assigned a Role that has permissions to create Audio Distribution.

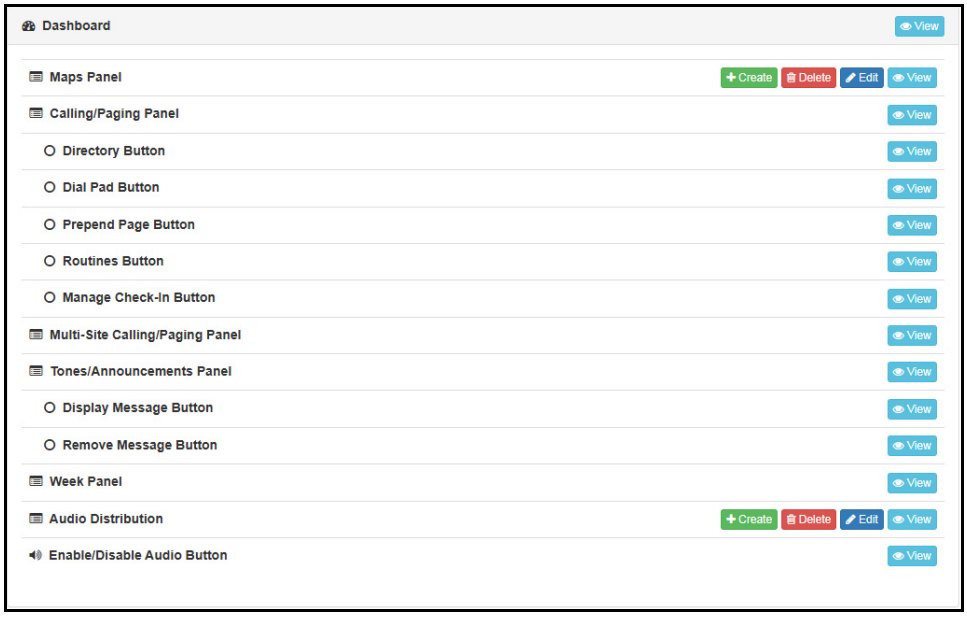


Figure 126. Role Permissions for Audio Distribution

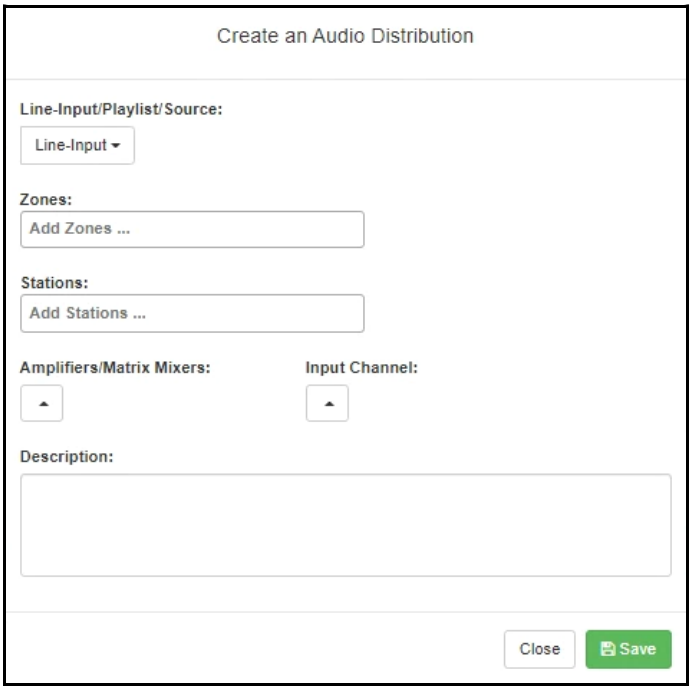


Figure 127. Create an Audio Distribution

To create an Audio Distribution:

1. If not already on your dashboard, select **Dashboard** from the navigation bar.
2. Select the **Add** icon next to **Audio Distribution**.
3. Complete the Create an Audio Distribution parameters (see *Table 102*).

Note: If you are using at least one Nyquist Matrix Mixer Pre-Amp, Line-Input appears as a Line-Input/Playlist/Source option.

4 Select the **Zones** and **Stations**.

5 If you select **Line-Input** as the Input Source/Playlist, select the **Amplifiers/Matrix Mixers** and **Input Channel**.

6 If you select a playlist and want to shuffle the song order, set **Shuffle** to **Yes**.

7 Select **Save**.

8 To end the playing of audio, select the **Stop** icon next to the playlist.

Table 102. Create an Audio Distribution Parameters

Line-Input/ Playlist/Source	Use the **Line-Input/Playlist/Source** drop-down menu to select the audio source. Audio sources can include a line-input from an MMPA or amplifier, available playlists previously created for your system, or Internet radio station sources.
Zones	Select **All Speakers** or a specific zone or zones where you want the audio to play. If the specified zones would result in a *zone overlap* condition (see *"Zone Overlap Messages" on page 372*), this change will not be allowed.
Stations	Select the stations where you want the audio to play.
Amplifiers/Matrix Mixers	Select the Amplifier or Matrix Mixer to use as the audio source.
Input Channel	Select the Input Channel to be used as the audio source.
Shuffle	If you select a playlist and want to shuffle the song order, set **Shuffle** to **Yes**.
Description	Add a description for the Audio Distribution. For example, you may want to note that the audio is for lunchtime.

Starting and Stopping Audio Distribution

Starting and stopping Audio Distribution can be done manually (via the Nyquist web interface dashboard, the NQ-T1100 or NQ-ZPMS Admin Phone's Audio Distribution menu, or the Zone Control feature) or automatically (via scheduled events, NQ-E7010 I/O controller input-contact closure rules, or Routines).

A list of existing Audio Distributions appears on the dashboard. An existing Audio Distribution can be edited or deleted, provided it is not currently playing, by selecting the **Edit** or **Delete** icon next to the Audio Distribution.

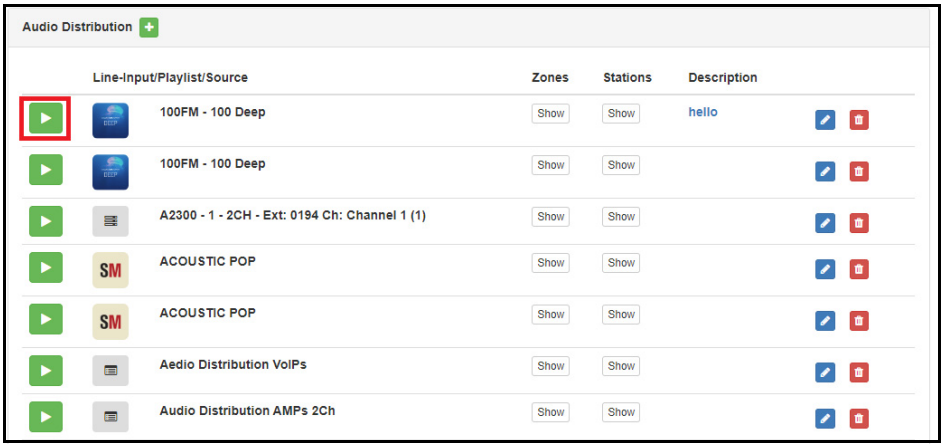


Figure 128. Audio Distribution Play Icon

To manually start and stop Audio Distribution:

1. If not already on your dashboard, select **Dashboard** from the navigation bar.
2. Select the **Play** icon next to the Audio Distribution that you want to start.
3. If a non-blank **Audio Distribution Password** has been configured (see *Table 23, "Edit System Parameters Page," on page 69*), a keypad will be displayed and an audio prompt will request either the audio distribution password value or a confirmation (i.e., the digit 1).
4. The selected audio distribution will start.
5. To end the playing of audio, select the **Stop** icon next to the playlist.
6. If a non-blank **Audio Distribution Password** has been configured (see *Table 23, "Edit System Parameters Page," on page 69*), a keypad will be displayed and an audio prompt will request either the audio distribution password value or a confirmation (i.e., the digit 1).
7. The selected audio distribution will stop.

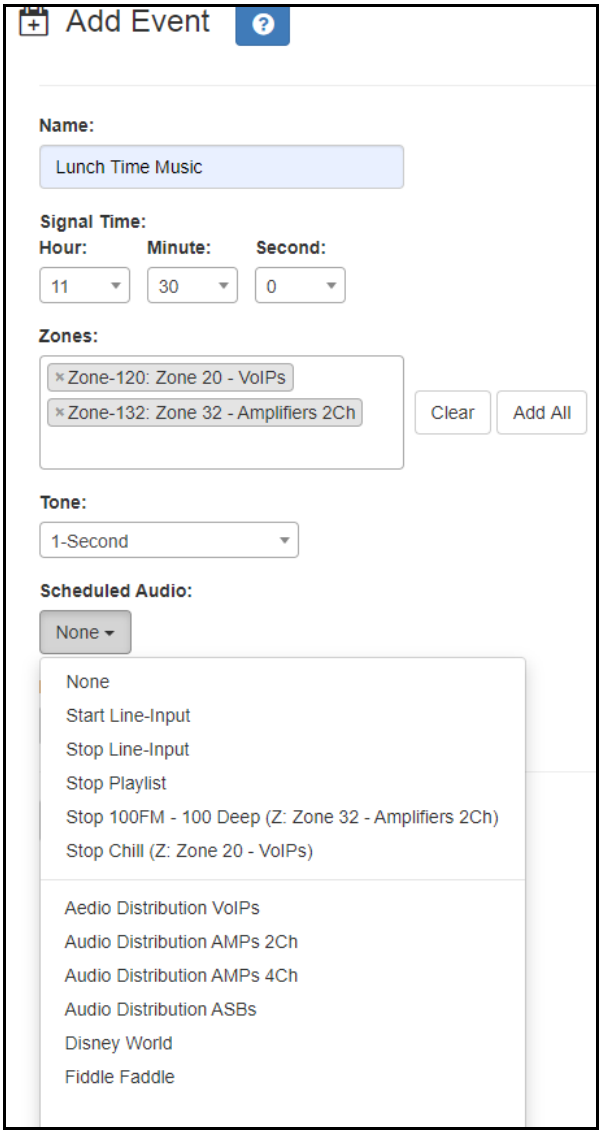


Figure 129. Adding Scheduled Audio

To automatically schedule audio as part of an event, follow the steps for creating an event, ensuring that you set the **Scheduled Audio** for the playlist, Matrix Mixer Pre-Amp channel, or amplifier to be used for this event. For more information, see *"Adding an Event" on page 270*.

You also can select to stop the **Scheduled Audio** by selecting **Stop Playlist** or **Stop Line-Input**.

If an airable/SoundMachine source is selected, the Scheduled Audio list includes selections to start or stop the audio stream. This list only includes airable/SoundMachine selections that apply to the specific zone. If the Audio Distribution zone selected includes a time zone and another zone type, such as Paging, that is not for time, the audio distribution does not appear in this **Scheduled Audio** list.

Automatically Starting a Routine When Audio Distribution is Started

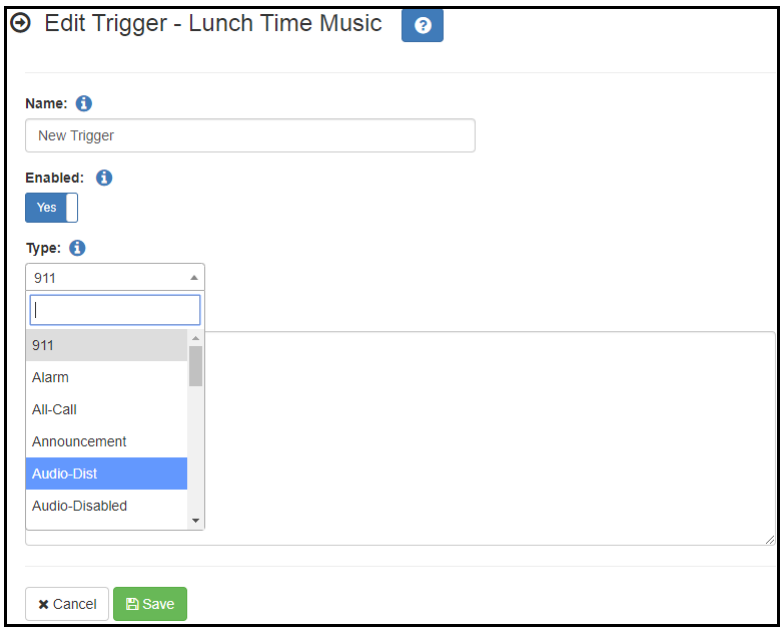


Figure 130. Adding Audio-Dist Trigger

The Routines feature lets you automatically start one or more actions using Audio Distribution (Audio-Dist) as a trigger. For example, maybe you want a bell or tone to sound in the kitchen when the lunch-time music begins, alerting kitchen staff that orders will soon be coming. To do this, you can create a routine, add an **Audio-Dist** trigger **Type**, and then create an action that plays a tone. See *"Adding a Routine" on page 450* for more information about creating a routine.

Using Routines to Start Audio Distribution

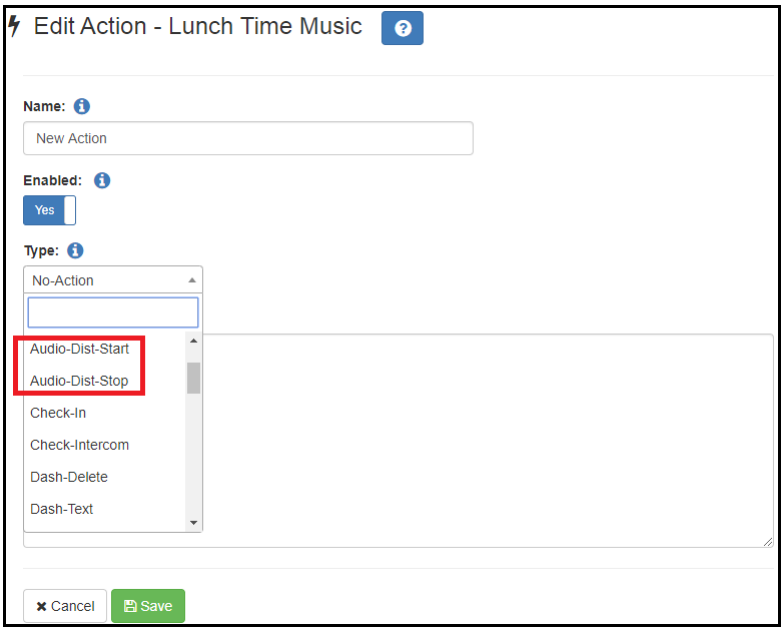


Figure 131. Audio Distribution Actions

You can create a routine that uses an action of either **Audio-Dist-Start** to start audio distribution or **Audio-Dist-Stop** to stop audio distribution.

You can also allow third-party systems, such as access control systems, to start a routine via I/O Controller Input Contact closure, or you can remotely start a routine using the Routines API.

For more information about using routines, see *"Using Routines" on page 425*.

Other Features and Audio Distribution

Audio Distribution will be paused automatically by higher priority feature activation (for example, All-Call Page, Paging, Tones) and will automatically resume when the higher priority feature is finished.

Audio Distribution volume to all speakers can be changed by setting **Audio Distribution Cut Level (dB)**, available in **System Parameters**. The Audio Distribution volume to zones can be changed by setting **Audio Distribution Cut Level (dB)** in **Edit Zone** or using the Zone Control feature (see *"Zone Control: Volume and Audio Distribution Panel" on page 344*). For information about editing a zone, see *"Editing Zone Configuration" on page 219*.

All Nyquist stations are preprogrammed to receive Audio Distribution to All Stations. To disable Audio Distribution to a specific station, change **Multicast Audio Distribution** to **No** on the Edit Station page (see *"Editing Station Configuration Settings" on page 155*).

Any Admin web UI user may stop the Audio Distribution if his or her station has the **Audio Distribution** CoS Configuration parameter enabled.

Scheduled Audio has a higher priority than Audio Distribution. If you are playing Audio Distribution and an event with Scheduled Audio interrupts, the Audio Distribution briefly plays between the tone and the Scheduled Audio.

A playlist will continue playing until manually stopped.

Audio Distribution Status

When you start Audio Distribution, a popup window appears letting you know that Audio Distribution was enabled.

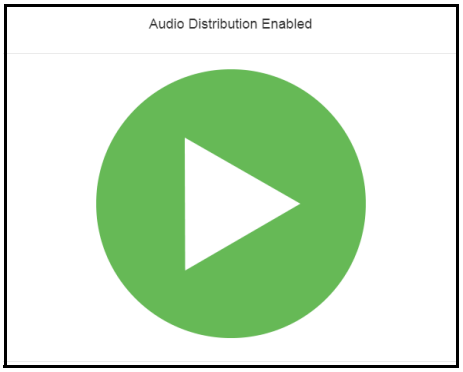


Figure 132. Audio Distribution Enabled

A popup window also appears when you stop Audio Distribution.

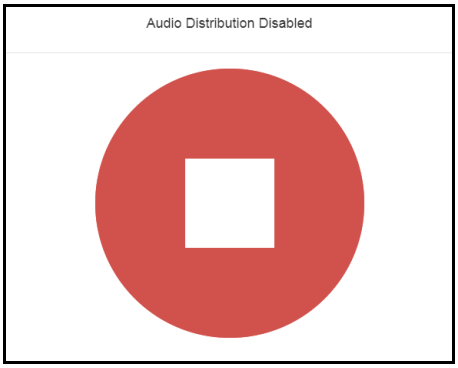


Figure 133. Audio Distribution Disabled

When Audio Distribution is enabled, an informational message appears in the Messages window of the Admin Web UI dashboard, indicating the song that is currently playing and to which speakers (all or selected) and to which zones audio is playing.

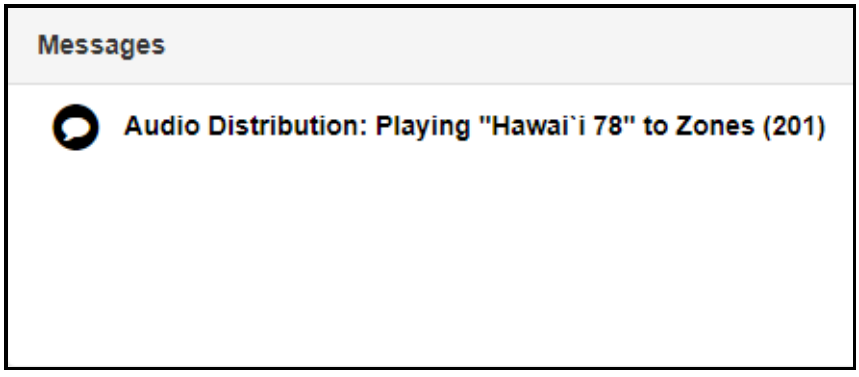


Figure 134. Audio Distribution Status

In the **Audio Distribution** section of the dashboard, the **Stop** icon will be displayed next to an audio distribution that is playing. Selecting the **Stop** icon will stop the audio distribution.

In the **Audio Distribution** menu of NQ-T1100 and NQ-ZPMS Admin phones, audio distributions that are currently playing are prefixed with "(P)" to indicate that the audio distribution is playing.

Using the Admin Phone

If you are using a Nyquist NQ-T1100 or NQ-ZPMS VoIP Phone as an Admin Phone, you can start and stop a specified Audio Distribution or stop all Audio Distributions by selecting the phone's Audio Distribution menu.

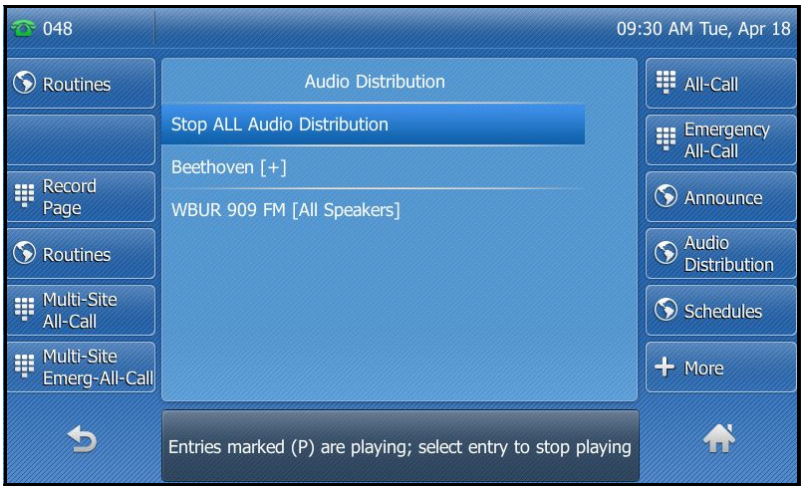


Figure 135. NQ-T1100 Admin Phone Audio Distribution Display

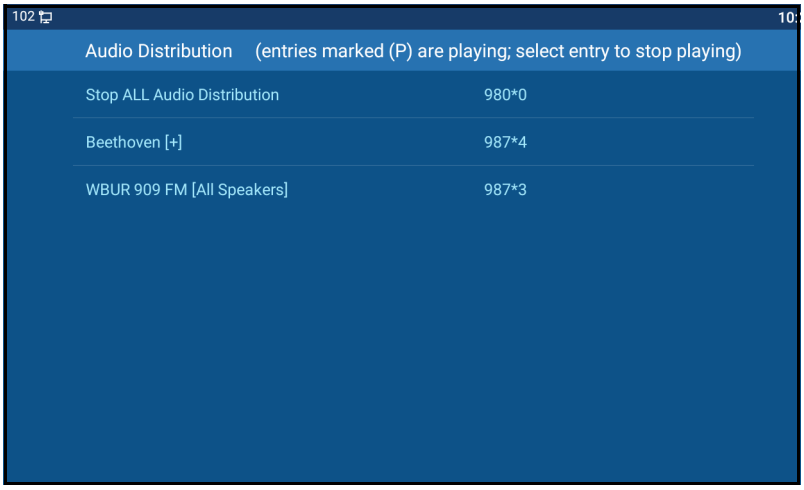


Figure 136. NQ-ZPMS Admin Phone Audio Distribution Display

For more information, refer to the Nyquist NQ-T1100 or NQ-ZPMS's Admin Phone User Guide.

Using Announcements

Announcements are prerecorded audio files that can be scheduled to play during specific times and in specific zones, played manually via the dashboard or DTMF codes, or played via routine actions.

Announcements can be either normal announcements, such as prerecorded announcements about upcoming site events, or emergency announcements, such as prerecorded shelter-in-place announcements that can be played during such events as tornado warnings or active shooter scenarios.

Note: Permissions to edit or delete announcements are granted separately for Emergency Announcements versus Normal Announcements. For example, some users may need to modify daily announcements, but not emergency announcements. For details on modifying permissions for a role, see *"Assigning and Editing Permissions" on page 248*.

Announcements can also precede a page.

Through the Nyquist web-based UI, you can add, edit, delete, and play announcements.

Announcements, Facilities, Zones, and Priorities

You can select to play an announcement to a zone, to all speakers, or to one or more facilities. The Nyquist system also supports the simultaneous playing of multiple announcements to different zones.

However, there are some set rules and priorities that govern how and when announcements play. For example, announcements played via an I/O controller can be played to a selected zone but not to **All Speakers**.

When you attempt to play a non-emergency, or **Normal**, announcement to a zone, you will receive a busy signal if any of the following are true:

- An announcement, page, or recorded page is being played on the zone.
- An announcement is being played to **All Speakers**.
- An Alarm, Tone, All-Call, or Emergency All-Call is being played.

A **Normal** announcement plays to **All Speakers** only if all zones are idle and no higher level audio is playing. You will receive a busy signal if any of the following are true:

- A **Normal** or **Emergency** announcement is already playing to **All Speakers**.
- An announcement is already playing to a zone.
- A page or queued page is already playing to a zone.
- An Emergency-All-Call, All-Call, Alarm, or Tone is already playing.

If you attempt to play an emergency announcement to a zone or to **All Speakers**, you will receive a busy signal if any of the following are true:

- An emergency announcement is already playing to the zone or to **All Speakers**.
- An Emergency All-Call is already playing.

If you attempt to play an emergency announcement to a zone or to **All Speakers** that is already playing a non-emergency announcement, an alarm or tone, a page or queued page, or an All-Call, the emergency announcement takes priority. A currently playing non-emergency announcement, alarm or tone, page or queued page, or All-Call will stop playing.

An **Emergency** announcement can be played on a zone while a Normal announcement plays on a different zone. Multiple **Emergency** and **Normal** announcements can be played to different zones (but not to **All Speakers**).

Scheduled Announcement Rules

Scheduled announcements follow slightly different rules. When you schedule an announcement, you can set the Maximum Wait Seconds parameter to indicate how many seconds to wait for an active page or announcement to finish before giving up.

For example, if the Maximum Wait Seconds is set to 120 seconds, when the system attempts to play the announcement at the scheduled time, if a page or announcement is already actively using the Zone, the scheduled announcement will wait up to 120 seconds for the Zone to become idle. If the Zone becomes idle in less than 120 seconds, the system will play the announcement. If the Zone is still busy after 120 seconds, the scheduled announcement will not play.

Facility Announcement Priorities

When making announcements to remote facilities, there is the possibility that one or more facilities may be unable to make the announcement due to higher priority features that are currently executing at that facility.

When you attempt to play a non-emergency, or **Normal**, announcement to remote facilities, you will receive a busy signal for any of the following scenarios.

- The local facility is targeted and it is executing a higher priority feature.
- Only one remote facility is targeted and it is executing a higher priority feature.

For all other scenarios, you will hear “Announcement on” and any facilities that were unable to play the announcement will record a busy status in the Call Details Record. This implies that when the local facility and one or more remote facilities are targeted, the busy signal and “Announcement on” indicators reflect the status of the local facility only; the announcement may or may not have played at the remote facilities.

Setting Up Facility Announcements

For announcements that will be played across remote facilities, ensure that the announcement has been added to each remote facility and that each has the same DTMF Code.

Because remote facility announcements cannot be stopped the same way as local announcements, announcements configured for continuous play (i.e., “Times to Play” property equal to zero) should not be used as facility announcements.

Tip: If you wish to play an announcement continuously on the local facility, yet use the same announcement remotely via Facility Announcements, configure two versions of the announcement at each facility: one for continuous play (i.e., "Times to Play" equals zero) and one for non-continuous play (i.e., "Times to Play" is non-zero). Ensure the DTMF code for the non-continuous announcements have the same value at each facility. Only the non-continuous version of the announcement will be displayed for play to remote facilities.

Recording Announcements

To record an announcement:

1. If not already on your dashboard, select **Dashboard** from the navigation bar.
2. Select the **Dial Pad** icon.
3. Dial *990 and press **Send**.
4. Follow the voice prompts to record your announcement.

Alternatively, the NQ-T1100 Admin Phone can be used by selecting **Record Announcement** in the phone's **Announce** menu, or the NQ-ZPMS Admin Phone can be used by selecting **Record Announcement** in the phone's **Announcements** menu.

After you finish recording an announcement, you can use the Announcements page to update the new announcement's name, DTMF code, and other parameters.

Note: When you record an announcement by dialing *990 or by selecting **Record Announcement** on the Admin phone's **Announce** menu, the initial DTMF code for the recorded and saved announcement will be set to the announcement's row ID. You can change the DTMF code after the announcement is saved by editing the announcement in the web interface **Announcements** view.

The saved announcement has **Play to Zone** set to blank (no zone selected). This means that when you play an announcement via an IP phone **Announcement** menu selection, you will be asked to enter a zone number (where 0 = All Speakers). You can define a permanent zone number for the saved announcement by updating **Play to Zone** after the recorded announcement has been saved.

Adding an Announcement

You can upload an announcement, which can be an audio recording, such as a message or tone. The announcement can be scheduled to play at certain times and in certain zones.

Through the Add Announcement page, you can also enter text to be converted into speech, provided you have the feature license that allows this option.

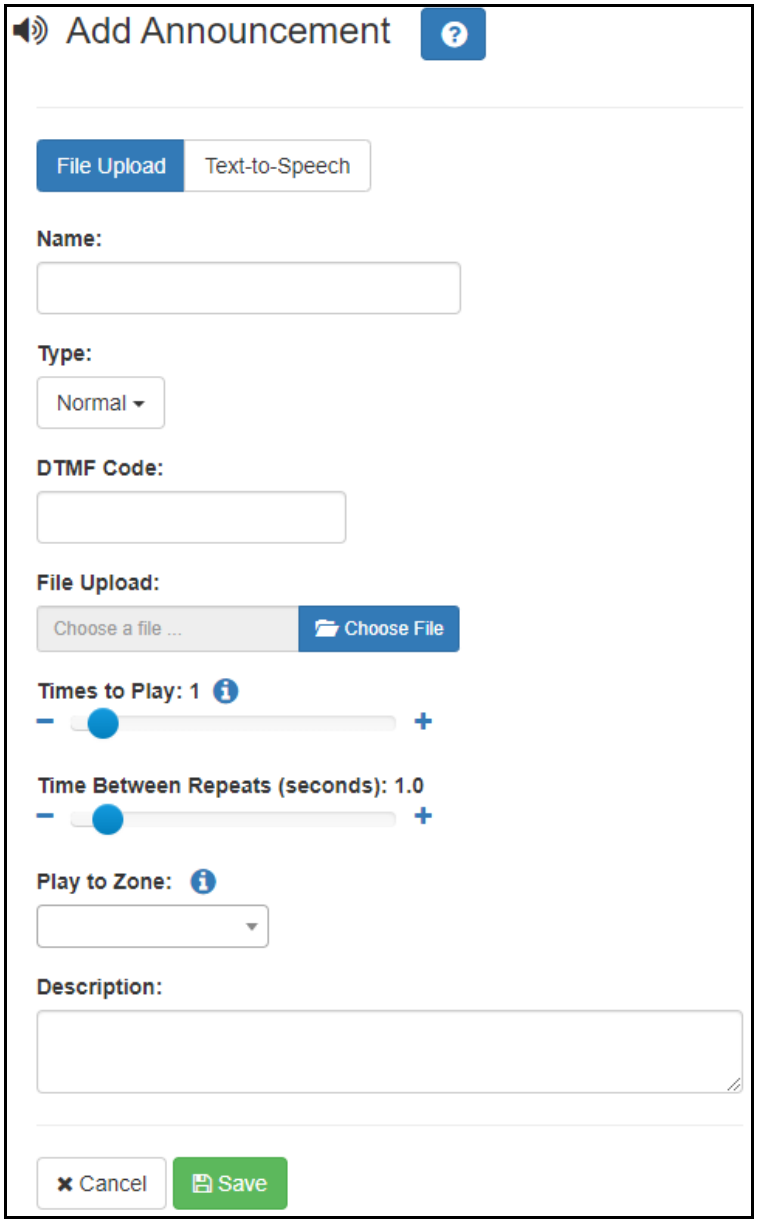


Figure 137. Add Announcement Page

To upload an announcement file:

1. On the navigation bar, expand **Audio**.
2. Select **Announcements**.
3. On the Announcements page, select the **Add** icon.
4. Complete the parameters on the Add Announcement page. (See *Table 103, "Add Announcement Page Parameters," on page 324*.)
5. Select **Save**.

Table 103. Add Announcement Page Parameters

File Upload / Text-to-Speech	Select whether this announcement will play an audio clip or use Text-to-Speech to convert the specified text into speech.
Name	Provide a name for the announcement. *Note:* Valid characters include uppercase letters (A–Z), lowercase letters (a–z), numerals (0–9), space, and the following special characters: ! @ $ * ? - . , .
Type	Use the drop-down menu to select if the announcement is Normal or Emergency.
DTMF Code	Provide a DTMF code for this announcement to use when manually starting the announcement from an Admin Phone. The number can have from 1 to 10 digits. You cannot assign the same DTMF code to multiple announcements. *Note:* When you record an announcement by dialing *990 or by selecting **Record Announcement** on the Admin phone's **Announce** menu, the initial DTMF Code for the recorded and saved announcement will be set to the announcement's row ID. You can change the DTMF Code after the announcement is saved by editing the announcement in the web interface **Announcements** view. *Note:* The saved announcement has **Play to Zone** set to blank (no zone selected). This means that when you play an announcement via an IP phone **Announcement** menu selection, you will be asked to enter a zone number (where 0 = All Speakers). You can define a permanent zone number for the saved announcement by updating **Play to Zone** after the recorded announcement has been saved.
File Upload	Select **Choose File**, navigate to the audio file for this announcement, and then select the file. Nyquist supports both WAV and MP3 file formats. *Note:* This option appears only if you have selected the **File Upload** tab.
Times to Play	Select the number of times the announcement will play. Parameters are between 0 and 10. *Note:* A setting of 0 results in the playing continuously until it is manually stopped via the dashboard or a Stop-Announcement routine action. *Note:* Announcements configured for continuous playback should not be used with the Facility Announcement feature.
Time Between Repeats (seconds)	Select the time in seconds between replaying of the announcement. You can select between 0.5 and 5.0 in 0.5 increments.
Text-To-Speech	Type the text that you want converted to speech for this announcement. Ensure that the **File Upload** parameter is blank. The system will generate a .wav file. *Note:* This option only appears if **Text-to-Speech** is selected and you have the Text-To-Speech feature license.

Table 103. Add Announcement Page Parameters (continued)

Play to Zone	Select either **All Speakers** or a specific zone for this announcement to play. *Note:* If the **Station Type** for the station is set to **Admin Web Interface**, **Admin Phone**, **IP Phone**, **Analog Phone**, or **Mobile Device** and an **Announcement Zone** was set for the station, the **Announcement Zone** overrides the **Play to Zone**.
Description	Provide a description of the announcement. *Note:* Valid characters include uppercase letters (A–Z), lowercase letters (a–z), numerals (0–9), space, and the following special characters: ! @ $ * ? - . , .

Using SSML for Text-to-Speech Entries

You can use Speech Synthesis Markup Language (SSML), an XML-based markup language for speech synthesis applications, when typing text that you want converted to speech for announcements. You can use SSML formatting to insert pauses, adjust speech rate, adjust voice pitch, adjust output volume, add emphasis to speech, or spell words phonetically. The following table provides examples of SSML formats that can be used when adding announcements.

Table 104. SSML Formats for Text-to-Speech Entries

Insert Silence/Pauses	• This is not <break strength='none' /> a pause. • This is a <break strength='x-weak' /> phrase break. • This is a <break strength='weak' /> phrase break. • This is a <break strength='medium' /> sentence break. • This is a <break strength='strong' /> paragraph break. • This is a <break strength='x-strong' /> paragraph break. • This is a <break time='3s' /> three second pause. • This is a <break time='4500ms' /> 4.5 second pause. • This is a <break /> sentence break.
Adjust Speech Rate	• I am now <prosody rate='x-slow'>speaking at half speed.</prosody> • I am now <prosody rate='slow'>speaking at 2/3 speed.</prosody> • I am now <prosody rate='medium'>speaking at normal speed.</prosody> • I am now <prosody rate='fast'>speaking 33% faster.</prosody> • I am now <prosody rate='x-fast'>speaking twice as fast</prosody> • I am now <prosody rate='default'>speaking at normal speed.</prosody> • I am now <prosody rate='.42'>speaking at 42% of normal speed.</prosody> • I am now <prosody rate='2.8'>speaking 2.8 times as fast</prosody> • I am now <prosody rate='-0.3'>speaking 30% more slowly.</prosody> • I am now <prosody rate='+0.3'>speaking 30% faster.</prosody>

Table 104. SSML Formats for Text-to-Speech Entries (continued)

Adjust Voice Pitch	• <prosody pitch='x-low'>This is half-pitch</prosody> • <prosody pitch='low'>This is 3/4 pitch.</prosody> • <prosody pitch='medium'>This is normal pitch.</prosody> • <prosody pitch='high'>This is twice as high.</prosody> • <prosody pitch='x-high'>This is three times as high.</prosody> • <prosody pitch='default'>This is normal pitch.</prosody> <prosody pitch='-50%'>This is 50% lower.</prosody> • <prosody pitch='+50%'>This is 50% higher.</prosody> • <prosody pitch='-6st'>This is six semitones lower.</prosody> • <prosody pitch='+6st'>This is six semitones higher.</prosody> • <prosody pitch='-25Hz'>This has a pitch mean 25 Hertz lower.</prosody> • <prosody pitch='+25Hz'>This has a pitch mean 25 Hertz higher.</prosody> • <prosody pitch='75Hz'>This has a pitch mean of 75 Hertz.</prosody>
Adjust Output Volume	• <prosody volume='silent'>This is silent.</prosody> • <prosody volume='x-soft'>This is 25% as loud.</prosody> • <prosody volume='soft'>This is 50% as loud.</prosody> • <prosody volume='medium'>This is the default volume.</prosody> • <prosody volume='loud'>This is 50% louder.</prosody> • <prosody volume='x-loud'>This is 100% louder.</prosody> • <prosody volume='default'>This is the default volume.</prosody> • <prosody volume='-33%'>This is 33% softer.</prosody> • <prosody volume='+33%'>This is 33% louder.</prosody> • <prosody volume='33%'>This is 33% louder.</prosody> • <prosody volume='33'>This is 33% of normal volume.</prosody>
Add Emphasis to Speech	• This is <emphasis level='strong'>stronger</emphasis> than the rest. • This is <emphasis level='moderate'>stronger</emphasis> than the rest. • This is <emphasis level='none'>the same as</emphasis> than the rest.
Spell Words Phonetically	You say <phoneme ph='t ah0 m ey1 t ow0'>tomato</phoneme>, I say <phoneme ph='t ah0 m aa1 t ow0'>tomato</phoneme>

Viewing Announcements

Through the Announcements page, you can view a list of all announcements that are available for scheduling, delete an announcement, and select to edit or add an announcement.

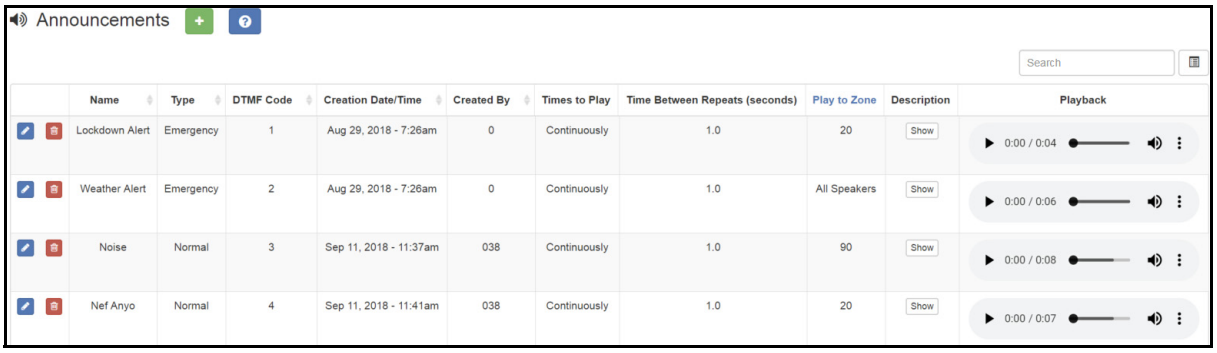


Figure 138. Announcements Page

To view a list of all announcements that are available for scheduling:

1. On the navigation bar, expand **Audio**.
2. Select **Announcements**.

The following parameters appear for each announcement file:

Table 105. Announcements Page Parameters

Schedule Announcements	Browses to the *Schedule Announcements* page (see *"Using the Schedule Announcements Feature" on page 278*).
Name	Displays the user-provided name of the announcement file. *Note:* Valid characters include uppercase letters (A–Z), lowercase letters (a–z), numerals (0–9), space, and the following special characters: **! @ $ * ? - . , .**
Type	Displays whether the announcement is a **Normal** or an **Emergency** announcement.
DTMF Code	Displays the DTMF code used to manually start the announcement via the dashboard Dial Pad or IP phone keypad.
Creation Date/Time	Displays when the announcement was created.
Created By	Displays the extension that is to be considered the source of the announcement for CoS considerations.
Times to Play	Displays the number of times the announcement will play. This number can range from 0 through 10. *Note:* A setting of 0 results in the announcement playing continuously until it is manually stopped via the dashboard. *Note:* Announcements configured for continuous playback should not be used with the Facility Announcement feature.

Table 105. Announcements Page Parameters

Times Between Repeats (seconds)	Displays the time in seconds before replaying the announcement.
Play to Zone	Displays either **All Speakers** or a specific zone for this announcement to play. *Note:* If the **Station Type** for the station is set to **Admin Web Interface**, **Admin Phone**, **IP Phone**, **Analog Phone**, or **Mobile Device** and an **Announcement Zone** was set for the station, the **Announcement Zone** overrides the **Play to Zone**.
Description	Provides a description of the announcement. *Note:* Valid characters include uppercase letters (A–Z), lowercase letters (a–z), numerals (0–9), space, and the following special characters: **! @ $ * ? - . ,** .
Playback	Allows you to preview the announcement. Selecting the **Menu** icon also allows you to download and save the announcement or adjust the pre-view playback speed.

Editing Announcements

From the Edit Announcement page, you can edit an audio file's parameters such as times to play.

To edit an announcement:

1. On the navigation bar, expand **Audio**.
2. Select **Announcements**.
3. On the *Announcements* page, select the **Edit** icon next to the announcement that you want to edit.
4. Make the desired changes (see *Table 106 on page 329*).
5. Select **Save**.

Table 106. Edit Announcement Page Parameters

Name	Displays the user-provided name of the announcement file. *Note:* Valid characters include uppercase letters (A–Z), lowercase letters (a–z), numerals (0–9), space, and the following special characters: **! @ $ * ? - . ,** .
Type	Indicates if the announcement is a **Normal** or an **Emergency** announcement.

Table 106. Edit Announcement Page Parameters (continued)

DTMF Code	DTMF code for this announcement to use when manually starting the announcement from an Admin Phone. The number can have from 1 to 10 digits. You cannot assign the same DTMF code to multiple announcements. *Note:* When you record an announcement by dialing *990 or by selecting **Record Announcement** on the Admin phone's **Announce** menu, the initial DTMF Code for the recorded and saved announcement will be set to the announcement's row ID. You can change the DTMF Code after the announcement is saved by editing the announcement in the web interface **Announcements** view. The saved announcement has **Play to Zone** set to blank (no zone selected). This means that when you play an announcement via an IP phone **Announcement** menu selection, you will be asked to enter a zone number (where 0 = All Speakers). You can define a permanent zone number for the saved announcement by updating **Play to Zone** after the recorded announcement has been saved.
Created By	Displays the number for the station used to create or download the announcement. *Note:* This field cannot be edited and only indicates which station created the announcement.
Times to Play	Select the number of times the announcement will play. Parameters are between 0 and 10. *Note:* A setting of 0 results in the playing continuously until it is manually stopped via the dashboard. *Note:* Announcements configured for continuous playback should not be used with the Facility Announcement feature.
Times Between Repeats (seconds)	Select the time in seconds between replaying of the announcement. You can select between 0.5 and 5.0 in 0.5 increments.
Play to Zone	Select either **All Speakers** or a specific zone for this announcement to play. You can leave this field blank if you want the Nyquist server to prompt for a zone number to use whenever an announcement is started from an IP phone. This will allow callers to direct the announcement to any zone desired at the time it is played. *Note:* If the **Station Type** for the station is set to **Admin Web Interface**, **Admin Phone**, **IP Phone**, **Analog Phone**, or **Mobile Device** and an **Announcement Zone** was set for the station, the **Announcement Zone** overrides the **Play to Zone**.
Description	Provides a description of the announcement. *Note:* Valid characters include uppercase letters (A–Z), lowercase letters (a–z), numerals (0–9), space, and the following special characters: **! @ $ * ? - . ,** .

Deleting an Announcement

Note: You cannot delete an announcement that is used in a routine with an **Announcement** action **Type** (see *"Understanding Action Parameters" on page 460*).

To delete an announcement that is associated with a schedule, you must delete the schedule announcement first and then delete the announcement. To delete the schedule announcement, see *"Using the Schedule Announcements Feature" on page 278*.

To delete an announcement:

1. On the navigation bar, expand **Audio**.
2. Select **Announcements**.
3. On the *Announcements* page, select the **Delete** icon next to the announcement that you want to delete.
4. When prompted, select **Delete**.

Creating Temporary Announcements from Routines

It is also possible to create and play an Announcement within a Routine. These announcements are known as Temporary Announcements because they are transient announcements that do not persist and are only usable within that Routine.

Creating a temporary announcement is quite simple. Within the Actions of a Routine, simply include three or more actions in the following sequence:

1. One **New-Announcement** action. This indicates the beginning of a temporary announcement.
2. One or more **Add-Announcement-Audio** actions. These actions specify the audio to be included in the announcement. Each one specifies one of the following Audio Source Types and the corresponding information:

Table 107. Add-Announcement-Audio audio sources

Announcement	Specifies a predefined Announcement (see *"Viewing Announcements" on page 328*).
Number	Specifies a number to be spoken. This includes whether to pronounce the number one digit at a time (e.g., a phone number) or as a number (e.g., a temperature) and whether or not to pronounce the fractional part of the number (i.e, to the right of the decimal point).
Text-to-Speech	Specifies the text to be spoken using text-to-speech (TTS) technology. This text can optionally include SSML formatting (see *"Using SSML for Text-to-Speech Entries" on page 325*).

3. One **Play-Announcement** action. This is the action that will actually pronounce the announcement.

4 To pronounce several announcements, the previous steps can be repeated multiple times within the same Routine.

For further details on these Announcement action types, see *Table 2, "Routine Action Type-Specific Parameters," on page 588*.

Managing Tones

Nyquist provides tones that can be used with events, such as schedules, or as audio indicators, such as alarms. You can use a provided tone, or you can upload an audio file, generate a customized tone, or use a line input channel as the tone source. White noise and pink noise tones are provided, which can be used to tune paging volumes for time-based zones. (See *"Tuning Volume with White or Pink Noise" on page 364*.)

Viewing Available Tones

Using the Tones page, you can view a list of available tones, delete user-provided tones, or select to add or edit a tone. You cannot delete a default tone, but you can prevent it from being viewed on the dashboard or on Admin Phones that have a tones/alarms menu; the hidden tone still appears on the Tones page.

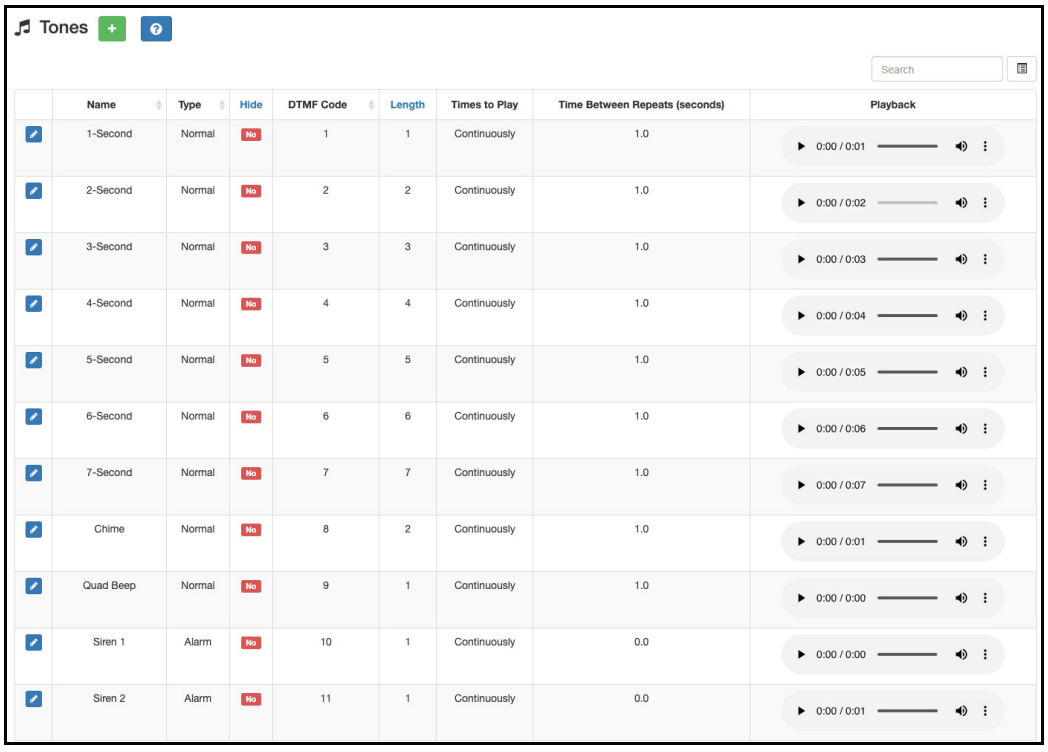


Figure 139. Tones Page

To view tones:

1 On the navigation bar, expand **Audio**.

2 Select **Tones**.

The following table describes the tones parameters that appear.

Table 108. Tones Page Parameters

Name	Provides a name for the announcement file. *Note:* Valid characters include uppercase letters (A–Z), lowercase letters (a–z), numerals (0–9), space, and the following special characters: **! @ $ * ? - . , .**
Type	Displays the tone type as **Normal** or **Alarm**.
Hide	Specifies if the tone should be hidden from the dashboard view or Admin Phone menu.
DTMF Code	Provides the DTMF code used when manually activating the tone via dashboard dial pad or IP phone keypad.
Length	Time in seconds that the tone plays.
Times to Play	Displays the number of times the tone plays. Parameters are 0 to 10. *Note:* A setting of zero (0) results in the tone playing continuously until it is manually stopped via the dashboard.
Time Between Repeats (seconds)	Displays the time in seconds before the tone is replayed. You can select between 0.5 and 5.0 in 0.5 increments.
Playback	Allows the user to manually play the tone. Selecting the **Menu** icon in this field displays the following options: • **Download** Download and save the tone. This option is only available if the tone was uploaded or generated (see *"Adding Tones" on page 333*). • **Playback speed** Adjust the playback speed during the manual playback.

Adding Tones

Nyquist provides three ways of adding a tone:

- Uploading a file that is located on your network, local computer, or removable media, such as a flash drive (see *"Uploading Tones" on page 334*).
- Generating a one-frequency tone that can be saved (see *"Generating Tones" on page 335*).
- Using a line-input channel from a two- or four-channel audio power amplifier or Matrix Mixer Pre-Amp which will provide a real-time tone (see *"Using Line Input for Tones" on page 338*).

In each scenario, you are adding a tone to your Nyquist system that can be used later via either a schedule (see *"Understanding Event Settings" on page 271*) or manual tone activation (see *"Managing Tones via the Dashboard" on page 389*).

Uploading Tones

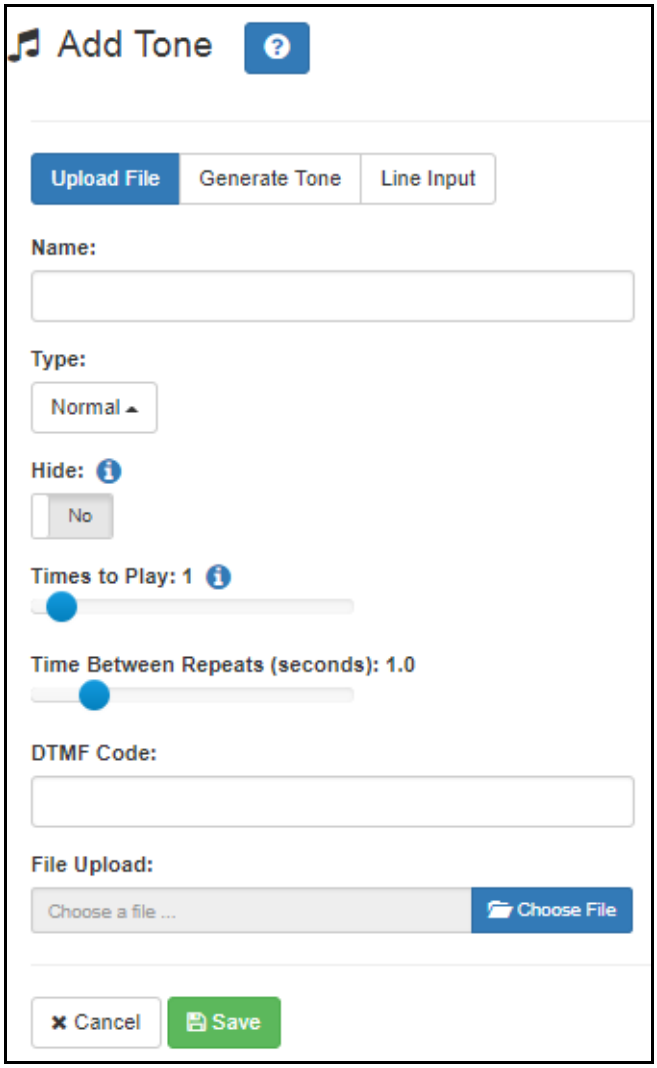


Figure 140. Add Tone – Upload File

To upload a tone:

1. On the navigation bar, expand **Audio**.
2. Select **Tones**.
3. On the *Tones* page, select the **Add** icon.
4. On the *Add Tone* page, ensure **Upload File** is selected.
5. Complete the parameters (see *Table 109*).
6. Select **Save**.

Table 109. Add Tone Page Parameters (Upload)

Name	Provide a name for this tone. *Note:* Valid characters include uppercase letters (A–Z), lowercase letters (a–z), numerals (0–9), space, and the following special characters: **! @ $ * ? - . ,** .
Type	Use the drop-down menu to select if the tone is **Normal** or **Alarm**.
Hide	Specify if the tone is to be hidden or displayed on the dashboard view.
Times to Play	Select the number of times the tone will play. Parameters are 0 through 10. *Note:* A setting of 0 results in the tone playing continuously until it is manually stopped via the dashboard.
Time Between Repeats (Seconds)	Select the time in seconds between replaying of the tone. You can select between 0.5 and 5.0 in 0.5 increments.
DTMF Code	Provide the DTMF code used when manually activating the tone via dashboard dial pad or IP phone keypad.
File Upload	Select **Choose File**, navigate to the audio file, and then select the file.

Generating Tones

Generating a one-frequency tone is another way to add a tone if you do not want to use the default tones or upload a tone from a network or removable media location.

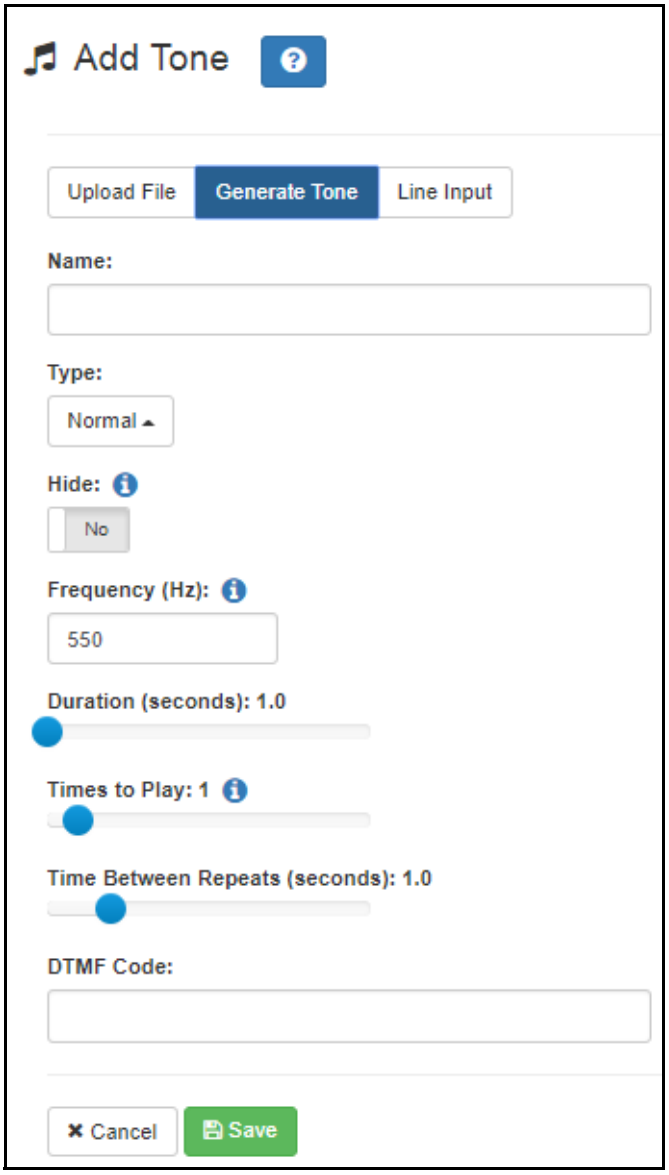


Figure 141. Add Tone – Generate Tone

To generate a tone:

1. On the navigation bar, expand **Audio**.
2. Select **Tones**.
3. On the *Tones* page, select the **Add** icon.
4. On the *Add Tone* page, select **Generate Tone**.
5. Complete the parameters (see *Table 110*).
6. Select **Save**.

Table 110. Add Tone Page Parameters (Generate)

Name	Provide a name for this tone. *Note:* Valid characters include uppercase letters (A–Z), lowercase letters (a–z), numerals (0–9), space, and the following special characters: **! @ $ * ? - . ,** .
Type	Select if the announcement to follow is a normal or an emergency announcement.
Hide	Specify if the tone is to be hidden or displayed on the dashboard view.
Frequency (Hz)	Enter the frequency for the tone. You can select a frequency from 300 to 2000 Hz.
Duration (seconds)	Enter the time in seconds that the tone is to play.
Times to Play	Select the number of times the file will play. Parameters are 0 through 10. *Note:* A setting of 0 results in the file playing continuously until it is manually stopped via the dashboard.
Time Between Repeats (seconds)	Select the time in seconds between replaying of the file. You can select between 0.5 and 5.0 in 0.5 increments.
DTMF Code	Provide the DTMF code used when manually activating the tone via dashboard dial pad or IP phone keypad.

Using Line Input for Tones

Selecting Line Input from the Add Tone page allows you to select a two- or four-channel audio power amplifier channel or Matrix Mixer Pre-Amp channel to use as a real-time source for a tone.

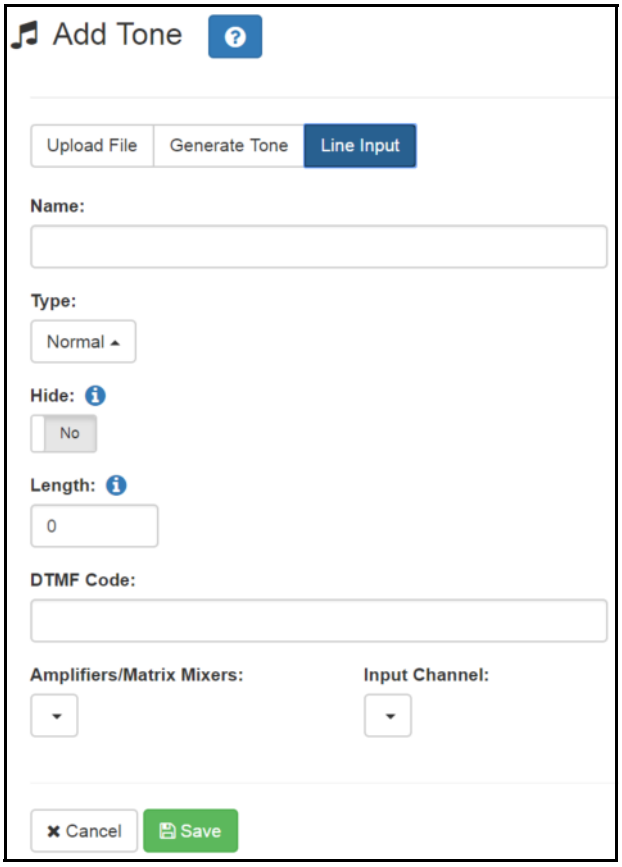


Figure 142. Add Tone – Line Input

To add a line input tone:

1. On the navigation bar, expand **Audio**.
2. Select **Tones**.
3. On the *Tones* page, select the **Add** icon.
4. On the *Add Tone* page, select **Line Input**.
5. Complete the parameters (see *Table 111 on page 339*).
6. Select **Save**.

Table 111. Add Tone Page Parameters (Line Input)

Name	Provide a name for this tone. *Note:* Valid characters include uppercase letters (A–Z), lowercase letters (a–z), numerals (0–9), space, and the following special characters: **! @ $ * ? - . ,** .
Type	Select if the announcement to follow is a normal or an emergency announcement.
Hide	Specify if the tone is to be hidden or displayed on the dashboard view.
Length	Enter the number of seconds for the tone to play. The length can range from 0 to 999999. *Note:* A setting of 0 results in the file playing continuously until it is manually stopped via the dashboard.
DTMF Code	Provide the DTMF code used when manually activating the tone via dashboard dial pad or IP phone keypad.
Amplifiers/Matrix Mixers	Use the drop-down menu to select the two- or four-channel audio power amplifier or Matrix Mixer Pre-Amp and its associated station number.
Input Channel	Specify the matrix channel being used for input.

Editing Tones

You can edit parameters of existing tones, but which parameters can be changed depends on whether the tone is a default tone or a user-added tone. For example, you cannot change the **Name** for a default tone, but you can change that parameter for a tone that you added. Some parameters appear only for Line Input tones. You also cannot change the **Type** of a tone if it is used in a routine (see *"Understanding Trigger Parameters" on page 456* and *"Understanding Action Parameters" on page 460*).

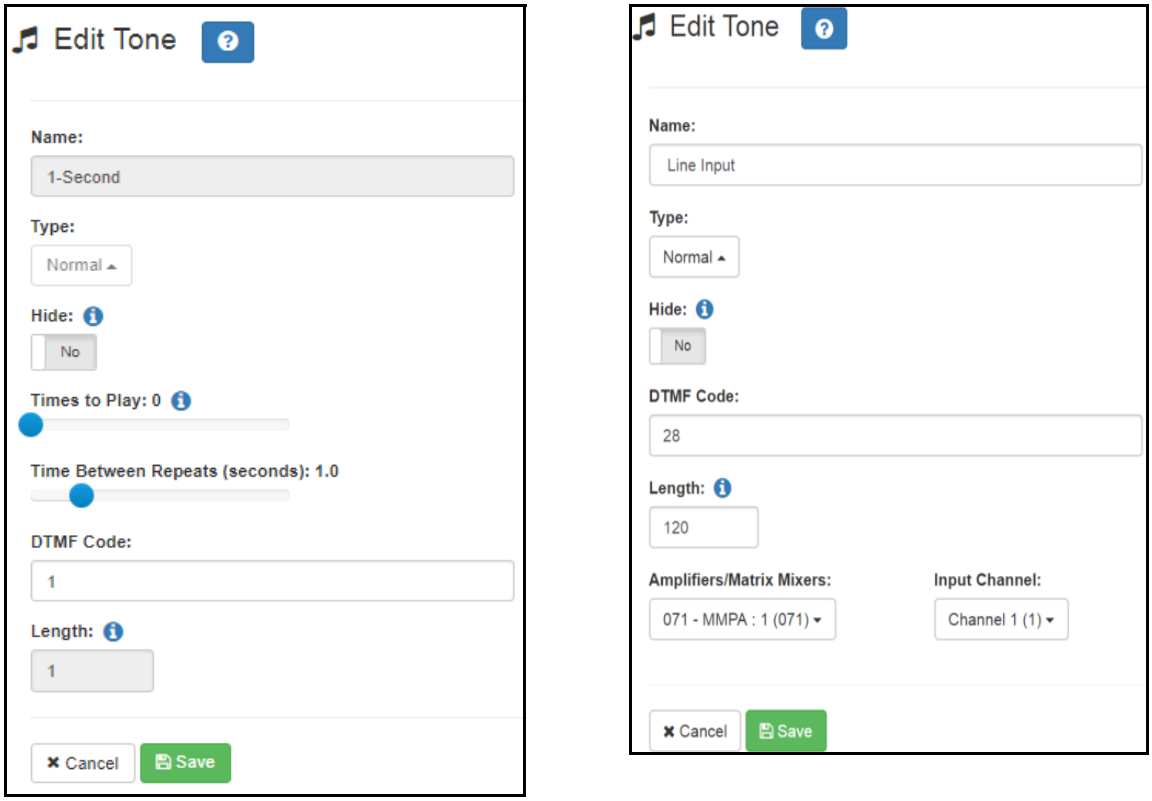


Figure 143. Edit Tone Pages

To edit a tone:

1. On the navigation bar, expand **Audio**.
2. Select **Tones**.
3. On the *Tones* page, select the **Edit** icon.
4. On the *Edit Tone* page, make changes to the parameters (see *Table 112 on page 340*).
5. After completing all changes, select **Save**.

Table 112. Edit Tone Page Parameters

Name	Displays the name for this tone. *Note:* This parameter cannot be changed for default system Tones. *Note:* Valid characters include uppercase letters (A–Z), lowercase letters (a–z), numerals (0–9), space, and the following special characters: **! @ $ * ? - . , .**
Type	Use the drop-down menu to select if the tone is Normal or Alarm.
Hide	Specifies if the tone is to be hidden from the dashboard view.

Table 112. Edit Tone Page Parameters (continued)

Times to Play	Displays the number of times the tone will play. Parameters are 0 through 10. *Note:* A setting of 0 results in the tone playing continuously until it is manually stopped via the dashboard. This parameter does not appear for Line Input tones.
Time Between Repeats (second)	Displays the time in seconds between replaying of the tone. You can select between 0.5 and 5.0 in 0.5 increments. *Note:* This parameter does not appear for Line Input tones.
DTMF Code	Provides the DTMF code used when manually activating the tone via dashboard dial pad or IP phone keypad.
Length	Provides the length of the tone. *Note:* This parameter cannot be changed except for Line Input tones.
File Upload	Select **Choose File**, navigate to the audio file, and then select the file if you want to choose a new file. *Note:* This parameter appears only for user-provided tones but not for Line Input tones.
Amplifiers/Matrix Mixers	Specifies the two-channel or four-channel audio power amplifier or Matrix Mixer Pre-Amp and its associated station number. *Note:* This parameter appears only for Line Input tones.
Input Channel	Specifies the matrix channel being used for input. *Note:* This parameter appears only for Line Input tones.

Deleting a Tone

Important: You cannot delete a tone that is used in a routine with a **Tone** action **Type** or if the tone is used as an alarm in an **Alarm** action **Type** (see *"Understanding Action Parameters" on page 460*).

You can only delete user-added tones.

To delete a tone:

1. On the navigation bar, expand **Audio**.
2. Select **Tones.**
3. On the *Tones* page, select the **Delete** icon next to the tone that you want to delete.
4. When prompted, select **Delete**.

Tone Operational Notes and Limitations

- The system supports playing multiple simultaneous tones, assuming the tones are playing to different zones. If a manual request to play a tone is made while a tone is playing to all Time–type zones, the requester will receive a busy signal and the tone will not be played.

- If a specific zone is not specified, the tone will play to all Time–type zones. In this case, if a queued page is playing in a Time–type zone, the queued page will be stopped and re-queued.
- If a specific zone is specified, the tone will play to the specified zone. In this case, if a queued page is playing in the specified zone, the queued page will be stopped and re-queued. If queued pages are playing in time type zones not equal to the specified zone, those queued pages will continue to play, along with the manual tone to the specified zone.
- If a specific zone is specified, the dashboard message will use the following format:

  Tone (<station_extension> -> <zone_name>): <tone_name>

  For example:

  Tone (100 -> Library): Chime
- Routine triggers that use the Tone or Scheduled-Tone trigger types do not include a zone filter, thus tone-based routine triggers are activated whenever a tone is played to any zone. The routine trigger does include a filter for the tone being played, so you can filter routine execution by the tone being played.

Managing Recordings

If your Nyquist systems allow call recording, and one or more stations have been configured for recording telephone calls, then you can manage these recordings through Nyquist's audio file management feature.

For more information about configuring Nyquist for call recording, see *"Using the Edit System Parameters Page" on page 67*. For information about configuring a station for call recording, see *Table 43, "View, Add, or Edit Station Configuration Parameters," on page 143*.

Through the audio file management feature, you can play back an individual call, delete selected recordings, or delete all recordings.

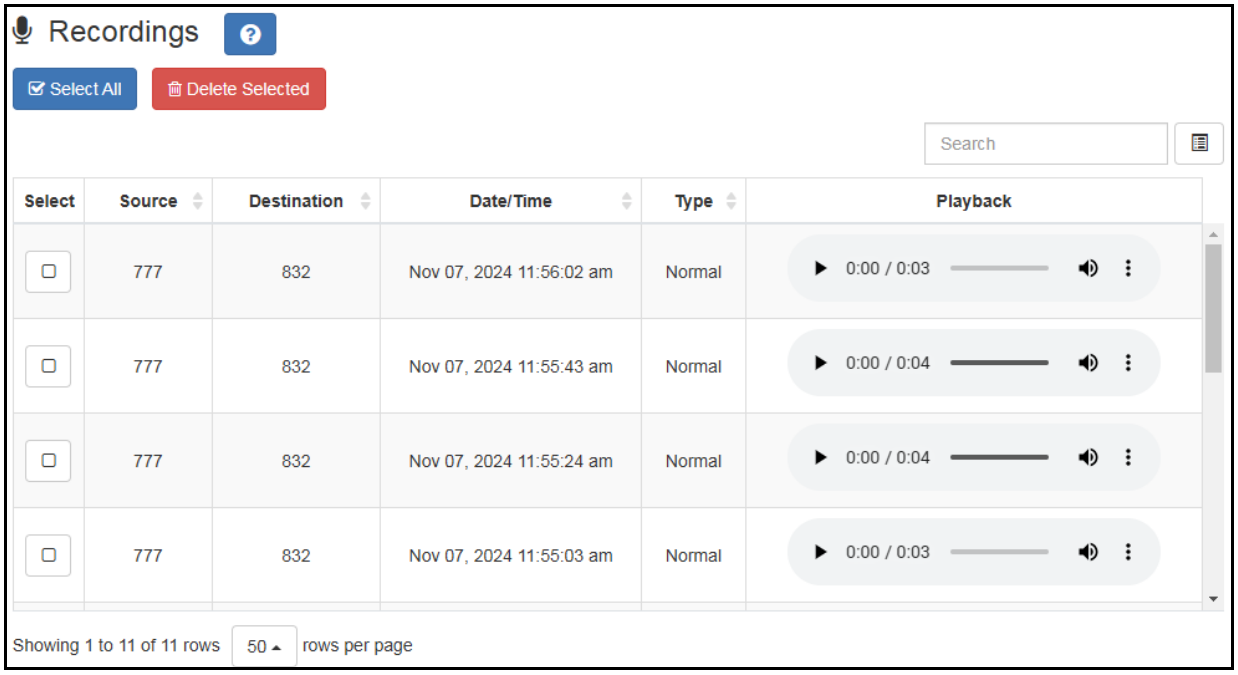


Figure 144. Recordings Page

To manage recordings:

1. On the navigation bar, expand **Audio**.
2. Select **Recordings**.
3. To play back a call, select the **Play** button in the Playback column for the call that you want to hear.
4. To delete a selected call or multiple calls, select the check box in the **Select** column for each call that you want to delete, and then select **Delete Selected**.
5. To delete all calls, select **Select All**, and then select **Delete Selected**.

The Recordings page provides the following information for recorded calls:

Table 113. Recordings Page Parameters

Select	Allows you to use the check box to select a call for deletion.
Source	Identifies the extension or number that placed the call.
Destination	Identifies the extension that received the call.
Date/Time	Identifies the date and time that the call was received.
Type	Identifies the type of call, such as Normal.
Playback	Allows you to play the recording.

Zone Control: Volume and Audio Distribution Panel

The Zone Control feature presents a simple user interface for controlling volume and audio distributions from any device that supports the Google Chrome, Microsoft Edge, or Apple Safari browser. Small devices such as touch-screen tablets can be used to operate Zone Control via the browser.

The Zone Control feature can be used to perform the following:

- Change volume of Audio Distributions and Paging Zones
- Start and stop Audio Distributions

In addition, it has its own configuration settings view. It has two display page views:

- Settings / Zone Filter view (see *Figure 145, "Zone Control Settings and Zone Filter View," on page 345*)
- Zone View, including an Audio Distribution view (see *Figure 146, "Zone Control Zone View," on page 347*).

Initial Setup and Settings

The Zone Control feature does not use the same login model as the Nyquist application. All users share the same password, specified as Zone Control Password in the System Parameters Page (see *Figure 27, "Edit Systems Parameters Page," on page 68*). The first time a user logs in, they will be directed to the Settings page for initial setup.

To perform the initial user setup:

1. Using a Chrome, Edge, or Safari web browser, enter:

   `https://<server>/zone-control/login`

   where `<server>` is replaced with the IP Address of your Nyquist server.

2. Enter a new username that has not previously been used.

Tip: The username can correspond to an actual user, but if the Zone Control view is to be shared by multiple users, it could correspond to a group, or even a location (e.g., Lobby, Studio3, Library, etc.).

---

3. Enter the Zone Control Password (see *Figure 27, "Edit Systems Parameters Page," on page 68*).

Note: This password is intended to secure the feature in general, and is used by all Zone Control users. Be sure to use a password that can be safely shared with anyone that is to use the Zone Control feature.

---

4. You are then presented with the Zone Control Settings and Zone Filter view (see *Figure 145, "Zone Control Settings and Zone Filter View," on page 345*).
5. Select the desired settings, as described in *Figure 114, "Zone Control Settings," on page 346*.
6. Use the Zone Filters to select the zones that you wish to display on the Zone View. The Zone Filter section displays a list of all audio distribution zones. Each includes a checkbox to enable or disable its display in the Zone View. The list also includes "All Speakers" zone (which controls Audio Distri-

bution Cut Level in system settings). When an audio distribution zone is enabled, the audio distribution zone will be displayed on the Zone View.

7 If Display Paging Zones is enabled, you can select the Paging Zones that you wish to display on the Zone View. When a paging zone is enabled, the paging zone will be displayed on the Zone View.

8 When you are finished making changes to Settings and Zone Filters, press "Save".

9 The Zone View will then be displayed (see *Figure 146, "Zone Control Zone View," on page 347*).

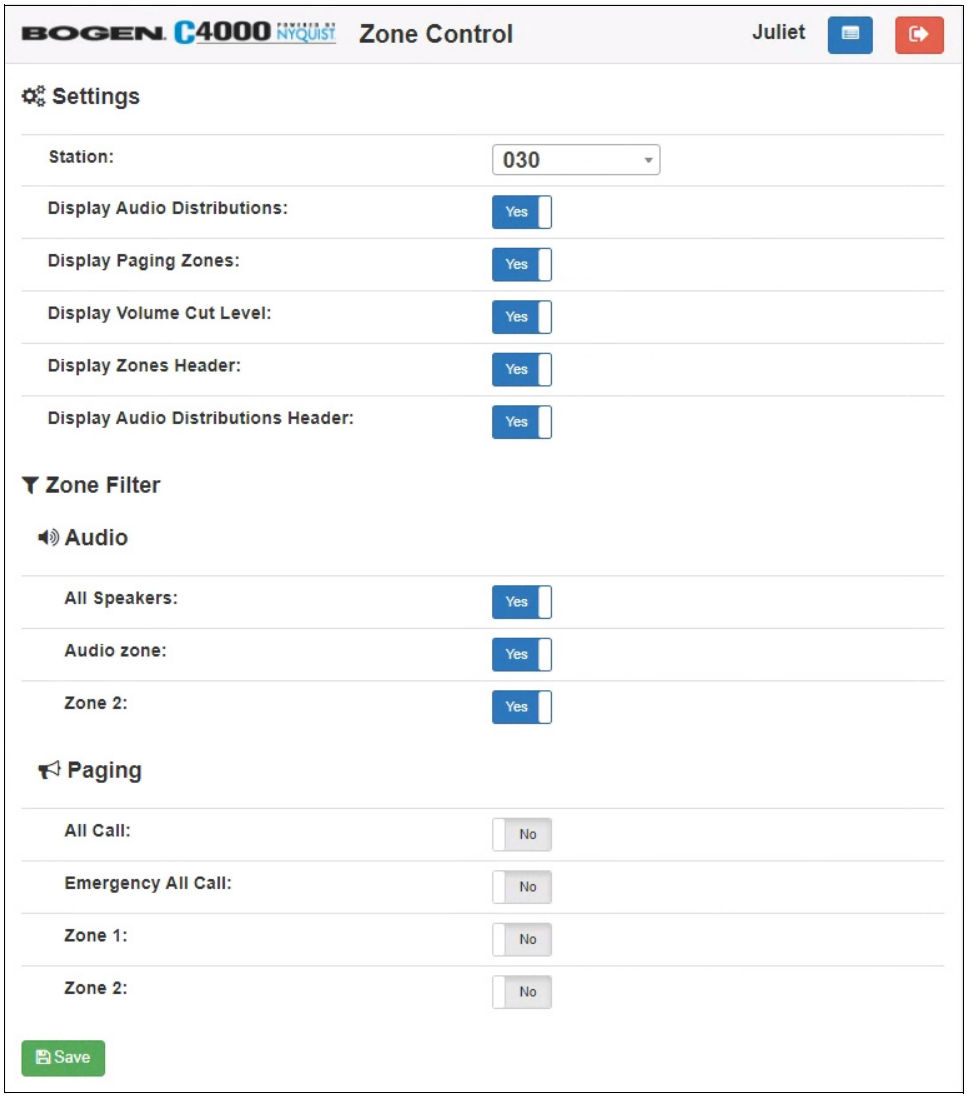


Figure 145. Zone Control Settings and Zone Filter View

Table 114. Zone Control Settings

Station	The **Admin Web Interface** station to be associated with this Zone Control login. The station selected will be used to determine the CoS settings to be used to grant audio distribution permissions (see *Table 28, "CoS Configuration Page Parameters," on page 101*). The station extension will also appear in the *Call Details* records when an Audio Distribution is started or stopped. *Tip:* You may want to create a custom Admin Web Station with limited access, which will then be used by Zone Control users. Keep in mind, however, that these Stations will appear in other feature lists throughout the Nyquist system (e.g., Dashboard's Audio Distribution list). *Tip:* You can also create a custom Station for each Zone Control user. The advantage of this is that Call Detail Records entries can then track which users started and stopped Audio Distributions.
Display Audio Distributions	When enabled, the Zone View will display available audio distributions for all zones that are selected in the Zone Filter. The audio distributions list is displayed under the related audio distribution zone. When disabled, an audio icon (i.e., a musical note) will be displayed next to each audio zone. Selecting the icon will display a page that shows the audio distributions for that zone.
Display Paging Zones	When enabled, the Zone Filter list will include Paging Zones, to allow selected Paging Zones to be displayed on the Zone View. *Note:* When you change this setting, the Zone Filter list does not immediately display the available Paging Zones; you must Save the settings, then go back into the Settings page to view and update the Paging Zones in the Zone Filter list.
Display Volume Cut Level (dB)	When enabled, the Zone View will display the numeric value for Cut Level to the right of each volume slider.
Display Zones Header	When enabled, a header will be displayed on the top of the page that labels Zone columns (e.g. Name, Description, Cut Level (dB)).
Display Audio Distributions Header	When enabled, a header will be displayed above each audio distribution list that labels the columns in the list (e.g. Line-Input/Playlist/Source, Zones, Description). *Note:* The Zones column label is not displayed on the All Speakers zone because the audio is played to All Speakers, not to zones.

Zone View

The Zone View can be used to control speaker volumes and audio distributions.

To display the Zone View:

1 Enter the following into a Chrome, Edge, or Safari browser:

`https://<server>/zone-control`

Tip: To create a shortcut to the Zone View, you can create a Map Object with an "Open URL" Action to open this link from the Dashboard.

---

2 If you are not already logged in, the *Zone Control* page will prompt you for a username and the Zone Control password.

3 After you have logged in, the Zone View is displayed (see *Figure 146, "Zone Control Zone View," on page 347*).

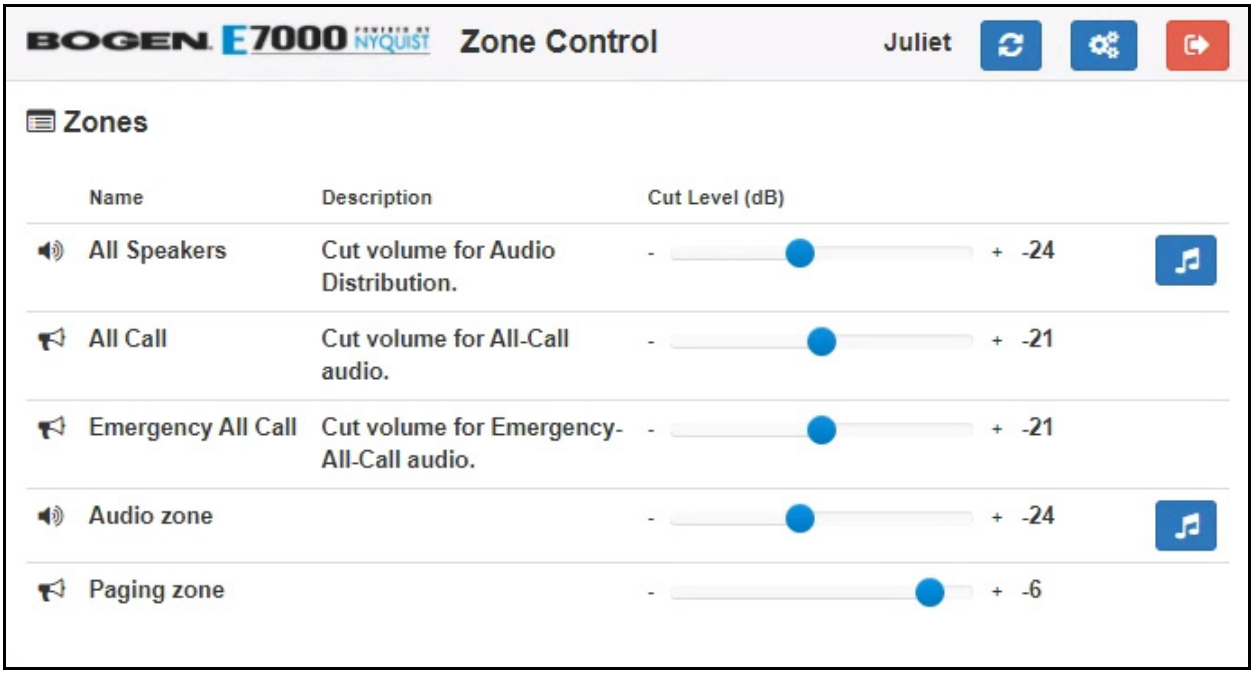


Figure 146. Zone Control Zone View

Table 115. Zone Control buttons

	Refresh: Press the Refresh button to have the Zone Controller refresh the volumes and audio distribution settings. *Note:* The status of zone volumes and audio distribution is *not* automatically updated. If a Nyquist web interface or scheduled event starts or stops an audio distribution, the state displayed on the Zone Controller may not be accurate. Whenever you wish to make a change to volume or audio distribution, you should press the refresh button first to ensure that you are starting with the correct state.
	Settings: Press the Settings button to access the Settings page for the logged in user.

Table 115. Zone Control buttons

	Zones: Press the Zones button to display the Zone View.
	Logout: Press the Logout button to log out of the Zone Controller.
	Audio: Press the Audio button to display the audio distributions that play to the selected Zone.

The Zone View displays the list of Zones that the user checked in the **Zone View Filter**.

Each listed Zone will include its name, a description, a volume slider, and an Audio icon (if **Display Audio Distributions** was disabled in the **Zone Control Settings**).

A zone's volume can be changed by simply sliding the volume control left or right for the desired zone. While using the slider, keep pressing the mouse or holding your finger down while sliding the volume left or right. When you lift up on the mouse or your finger, you will notice the volume change after a couple of seconds.

If you want to start or stop an Audio Distribution for a displayed zone, press the audio icon. After pressing the audio icon, a window will display a list of audio distributions that play to the selected Zone (see *"Audio Distribution Window" on page 348*). After the user presses start or stop for the desired audio distribution, the window closes and the Zone View is displayed.

If **Display Audio Distributions** is enabled under settings, you will see the available Audio Distributions displayed under each Zone, and can control (i.e., start and stop) the Audio Distribution from the Zone View.

Audio Distribution Window

The Audio Distribution window displays a list of Audio Distributions that play to the selected zone.

Each Audio Distribution in the list includes the start or stop button, a name, a zones list, and a description. The zones list works like the current Dashboard-based Audio Distribution zone list; it indicates when a distribution is being played to multiple zones.

Press the **Start** or **Stop** button for the desired Audio Distribution to start or stop.

After pressing **Start** or **Stop** for the desired audio distribution, the window closes and the Zone View is displayed.

Note: The Audio Distribution Window is only available when **Display Audio Distributions** is set to No. When **Display Audio Distributions** is set to Yes, the Audio Distribution selections are displayed on the Zones page.

Maintenance and Troubleshooting

This section provides detail instructions on several of the Nyquist features that are designed to help maintain and troubleshoot your system.

Backing Up Your Nyquist System and Files

You can create a full system backup of all configuration settings, back up only voice mail files, or back up only recordings. You can also schedule an automatic full system backup. Information backed up during a full system backup includes any custom alarm, tones, announcements, and music files. Phone calls and location recordings are not backed up.

You should do a system backup after a change is made to system configuration, including station and zone configuration. You should also do a system backup before updating your system to a new Nyquist release and export the backup.

You can set retention periods for each type of backup. You also have the option to disable backups of voicemail message and/or call recordings. (*See* .)

Check Server Status can be used to view how much disk space is currently being used by backups. On the *System Parameters* page, press **Check Server Status**, then scroll down to the "Disk space used by" section where you will find "backups," which indicates how much disk space is currently being used by backups.

Viewing System Backup Files

The System Backup/Restore page allows you to see all backup files available for restore.

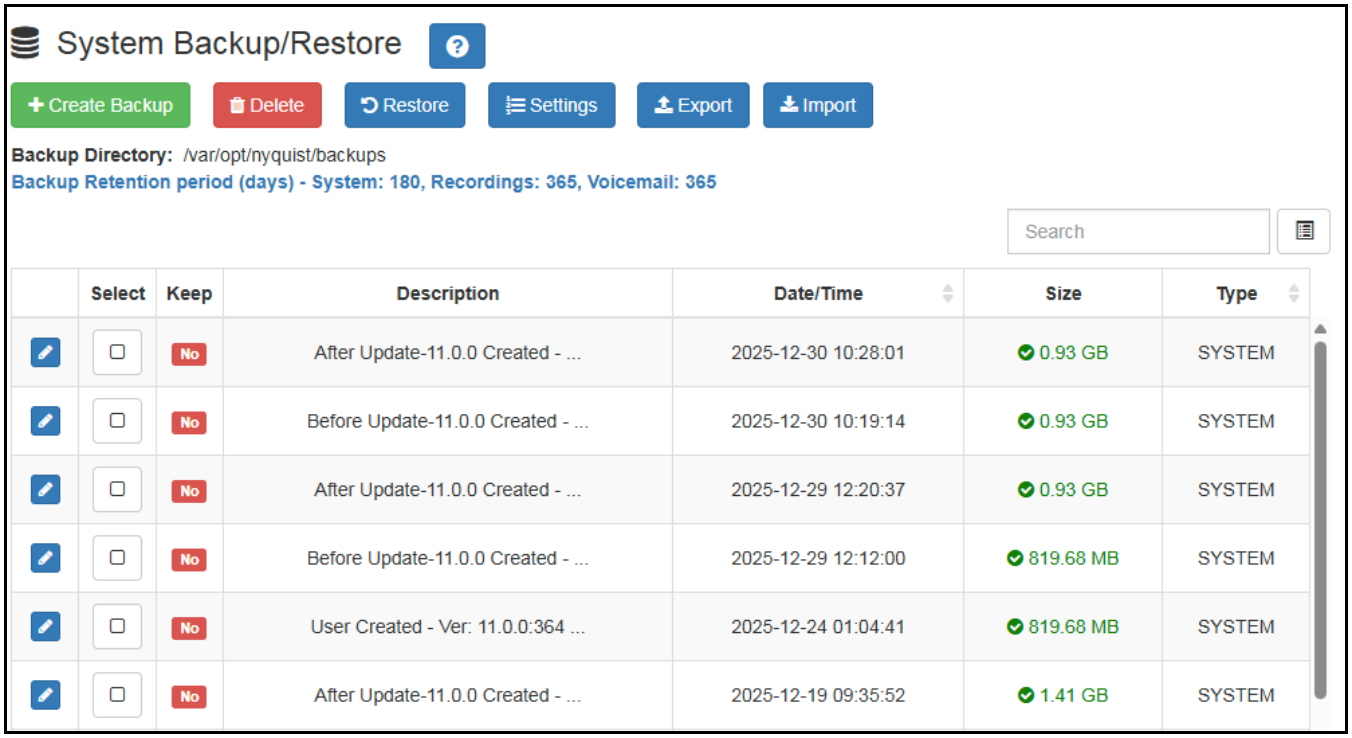


Figure 147. System Backup/Restore Page

To view system backup files:

On the navigation bar, select **System Backup/Restore**.

The following are displayed at the top of the page:

Table 116. System Backup/Restore

Create Backup

Delete

Restore

Settings

Export

Import

Table 116. System Backup/Restore

Backup Directory	Indicates the path at which the C4000 will store backups. This can be modified via the .
Backup Retention period (days)	Indicates the configured number of days that System, Recording, and Voicemail backups will be stored before being deleted. This setting can be configured via the three **Backup Retention** system parameters (see *Table 23, "Edit System Parameters Page," on page 69*) or the *Edit Backup Settings* page).

The backup directory (within the Nyquist system) is displayed, as well as the backup retention period for each backup type.

Tip: To modify the backup retention periods, update the corresponding **Backup Retention** system parameters, as described in *Table 23, "Edit System Parameters Page," on page 69* or the *Edit Backup Settings* page).

The following table describes the information that appears for each file:

Table 117. Viewing Backup File Data

Select	Select the file to restore, export, edit, or delete.
Keep	Indicates if the backup file is configured to be kept past the retention period. **Important:** See *"Using the Edit System Parameters Page" on page 67* to specify the retention periods for system, recordings, and voicemail backups.
Description	Displays the description of the backup
Date/Time	Provides the month, day, year, and time that the job was created.
Size	Displays the size of the backup. If the size is greater than the import limit (i.e., 8 GB), the size is displayed in a red font; otherwise it is displayed in a green font.
Type	Indicates what type of data was backed up. Possible values are SYSTEM, RECORDINGS, and VOICEMAIL.

Creating a Backup File

You can manually create a backup of all system files, voicemail files, or recordings.

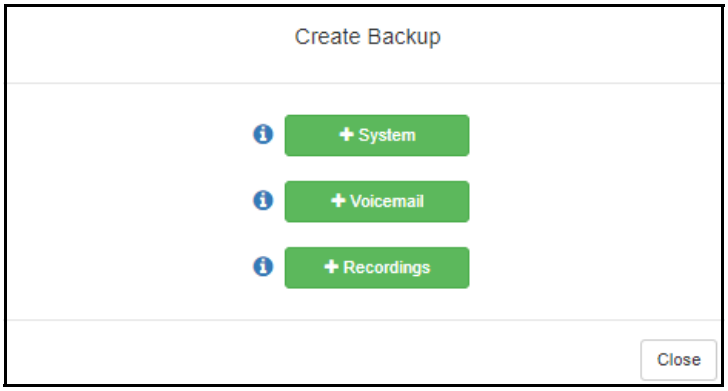


Figure 148. Create Backup Page

To create a backup file:

1. On the navigation bar, select **System Backup/Restore**.
2. On the *System Backup/Restore* page, select **Create Backup**.
3. On the *Create Backup* popup window, select one of the following options:
   - **System**
   - **Voicemail**
   - **Recordings**

The new backup file appears in the *System Backup/Restore* list.

Important:	If the system does not have sufficient available disk space before creating a voicemail or recordings backup (i.e., at least 20 GB), the backup operation will be aborted and an appropriate warning will be posted to the dashboard.

Deleting a Backup File

You can delete a single backup file or select to delete multiple backup files. By default, Nyquist does not automatically purge a backup file, even if the file has passed its retention period (see *"Using the Edit System Parameters Page" on page 67*). However, you can select to delete any files; the system will warn you if you select to delete a file marked to keep.

To delete a backup file:

1. On the navigation bar, select **System Backup/Restore**.
2. On the *System Backup/Restore* page, select the backup file or files that you want to delete.
3. Select **Delete**.
4. When prompted, select **Delete**.

Editing System Backup/Restore Information

You can edit the description of user, system, and installation-created backup or restore files.

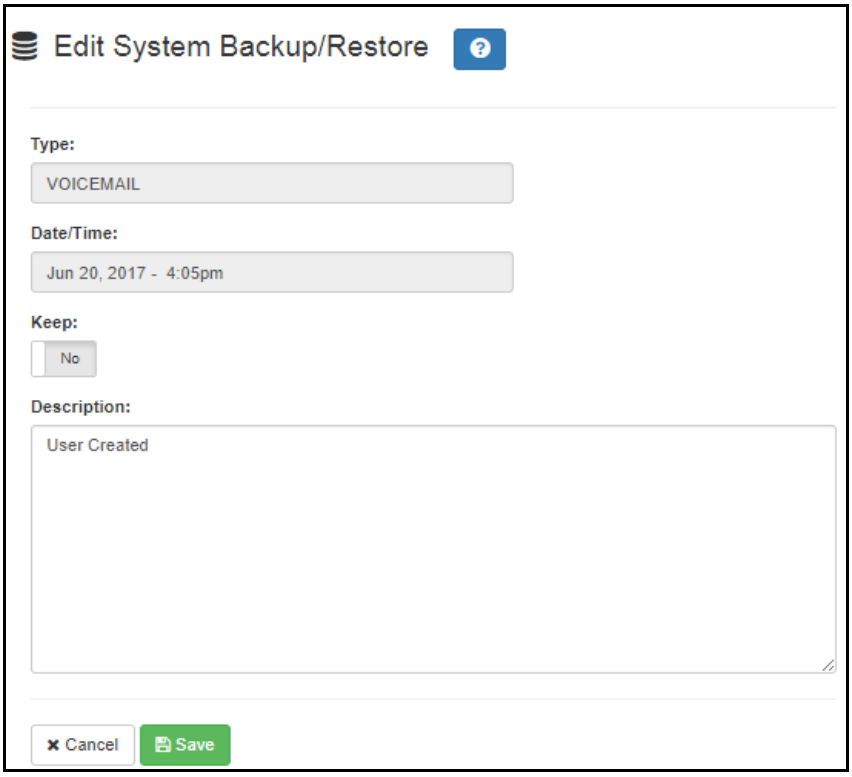


Figure 149. Edit System Backup/Restore Page

To edit the file's description:

1. On the navigation bar, select **System Backup/Restore**.
2. On the *System Backup/Restore* page, select the **Edit** icon next to the desired file.
3. Edit the description.
4. Select **Save**.

Table 118. Edit System Backup/Restore Parameters

Type	Displays the file type, such as SYSTEM for a system backup, RECORDINGS for a call recordings backup, or VOICEMAIL for a voicemail backup. This parameter cannot be edited.
Date/Time	Displays the date and time that the file was created. This parameter cannot be edited.

Table 118. Edit System Backup/Restore Parameters (continued)

Keep	Select **Yes** if you want to have Nyquist keep the file even if the retention period has expired. Nyquist keeps at least one backup file even if the retention period has expired.
Description	Provides a system or user-provided description. By default, the description is **User Created** for user-created backup or restore files, **System Created** for backups automatically created based on specified settings, or **Installation Created** for backups created via the installation process

Editing Backup Settings

Backup settings allow you to schedule an automatic backup and set specific backup parameters for system backups, including the backup directory where the files will be stored.

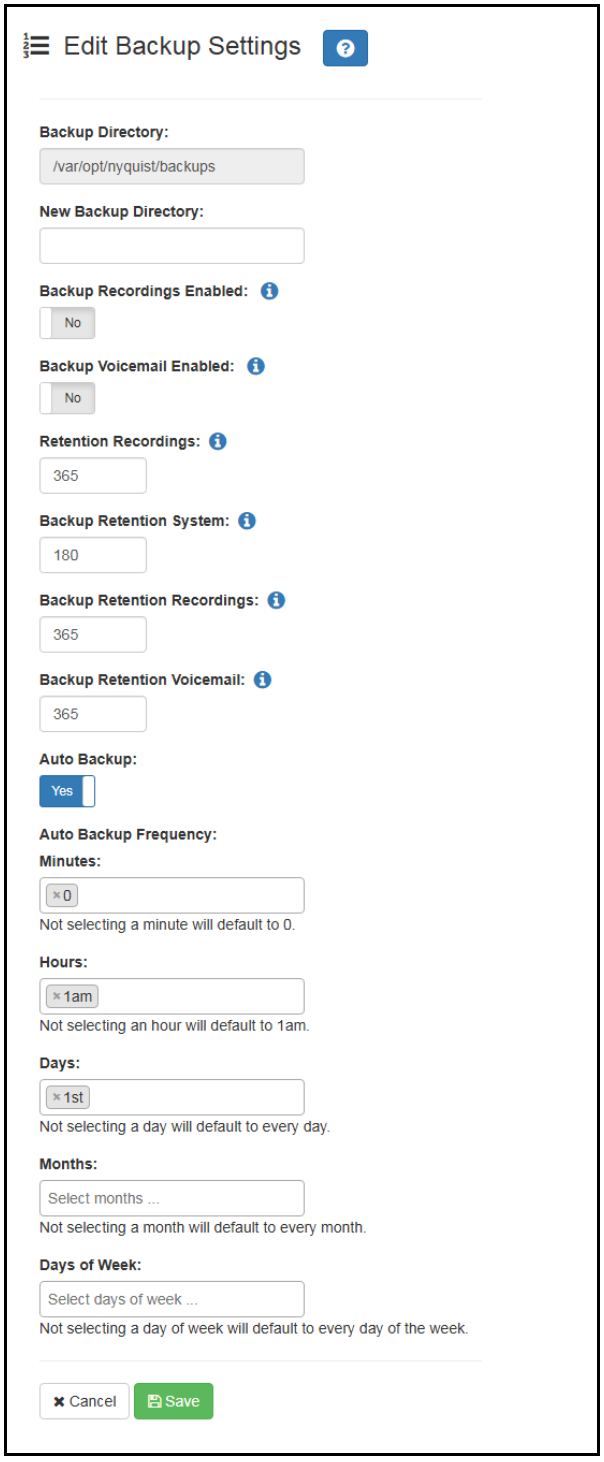


Figure 150. Edit Backup Settings Page

To edit backup settings:

1. On the navigation bar, select **System Backup/Restore**.
2. On the *System Backup/Restore* page, select **Settings**.
3. Make desired changes (see *Table 119, "Backup Settings Page Parameters," on page 356*).
4. Select **Save**.

Table 119. Backup Settings Page Parameters

Backup Directory	Displays the current path for backup file. The default value is `/var/opt/nyquist/backups`.
New Backup Directory	Enter a new path for the Backup Directory, if applicable. To create backup files on a USB drive connected to the C4000, use **Check Server Status** (see *"Check Server Status" on page 44*) and find the **Mounted on** value for the connected USB drive to determine the path to the USB drive, then specify that value (or a subdirectory thereof) as the **New Backup Directory**. For example, if the Mounted on value of the USB drive is `/media/mydrive`, you might specify `/media/mydrive/data/Bogen-Backups` as the **New Backup Directory**. *Tip:* Storing backup files on an external USB drive allows more disk space to be available for C4000 system usage. It can also allow a Nyquist system controller to access the log files from a previous controller by using the USB drive from the old controller.
Backup Recordings Enabled	If enabled, call recordings will be backed up according to the specified frequency and retention period. This setting is also available via the corresponding System Parameters setting (see *"Edit System Parameters Page" on page 69*).
Backup Voicemail Enabled	If enabled, voicemails will be backed up according to the specified frequency and retention period. This setting is also available via the corresponding System Parameters setting (see *"Edit System Parameters Page" on page 69*).
Retention Recordings	Identifies the number of days to retain recordings. Recordings that are older than the retention period are automatically deleted. You can set a maximum retention period of 99,999 days. This setting is also available via the corresponding System Parameters setting (see *"Edit System Parameters Page" on page 69*).
Backup Retention System	Identifies the number of days to retain system backup files. System backups that are older than the retention period are automatically deleted, provided at least one system backup file remains. You can set a maximum retention period of 99,999 days. This setting is also available via the corresponding System Parameters setting (see *"Edit System Parameters Page" on page 69*).
Backup Retention Recordings	Identifies the number of days that backups of recordings are retained. Backups that are older than the retention period are automatically deleted, provided at least one backup remains. You can set a maximum retention period of 99,999 days. This setting is also available via the corresponding System Parameters setting (see *"Edit System Parameters Page" on page 69*).

Table 119. Backup Settings Page Parameters (continued)

Backup Retention Voicemail	Identifies the number of days that voicemail backups are retained. Backups that are older than the retention period are automatically deleted, provided at least one backup remains. You can set a maximum retention period of 99,999 days. This setting is also available via the corresponding System Parameters setting (see *"Edit System Parameters Page" on page 69*).
Auto Backup	Indicates if the backup is to be automatically generated.
Auto Backup Frequency	
Minutes	Specifies one or more values to indicate at which minutes of the specified **Hours** that the backup job is to run. If unspecified, the default will be zero (0).
Hours	Specifies one or more values to indicate at which hours of the specified **Days** and **Days of the Week** that the backup job is to run. Selections are formatted with the hour and either "am" or "pm". If unspecified, the default will be "1am".
Days	Specifies the days of the month that the backup job is to run. If this and **Days of the Week** are both unspecified, the default will be every day of the month.
Months	Specifies the months of the year that the job is to run. If unspecified, the default will be every month.
Days of the Week	Specifies the days of the week that the job is to run. If this and **Days** are both unspecified, the default will be every day of the week.

Exporting a Backup File

You can export a backup file as a .gz file, which can be stored on the Admin Station or downloaded to removable media, such as a thumb drive, to be stored off site.

To export a backup file:

1. On the navigation bar, select **System Backup/Restore**.
2. On the System Backup/Restore page, select the backup file that you want to export.
3. Select **Export**.

Once saved, an icon with the downloaded report name appears in the lower left section of the web browser window, giving you the option to open the report. For Android devices, files are automatically downloaded and saved to the device's Download folder.

Important: We *strongly* recommend that you export your backups to external media to use in the event that a Nyquist drive fails. If the Nyquist drive fails, the backups stored on the Nyquist server will no longer be available, and externally stored backups will be the only backups available to use in recovering your system configurations and files.

Restoring a Backup File

You can restore the facility configuration to that saved during a system backup. You can also restore voicemail or recordings backups.

Important: Nyquist system backups are backward compatible. The C4000 can restore a backup created from its current release or any previous release. If a system backup from a previous release is restored, the configuration data will automatically be upgraded to the new release.

To restore a file:

1. On the navigation bar, select **System Backup/Restore**.
2. On the *System Backup/Restore* page, select the backup file that you want to restore.
3. Select **Restore**.
4. When prompted, select **Restore**.
5. A dialog box appears asking if you want to restore the License Activation Keys. If you have already activated the License Activation Keys on this C4000 (e.g., you are restoring to the same C4000 from which the backup was taken and the licenses are still active), select **No**. If not (e.g., you are restoring to a new C4000 and have not already activated the licenses), select **Yes**.

   To cancel the restore operation, select **Cancel**.
6. If you did not cancel the restore operation, a dialog box appears notifying you that the restore is in progress. If the restore dialog box disappears and a login screen appears, log back into the system.
7. When the restore is completed, a new message appears on the dashboard to indicate the restore has completed.

Importing a Backup File

You can import a backup file that was previously exported. You can subsequently select to restore this file.

To import a backup file:

1. On the navigation bar, select **System Backup/Restore**.
2. On the System Backup/Restore page, select **Import**.
3. Select **Choose file**, and then navigate to the backup file that you want to import.
4. Select **Open**.
5. Select **Import**.

Software Components List

The version numbers for several key software components that are installed and used by the Nyquist system are listed in the *Software Components* section of the **Check Server Status** report (see *"Check Server Status" on page 44*). The version numbers are dynamic and may change after the **Upgrade Debian Operating System Components** feature has been used (see *"Upgrade Debian Operating System Components" on page 38*).

The following is an example of the *Software Components* section of the report:

```
Software Components:
 Asterisk 18.20.2
 apache2 Version: 2.4.62-1~deb12u1
 bash Version: 5.2.15-2+b7
 bind9 Version: 1:9.18.28-1~deb12u2
 binutils Version: 2.40-2
 curl Version: 7.88.1-10+deb12u8
 dnsutils Version: 1:9.18.28-1~deb12u2
 exim4 Version: 4.96-15+deb12u5
 ffmpeg version 7.0.1
 glibc Version: 2.36-9+deb12u8
 isc-dhcp-server Version: 4.4.3-P1-2
 Laravel Framework 9.52.16
 libssh Version: 0.10.6-0+deb12u1
 libssl Version: 1.1.1w-0+deb11u1
 linux kernel 6.1.0-26-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.112-1 (2024-09-30) x86_64 GNU/Linux
 lsyncd Version: 2.2.3-1+b1
 mosquitto Version: 2.0.11-1.2+deb12u1
 msmtp Version: 1.8.23-1
 mysql  Ver 15.1 Distrib 10.11.6-MariaDB
 nmap Version: 7.93+dfsg1-1
 ntp Version: 1:4.2.8p15+dfsg-2~1.2.2+dfsg1-1+deb12u1
 openssh Version: 1:9.2p1-2+deb12u3
 openssl Version: 3.0.14-1~deb12u2
 php Version: 8.2.24-1~deb12u1
 php-ldap Version: 2:8.2+93
 pjsip 2.13.1
 rsync Version: 3.2.7-1
 rsyslog Version: 8.2302.0-1
 snmpd Version: 5.9.3+dfsg-2
 sox Version: 14.4.2+git20190427-3.5
 sudo Version: 1.9.13p3-1+deb12u1
 systemd Version: 252.30-1~deb12u2
 tar Version: 1.34+dfsg-1.2+deb12u1
 tcpdump Version: 4.99.3-1
 tftpd-hpa Version: 5.2+20150808-1.4
 wget Version: 1.21.3-1+b2
```

Using System Log Files

A log file records either events or messages that occur when software runs and is used when trouble-shooting the system. The following parts of the Nyquist system generate log files:

- *Server*: Provides access to the Debian Linux OS server log files.
- *Nyquist C4000*: Provides access to the Nyquist application log files.
- *Web Server*: Provides access to the web server log files.

From the web-based UI, system logs can be viewed directly or exported via download to your PC, Mac, or Android device and then copied to removable media or attached to an email to technical support.

Table 120. System Logs

File	Description
Server	
aptitude	Records information about packages installed or upgraded on the server.
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 background daemons that run on the system.
debug	Contains errors and debug information.
dmesg	Contains kernel ring buffer information. When the system boots up, the screen displays information about the hardware devices that the kernel detects during the boot process. These messages are available in the kernel ring buffer, and whenever a new message comes, the old message gets overwritten.
dpkg.log	Contains information that is logged when a package is installed or removed using dpkg command.
faillog	Contains user failed login attempts.
fontconfig.log	Logs use of fontconfig program to configure or substitute fonts to other programs.
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 global system messages, including the messages that are logged during system startup. Items logged in the messages file include cron, daemon, kern, auth, and so on.
mysql.err	Contains a record of mysql errors that occur when the server is running.
mysql.log	Contains a general record of what mysql is doing (connect, disconnect, queries).
nyquist_af_alerts.log	Contains Automatic Failover alerts, used by Technical Support to help diagnose any issues.
nyquist_af_setup.log	Contains Automatic Failover setup information, used by Technical Support to help diagnose any issues.
nyquist_af_status.log	Contains Automatic Failover status updates, which includes all server state transitions that have been performed (e.g., Secondary becomes Master, Primary placed into Standby mode, etc.).
nyquist_mysql_table_check	Contains status of Nyquist database tables after a Nyquist server reboot. All tables should display a status of OK. If a table shows anything other than OK, contact Bogen Technical Support for assistance.
syslog	Contains list of errors that occur when the server is running, such as hard disk SMART warnings and errors, and server start and stop records.
user.log	Contains information about all user-level logs.
Nyquist C4000	
api_log	Contains a record of all commands received from 3rd-party systems to the Routines API v1.

Table 120. System Logs (continued)

File	Description
api2_log	Contains a record of all commands received from 3rd-party systems to the Routines API v2.
checkin	Contains historical record of actions that occurred during a check-in. (See *"Check-In Log and Call Detail Records" on page 533*.) Contains events recorded for the Station Check-In process. These include times and data for Check-In Start, Stop, Reset, Done, Vacancy Add, Vacancy Delete, and individual stations' Check-in.
device_status	Record of station unavailability events recorded by Station Monitoring.
messages	Contains messages generated by Nyquist.
nyquist_routines.log	Contains records of Nyquist routine events (e.g., started and stopped) as well as messages logged via the Log-Text action or the `logText(<text>)` function from within a routine action condition's CODE segment (see *"Routines Log" on page 492* for details).
Web Server	
access.log	Contains access records for the web server.
error.log	Contains information about errors that the web server encountered when processing requests, such as when files are missing.
other_vhosts_access.log	Contains access records for vhosts that don't define their own logfiles.

Viewing System Log Files

You can view a specific log for the Linux server, Nyquist server, or web server.

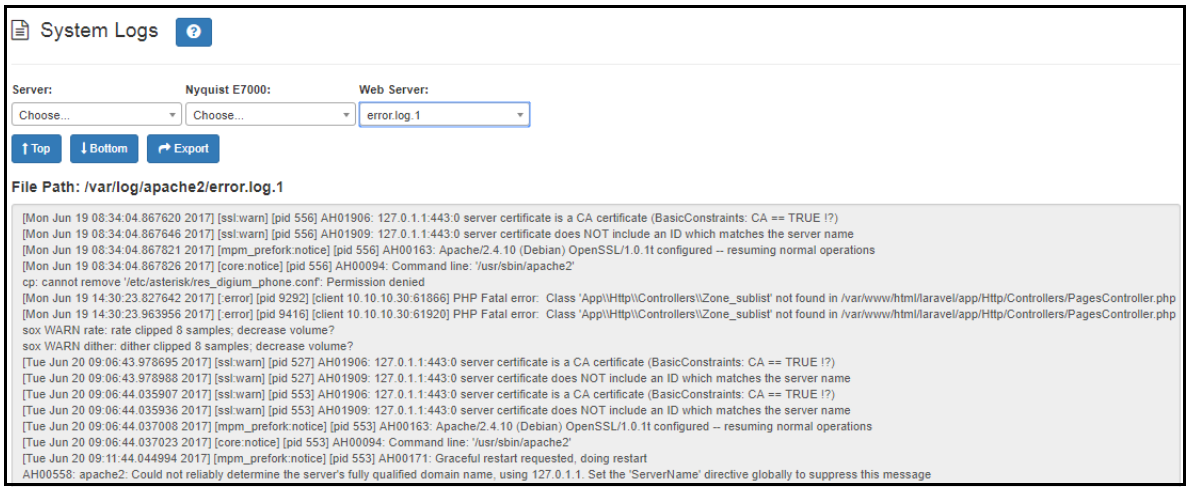


Figure 151. System Logs

To view a log file:

1. On the navigation bar, select **System Logs**.
2. Use the drop-down menu of the desired server to select the specific log file that you want to view.

The file path and contents appear on the *System Logs* page.

Exporting a Log File

To export a log file:

1. On the navigation bar, select **System Logs**.
2. Use the drop-down menu of the desired server to select the log file that you want to export.
3. Select **Export**.

If the Save As dialog box appears, you can select where to download and save the log file; if not, it will be downloaded to the browser's configured download location.

For Android devices, files are automatically downloaded and saved to the device's Download folder.

Note: Exporting a log file does not remove it from the C4000. To remove log files, contact Tech Support.

Using the Call Details Feature

The Call Details feature allows you to view or print detail records of every call in a facility in a call log format. Calls include scheduled announcements, paging, and internally and externally placed or received telephone calls.

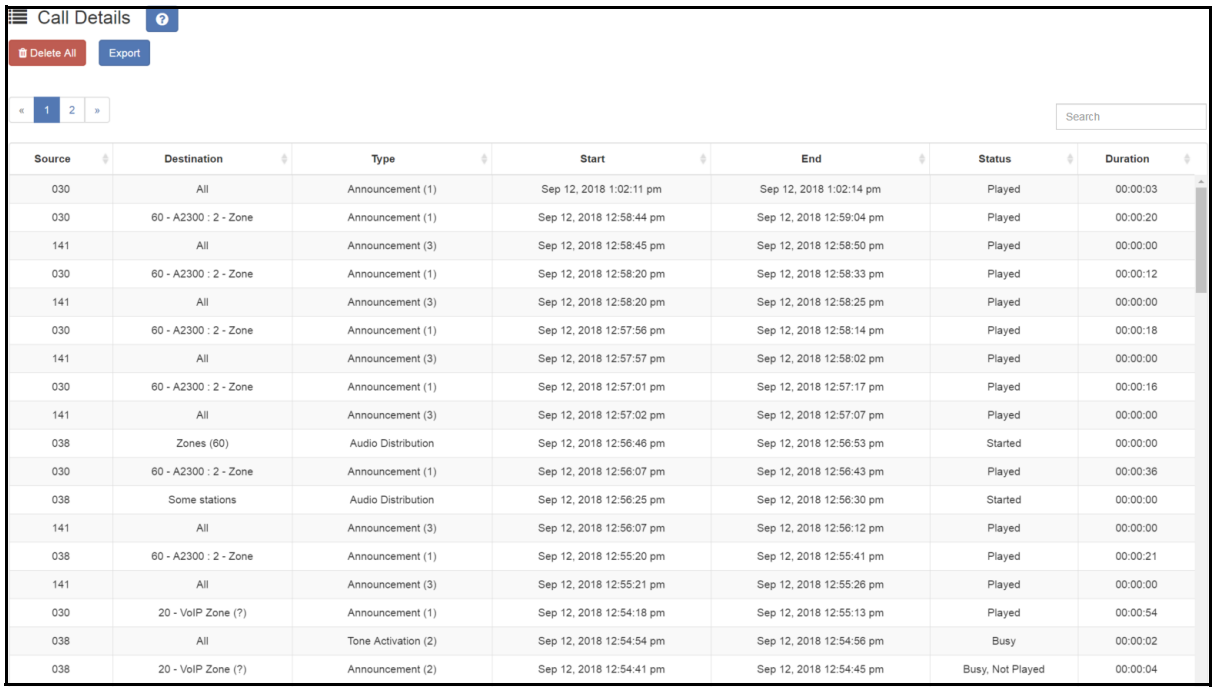


Figure 152. Call Details Page

Viewing Call Details Records

To view the call details records for the facility:

1. On the navigation bar, select **Call Details**.
2. Optionally, specify a value in the **Search** field to filter the list of call details records.

The following table describes the *Call Details* parameters:

Table 121. Call Details Page Parameters

Source	Provides the extension where the call originated or the station that recorded a page for page queuing.
Destination	Provides either the extension to which the call was directed, or the target zone or facilities of the page or announcement. A **Destination** of **None entered** means that an invalid zone was entered, while **All** means all stations were targeted.
Type	Provides the type of call, such as Emergency Call, Admin Call, Announcement, and so on.
Start	Provides the date and time that the call began.
End	Provides the date and time that the call ended.
Status	Provides information about whether the call was answered or not answered. For queued pages, the status could be: • **Played**: Page was successfully recorded and was played to the specified zone. • **Queued**: Page was successfully recorded and is queued for playing to the specified zone. • **Not Recorded**: Either zone was not defined or the user hung up without pressing hashtag (#) after the recording. • **Timed Out**: Page timed out and was not saved either because there was more than 60 seconds of silence or because the recording exceeded 60 minutes in length. • **Requeued**: Page message was interrupted while being played and was returned to the queue.
Duration	Provides the number of hours, minutes, and seconds that the call lasted.

Exporting and Printing a Call Log

To export and print a call details report:

1. On the navigation bar, select **Call Details**.
2. Select **Export**.

When the **Save As** dialog box appears, you can name the report and select where the report is to be downloaded or saved. The default name is `call_details_<yyyymmddhhhmmss>.csv`.

3 In the lower left corner of the browser, select the downloaded CSV file, open it (presumably using a spreadsheet application, such as Excel, or a text editor), and optionally print it.

For example, if using Excel:

a) Open the Excel spreadsheet, select **Page Layout,** and set the desired parameters.

b) Select **File**, and then select **Print**.

> *Tip:*If Excel is not available, you can use PowerShell to import, filter, display, or print the call logs from one or more downloaded files. See the following for a few examples:
>
> ```
> Import-Csv -Path call_details_<xxxx>.csv | Out-GridView
> Get-ChildItem -Path call_details_*.csv | Import-Csv | Format-Table
> Import-Csv -Path call_details_<xxxx>.csv | Where-Object Source -eq '010' | Format-Table
> Import-Csv -Path call_details_<xxxx>.csv | Format-Table | Out-Printer
> ```

Deleting All Call Records

To delete all call detail records:

1 On the navigation bar, select **Call Details**.

2 Select **Delete All**.

3 When prompted, select **Delete**.

Tuning Volume with White or Pink Noise

Nyquist provides white noise and pink noise files to help tune, or adjust, the volume of speakers in a zone.

White noise has equal energy for each frequency that the human ear can hear. Pink noise sounds less harsh than white noise because humans hear in octaves (the doubling of a frequency band). The energy in pink noise decreases by half as the frequency doubles, making the noise sound more balanced.

Both white and pink noise files are provided by default in Nyquist as both tones and songs. You can use the tone files as a tone generator to help adjust volume and frequency for pages in time-based zones. You can use the song files to help adjust volume and frequency in audio zones that play audio distribution.

Remember that when creating, editing, or viewing a zone, the **Type** identifies the zone as being able to receive paging, time, audio, or a combination of paging, time, or audio. (See *"Viewing Zone Information" on page 214*.)

To start a white noise or pink noise file as a tone, follow the steps listed in *"Managing Tones via the Dashboard" on page 389*, selecting either the White Noise or Pink Noise file.

To play a white noise or pink noise file to a zone that plays audio distribution, first create a playlist that contains the white or pink noise song (see *"Creating a Playlist" on page 300*) and then follow the steps listed in *"Using Audio Distribution" on page 402* to start the audio distribution.

If the zone can receive a combination of paging, time, and audio, you should use both the tone files and the song files to tune the speaker volume.

Troubleshooting Common Issues

The following table provides some possible causes and solutions for common Nyquist issues.

Table 122. Troubleshooting Issues

Issue	Possible Cause	Possible Solution
This web interface station is not connected to the server.	The Bogen root certificate has not been installed correctly, or the browser has not refreshed the certificate information.	Follow the instructions for installing the Bogen certificate (see *"Client Requirements" on page 8*). If the certificate has already been installed, use Ctrl+Shift+Del, clear the "Cookies and other site data," and retry. The browser may need to be restarted. *Tip:* Accessing the application from an incognito browser session may provide more accurate validation of certificate issues.
Day calls are not being routed to the proper Admin Station.	The system parameters that affect day calls being routed to an Admin Station may be incorrectly set.	On the navigation bar, select **System Parameters**, and then review the Day Start time. If the time is not properly set to when the Admin Station should receive the day calls, select the **Edit** icon and enter the correct time for Day Start.
Night calls are not being routed to the proper Admin Station.	The system parameters that affect night calls being routed to an Admin Station may be incorrectly set.	On the navigation bar, select **System Parameters**, and then review the Night Start time. If the time is not properly set to when the Admin Station should receive the day calls, select the **Edit** icon and enter the correct time for Night Start.

Table 122. Troubleshooting Issues

Issue	Possible Cause	Possible Solution
The Nyquist server is not getting the correct date and time.	Either the Network Time Server being used is incorrect or the server date and time is incorrect.	On the navigation bar, select **System Parameters**, and then review the parameters set for the NTP server and for the server date/time. Select the **Edit** icon and make any necessary changes.
A station is not able to initiate non-emergency calls during the day.	The station may not have the correct CoS assigned to allow Normal+Emergency calls.	On the navigation bar, select **CoS Configuration**. Note which configurations allow a Call in Level of Normal+Emergency. Next, select **Stations**, navigate to the station's extension number, and then use the slider to determine what the station's Day CoS is. If the station's Day CoS does not allow the correct Call in Level, select the **Edit** icon, and then select a CoS configuration that has the correct Call in Level.
The station is not receiving Audio Distribution.	The station is on the Paging Exclusion list.	Remove the station from the Paging Exclusion list. (See *"Excluding Stations from Paging" on page 208*.)
	The station is not a member of audio distribution zone.	Add the station to an audio distribution zone. (See *"Editing Zone Configuration" on page 219*.)
	The station's **Multicast Audio Distribution** parameter is disabled.	Enable the station's **Multicast Audio Distribution** parameter. (See *"Editing Station Configuration Settings" on page 155*.)
	Multicast IP packets are being blocked or not routed.	Ensure that multicast IP packets are flowing between the Nyquist server and Nyquist stations.

Table 122. Troubleshooting Issues

Issue	Possible Cause	Possible Solution
When the button on the Digital Call Switch (DCS) is touched, the DCS's LED changes from solid blue to solid green as if a normal call is being made. However, no call is made.	The DCS may be attached to a device that is not configured to support a **Station Type** of **Digital Call Switch & Speaker**.	Determine what **Device Type** the DCS is attached to and use the Stations list to determine if the **Station Type** is set as **Digital Call Switch & Speaker**. (See *"Viewing Station Configuration Settings" on page 142*.)
Communication issues with a device.	Network issues or a firewall may be preventing the device from sending and/or receiving TCP/IP communications between the C4000 and the device.	Ping the device from the C4000 to verify communications between the C4000 and the device. Display the Device Status of the device by selecting the Information button of the *Stations*, *Bridge Devices*, *Amplifier and Gateway Devices*, or *Simplified Configuration* pages. The C4000 will ping the device and display the results. Though not a solution, temporarily disabling the Nyquist firewall (see *Table 18, "Manage Firewall," on page 51*) may help in troubleshooting communication issues.

Dashboard Messages

The Admin web UI dashboard and the Admin Phone display error, warning, and information messages during Nyquist operations. Error and warning messages include notices that an operation failed and information about why the failure occurred. You can delete these messages using the Delete icon (if shown), but you may want to note the error and pass the information about the error to system administrator or information technology personnel.

Informational messages often provide status about an operation or condition and are usually cleared automatically when an operation completes. The following table describes the informational messages that may appear:

Table 123. Dashboard Informational Messages

Message	Meaning
Alarm (<extension>): <alarm-name>	The listed extension is starting an alarm.
Tone (<extension>): <tone-name>	The listed extension is starting a tone.

Table 123. Dashboard Informational Messages (continued)

Message	Meaning
Page (<extension>): Zone: <zone-number> - <zone-name>	The listed extension is starting a page for the listed zone.
Announcement (<extension>): <announcement-name>	The listed extension is starting the listed announcement.
Emergency Announcement (<extension>): <e-announcement-name>	The listed extension is starting the listed emergency announcement.
All-Call (<extension>)	The listed extension is starting an All-Call page.
Emergency All-Call (<extension>)	The listed extension is starting an Emergency All-Call page.
Scheduled Announcement	A scheduled announcement is playing.
Multi-Site Emergency All-Call (<extension>)	The listed extension is starting a multiple site Emergency All-Call page.
Multi-Site All-Call (<extension>)	The listed extension is starting a multiple site All-Call page.
Multi-Site Page [<site(s)>] (<extension>)	The listed extension is starting a page for the listed site(s).
Multi-Facility Announcement (<announcement>) [<site(s)>] (<extension>)	The listed extension is starting the specified announcement DTMF code at the listed site(s).
Facility All-Call (<extension>) -> <facility-name>	The listed extension is starting a facility-wide All-Call page.
Audio Distribution: Playing <song-name> to Zone (<zone-number(s)>)	The Audio Distribution feature is playing the listed song to the listed zone. The message may optionally include "and All Speakers" or "and selected stations."
Audio Enabled	Audio (paging, Scheduled Audio, audio distribution) is enabled. See *"Enabling and Disabling Audio" on page 404* for more information.
Audio Disabled	Audio (paging, Scheduled Audio, audio distribution) is disabled. See *"Enabling and Disabling Audio" on page 404* for more information.
System is running in demonstration mode	All Nyquist functions are enabled but the maximum station count is set to 6 and the maximum number of simultaneous calls is set to 2.

User-created messages set up for I/O Controller rules also appear on the dashboard. See *"Configuring I/O Controller Input Rules" on page 162* and *"Configuring I/O Controller Output Rules" on page 164* for additional information.

User-created messages set up by Routines also appear on the dashboard. See the Dash-Text command in *Table 2, "Routine Action Type-Specific Parameters," on page 588* for additional information.

911 Call Errors

The following errors may occur when an extension attempts to place a 911 call:

- Call to 911 from <extension> failed due to no outbound lines available.
- Call to 911 from <extension> failed due to no 911 access.

The first message means that all outbound lines from the facility are currently busy. To prevent this error from occurring, set the **Bump on 911** system parameter to **Yes**. (See *"Using the System Parameters Page" on page 21*.) You also want to ensure that outside line access is enabled. (See *"Editing Outside Lines" on page 125*.)

If the second error message appears, then the station, or extension, attempting to make the 911 call does not have the 911 Route parameter and Outside Access parameters correctly set. (See *"Editing Station Configuration Settings" on page 155*.)

Maximum Concurrent Call Error

If you reach your maximum concurrent call limit, the following error message appears:

- Maximum concurrent calls reached. Contact Customer Service to increase maximum concurrent calls limit.

In this case, calls include telephone calls, pages, tones, alarms, and announcements.

To view the concurrent call limit set for your system:

1. From the navigation bar, select **System Parameters**.
2. Select **Product License**.
   The **Maximum Concurrent Calls Limit** appears under **Licensing Information**.

The limit is based on your licensing setup and can only be changed by contacting Customer Service.

If you are using the Record Page feature, you must be below your concurrent calls limit by two calls for the page to play. Otherwise, the page remains in the queue.

Equipment Errors

The following table describes equipment error messages that may appear:

Table 124. Equipment-Related Errors

Error Message	Cause
NOTICE: Server was restarted due to error. Contact Technical Support.	The server probably experienced a crash. Contact Technical Support to ensure that the crash did not cause any issues. Note that the server may also restart during an install or upgrade.
<date time> Extension <extension number> not available, check device status.	You may be experiencing connectivity issues that prevents the station from being registered with the Nyquist server. You may want to reboot the device to see if that takes care of the problem.
Line-Input busy (Matrix Mixer: <mixer extension>. Channel: <mixer channel number>.	You are attempting to use an input channel that is already in use.
WARNING: I/O Controller - <name> (<controller extension>) is Unavailable.	If it is listed as unavailable, the device is not registered with the Nyquist server.
WARNING: I/O Controller - <name> (<controller extension>) is Unknown.	The server is unable to determine the state of the device.
WARNING: I/O Controller - <name> (<controller extension>) is Unreachable.	The device is registered with the Nyquist server but cannot be reached (communication to device fails). This situation is probably due to a network or cable issue or the device is rebooting.

Facility Error Conditions

If you cannot reach a facility that is listed and enabled in the Facilities list, the following error messages appear on the Admin dashboard or the Bogen Admin IP phone:

- WARNING: Not registered with Facility: <Facility-Name>
- WARNING: Remote Facility not registered: <Facility-Name>
- WARNING: Remote facility not registered with this Facility: <Facility-Name>

Error messages also appear when multi-site and facility calls are initiated but cannot be completed due to issues with the remote facility.

To troubleshoot these error messages:

1. On the navigation bar, select **Facilities**.
2. Ensure the **Status** for the facility appears as **Enabled** and that the following facility parameters are correct:
3. Password

4 Name

5 Host (Host Name or IP address)

6 If parameters are incorrect, select the **Edit** icon for the facility and make the necessary changes. (See *"Editing a Facility" on page 135*.)

In addition to performing the troubleshooting steps through the Nyquist Admin Web UI, do the following:

- Check for network issues (Local Area Network (LAN), Wide Area Network (WAN), VLAN, ports) that are preventing facility servers from communicating with each other.
- Ensure that you can access and operate the remote Nyquist facility server by logging on to the Admin Web UI for that server and attempting to initiate a call or page.

Automatic Failover Messages

There are a number of messages that will be shown on the Dashboard to reflect changes to the Automatic Failover status. Each will be prefixed with an icon, date, time, and "Automatic Failover - ".

Some messages will only be shown while the user is logged into a server by the Primary or Secondary IP address, while others are only shown when logged into the server by Master IP address.

Tip: When accessed via the Master IP address, the Operation Commands section of the Automatic Failover page provides a direct link to the Primary and Secondary servers,

Table 125. Automatic Failover Dashboard Messages

Message	Type	Server(s)
Lost contact with Primary node	Warning	Secondary Master
Lost contact with Secondary node	Warning	Primary Master
Ethernet Port-A network failure, Primary node not providing service	Warning	Primary
Ethernet Port-A network failure, Secondary node not available	Warning	Secondary
Primary node not providing service	Warning	Primary
Warning: Secondary node is starting service. Please contact technical support and avoid making configuration changes.	Warning	Secondary Master
Warning: Secondary node is now providing service. Please contact technical support and avoid making configuration changes.	Warning	Secondary Master

Table 125. Automatic Failover Dashboard Messages

Message	Type	Server(s)
Primary node is starting service	Information	Primary Master
Primary node is now providing service	Success	Primary Master
Secondary node is now in slave mode	Success	Secondary
Primary node is now in standby mode	Warning	Primary
Secondary node is now in standby mode	Warning	Secondary

Zone Overlap Messages

Zone overlap occurs when two or more target zones of a scheduled event or audio distribution include the same station (or stations). If a zone overlap is detected while adding or editing a zone, scheduled event, or audio distribution, the C4000 will display a notification growl message and prevent the addition or edit operation from completing.

If a zone overlap somehow occurs, perform a **Check Server Status** operation (see *"Check Server Status" on page 44*) to determine which scheduled event or audio distribution references two or more target zones that include the same station. To fix this, either remove the shared station from all but one target zone, or remove the overlapping target zone(s) from the scheduled event.

Finding Nyquist System Controller's IP Address

If you do not know the IP address of the Nyquist System Controller (NQ-SYSCTRL), there are several ways to obtain it.

- The factory default IP address of the C4000's network Port A is 192.168.1.10. Port B, however, is configured by default to have its IP address assigned by a DHCP server.
- If you have physical access to the Nyquist System Controller, you can obtain the IP address by attaching an HDMI monitor to the controller's HDMI port; the IP configuration should be displayed on the screen. If it is not displayed, perform a hardware reset and wait for it to reboot (approximately one minute). The IP address (`xxx.xxx.xxx.xxx`) and subnet mask (`yy`) for each network adapter can be found within the displayed text as:

  ```
  inet xxx.xxx.xxx.xxx/yy
  ```

- If the IP address was assigned to the Nyquist System Controller by your DHCP server, the IP address can usually be determined by interrogating your DHCP server. Look for a DHCP client name of **debian** or **nq-sysctrl-003018xxxxxx** or for the System Controller's MAC address, which is available on the chassis of the System Controller and begins with `00:30:18`.

- The following PowerShell command may be able to retrieve the IP address. Replace `00-30-18-xx-xx-xx` with your Nyquist System Controller's MAC address, which is available on the chassis of the System Controller, or replace `xx-xx-xx` with the asterisk (*) wildcard character.

  ```
  Get-NetNeighbor -LinkLayerAddress 00-30-18-xx-xx-xx
  ```

  or

  ```
  Get-NetNeighbor -LinkLayerAddress 00-30-18-*
  ```

- If you do not have access to the network switch or the facility DHCP server, it might be necessary to download and install an IP scanner (e.g., Advanced IP Scanner or nmap) on your client computer to scan the network and identify the IP address. Look for the associated MAC address or a host name of "JET" in the scan results.

Changing a System Controller's IP Address

If you need to change the IP address for the Nyquist System Controller, run the Setup Assistant to reconfigure network settings.

To change the System Controller's IP Address:

Warning If your system is currently configured to use the Automatic Failover feature, you must first disable the Automatic Failover feature before you change the Server's IP address. After you change the Server's IP address, you will need to reconfigure the Automatic Failover feature.

1 Type `https://<address>/setup/network` in the web browser's address bar. Replace `<address>` with the C4000's current IP address (see *"Finding Nyquist System Controller's IP Address" on page 372*).

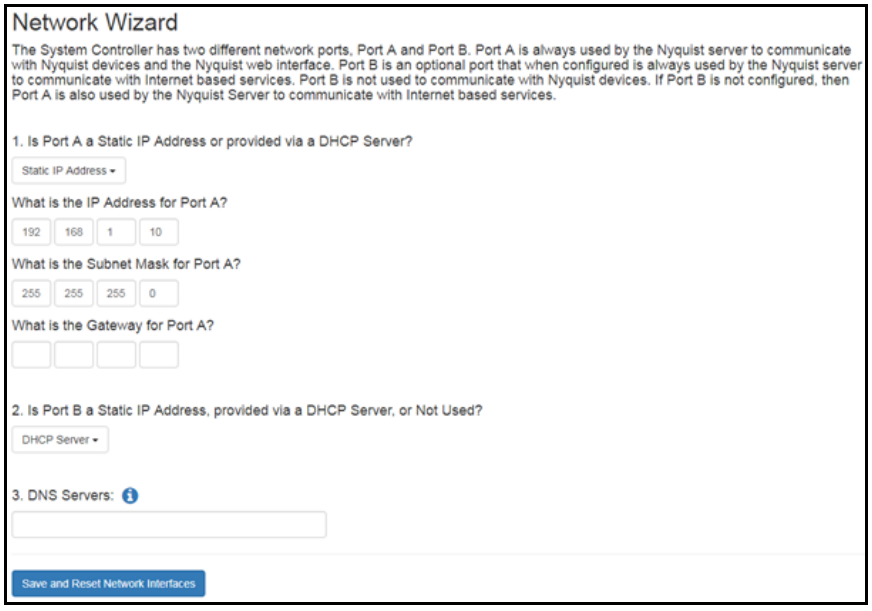


Figure 153. Network Wizard

2 Complete the wizard and select **Save and Reset Network Interfaces**.

Resetting the network interfaces will take several minutes. A progress bar will appear on the screen.

3 Log into your Nyquist server using the System Controller's new IP address.

4 On the *System Parameters* page, check the current value of **Server IP Address** to make sure it matches the new Server IP address. If it does not match, then change it to the new Server IP address.

Note: After using the Network Wizard to change the server's IP address (and/or Port-B IP address), if you have previously entered IP addresses into the **Additional IP Addresses and/or DNS names to include in the Server Certificate** field (on the System Parameters page) and you still need the server certificate to include those IP addresses, you will need to edit the System Parameters (see *"Setting System Parameters" on page 67*) and press the **Generate Server Certificate** button to re-create the certificate with the new server IP address and the additional IP addresses (see *Table 24, "System Tools," on page 78*).

Performing Tasks via the Dashboard

Note: This section is intended as a quick operations guide for personnel who use the Nyquist dashboard. For information about starting routines, refer to *"Using Routines" on page 425*. For information about managing check-in, refer to *"Manage Check-In" on page 523*. For further information about the Dashboard, refer to *"Accessing the Dashboard" on page 8*.

You can use the dashboard for most daily tasks, including, but not limited to:

- Starting intercom pages (*"Starting Pages" on page 377*)
- Recording intercom pages (*"Record Page" on page 379*)
- Starting and stopping alarms, tones, and announcements
  (*"Managing Alarms via the Dashboard" on page 388*)
  (*"Managing Tones via the Dashboard" on page 389*)
  (*"Managing Announcements via the Dashboard" on page 390*)
- Placing, answering, or disconnecting telephone calls
  (*"Managing Calls via the Dashboard" on page 393*)
- Using page exclusion (*"Using Page Exclusion" on page 399*)
- Viewing the schedules for the week (*"Viewing the Schedule for the Week" on page 401*)
- Performing audio distribution (*"Using Audio Distribution" on page 402*)
- Managing display messages (*"Managing Display Messages" on page 498*)
- Managing check-in (*"Manage Check-In" on page 523*)
- Starting routines (*"Starting and Stopping a Routine from the Admin Web UI" on page 426*)
- Control I/O Controller output contacts (*"Manually Controlling Output Contacts" on page 406*)

Which items appear on your dashboard depends on your assigned permissions and the station's CoS. (*See "Managing Roles and Users" on page 246* and *"Using CoS Configuration" on page 100*.)

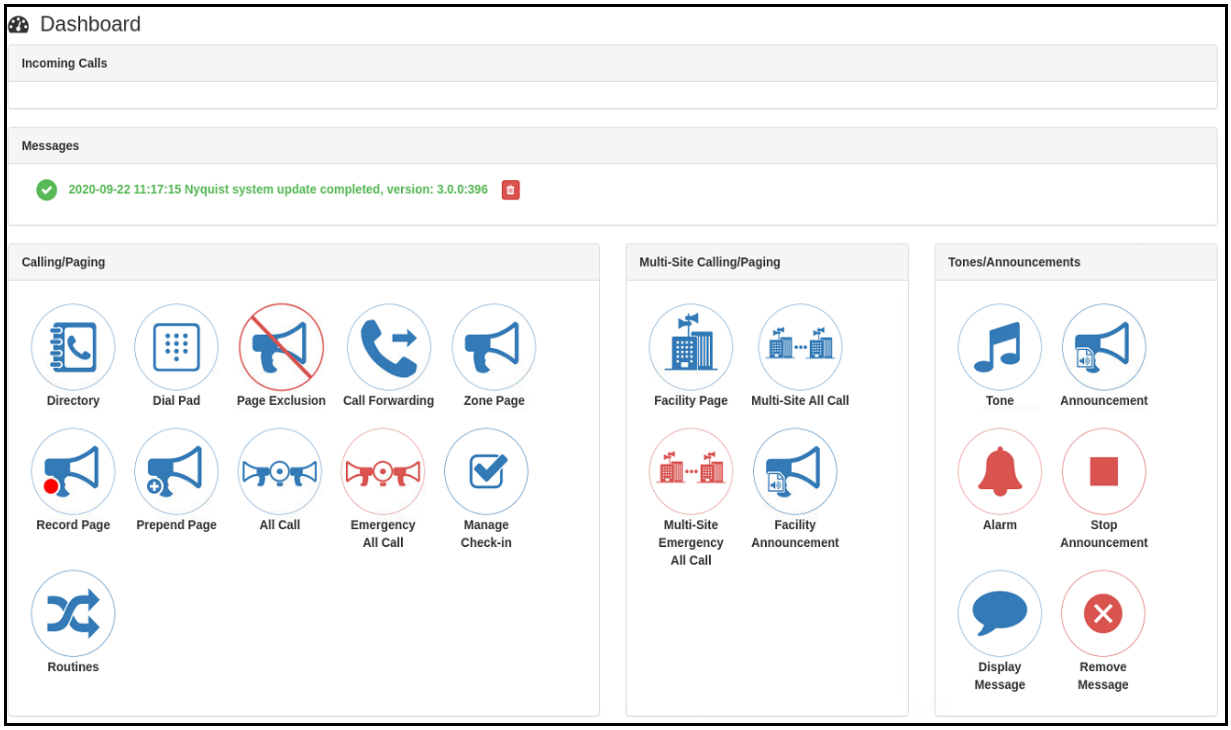


Figure 154. Nyquist Dashboard

Viewing Messages

The Dashboard displays a list of active messages about the system. These can include messages about system updates, device communications, weather alerts, or any of a number of other messages.

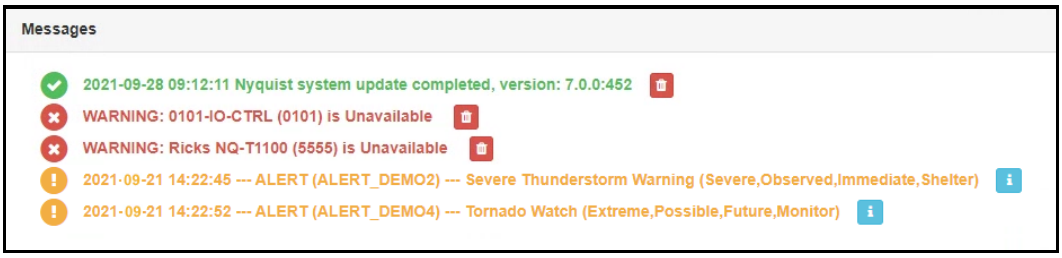


Figure 155. Dashboard Messages

To remove the message from the Dashboard, click the Delete icon next to the message. To remove all messages, restart the system (see *"Restarting the Server" on page 29*).

Weather Alert messages

When National Weather Service (NWS) alert notices are displayed, clicking the Information button to the right of any displayed alert notice will open a window entitled "National Weather Service Alerts," which displays the text of all active NWS alerts (see *Figure 156, "National Weather Service Alerts," on page 377*).

Note: The NWS Alerts text display feature depends on an executing Routine that generates NWS alerts using a Display-Msg action with the `$alerts()` variable in the Display-Msg Text field (see *"NWS Alert Routines" on page 539*) and with the POST_DASH_PHONE_TEXT parameter included in the `$alerts()` parameter list (see *"Setting Variables for the Display Message" on page 548*).

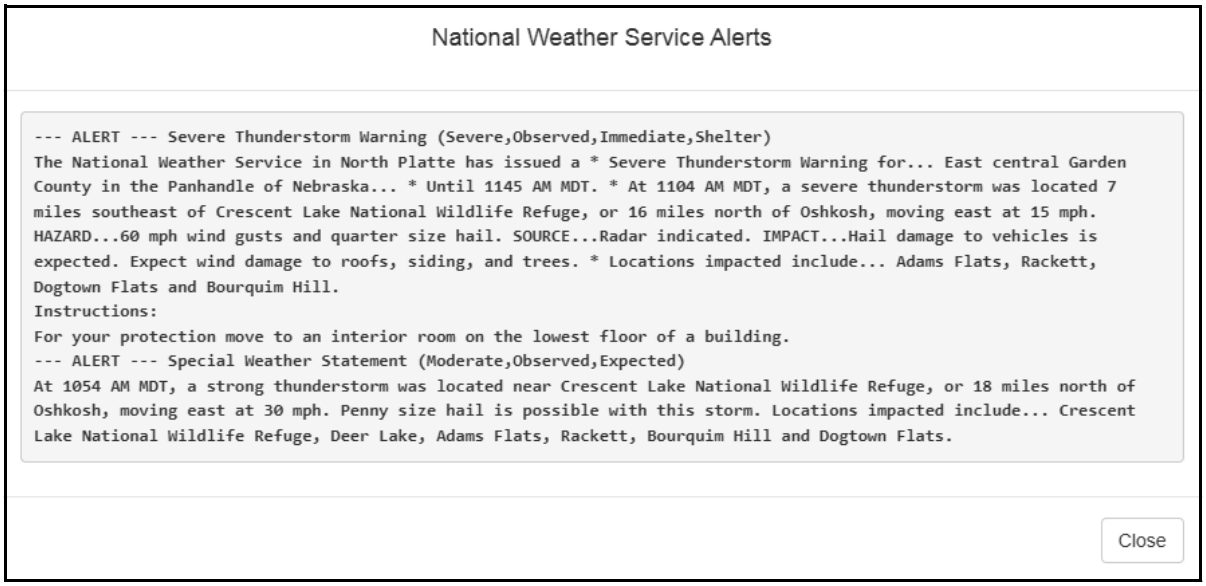


Figure 156. National Weather Service Alerts

Starting Pages

Depending on how your Nyquist system is set up, you can start Normal, All Call, and Emergency All Call pages for a specific zone, the entire facility, or multiple sites. You can also select an announcement to play before you make a page.

Single-Zone Paging

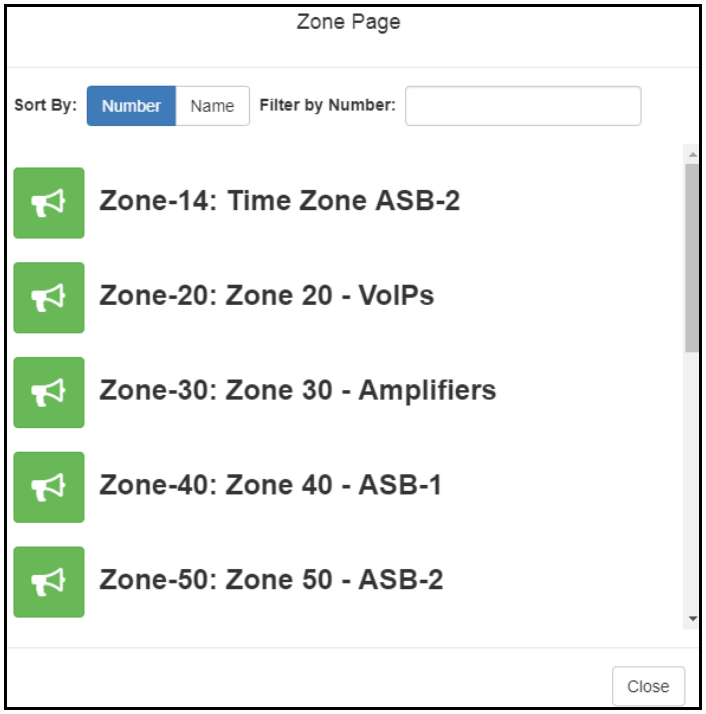


Figure 157. Paging Single Zone

To make a single-zone page via the dashboard:

1. If not already on your dashboard, select **Dashboard** from the navigation bar.
2. Under Calling/Paging, select **Zone Page**.
3. On the Zone Page popup, select the zone that you want to page.

Note: You can sort the zones by Name or Number.

4. If you must enter a password to complete this task, select **Dial Pad** and enter the 4-digit password.
5. If prompted, enter 1 for confirmation.
6. If prompted, allow Nyquist to use the microphone associated with your station.

Warning If you turn off the microphone on your computer, you cannot start audio distribution, tones, alarms, and so on. When attempting to make a call with the computer's microphone turned off, Nyquist automatically hangs up the call. If you make a second call, the dashboard displays a message that the phone is in use. Also, when the microphone is off and a bell tone comes in, Nyquist rings as opposed to auto answering.

7. After you hear the tone, speak into the microphone.
8. Select **End Call** to end the page.

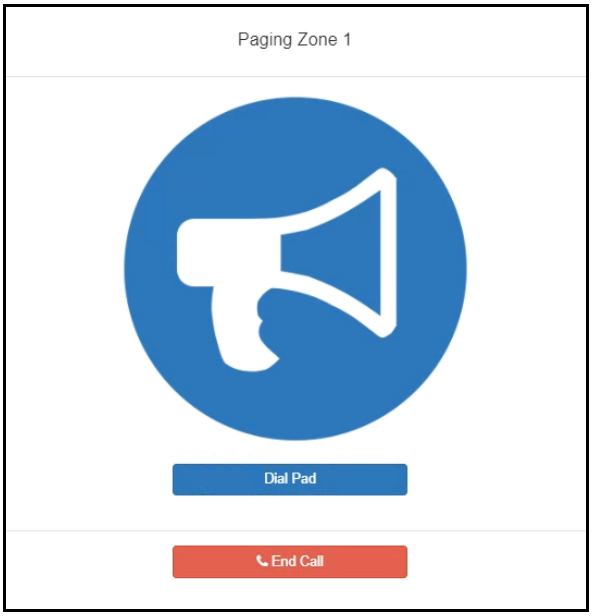


Figure 158. End Call

Record Page

You can record a page to be added to a zone queue. (For information about queues, see *"Viewing Queues" on page 227*.) The maximum recording time for a page is 60 minutes; if the recording exceeds 60 minutes, it will time out and not be saved. If the recording is silent for 60 seconds, it will time out and not be saved.

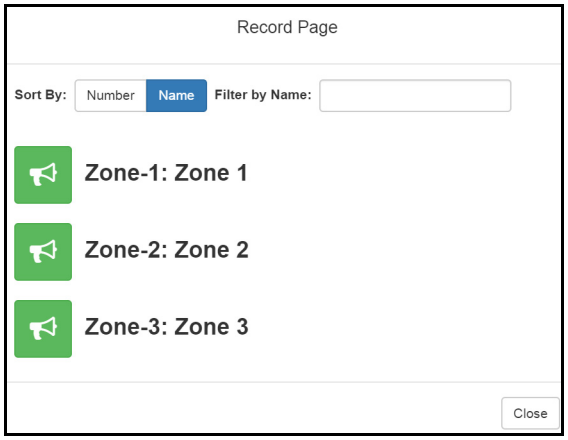


Figure 159. Record Page

The pages in the zone's queue are played in the order that they are placed in the queue.

A live page started on a zone that is playing a recorded page will cause the recorded page to be terminated and sent back to the queue. The interrupted message will play again, from the beginning of the message, when the zone becomes idle. Multi-Site Emergency-All-Call, Multi-Site All-Call, Emergency All-Call, All-Call, Alarm, Tone, and Emergency Announcement will also interrupt any playing recorded

zone messages. All re-queued interrupted messages will play again, from the beginning of the message, when the zones becomes idle.

Selecting **Disable Audio** will cause all recorded messages to stop. The messages will resume play from the beginning when audio is re-enabled.

To record a page for page queuing:

1. If not already on your dashboard, select **Dashboard** from the navigation bar.
2. Under Calling/Paging, select **Record Page**.
3. On the Record Page popup, select the zone that you want to page.

Note: You can sort the zones by Name or Number.

---

4. Wait for the prompt (if system parameter **Enable Queued Paging Instruction Message** is set to Yes) or tone (if set to No) and then record your message.
5. Hang up to end the recording.

Note: Pressing any key terminates the recording without adding the page to the queue.

Prepend Page

You can prepend a page with a special announcement. For example, if you have a prerecorded weather alert announcement, you can prepend that announcement file so that it plays first as you prepare to make a page.

Figure 160. Prepend Page

To prepend a page:

1. If not already on your dashboard, select **Dashboard** from the navigation bar.
2. Under Calling/Paging, select **Prepend Page**.

3 Select the Announcement for which you want to prepend a page.
4 On the Prepend Page popup, select the zone that you want to page.
5 If you must enter a password to complete this task, select **Dial Pad** and enter the 4-digit password.
6 If prompted, enter 1 for confirmation.
7 If prompted, allow Nyquist to use the microphone associated with your station.
8 After the prepend announcement ends, speak into the microphone.
9 Select **End Call** to end the page.

All Call Paging

All Call paging is a simultaneous page to all facility stations, unless the station has been excluded from pages. An All Call page takes higher priority over zone paging, queued zone paging, non-emergency announcements, and audio distribution. If a queued zone page is interrupted by an All Call page, the queued zone page will repeat after the All Call page is finished.

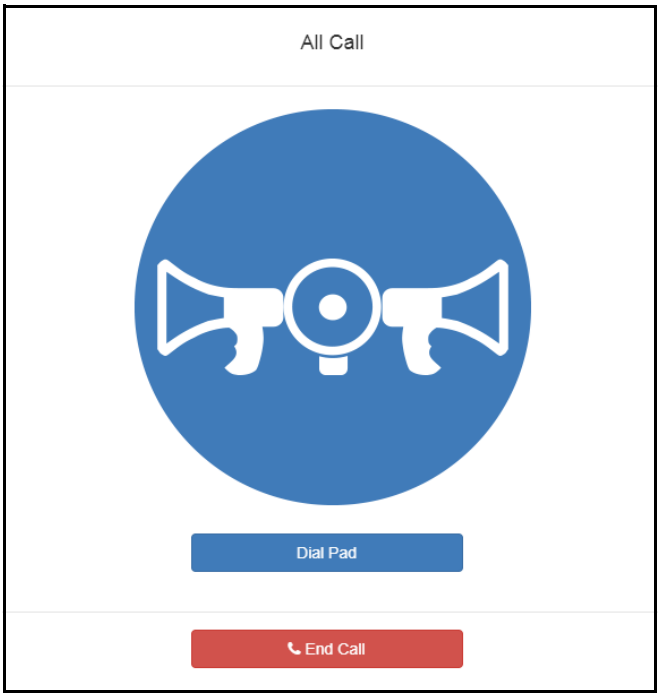


Figure 161. All Call

To start an All Call page:

1 If not already on your dashboard, select **Dashboard** from the navigation bar.
2 Under Calling/Paging, select **All Call**.
3 If you must enter a password to complete this task, select **Dial Pad** and enter the 4-digit password.
4 If prompted, enter 1 for confirmation.
5 If prompted, allow Nyquist to use the microphone associated with your station.

Warning If you turn off the microphone on your computer, you cannot start audio distribution, tones, alarms, and so on. When attempting to make a call with the computer's microphone turned off, Nyquist automatically hangs up the call. If you make a second call, the dashboard displays a message that the phone is in use. Also, when the microphone is off and a bell tone comes in, Nyquist rings as opposed to auto answering.

6 After you hear the tone, speak into the microphone.

7 Select **End Call** to end the page.

Emergency All Call Paging

An Emergency All Call page is a high priority page that is transmitted to all stations, even those stations that have been set up for page exclusion. Starting an Emergency All Call page will terminate all audio currently being played on the system (e.g. All-Call page, Zone paging, Announcements, Tones, Alarms, and Audio Distribution).

Note: Audio Distributions that are terminated by Emergency All Call pages are not resumed after the page is finished.

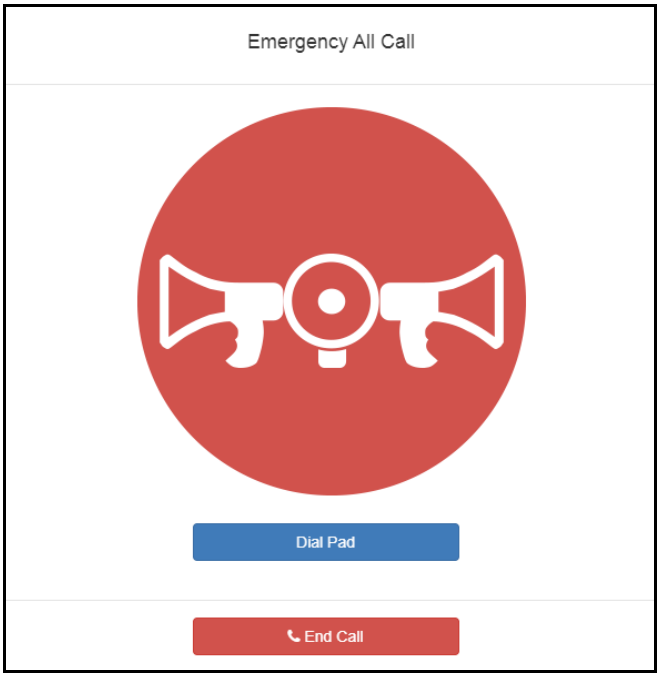


Figure 162. Emergency All Call

To start an Emergency All Call page:

1 If not already on your dashboard, select **Dashboard** from the navigation bar.

2 Under Calling/Paging, select **Emergency All Call**.

3 If you must enter a password to complete this task, select **Dial Pad** and enter the 4-digit password.

4 If prompted, enter 1 for confirmation.

5 If prompted, allow Nyquist to use the microphone associated with your station.

Warning If you turn off the microphone on your computer, you cannot start audio distribution, tones, alarms, and so on. When attempting to make a call with the computer's microphone turned off, Nyquist automatically hangs up the call. If you make a second call, the dashboard displays a message that the phone is in use. Also, when the microphone is off and a bell tone comes in, Nyquist rings as opposed to auto answering.

6 After you hear the tone, speak into the microphone.

7 Select **End Call** to end the page.

Facility Paging

If your system is configured to use multiple facilities, you can start a Facility Page. For information about configuring facilities, see *"Configuring Facilities" on page 133*.

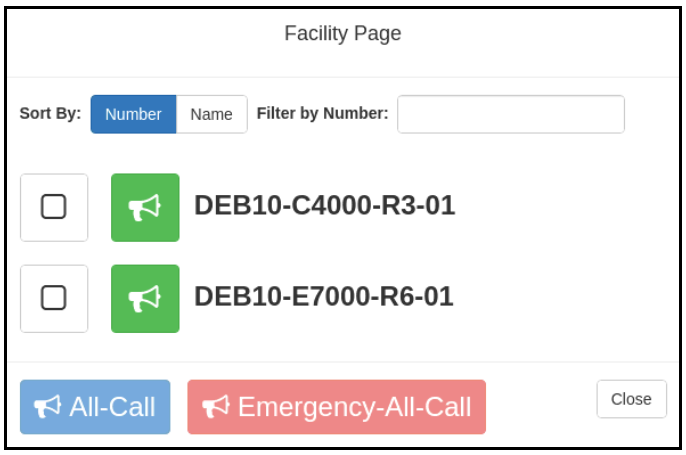


Figure 163. Facility Page

To start a facility page:

1 If not already on your dashboard, select **Dashboard** from the navigation bar.

2 Under Multi-Site Calling/Paging, select **Facility Page**.

3 On the Facilities page, select one or more facilities that you want to page. Note that you can sort and filter the facilities by Name or Number.

4 Select All-Call or Emergency-All-Call, depending on whether you want to make a normal or emergency page.

Tip: As an alternative to the previous two steps, you can select the green announcement button for a specific facility to place an immediate non-emergency page to only that facility.

5 If you must enter a password to complete this task, select **Dial Pad** and enter the 4-digit password.

6 If prompted, enter 1 for confirmation.

7 If prompted, allow Nyquist to use the microphone associated with your station.

Warning If you turn off the microphone on your computer, you cannot start audio distribution, tones, alarms, and so on. When attempting to make a call with the computer's microphone turned off, Nyquist automatically hangs up the call. If you make a second call, the dashboard displays a message that the phone is in use. Also, when the microphone is off and a bell tone comes in, Nyquist rings as opposed to auto answering.

8 After you hear the tone, speak into the microphone.

9 Select **End Call** to end the page.

Multi-Site All Call Paging

If your station's CoS allows multi-site paging, you can start a Multi-Site All Call page. (*See "Using CoS Configuration" on page 100* for information about setting up CoS for multi-site paging.)

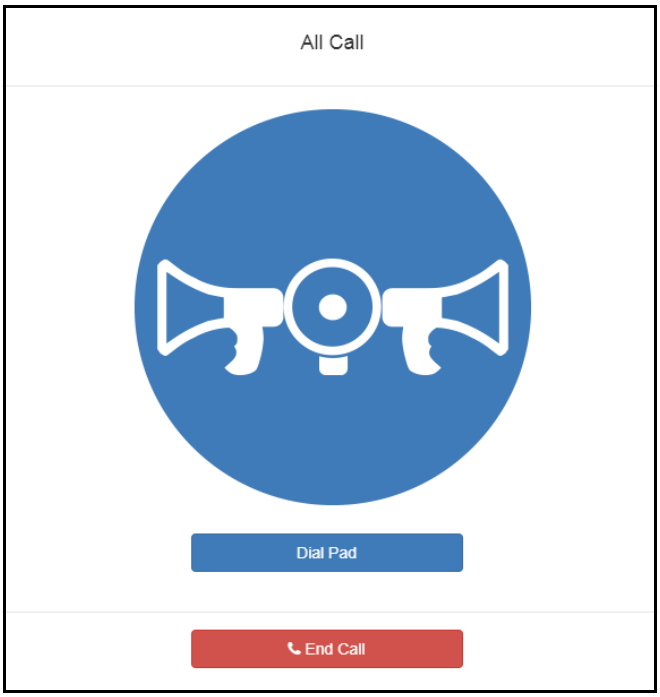


Figure 164. Multi-Site All Call

To start a Multi-Site All Call page:

1 If not already on your dashboard, select **Dashboard** from the navigation bar.

2 Under Multi-Site Calling/Paging, select **Multi-Site All Call**.

3 If you must enter a password to complete this task, select **Dial Pad** and enter the 4-digit password.

4 If prompted, enter 1 for confirmation.

5 If prompted, allow Nyquist to use the microphone associated with your station.

Warning If you turn off the microphone on your computer, you cannot start audio distribution, tones, alarms, and so on. When attempting to make a call with the computer's microphone turned off, Nyquist automatically hangs up the call. If you make a second call, the dashboard displays a message that the phone is in use. Also, when the microphone is off and a bell tone comes in, Nyquist rings as opposed to auto answering.

6 After you hear the tone, speak into the microphone.

7 Select **End Call** to end the page.

Multi-Site Emergency All Call

If your station's CoS allows multi-site paging, you can start a Multi-Site Emergency All Call page. A Multi-Site Emergency All Call page has priority over any other pages. (*See "Using CoS Configuration" on page 100* for information about setting up CoS for multi-site paging.)

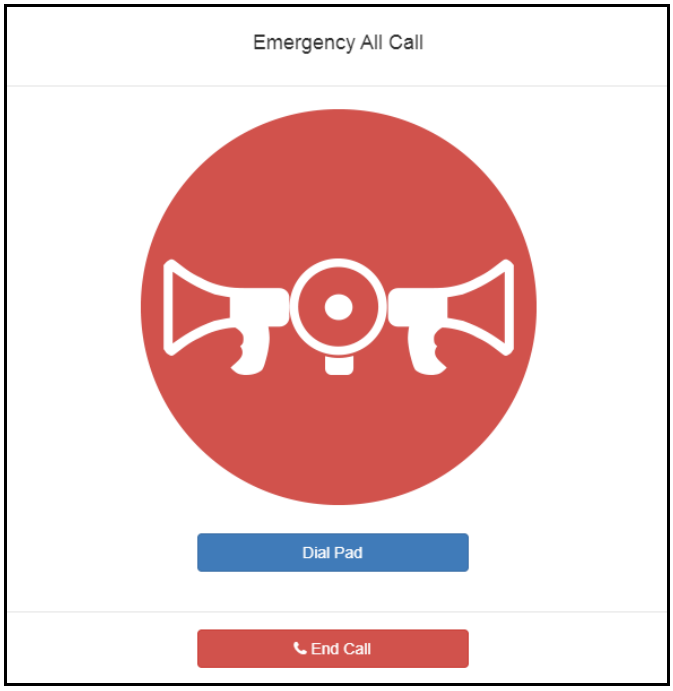


Figure 165. Multi-Site Emergency All Call

To start a Multi-Site Emergency All Call page:

1 If not already on your dashboard, select **Dashboard** from the navigation bar.

2 Under Multi-Site Calling/Paging, select **Multi-Site Emergency All Call**.

3 If you must enter a password to complete this task, select **Dial Pad** and enter the 4-digit password.

4 If prompted, enter 1 for confirmation.

5 If prompted, allow Nyquist to use the microphone associated with your station.

Warning If you turn off the microphone on your computer, you cannot start audio distribution, tones, alarms, and so on. When attempting to make a call with the computer's microphone turned off, Nyquist automatically hangs up the call. If you make a second call, the dashboard displays a message that the phone is in use. Also, when the microphone is off and a bell tone comes in, Nyquist rings as opposed to auto answering.

6 When the Emergency page appears, select **OK**.

7 After you hear the tone, speak into the microphone.

8 Select **End Call** to end the page.

Backup Paging from an NQ-T1100 Admin Phone

NQ-T1100 Admin Phones include the ability to perform Paging even if the Nyquist Server is down (by using backup paging). This is a great feature if you are concerned about the Nyquist server being a single point of failure. When combined with the Backup Bell Schedule feature, in the unlikely event that the Nyquist server becomes unavailable, users will still be able to perform paging and receive bell tones.

When the user attempts to perform a Page but does not get a response from the Nyquist server, the user can perform a backup Page by using the following step on the NQ-T1100 Admin Phone.

1 Press the **Menu** button on the NQ-T1100 Admin Phone.

2 Press the **Features** button.

3 Scroll down the menu on the left side of the screen, then press the **Paging List** button.

4 Select the entry for Emergency-All-Call, All-Call, or a Paging Zone.

5 Press the **Paging** button, located on the bottom right of the display.

The NQ-T1100 will immediately start a Page to the selected Zone. A preannounce tone will not be played because backup paging does not support preannounce tones, but the caller will hear a tone to indicate that the Page has started.

The backup paging feature should *never* be your first choice for paging; it should *only* be used as a backup in the event that the Nyquist server is down.

The NQ-T1100 station needs to have the following CoS configured to initiate paging:

- Emergency All-Call
- All-Call Paging
- Zone Paging

Entries will only be available in the Paging List if the required CoS is enabled for the station.

How to disable the Nyquist Backup Paging feature

If you do not want the Nyquist Backup Paging feature enabled, you can add the following custom variable to the Actions and Custom Variables section of the Custom Configuration page to disable it:

```
backup_paging=disabled
```

When the feature is disable, it is disabled for all NQ-T1100 IP phones connected to the Nyquist system.

To re-enable the Backup Paging feature, use the following:

```
backup_paging=enabled
```

If you are using the NQ-T1100 web interface to manually configure the phone's paging list, you can use the following to instruct the Nyquist system to not make changes to your configuration:

```
backup_paging=custom
```

Inter-Facility Calling and Paging Passwords

Using the **Edit System Parameters** page (see *Table 23, "Edit System Parameters Page," on page 69*), you can configure the system to require that a password be entered for calling, paging, or making announcements to the local facility, remote facilities, or both. When starting pages or announcements at multiple facilities, if the local facility is included, it is quite possible for more than one password to be required—one for the local facility, one for the remote facilities—even though only one operation is being performed.

For example, both the All-Call (local) and Facility Page (remote) passwords may be required for a Multi-Site All Call Page operation. Similarly, the Emergency-All-Call (local) and Multi-Site-Emergency-All-Call (remote) passwords may be required for a Multi-Site Emergency All Call page.

To avoid this confusion, particularly when an emergency may be involved, the Nyquist system only requires one password to be entered in these scenarios. If only one of the two locations (i.e., local or remote) requires a password, the user will be prompted for that one. If both require a password, the user will be prompted for the password associated with the remote facility operation (e.g., Facility Page or Multi-Site-Emergency-All-Call password), as operations on a remote facility are typically more restricted.

Tip: To prevent accidental remote facility paging, you should set Facility-Page Password and Multi-Site-Emergency-All-Call Password to 4-digit passwords in **Edit System Parameters** (see *Table 23, "Edit System Parameters Page," on page 69*).

Managing Alarms via the Dashboard

Alarms are audio files used to indicate a situation, such as a fire. When you elect to sound an alarm, only the tones with a type of Alarm appear in the selection list.

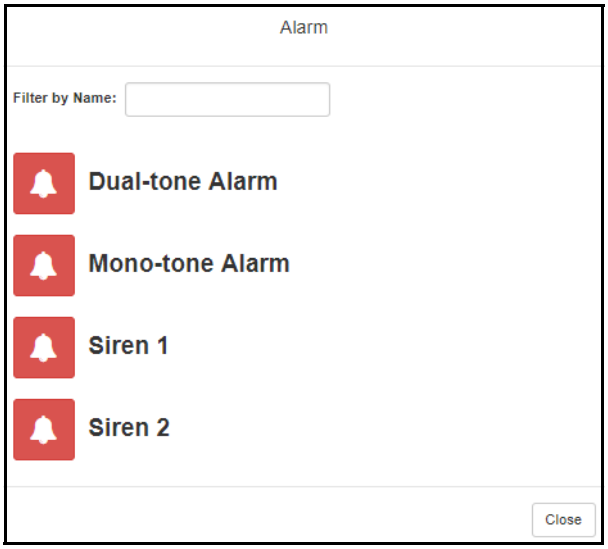


Figure 166. Alarm Page

To start and stop an alarm:

1. On the navigation bar, select **Dashboard**.
2. Under Tones/Announcements, select **Alarm**.
3. On the Alarm page, select the alarm that you want to sound.
   The **Alarm** icon changes from a red bell to a red box.
4. If you must enter a password to complete this task, select **Dial Pad** and enter the 4-digit password.
5. If prompted, enter 1 for confirmation.
6. To end the alarm, select **Stop**.

Tip: To end an alarm started by a different station, select the Dashboard's (red square) **Alarm** icon.

Managing Tones via the Dashboard

Tones are similar to alarms, but are usually used to signal an announcement or time-based event. Starting a tone sends a tone to all zones with a **Type** of Time or a combination of Time and Paging, Audio, or both.

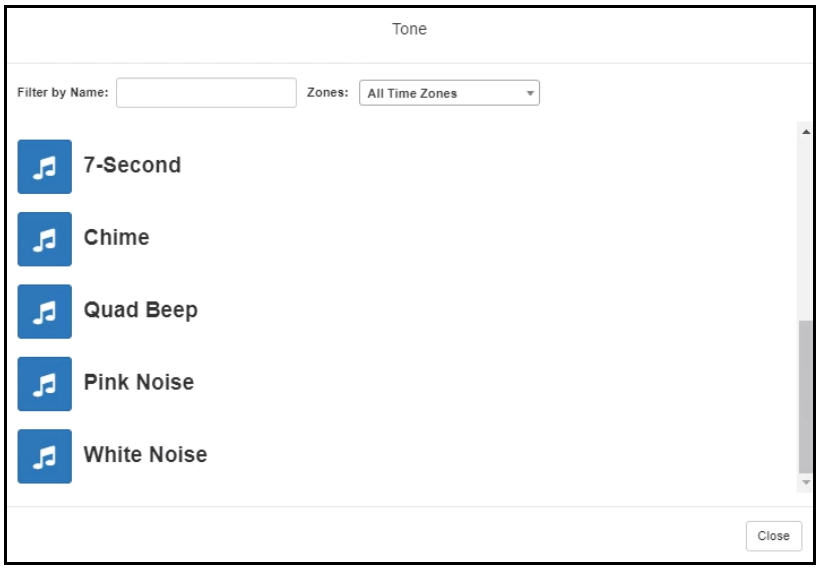


Figure 167. Tone Page

To start and stop a tone:

1. If not already on your dashboard, select **Dashboard** from the navigation bar.
2. Under **Tones/Announcements**, select **Tone**.
3. Select the zone at which you want the tone to play, or select All Time Zones.

Note: The only zones that are available are those with a **Type** of Time.

---

4. On the *Tone* page, select the tone that you want to sound.

   Only tones that have not been hidden appear. (*See "Managing Tones" on page 332* for information about hiding tones.)

Note: When a tone is started, the Tone icon on the Dashboard changes from a blue note to a red box to indicate that pressing the button will stop the Tone that is currently playing.

Note: A tone will play continuously if one of three conditions exist: its **Type** is Alarm, its **Times to Play** is set to zero (0) while using Line-Input as tone source, or its **Length** is set to zero (0).

---

5. If you must enter a password to complete this task, select **Dial Pad** and enter the 4-digit password.
6. If prompted, enter 1 for confirmation.

7 Select the **Stop** icon to end the tone.
A tone will stop playing automatically after it has reached its number of times to play. (*See "Managing Tones" on page 332.)*

Tip: To end a tone started by a different station, select the Dashboard's (red square) **Tone** icon.

Managing Announcements via the Dashboard

You can start previously recorded announcements from the dashboard and select the zone where the announcement will play.

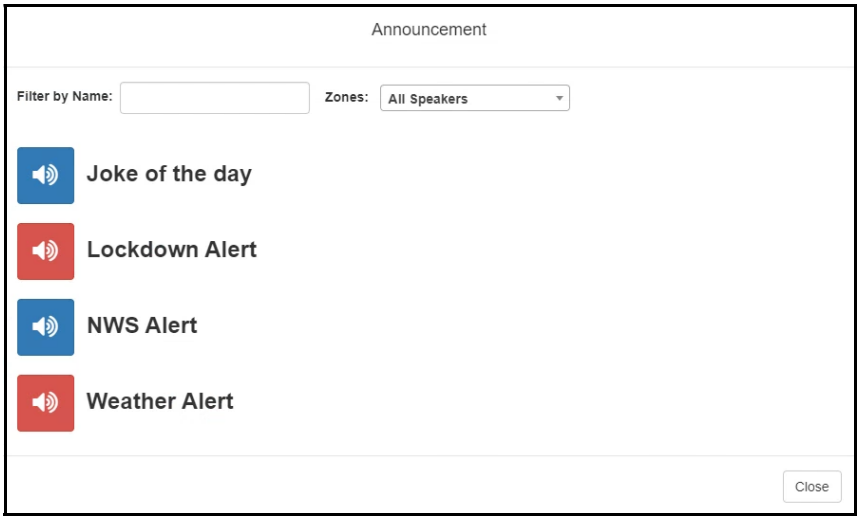


Figure 168. Announcement Page

To start and stop an announcement:

1 If not already on your dashboard, select **Dashboard** from the navigation bar.
2 Under **Tones/Announcements**, select **Announcement**.
3 On the *Announcement* page, Normal announcements display a blue icon and Emergency announcements display a red icon. Use the **Zones** drop-down menu to select the zone where the announcement will play and enter text in **Filter by Name** to search the list of announcements.
4 Select the announcement that you want to start.
5 If you must enter a password to complete this task, select **Dial Pad** and enter the 4-digit password.
6 If prompted, enter 1 for confirmation
7 To end the announcement, select **Stop** (or **Close**, if the **Dial Pad** is displayed).
8 You can also stop an announcement by performing the following steps:
   a) Under **Tones/Announcements**, select Stop Announcement.
   b) Follow screen prompts.

An announcement will end automatically after it has reached its number of times to play. (*See "Using Announcements" on page 319*.)

If multiple announcements are playing, you can select to stop a specific announcement or to stop all active announcements.

To stop an announcement when multiple announcements are running:

1. If not already on your dashboard, select **Dashboard** from the navigation bar.
2. Under **Tones/Announcements**, select **Stop Announcement**.
3. On the *Stop Announcement* page, select the announcement that you want to stop or select **Stop All Announcements**.
4. If you must enter a password to complete this task, select **Dial Pad** and enter the 4-digit password.

Facility Announcement

If your system is configured with multiple facilities, you can use the Facility Announcement feature to play a predefined announcement at any one or more facilities.

Because the announcement will play simultaneously but independently at each facility, there are several behaviors of which the user should be aware:

- The announcement will *not* be synchronized across speakers from different facilities. If there are locations that are within hearing range of speakers from more than one facility, this could result in overlapping but unsynchronized audio playback.
- When playing announcements at remote facilities, the actual Announcement Audio to be played at each facility is determined by the DTMF code of the selected announcement. If a remote facility is configured with a different Announcement Audio for that DTMF code than that of the local facility, that facility will play a different audio announcement.
- Stopping the announcement through the Dashboard will only stop the audio for the current facility. To stop the announcement at other facilities, the user must log into the Dashboard of each facility and stop the announcement using the Stop Announcement button. For this reason, it is strongly recommended that announcements *not* be configured for continuous play (i.e., "Times to Play" equal to zero) if they will be used for multi-facility announcements.

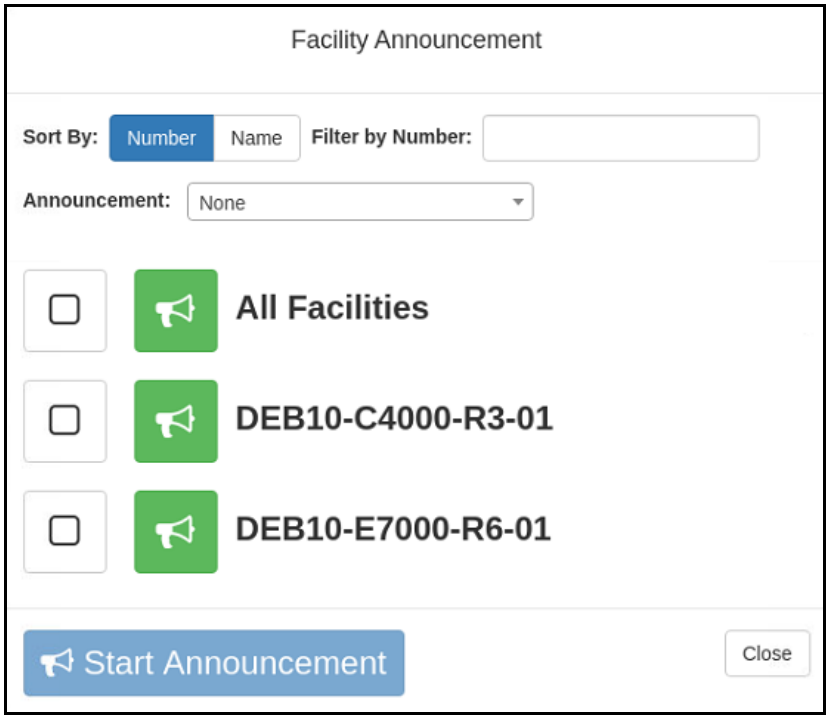


Figure 169. Facility Announcement

To start a facility announcement:

1. If not already on your dashboard, select **Dashboard** from the navigation bar.
2. Under **Multi-Site Calling/Paging**, select **Facility Announcement**.
3. Select the announcement that you want to play from the **Announcement** drop-down. The announcement type (Normal or Emergency) is displayed in parentheses.

Note: Announcements that are defined to play continuously are not available for a Facility Announcement.

---

4. Select one or more of the specified facilities at which the announcement is to be played. Selecting **All Facilities** will select all the facilities for you. Note that you can sort and filter the list of facilities by Name or Number.
5. Select the **Start Announcement** button.

Tip: As an alternative to the previous two steps, you can select the green announcement button next to a listed facility to immediately start the announcement at that one single facility.

---

6. If you must enter a password to complete this task, select **Dial Pad** and enter the 4-digit password.
7. If prompted, enter 1 for confirmation.

Warning If you turn off the microphone on your computer, you cannot start audio distribution, tones, alarms, and so on. When attempting to make a call with the computer's microphone turned off, Nyquist automatically hangs up the call. If you make a second call, the dashboard displays a message that the phone is in use. Also, when the microphone is off and a bell tone comes in, Nyquist rings as opposed to auto answering.

8 If prompted, allow Nyquist to use the microphone associated with your station.

Note: See *"Facility Announcement Priorities" on page 321* for details on how to determine if the announcement was successfully played.

9 To end the announcement at the current facility, select Stop (or Close, if the Dial Pad is displayed).

Managing Calls via the Dashboard

Receiving Calls

Receiving calls via the Dashboard is simple. When a call to the Admin's extension is received, a pop-up will appear, displaying the calling station's name and extension and prompting the user to accept (**Answer**) or reject (**Busy**) the call. To accept the call, select **Answer** and begin talking.

Important: Calls can only be received when the Dashboard is displayed. If the web interface is displaying a different page, the caller will be notified that the callee is unavailable and given the option to leave a message.

Figure 170. Incoming Call to Admin Extension

When a call placed using a station's call-switch is received, the incoming call will be displayed on the Dashboard in the Incoming Call section, displaying the calling station's name and the call priority. To accept the call, press **Answer**; to reject it, press **Busy**.

Figure 171. Incoming Call from Call-Switch

Placing Calls

Nyquist provides two ways to place a call via the dashboard:

- Through the use of a directory
- Through the use of a dial pad

If you are calling a second-generation "Digital Call Switch & Speaker" station and no one answers the call (or the station is busy), you can request a callback (see *"Requesting a Callback" on page 398* for details). The call recipient will see a flashing LED as a Callback Request Indicator (CRI) to indicate that a callback has been requested.

Note: The callback request feature is only available on a Nyquist system if the Enable Callback Request Indicator system parameter is enabled. A related parameter, Callback Request Indicator Expiration, specifies for how many hours an indicator will be displayed before it is automatically turned off (see *"Edit System Parameters Page" on page 69*).

Note: Placing intercom calls requires an Intercom License.

Placing Call Using Directory

The Nyquist directory is a list of all stations that can receive calls. These can include computers with the Admin Web UI, telephones, VoIP speakers, or digital call switches and speakers.

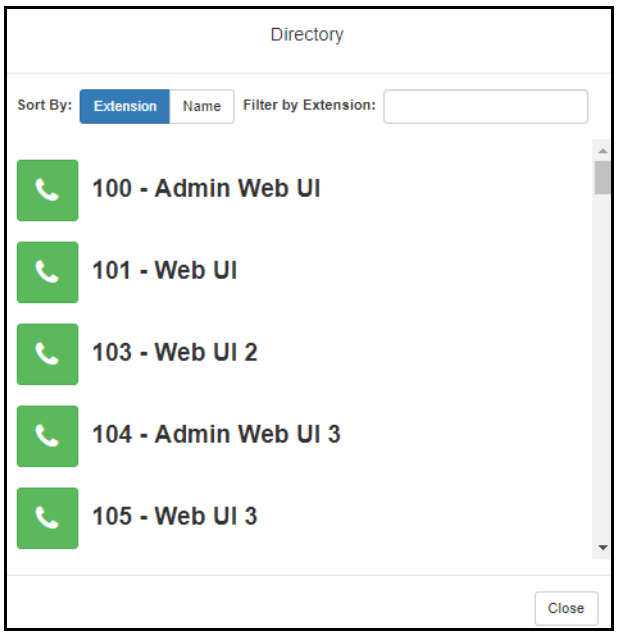


Figure 172. Directory Page

To place a call using the directory:

1. If not already on your dashboard, select **Dashboard** from the navigation bar.
2. Under **Calling/Paging**, select **Directory**.
3. On the **Directory** popup, select the extension that you want to call.
   Note that you can sort the list of extensions by extension number or name.
4. Select **End Call** to end the call.

Placing Call Using Dial Pad

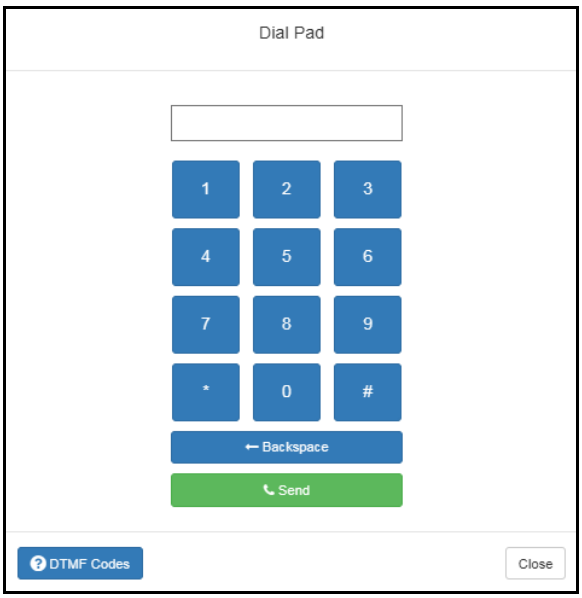


Figure 173. Dial Pad

To place a call using the Dial Pad:

1. If not already on your dashboard, select **Dashboard** from the navigation bar.
2. Under **Calling/Paging**, select **Dial Pad**.
3. Dial the extension or number that you want to call and select **Send**. To dial an external number, precede the number with the outside call prefix, 98.

Tip: Select the **DTMF Codes** button to view documentation on the available DTMF codes (see *"Nyquist DTMF Feature Dialing Codes" on page 574*).

---

4. Select **End Call** to end the call.

To answer a call from another extension:

1. If not already on your dashboard, select **Dashboard** from the navigation bar.
2. Select **Answer**.
3. Select **End Call** to end the call.

911 Dashboard Alerts

When an outbound 911 call is placed by any device in the system, a popup message dialog will be displayed on all Admin Web Interface dashboards, as shown in *Figure 174, "911 Alert," on page 397*.

Figure 174. 911 Alert

The Admin can monitor the 911 call by pressing the **Monitor** button. The popup message dialog will change to indicate that the call is being monitored, as shown in *Figure 175, "911 Monitor," on page 397*.

Figure 175. 911 Monitor

The Admin will be muted and can listen to the conversation. The Admin can press **Unmute** to join the call and be able to speak to the caller and callee.

Call Forwarding

Incoming call can be forwarded to a different station. Call forwarding can be enabled or disabled via the Dashboard or via the Admin Phone touch screen.

*To enable or disable call forwarding via the Admin Phone, do **one** of the following:*

- Touch **Menu**, touch **Features**, and touch **Call Forward**.
- Touch **Directory**, touch **Features**, and touch **Call Forwarding**.
- Touch **Features** and touch **Call Forwarding**.
- Pick up the handset and touch **Forward**.

See the *NQ-T1100 Admin Phone User Guide* for further details.

To enable or disable call forwarding from the Dashboard:

1. Ensure you are logged into the station whose incoming calls will be forwarded.
2. If not already on the dashboard, select **Dashboard** from the navigation bar.
3. Under **Calling/Paging**, select **Call Forwarding**.
4. Next to **Forward To**, select the station to which calls will be forwarded.
5. Select the desired forwarding operation:

   Always Forward: Forward all incoming calls.

   Busy Forward: Forward incoming calls received while the station is busy.

   No Answer Forward: Forward incoming calls that are not answered within 15 seconds.

   Busy or No Answer Forward: Forward incoming calls received while the station is busy or that are not answered within 15 seconds.

   Cancel Forwarding: Stop forwarding incoming calls.

   Current Forwarding Status: Play a voice announcement that identifies the current call forwarding status for the station.

An entry of type *Call Forward Setup* will be recorded to the Call Detail Records upon modifying the call forwarding settings (see *"Using the Call Details Feature" on page 362*).

Tip: If Call Forwarding is not working for a station, verify that the **Call Forwarding** CoS is enabled for that station.

Requesting a Callback

To request a callback, simply dial *7 after the call is auto-answered. If you place a call to a busy station that has a second-generation Digital Call Switch (DCS-G2), the system will ask you if you would like to initiate a callback request.

To cancel a callback request, call the station again and dial *8.

Tip: To request a callback without placing a call, dial *7<station-extension>. To cancel a request, dial *8<station-extension>.

Note: A callback request using *7<station-extension> can only be placed if the calling station's CoS has "Call Any Station" enabled and the called station has a Call-in Level of Normal+Emergency or Urgent+Emergency and is equipped with a DCS-G2.

Note: Stations placing intercom calls to remote facility stations are not able to activate the CRI feature for the remote station.

Note: Callback requests initiated by remote PBX-based callers are not supported.

Receiving and Returning a Callback

The station that receives a callback request will indicate that a callback request is pending by displaying a Callback Request Indicator (CRI)—flashing its LED once per second (the color will be the same as the station's current status).

When the station with an active callback request places a call using the call-switch, it will call the station that requested the callback.

If the station's CRI is active and the next call initiated from the station is an Emergency call, the CRI shall remain active after the Emergency Call is completed. It will also remain active if the station is restarted.

When returning a callback, if the requesting station does not answer within 60 seconds, the call will either be terminated (for a non-Admin Station) or the call will be forwarded to the caller's admin group (for an Admin Station), and the CRI deactivated.

Using Page Exclusion

You can exclude stations from paging except for alarms, emergency announcements, and emergency pages. Alarms, Emergency All-Call pages, Multi-Site Emergency All-Call pages, and Emergency Announcements to all speakers will be sent to and heard at the station even if that station is set to exclude paging. The following are not sent to the station: All-Call Page, Multi-site All-Call Page, Zone Page, Facility Page, Facility Zone Page, Recorded Page, Prepended Page, Tones, Announcements (normal, emergency to zones), and Facility Announcements (normal, emergency to zones).

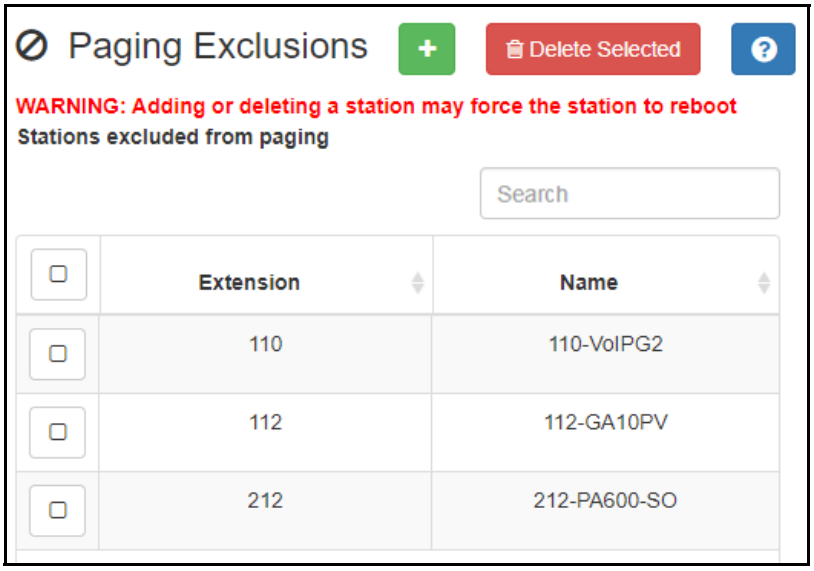


Figure 176. Paging Exclusions Page

To exclude a station from paging via the dashboard:

1. If not already on your dashboard, select **Dashboard** from the navigation bar.
2. Under **Calling/Paging**, select **Page Exclusion**.
3. Optionally, filter the displayed list of stations by extension or name.
4. Select one or more stations to be excluded. Click **Toggle All** to select (or deselect) the entire list of stations.
5. Select the **Add Exclusions** button to add the selected stations to the **Page Exclusions** list.

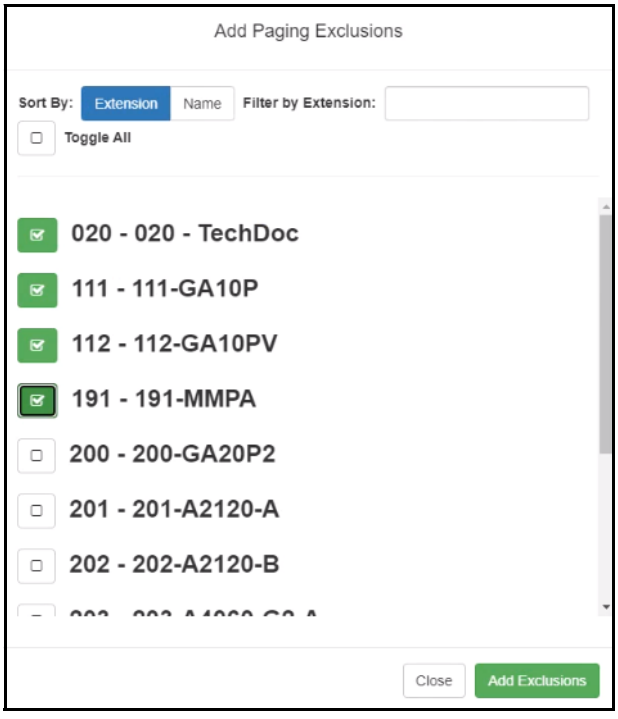


Figure 177. Add Paging Exclusion Page

Tip: You can also add or remove stations to or from the Paging Exclusion list using the Page-Exclusion Routine Action (see *Table 2, "Routine Action Type-Specific Parameters," on page 588*).

Warning Adding or deleting a station from the page exclusions list may force the station to reboot.

Deleting From Page Exclusion List

To delete an extension from the Page Exclusion list:

1. If not already on your dashboard, select **Dashboard** from the navigation bar.
2. Under **Calling/Paging**, select **Page Exclusion**.
3. Select one or more extensions to be deleted from the exclusion list.
   a) Optionally, toggle the checkbox in the header row above the selection checkboxes to select (or deselect) the entire list of stations.
4. When all selections are ready, click **Delete Selected** to remove the selected extensions from the list.

Viewing the Schedule for the Week

From the dashboard, you can view this week's schedule or use the **Prev** and **Next** buttons to view the schedule for other weeks. If you select a specific schedule for a day, you can also view details of that schedule.

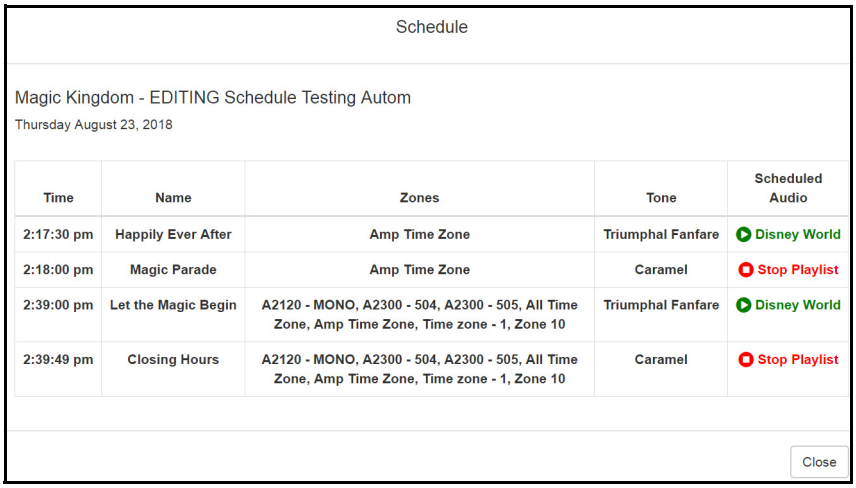


Figure 178. Schedule Popup Window

To view this week's schedule:

1. If not already on your dashboard, select **Dashboard** from the navigation bar.

2 Scroll to the **Weekly Schedule** panel.

3 To view details of a schedule, select a schedule listed, or use the **Prev** or **Next** buttons to navigate to the desired schedule and select that schedule.

The *Schedule* popup window appears. (*See "Schedule Popup Window Parameters" on page 274.*)

4 Select **Close** when done viewing.

Using Audio Distribution

Audio distribution specifies an audio program for distribution to stations or zones. It involves creating a playlist or selecting an input source and specifying which zones or stations hear the playlist or input source. Through the Scheduled Audio feature, audio distribution can be tied to a specific event in a schedule. For information about the Scheduled Audio feature, *see "Understanding Event Settings" on page 271.*

Note: Before using the Audio Distribution feature, make sure that stations and zones have been configured and that the station you are using to start Audio Distribution has the appropriate Class of Service (CoS) parameters set.

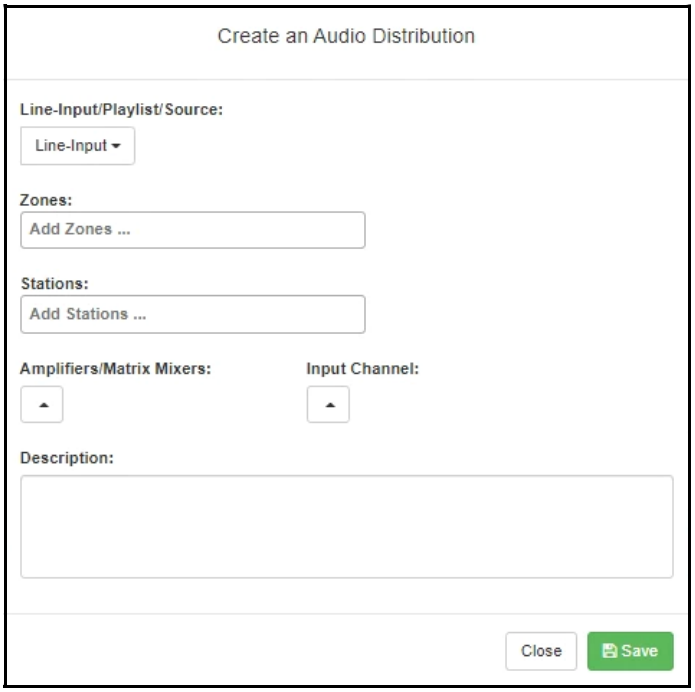


Figure 179. Create an Audio Distribution

Note: If an audio distribution playlist that has a station assigned to it is playing, you cannot play another audio distribution playlist with a station assigned.

To create an audio distribution:

1 If not already on your dashboard, select **Dashboard** from the navigation bar.

Note: If you are using at least one Nyquist Matrix Mixer Pre-Amp, **Line-Input** appears as a **Line-Input/Playlist/Source** option.

2 Select the **Add** icon in the **Audio Distribution** section.

3 Use the **Line-Input/Playlist/Source** drop-down menu to select the audio source. Audio sources can include a line-input from a Matrix Mixer Pre-Amp, available playlists previously created for your system, or Internet radio station sources.

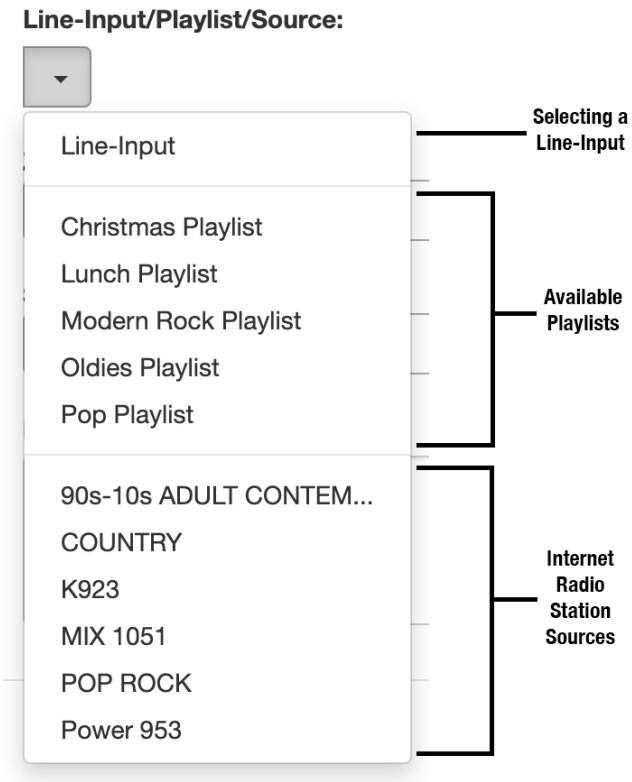


Figure 180. Audio Distribution Sources

4 Select the **Zones** and **Stations**.

5 If you select Line-Input as the **Line-Input/Playlist/Source**, specify the Amplifiers/Matrix Mixers and Input Channel.

6 If you select a playlist and want to shuffle the song order, set **Shuffle** to Yes.

7 Select **Save**.

8 To end the playing of audio, select the **Stop** icon next to the playlist.

To start a previously created audio distribution:

1 If not already on your dashboard, select **Dashboard** from the navigation bar.

2 Select the **Play** icon next to the audio distribution that you want to start.

3 If a non-blank **Audio Distribution Password** has been configured (see *Table 23, "Edit System Parameters Page," on page 69*), a keypad will be displayed and an audio prompt will request either the audio distribution password value or a confirmation (i.e., the digit 1).

4 The selected audio distribution will play.

5 To end the playing of audio, select the **Stop** icon next to the playlist.

An existing Audio Distribution can be edited or deleted, provided it is not currently playing or linked to a routine, by selecting the **Edit** or **Delete** icon next to the Audio Distribution.

When Audio Distribution is active, an informational message appears in the Messages window of the Admin Web UI dashboard indicating the audio that is currently playing, to which speakers (all or selected), and to which zones.

Audio distribution will be paused automatically by higher priority feature activation (for example, All-Call Page, Zone Paging, Announcements, Tones) and will automatically resume when the higher priority feature is finished.

Audio Distribution may also be started or stopped using Admin Phones. (Audio Distribution is available on the NQ-T1100 and NQ-ZPMS Admin Phones by selecting the Audio Distribution key and then selecting the desired Audio Distribution from the displayed menu.)

Audio Distribution volume to all speakers can be changed by setting **Audio Distribution Cut Level**, available in *System Parameters*. The Audio Distribution volume to zones can be changed by setting **Audio Distribution Cut Level** in **Edit Zone**. For information about editing a zone, see *"Editing Zone Configuration" on page 219*. Audio Distribution volume can also be changed using the Zone Control feature (see *"Zone Control: Volume and Audio Distribution Panel" on page 344*).

All Nyquist stations are preconfigured to receive Audio Distribution to All Speakers (stations). To disable Audio Distribution to All Speakers for a specific station, change **Audio Distribution to All Speakers** to **No** on the *Edit Station* page.

Any Admin Web Interface or Admin Phone user may start or stop an Audio Distribution if their station has the **Audio Distribution** CoS Configuration parameter enabled.

Audio Distributions continue playing until manually stopped or until stopped by a scheduled event, I/O Controller Input rule, or Routine.

If you use a USB flash drive as storage for songs on a playlist and the USB flash drive is removed from the USB drive, the metadata for the songs and the playlist still resides in the Nyquist song list and playlist, but audio distribution cannot play the songs. The USB flash drive must remain inserted into the system to provide the system access to the songs.

Audio Distribution can be started and stopped via routines. For information about starting or stopping audio distributions via a routine, see *"Using Routines" on page 425*.

Enabling and Disabling Audio

If a station's CoS has been set up to enable and disable audio, then **Enable Audio** and **Disable Audio** icons appear in the lower section of the dashboard. These icons allow a station to control audio for the system during events such as fire alarms. Selecting **Disable Audio** stops all audio output on the system—such as Scheduled Audio, audio distribution, and paging—and prevents future audio output

until **Enable Audio** is selected. Alternatively, audio can be enabled or disabled from a Routine via the Enable-Audio or Disable-Audio actions.

If you select **Disable Audio**, you must select **Continue** when prompted to stop audio.

The **Disable Emergency All-Call and Intercom when Audio Disabled** system setting (see *Table 23, "Edit System Parameters Page," on page 69*) also affects the behavior of the Disable Audio feature. When set to **Yes**, the system will also disable Emergency All-Call pages and intercom calls, otherwise these actions will still be allowed. The default value is **No**.

When **Disable Emergency All-Call and Intercom when Audio Disabled** is set to **Yes**, the following Nyquist features will be blocked:

- Incoming calls from PSTN-based callers
- Outgoing calls to PSTN-based numbers
- Outgoing calls to 911
- Incoming DISA calls
- Intercom call from station
- All-Call
- Emergency-All-Call
- Zone Page
- Record Zone Page
- Record Message
- Facility Zone Page
- Facility Intercom Call
- Alarms
- Tones
- Multi-site Emergency All-Call
- Intercom calls to/from remote facilities
- Station monitoring (Spy)
- Audio Distribution
- Call to retrieve voicemail
- Playback Recorded Messages
- Start/Join Audio Conference

When a caller initiates one of the above features, they will hear the following message before the feature is blocked:

"Audio disabled due to fire alarm activation."

The following Nyquist features will be blocked without playing the message:

- Routine-based automatic outgoing call and announce

- Routine-based calls not initiated by an actual caller.
- Scheduled Announcements
- Scheduled Bells and Tones
- Scheduled Audio
- Zone pages from recorded pages (they get re-queued)
- Check-in

The following features are still enabled:

- Call Forwarding setup and status
- Change Bell Schedule (via DTMF or Admin phone menu)

Manually Controlling Output Contacts

If you are using the Nyquist I/O Controller to recognize third-party contact closures, you can manually control output contacts.

Prerequisites for using manual controls are (1) adding an I/O Controller as a station and (2) configuring a controller rule for at least one output contact with the Action set as Manual. (See *"Configuring I/O Controller Output Rules" on page 164*.)

Figure 181. Output Control Section

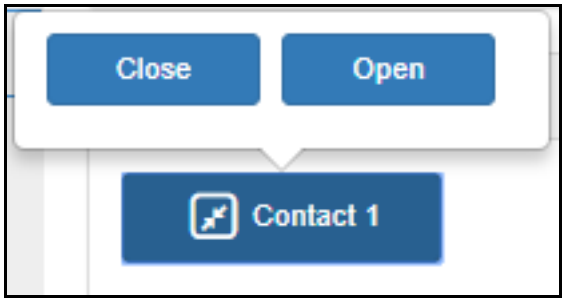


Figure 182. Manual Control Buttons

To manually control an output contact:

1. If not already on your dashboard, select **Dashboard** from the navigation bar.
2. In the **Output Contact Control** section, select the desired contact.

Note: If you have set up a rule with a duration of zero (0), then selecting the contact displays two buttons—one for opening and one for closing the circuit. If duration is set to a number other than zero (0), you can only close the circuit.

---

3. Select the button for the action that you want. The button labels are set in the rule for the output contact.

Using the Maps Feature

With the Maps feature, you can select rooms, buildings, or other defined areas, such as loading zones, from a graphic image to start intercom calls or pages. You can use the Maps view to display check-in status, listen to specific areas, and if the area has a camera, view video of the area. You can also create buttons to open a URL or execute a previously created routine.

To use the Maps feature, you must have the appropriate license and permissions (see *"Map-Based Paging License (NQ-C4000MBP)" on page 624* and *"Assigning Maps Panel Permissions" on page 409*).

When setting maps up in a Nyquist system environment, you can import JPEG or PNG graphics of your facility, buildings, rooms, or objects, such as icons or landmarks. You can then set up various defined action objects. Action objects are interactive shapes on the map that allow the starting of intercom calls, zone pages, announcements, and even routines.

Each map can have an unlimited number of levels, each level having its own image, action items, and optionally more nested levels. For example, an office administrator could navigate to the map of a building, then the map of a specific floor in that building, and then the map of a specific room on the selected floor. For locations that are frequently called or paged, a defined action object can be placed as a button on a top level or sub-level view so that navigating through multiple levels of maps is not required to initiate a call or a page. The action object button can even be configured to be viewable on all levels, which makes that object visible at every nested level of the map.

In addition, Nyquist also supports the ability to create multiple top-level maps, such as for multi-site campuses. Each site can define its own map objects and restrict calls and paging to its own administrator, as well as having its own hierarchy of nested levels.

Tip: Although the Maps feature is designed to display buttons on a map, the map image is not strictly required. You may want to create one or more "maps" or map levels that only contain buttons and behave as custom control panels. For example, a map could contain buttons to activate one or more frequently used Routines, call frequently used extensions. or page a predefined subset of facilities. Several maps of this type could be used as a customized menu of virtual dashboards, even including links to switch between menus.

Maps Panel Overview

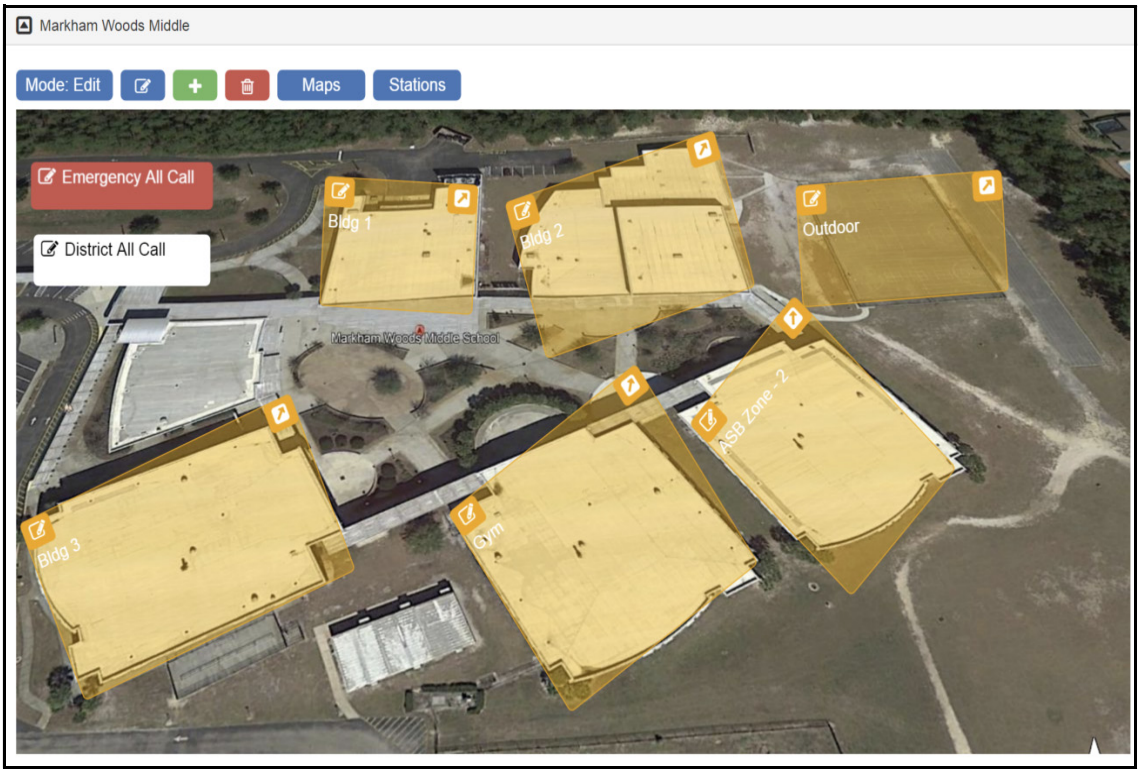


Figure 183. Maps Panel

When Maps is licensed and configured for a Nyquist system, you can view the Maps Panel from the Dashboard. In addition to the site map and defined action objects, various buttons and icons appear on the area above the graphic. These buttons can vary depending on the various parameters set for your system. Possible buttons and icons are as follows:

Indicates which mode your system is in. The **Mode** can be either **Edit** or **Live**. If you are not authorized to edit the Maps parameters or to set up defined action objects, the Mode button does not appear.

Select the **Mode** button to toggle between Edit and Live modes.

Select the **Edit** icon if you want to edit the currently displayed map. This icon does not appear if you are in **Live** mode.

Select the **Add** icon if you want to add a new map. This icon does not appear if you are in **Live** mode.

Select the **Delete** icon if you want to delete a map. This icon does not appear if you are in **Live** mode.

Select the **Maps** button to select which map you want to have appear on the Dashboard.

Select the **Stations** button to view which stations are allowed to add defined action objects or make other changes to the map. This icon does not appear if you are in **Live** mode.

Configuring Parameters for the Maps Feature

To use the Maps feature:

- You must have the Nyquist C4000 Maps-Based Paging feature license.
- You must have the correct Maps Panel permissions set.
- You must be associated to a station that has the necessary CoS configuration.
- The **Station Type** for the associated station must be an **Admin Web Interface**.
- You must select a map on the associated station.

Assigning Maps Panel Permissions

Importing graphics and creating defined action objects are restricted to users associated with roles having **Create** and **Edit Maps Panel** permissions. A user only requires **View Maps Panel** permissions to use the Maps feature for initiating pages and calls and viewing check-in status.

Note: To perform this task, you must be logged in with a role that has permission to assign or edit permissions.

To set Maps Panel Permissions:

1. On the navigation bar, select **Roles**.
2. On the *Roles* page, select the **Permissions** icon next to the role for which you are assigning or editing permissions.
3. On the *Edit <role> Permissions* page, select the appropriate buttons to assign **Maps Panel** permissions to the role.
4. Select **Save**.

Setting CoS Configurations for the Station

The **All Call** and **Emergency All Call** buttons do not appear in the Maps panel section of the Dashboard if the correct CoS parameters are not set for the station. The ability to call any station or to initiate zone paging are also set for the station through CoS Configuration.

To set CoS Parameters for the Map Feature:

1. On the navigation bar, select **CoS Configuration**.
2. Select the **Edit** icon for the CoS configuration corresponding to the target station's **Day CoS** and/or **Night CoS**.
3. Specify the desired CoS capabilities for the station. To display **All Call** and **Emergency All Call** buttons for the station, enable **All-Call Paging** and **Emergency All-Call**.

   For information about the settings, see *Table 28, "CoS Configuration Page Parameters," on page 101*.
4. After all changes are made, select **Save**.

Assigning the Default Map

Your Dashboard will not show the Maps Panel until you have selected at least one map for your station. You must assign the default map (Site) to the station first. You can then create a new map for your station.

To assign the default map:

1. On the navigation bar, select **Stations**.
2. If you are adding your station, select the **Add** icon and ensure that the **Station Type** is Admin Web Interface. Then, complete all of the options for your station.
3. If you are editing your station, select the **Edit** icon next to your station.
4. Scroll to the **Maps** parameter and select the default map.
5. Select **Save**.

Adding a Site Graphic

You can add a site graphic to your Nyquist system UI by uploading a PNG or JPEG file.

To add a graphic:

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

2 If the Site section is collapsed, expand it by clicking the down-arrow link.

3 If **Mode** is set to **Live**, select the button to toggle it to **Edit**.

Note: If you do not have create or edit permissions, the **Mode** button does not appear.

---

4 Select the **Edit** icon.

5 Enter the parameters (see *Table 126, "Edit Image Parameters," on page 411*).

6 Select **Choose file** and navigate to the desired file.

7 Select **Save**.

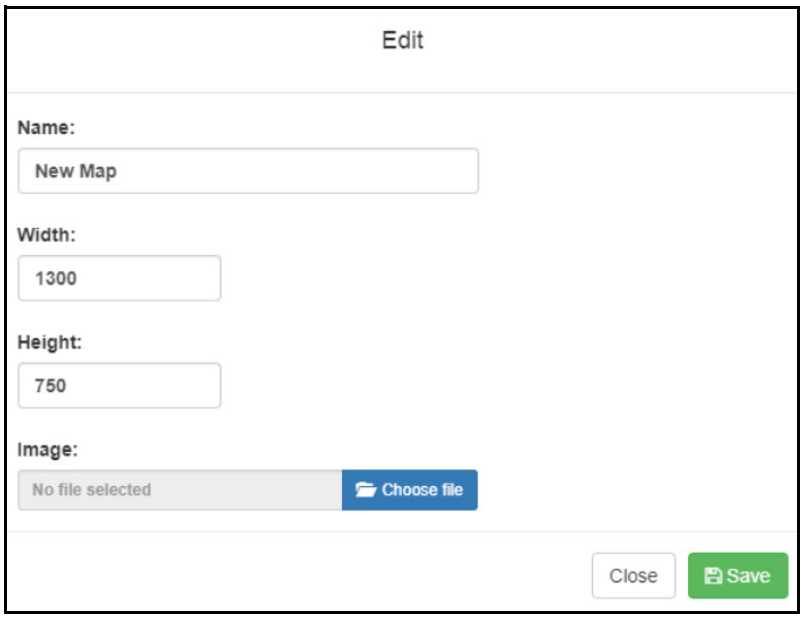


Figure 184. Edit Dialog Box

Table 126. Edit Image Parameters

Name	Enter a name for the image, such as the name of the site. The maximum character length for this parameter is 20.
Width	Enter the width for the image canvas. This width will be the canvas size for all views that appear when drilling down into the map.
Height	Enter the height for the image canvas. This height will be the canvas size for all views that appear when drilling down into the map.
Image	Displays the file name for the image. Select **Choose file** to navigate to the desired file.

Adding a Defined Action Object

After the top level graphic has been added, you can create defined action objects on the graphic map and then select image files to appear when the object is selected. For example, if your top level graphic

is a site graphic that shows multiple buildings, you might want to make each building a defined action object. Each building could then have multiple defined action objects, such as multiple zones or stations.

Note: If you move a defined action object or button outside of the map's dimensions or too far to the edge of the map image, you may not be able to use or even see the button. In this situation, you must edit the map's dimensions to view the object or button and then move it to within the map image.

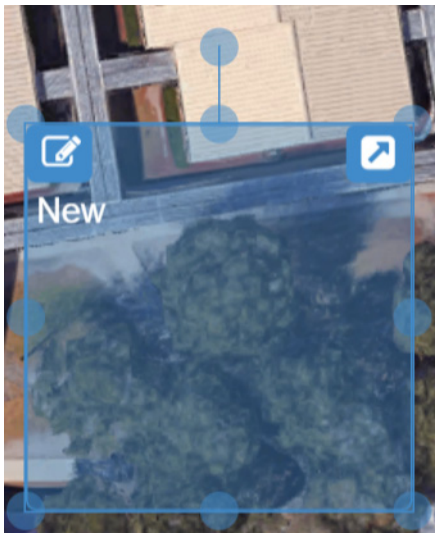


Figure 185. Defined Action Object

Note: Stations and zones must first be added to your Nyquist system before they can be added to a graphic as a defined action object.

To add a defined action object to a graphic:

1. From the dashboard, ensure the **Mode** is Edit.
2. Double-click the map. A rectangle appears.
3. Drag the rectangle to the desired location.
4. Resize the rectangle by selecting a point marked by circle and dragging the point. You can select circle outside the rectangle to rotate the image as needed.
5. Repeat steps 1–4 for each selectable object desired.

Assigning an Image to Defined Action Object

You can assign an image to a defined action object. For example, if the main image is of a site, you can add a defined action object for a building on the site graphic. The selectable object for the building can be assigned a graphic that depicts rooms inside the building.

To assign an image to a defined action object:

1. From the dashboard, ensure the **Mode** is Edit.

2 Select the arrow on the top right of the selectable object to “go into” the object.

3 Select the **Edit** icon next to the **Mode** button.

4 On the *Edit* screen that appears, provide a name for the object and then select **Choose file** and navigate to the location of the image file.

5 Select **Save**.

Editing a Defined Action Object

Editing a defined action object allows you to choose how the object appears on the Map panel and what action is assigned to the object.

Figure 186. Defined Action Object With Edit Icon (Left Corner)

To edit a defined action object:

1 From the dashboard, ensure the **Mode** is Edit.

2 Click the **Edit** icon on the selectable object.

3 Complete the *Edit Map Object* parameters (see *Table 127 on page 414*).

4 Select **Save**.

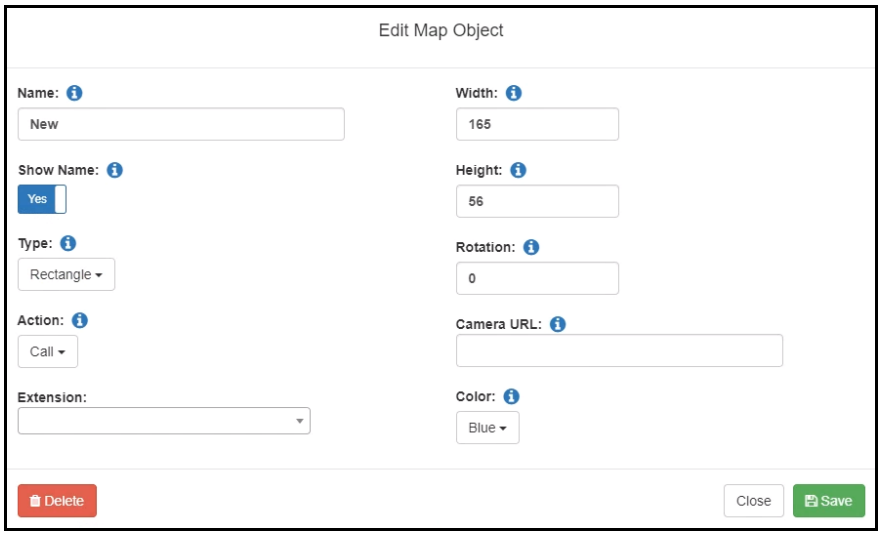


Figure 187. Edit Map Object Dialog Box

Table 127. Edit Map Object Parameters

Name	Enter a name for the selectable object. The name can have up to 40 characters.
Show Name	Select **No** if you do not want the name to appear on the map. The default is **Yes**.
View on All Levels	Select **Yes** if you want this object to appear on all levels of the current map. *Note:* This does not make the object appear on all maps, only on all levels of the current map.
Type	Select **Rectangle** if you want the object to cover a building or site. Select **Button** if you want the object to become a button that is associated with an action. For more information about buttons, see *"Creating a Defined Action Object Button" on page 416*.
Action	Select what action is to be assigned to this object. Options are: • **None**: By default, no action is associated with the object. • **Call**: If you select this option, a drop-down menu appears so that you can select an **Extension** for the object. Extensions must have previously been associated to a Nyquist system station when stations were created. • **Page**: If you select this option, a drop-down menu appears so that you can select a **Paging Zone** for this option. Zones must have previously been created and stations added to the zones before a zone can be associated to a defined action object. • **All Call**: Creates a button to use for making an All Call page. • **Emergency All Call**: Creates a button to use for making an Emergency All Call page. • **Multi-Site All Call**: Creates a button to use for making a Multi-Site All Call page. • **Multi-Site Emergency All Call**: Creates a button to use for making a Multi-Site Emergency All Call page. • **Facility All-Call Page**: Creates a button to use for making a Facility All-Call Page. If this option is selected, you must also select a **Facility**. • **Facility Zone Page**: Creates a button to use for making a Facility Zone Page. If this option is selected, you must also select a **Facility**. • **Facility Station Call**: Creates a button to use for calling a specific station in a facility. If this option is selected, you must also select a **Facility** and an **Extension**. • **Open URL**: Creates a button to use to open a URL. If this option is selected, you must also enter the web address or other web resource that you want the button to open in the **URL** field.

Table 127. Edit Map Object Parameters

	• **Execute Routine**: Creates a button that starts a specified routine. If this option is selected, you must also select the specific **Routine**. • **Select-Facility**: Creates a button with a round, selectable control, displayed in the top left corner, which can be checked or unchecked by the operator to select the associated facility. This selection will later be used when a button with the **Page-Selected-Facilities** or **Announce-Selected-Facilities** action is clicked. If this action is selected, you must also specify the associated **Facility**. • **Page-Selected-Facilities**: Creates a button used for paging all the Facilities selected via the aforementioned **Select-Facility** action. • **Announce-Selected-Facilities**: Creates a button used for playing an announcement at all the Facilities selected via the **Select-Facility** action. • **Page-Facilities**: Creates a button used to page all of the specified **Facilities**. If this action is selected, you must specify one or more **Facilities.** • **Announce-Facilities**: Creates a button used to play an announcement at all the specified **Facilities**. If this action is selected, you must specify one or more **Facilities**.
Extension	Use the drop-down menu to select an extension. This option appears only if **Action** is set to **Call**, **Page**, or **Facility Station Call**.
Width	Enter the desired width in pixels. Width must be a number 70 or above.
Height	Enter the desired height in pixels. Height must be a number 30 or above.
Rotation	Enter the desired angle of the object in degrees. The available range is 0 to 359.
Facility (or Facilities)	Use the drop-down menu to select one (or more) of the displayed facilities. This option appears only if Action is set to **Select-Facility, Page-Facilities, Announce-Facilities, Facility All-Call Page, Facility Zone Page,** or **Facility Station Call**.
Announcement	Use the drop-down menu to select the announcement to play. This option appears only if **Action** is set to **Announce-Facilities** or **Announce-Selected-Facilities**.
Paging Zone	Select the zone in which to play the page. This option appears only if **Action** is set to **Page**.
Zone Number	Enter the zone number of the remote facility at which to play the page. This option appears only if **Action** is set to **Facility Zone Page**.
URL	Enter the full name of the URL that you want to open when this button is clicked. This option appears only if **Action** is set to **Open URL**.
Video URL	Enter the full name of the URL for a room camera.

Table 127. Edit Map Object Parameters

Routine	Select the routine that you want to execute when this button is selected. This option appears only if **Action** is set to **Execute Routine**.
Color	Use the drop-down menu to select a color for this object. The default color is Green. Other options are: • **Blue** • **Brown** • **Gray** • **Orange** • **Pink** • **Purple** • **Red** • **White** • **Yellow**

Creating a Defined Action Object Button

Instead of associating a defined action object to a particular object on a map or a graphic, you can create a defined action object that serves as a button. For example, suppose you have layers of maps that include the buildings and each floor in a building, but you most frequently call one or two extensions. Rather than drilling down multiple maps or objects each time you call an extension, you can create a defined action object that is associated with that extension. The selectable object can be named for the extension and placed on the first level graphic.

Another reason for creating a defined action object that serves as a button would be if your Nyquist system server is managing multiple sites on a single campus. All Call and Emergency All Call pages would go to all stations on the Nyquist system. If you want to make a page to all stations of a single site in a multiple site campus, you can create a defined action object that starts a page to all stations in that site only.

Opening a URL

If you select **Open URL** as the **Action** for a defined action option button, you can use the button to open a specific web page or to reference a specific application, such as a video feed from a conference room. The full name, or path of the URL, must be entered in the URL field (see *Table 127, "Edit Map Object Parameters," on page 414*). For example, to access the main Bogen website, you would enter `http://www.bogen.com/`.

When the **Open URL** button is selected in **Live** mode, the web page opens a new tab in the browser.

Execute Routine

If you select **Execute Routine** as the **Action** for a defined action option button, you can use the button to manually start a routine.

Only routines that have been previously created, are **Enabled**, and have **Allow DTMF** set to **Yes** appear in the **Routine** list on the *Edit Map Object* popup (see *Table 127, "Edit Map Object Parameters," on page 414*).

For information about enabling routines and the **Allow DTMF** option, see *Table 132, "Routines Parameters," on page 449*.

Starting Pages and Announcements via the Map Feature

Depending on the parameters set, you can start pages to an individual zone, start pages and announcements to multiple selected facilities, start All Call pages, or start Emergency All Call pages.

Zones must be created and stations added to the zones before the zones can be associated to a defined action object or paged via the Maps feature. For information about creating zones, see *"Managing Stations, Zones, and Queues" on page 141*.

Page an Individual Zone

If the **Action** for a defined action object is set to **Page**, then a **Page** icon appears in the left side of a defined action object.

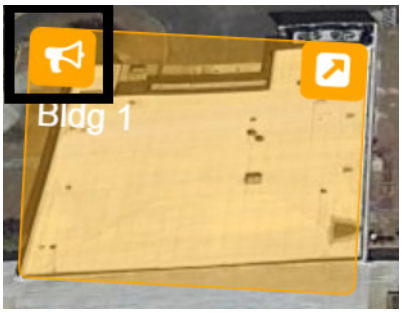


Figure 188. Page Icon

To page an individual zone using the Maps feature:

1. From the dashboard, ensure the **Mode** is **Live**.
2. Click the **Page** icon on the defined action object.

Page or Play Announcement at Multiple Selected Facilities

There are two ways in which users can page or play an announcement at multiple selected facilities simultaneously via the map. One provides a button that will page or play an announcement at a pre-defined list of facilities. The other allows the user to select one or more facilities on the map, then click a button to page or play an announcement at each of those facilities.

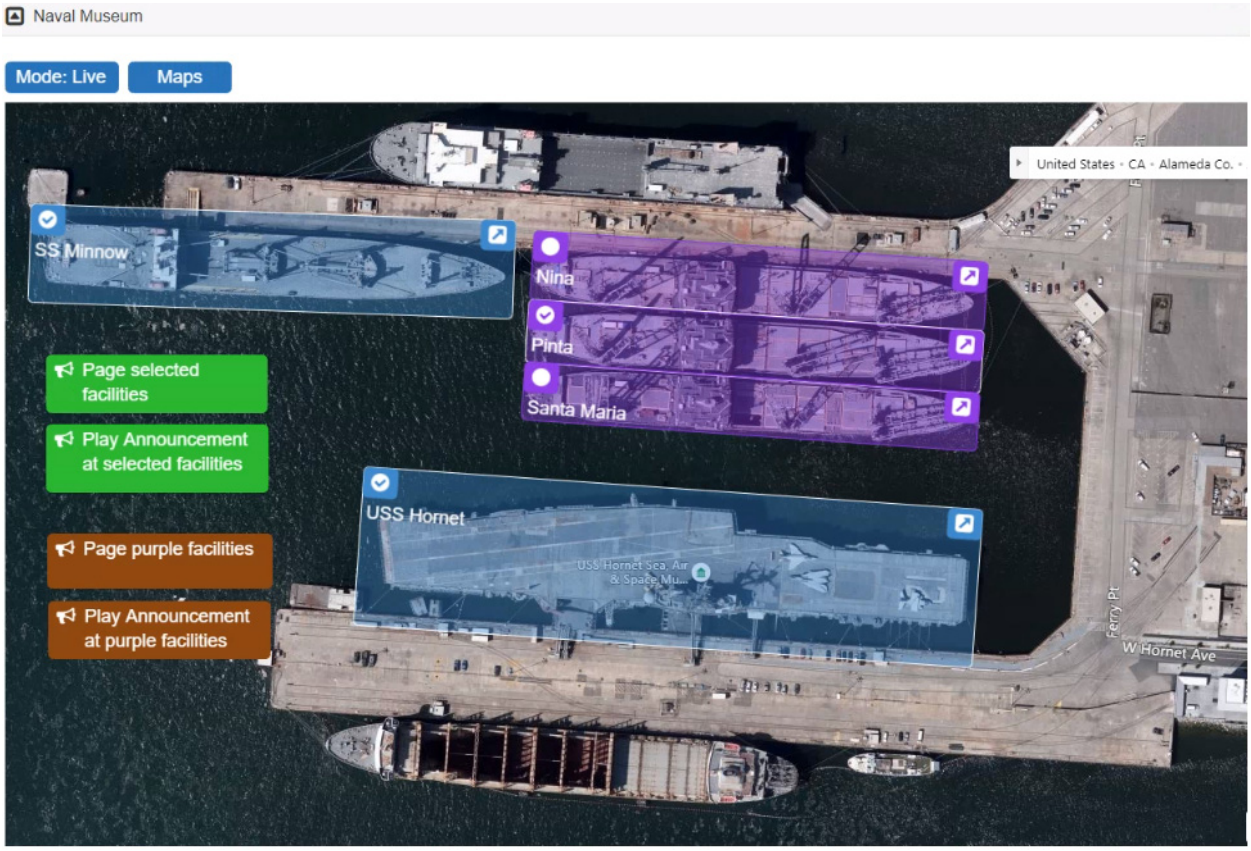


Figure 189. Paging or playing an announcement to multiple selected facilities

Page or play announcement at a predefined list of facilities

The map must have a map object button defined with the **Page-Facilities** or **Announce-Facilities** action and one or more selected facilities, which when clicked, will page or play an announcement at the specified facilities. In the example shown in *Figure 189*, two examples are shown as small brown buttons.

To start a Facility Page or Facility Announcement:

1. From the dashboard map, ensure the map's **Mode** is Live.
2. Select the **Page-Facilities** or **Announce-Facilities** button.
3. Follow subsequent audio instructions.

Page or play announcement at a user-selected list of facilities

The map must have at least two map objects defined:

- One or more map objects with the **Select-Facility** action, each of which corresponds to a specific facility. The user can select any number of these objects to specify which facilities will receive the page or announcement. In the example shown in *Figure 189*, there are five of these map objects shown as blue and purple rectangles, each corresponding to a ship.
- One map object with the **Page-Select-Facilities** or **Announce-Select-Facilities** action, which when clicked will initiate a page or an announcement to the selected facilities. In *Figure 189*, two examples are shown as small green buttons.

To start a Selected Facilities Page or a Selected Facilities Announcement:

1. From the dashboard map, ensure the map's **Mode** is **Live**.
2. Select the circular icon in the top left corner of one or more map objects, which should then display a check mark in the circle.
3. Select the **Page-Select-Facilities** or the **Announce-Select-Facilities** button.
4. Follow subsequent audio instructions.

Start All Call or Emergency All Call Pages

CoS parameters must be set before you can create **All Call** and **Emergency All Call** buttons that will appear in the Maps panel section of the Dashboard. (See *"Setting CoS Configurations for the Station" on page 410*.)

An All Call page is made to all zones associated with your Nyquist system server unless a zone is excluded from paging. An Emergency All Call page is made to all zones associated with the Nyquist system server; page exclusion does not affect Emergency All Call pages.

If you are using the same server on a multiple site campus and do not want the pages to go to all sites, you can create a zone for all stations in an individual site.

To start an All Call or Emergency All Call page:

1. From the dashboard, ensure the **Mode** is **Live**.
2. Select either **All Call** or **Emergency All Call**.

Calling an Extension via the Maps Feature

If the **Action** for a defined action object is set to Call, then a Call icon appears in the left side of a defined action object.

Figure 190. Call Icon

To call an extension using the Maps feature:

1. From the dashboard, ensure the **Mode** is Live.
2. Click the **Call** icon on the defined action object.

If a Camera URL value was provided in the definition of the Map Object, a **Camera** icon appears on the action object (or in the hamburger menu of the object). Clicking this **Camera** icon will open a browser tab or window to the Camera URL.

To open the Camera URL using the Maps feature:

1. From the dashboard, ensure the **Mode** is Live.
2. Click the **Camera** icon on the defined action object.

Tip: Although specifically intended for a camera, the Camera URL could be any URL. For non-camera URLs, however, you probably want to use an Open URL action Map Object to avoid confusion for users.

Using Maps for Check-In

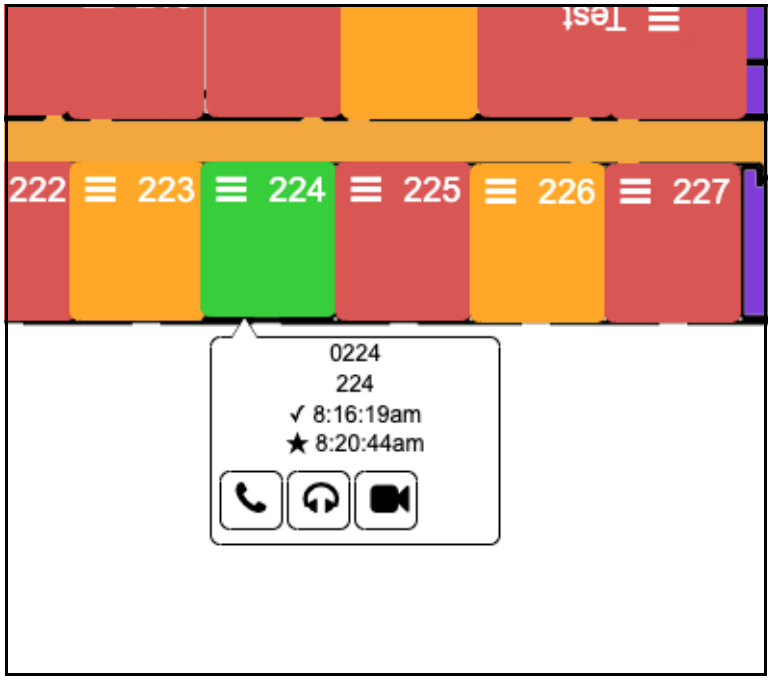


Figure 191. Maps Check-In View

From the *Maps* view, you can monitor check-in or start a routine that starts or stops check-in.

To use *Maps* for check-in, the following conditions must be met:

- You have permissions configured to view maps (see *"Assigning and Editing Permissions" on page 248*).
- Your **Station Type** is **Admin Web Interface** (see *"Editing Station Configuration Settings" on page 155*).
- Check-in has been configured for your system (see *"Configuring Check-In" on page 528*).
- You have an available map that shows the rooms or areas that you want to monitor (see *"Adding a Site Graphic" on page 410*).
- You have created a map object for each station that you want to monitor (see *"Creating a Map Object for Check-In" on page 422*).

To use a routine to start or stop check-in, the routine must have been previously created with either a trigger or an action Type of Check-In (see *"Adding a Routine" on page 450*).

Note: You can only listen in areas or rooms that allow two-way communications; in other words, the station in that room must be associated with a speaker with a microphone.

Creating a Map Object for Check-In

To create a map object for an area or room, first follow the steps for adding an action object to your map (see *"Adding a Defined Action Object" on page 411*).

To edit a defined action object:

1. From the dashboard, ensure the **Mode** is **Edit**.
2. Click the **Edit** icon on the selectable object.
3. Complete the *Edit Map Object* parameters, ensuring that **Action** is set as **Call**. (See *Table 127, "Edit Map Object Parameters," on page 414* for more information about the available parameters.
4. Select **Save**.

Note: You must create a defined action object for each room or area that you want to monitor.

Monitoring Check-In

Figure 192. Map Object in Live Mode

When a check-in is active, the Map panel changes to **Live Mode** and the map objects for all stations being monitored will no longer show the **Edit** icon. Instead, you will see icons for **Call**, **Listen**, **Video**, and **Information**.

The **Listen** icon only works if the station is associated with a speaker that allows two-way communication. The **Video** icon only works with Map objects that have been configured with a Video URL (*Table 127, "Edit Map Object Parameters," on page 414*). If the map object isn't large enough to display the icons, a hamburger menu (also known as a three-line menu or menu button) appears in the top corner.

Figure 193. Map Object With Hamburger Menu

From the hamburger menu, you can select the desired action.

During a check-in, the colors on the station map objects will change to reflect what appears on the Check-In view:

Color	Status
Green	Checked in
Red	Not checked in
Gray	Check-in is not expected because the station is on either the vacant or excluded lists.

A vacant station can check in. The text **Was Vacant** will then appear in the button information.

Using Check-In Routines from Maps View

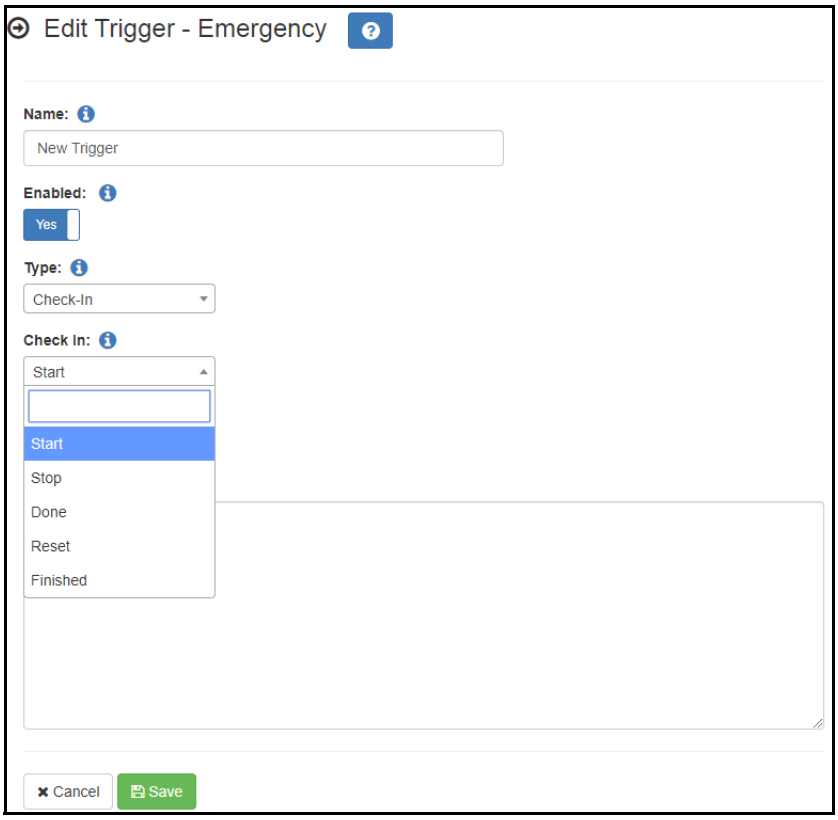


Figure 194. Check-In Options for Trigger

Provided routines have been created for either trigger or action Check-In types, you can start a routine to do one of the following:

- Start check-in.
- Stop check-in.
- Change check-in status to **Done**.
- Reset check-in status of stations.

- Change check-in status to **Finished**.

Routines must be created in the Routines view and **Execute Routine** must be selected as the Map object's **Action** (see *"Execute Routine" on page 417*).

Deleting a Defined Action Object

If you have delete permission for the Maps feature, you can delete a defined action object.

To delete a defined action object:

1. From the dashboard, ensure the **Mode** is **Edit**.
2. Double-click the **Menu** icon in the defined action object that you want to delete.
3. Select **Delete**.
4. When prompted, select **Delete** again.

Deleting a Graphic

If you have delete permission for the Maps feature, you can delete a graphic.

To delete a graphic:

1. From the dashboard, ensure the **Mode** is **Edit**.
2. Select the **Delete** icon.
3. From the *Delete Map* prompt, select **Delete**.

Using Routines

A routine automatically starts a procedure, or sequence of actions, that the Nyquist system executes as the result of an input trigger (see *Table 27, "Failover Event Routine Triggers," on page 97* and *Table 4, "Routine Trigger Types and Parameters," on page 615*). Routines can support your crisis plans for situations such as site lockdown, weather events, or emergency evacuation. They also have the ability to integrate with emergency alert systems by parsing Common Alerting Protocol (CAP) messages to display and respond to emergency messages (see *"Alert Filters Configuration" on page 535*).

Important: You should *always* run a test of a routine after creating or editing it.

A routine can be started manually via the Admin Phone or the Admin Web UI. A routine can also be automatically started:

- by an event, such as playing a specific announcement;
- via third-party switch contact closures recognized by the Nyquist I/O Controller;
- as a Scheduled Routine (see *"Using the Schedule Routines Feature" on page 283*);
- or via the Routines API that can be used by third-party systems, including fire systems, access control systems, and video security systems.

A routine that has **Allow DTMF** enabled does not need a trigger. However, most routines will have at least one associated trigger and one or more actions. For example, if an administrator manually triggers a lockdown routine, several actions could result, such as:

- Play a lockdown announcement.
- Display lockdown instructions on monitors connected to NQ-GA10PV devices.
- Close I/O controller output contacts to trigger third-party systems that lock doors.
- Initiate the check-in process.
- Start an emergency all call announcement.

To use the Routines feature, you must have the appropriate permissions (see *"Assigning and Editing Permissions" on page 248*) and the station being used to start the routine must have the CoS parameter **Execute Routines** enabled (see *"Using CoS Configuration" on page 100*).

Important: To initiate a routine from a web interface station, the station places a SIP call to the server. A microphone is required to initiate a SIP call, so a microphone must be connected to the station and enabled in the station's web browser to initiate a routine from the web interface, even if it will not be used.

To start a routine via the Routines API, you must enable **Allow API** for the routine.

You can import or export routines by selecting the appropriate button from the *Routines* view. When importing a routine, the routine file must have an SQL extension. See *"Exporting a Routine" on page 494* or *"Importing a Routine" on page 494* for more information.

Starting and Stopping a Routine from the Admin Web UI

You can manually start a Routine that has **Allow DTMF** enabled and stop a running Routine from the Admin Web UI.

To start a Routine from the Admin Web UI:

1. If not already on your dashboard, select **Dashboard** from the navigation bar.
2. Under **Calling/Paging**, select **Routines**.
3. Select one of the listed routines.
4. If you must enter a password to complete this task, select **Dial Pad** and enter the 4-digit password.
5. If prompted, enter **1** for confirmation.
6. To end the routine, select **Stop**.

Tip: To pass parameters to a Routine (i.e., `$cmdParam1` and `$cmdParam2`), use the Dial Pad and follow the same process used to start a routine from the Admin Phone (see *"Starting and Stopping a Routine from the Admin Phone" on page 426*). To pass different parameters to a Routine, use the Routines API (see *"Using the Routines API" on page 428*).

To stop a routine from the Admin Web UI:

1. If not already on your dashboard, select **Dashboard** from the navigation bar.
2. Under **Calling/Paging**, select **Routines**.
3. Select **Routines Manager**.
4. Select the routine that you want to stop (icons for running routines are red).

Note: Stopping a routine does not reverse any actions that the routine has already started. You may need to clear the actions manually.

---

5. Select **Yes**.

Starting and Stopping a Routine from the Admin Phone

You can manually start a routine that has **Allow DTMF** enabled from an Admin Phone by doing one of the following:

Note: The `*<cmdParam#>` parameters (including the preceding asterisks) are only required if the Routine uses them.

- Dial: `*94<routine-DTMF-code>*<cmdParam1>*<cmdParam2>`
- Dial: `0000094<routine-DTMF-code>*<cmdParam1>*<cmdParam2>`
- Select the **Routines** menu from the Admin Phone and then select the routine that you want to start.

Note: Only routines with **Allow DTMF** enabled appear in the menu.

The variables `$cmdParam1` and `$cmdParam2` are available to `CODE:` segments of the Routine Action's Condition field. For example:

```
CODE:
$user_var[1] = $cmdParam1;
$user_var[2] = $cmdParam2;
```

Then you can use the `$user_var[]` variables in Routine Action fields that support the use of the `$user_var[]` variables (see *Table 138, "Variables, Definitions, and Availability," on page 468*).

Note: The $cmdParam1 and $cmdParam2 variables can only be accessed from an Action's Condition field. They are *not* related to $apiParam1 and $apiParam2, which cannot be specified via the DTMF code.

For example, the following will execute Routine 123, passing 60 as `$cmdParam1` and 120 as `$cmdParam2`:

```
*94123*60*120
```

If you disconnect the call during a routine, the routine continues until finished. If the routine includes **Pause** actions, the call will not disconnect until all **Pause** actions have been executed.

A routine started from the Admin Phone may end with any of the following page commands, provided the Admin Phone has the appropriate CoS enabled:

- All-Call
- Emergency-All-Call
- Facility-Page
- Multi-Site-All-Call
- Multi-Site-Emergency-All-Call
- Zone-Page

You can stop a specific routine by dialing one of the following:

- `*95<Routine-DTMF-Code>`
- `0000095<Routine-DTMF-Code>`

Note: If the **Allow DTMF** parameter for the specified routine is set to **No**, you will be prompted to enter the system password.

Using the Routines API

The Routines API is an HTTP-based interface accessible to any client capable of making a web request. Using this interface, you can remotely start a routine from a web browser, a custom script, an application, or even a command prompt. You can even allow a third-party system, such as an access control system, to start routines.

To execute a routine using the Routines API, there are several prerequisite conditions and configuration settings.

- ☐ The Bogen Root Certification Authority certificate should be installed on the client computer (i.e., the computer making the request). For details, see *"Client Requirements" on page 8*.

Caution If certificate validation will not be enforced by the API client, this step may be skipped, but validation is strongly encouraged.

- ☐ The global **Enable Routines API** setting must be enabled on the *Routines* page (see *"Viewing Routines" on page 448*).

Important: When enabling the **Enable Routines API** setting, the *Routines API License Agreement* form will be displayed and must be completed. Provide the requested contact information and agree to the Routines API License Agreement.

- ☐ The **Allow API** setting must be enabled for the routine to be executed (see *"Editing a Routine" on page 451*).
- ☐ The station specified by the routine's **Extension** must meet the following conditions:
  - ☐ The **Station Type** setting must be "Admin Web Interface" (see *"Editing Station Configuration Settings" on page 155*).
  - ☐ The **Execute Routines** setting must be enabled for the **CoS Configuration** specified by the station's **Day CoS** and/or **Night CoS** settings (see *"Using CoS Configuration" on page 100*).
- ☐ The routine cannot end with a paging action or any call type action that requires a user to speak.

Invoking a Routine via the Routines API

There are two versions of the Routines API: v1 and v2. Both versions are supported, but there are important differences.

The primary function of the Routines API is to execute an existing Routine. A Routine can access variables specified by the API caller, but the capabilities and syntax used to retrieve variables from a v1 caller is different from that of a v2 caller. A routine designed for a v1 caller is limited to two variables—available as `$apiParam1` and `$apiParam2`—while that of a v2 caller can access far more variables—`$apiParam1` through `$apiParam20` as well as custom variables.

Using the Routines API v2, the caller can override the properties of some Actions (see *Table 3, "Routine Action Parameter Overrides via Routines API v2," on page 611*) by specifying Routine parameter values via embedded JSON structures. In addition, some Actions (e.g., Add-Announcement-Audio and

Display-Msg) can use image or audio files that are provided by the API caller, allowing extensive runtime customization of the Routine and its actions.

Both versions use the same authorization mechanism. The **Routines API Key** property, found on the *Edit System Parameters* page (see page 80), is used as a passcode, authorizing the caller to perform the specified actions. The "Authorization" HTTP header of each web request must be a string, formatted as "Bearer <passcode>".

Important: The same API Key value is used by all clients of the Routines API, so if this value is changed, all clients must be updated.

Warning The Routines API Key is an application security passcode and should be kept confidential. If this key has been compromised—such as by making a non-secure request (i.e., using HTTP instead of HTTPS), thus exposing the key in an unencrypted format over the Internet—it should be considered unsafe and should be invalidated by generating a new key using the Routines API Key's **Reset** button on the *System Parameters Edit* page (see *Table 24, "System Tools," on page 78*). All Routines API clients will subsequently need to use the new API Key value.

Routines API v2

Routines API v2 provides more functionality than Routines API v1. The routine to execute and its related data are specified via an HTTPS multipart-form POST submission.

The URL of a Routines API v2 web request uses the following form:

```
https://<server>/routine/api2
```

The routine to execute, its parameters, and any image or audio files to be used by the Routine are passed as HTTP multipart form data (i.e., encoded with a Content-Type header of `multipart/form-data`), which is comprised of key/value pairs referred to as *parts*.

The multipart form can contain:

- a part named `data`, whose value is a JSON-encoded string (or a part named `json`, whose value is a file containing a JSON-encoded string),
- parts specifying the DTMF code and/or wait flag (which can optionally be specified in the `data` or `json` part instead),
- an optional XML-encoded CAP message specified via a part named `xml`,
- and one part for each image and audio file referenced by the Routine.

The parts are described in *Table 128, "Routine API v2 request Form parts," on page 430*.

Important: Although Routines API v2 routines are available via DTMF, it is impossible to access most of the functionality using DTMF alone (because DTMF cannot specify parameters or files), which can result in unexpected and incorrect behavior. We recommend disabling the **Allow DTMF** setting for any Routine using such functionality.

Table 128. Routine API v2 request Form parts

Part	Type	Description
`data/json`	string	A JSON string (`data`) or a JSON file (`json`) that specifies the DTMF code of the routine to execute, whether or not to wait for the Routine to complete, upload file aliases, and parameter and Action override values. *Note:* If the `data` and `json` parts are both specified, the results are unpredictable. For details, see *Table 129, "Routines API v2 `data/json` part JSON elements," on page 432*. **Caution** The size of the `data` or `json` part should never exceed 5 MB. Although image and audio files are enumerated in this part, the file contents are not included here; the contents are included in their own parts, each of which should not exceed 5 MB (5×10^6 bytes).
`dtmf_code`	string	Indicates the DTMF code (as a string) of the routine to execute. If the `dtmf_code` JSON element of the `data` (or `json`) part is specified (see *Table 129, "Routines API v2 `data/json` part JSON elements," on page 432*), this part is optional. If both are specified, this part overrides the JSON element..
`wait_flag`	string	Indicates whether the call will ("1") execute synchronously and wait for the routine to complete before returning, or ("0") execute asynchronously and return immediately. If the `wait_flag` JSON element of the `data` (or `json`) part is specified (see *Table 129, "Routines API v2 `data/json` part JSON elements," on page 432*), this part is optional. If both are specified, this part overrides the JSON element.
`xml`	file	An XML-encoded CAP v1.2 file, as documented here: https://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.html Elements of this structure can be referenced within the Routine via the $CAP_* variables (see *Table 138, "Variables, Definitions, and Availability," on page 468*) or via the getCap* functions (see *"CAP Message Functions" on page 487*). *Note:* The `xml` part cannot be used in conjunction with the `data` or `json` parts.

Table 128. Routine API v2 request Form parts (continued)

Part	Type	Description
`<image>`	file	One `<image>` part must be specified for each image file (PNG or JPG) to be uploaded with the request. The value should be specified as a file (e.g., using the @ prefix in curl) and the name should match the name of the corresponding property of the `images` element (see `images` in *Table 129, "Routines API v2 `data/json` part JSON elements," on page 432*). Valid image formats include: • PNG (image/png) • JPEG (image/jpeg) An API request can include a cumulative maximum of 19 images and audio files. For example, it can contain 19 images, or 10 images and 9 audio files. The maximum size of each image file is 5 MB (i.e., 5000000 bytes).
`<audio>`	file	One `<audio>` part must be specified for each audio file (WAV or MP3) to be uploaded with the request. The value should be specified as a file (e.g., using the @ prefix in curl) and the name should match the name of the corresponding property of the `audio` element (see `audio` in *Table 129, "Routines API v2 `data/json` part JSON elements," on page 432*). Valid audio formats include: • WAV (audio/x-wav or application/octet-stream) • MP3 (audio/mpeg) An API request can include a cumulative maximum of 19 images and audio. For example, it can contain 19 images, or 10 images and 9 audio files. *Tip:* Audio files are automatically deleted from the server immediately after they are used, which means they can only be used by one Action of a Routine. If an audio file must be used by multiple Actions within a Routine, include the same file multiple times (e.g., as `audio1`, `audio2`, etc.). The maximum size of each audio file is 5 MB (5000000 bytes).

The `data` or `json` part is a JSON string or file formatted as described in *Table 129, "Routines API v2 `data/json` part JSON elements," on page 432*.

Table 129. Routines API v2 `data/json` part JSON elements

Element	Description
`dtmf_code` (optional)	If the `dtmf_code` form parameter is not specified (see *Table 128, "Routine API v2 request Form parts," on page 430*), this element indicates the DTMF code (as a string) of the routine to execute.
`wait_flag` (optional)	If the `wait_flag` form parameter is not specified (see *Table 128, "Routine API v2 request Form parts," on page 430*), this element indicates whether the call will ("1") execute synchronously and wait for the routine to complete before returning, or ("0") execute asynchronously and return immediately.
`routineApiParams`	An object containing one or more properties, each named `apiParam<n>` (where `<n>` is an integer between 1 and 20) whose value is accessible from the routine's conditions and actions via the `$apiParam1` through `$apiParam20` API parameter variables (see *"Available Condition Variables" on page 487* and *"Using Variables in Display-Msg Text" on page 478*). *Note:* The parameters `apiParam1` through `apiParam9` do not include leading zeros.
`images`	An object containing one property for each image to be uploaded in the request. Each `images` property name must match the name of the corresponding `<image>` part that specifies the actual image file (see `<image>` in *Table 128, "Routine API v2 request Form parts," on page 430*). The name and value should be identical. Each image is accessible from the Display-Msg routine action as `<imageName>`. For example, if the part containing an image file is named `logo`, it can be referenced as `logo` in the **Form Field Parameter Name** field of the Display-Msg action (with **Type** specified as **JSON-Uploaded-Image**). **Caution** Image parameter names must be unique across *all* Routines in the controller. For this reason, references to images files, such as `image01`, are not exported (see *"Exporting a Routine" on page 494*) and must be manually updated after importing. Ensure that updated parameter names are unique across all Routines.

Table 129. Routines API v2 `data/json` part JSON elements

Element	Description
`audio`	An object containing one property for each audio file to be uploaded in the request. Each `audio` property name must match the name of the corresponding `<audio>` part that specifies the actual audio file (see `<audio>` in *Table 128, "Routine API v2 request Form parts," on page 430*). The name and value should be identical. Each audio files is accessible from the Add-Announcement-Audio routine action as *`<audioName>`*. For example, if the part containing an audio file is named beep, it can be referenced as beep in the **Form-Field Parameter Name** field of the Add-Announcement-Audio action (when **Audio Source Type** is specified as JSON-Uploaded-File). **Caution** Audio parameter names must be unique across *all* Routines in the controller. For this reason, references to audio files, such as `audio01`, are not exported (see *"Exporting a Routine" on page 494*) and must be manually updated after importing. Ensure that updated parameter names are unique across all Routines.

Table 129. Routines API v2 `data/json` part JSON elements

Element	Description
`<actionType>Params`	An array of objects, each of which corresponds to an Action within the Routine whose name matches the `name` property of the object and specifies one or more Action parameters to be overridden when that Action executes. The name of the array indicates the Action Type of all items within the array (with hyphens removed and formatted in camelCase) with "Params" appended. For example, an array to override parameters of Display-Msg actions would be called `displayMsgParams`. Multiple arrays can be specified, one for each Action Type in the routine. This mechanism can be used to override parameters for the following Actions: • **Alarm** • **Display-Msg** • **Emergency-Call** • **Intercom-Call** • **New-Announcement** • **Output-Contact-Open** • **Output-Contact-Close** • **Tone** • **Urgent-Call** To view details about the parameters available for each action, see *Table 3, "Routine Action Parameter Overrides via Routines API v2," on page 611*.

Table 129. Routines API v2 `data/json` part JSON elements

Element	Description
`<custom>`	Zero or more user-defined objects and optional properties, which can be referenced within a routine's actions or conditions as `{{object}}` or `{{object.property}}`, where `object` is the user-defined object and `property` indicates the property to be referenced. Custom objects are available to the following Actions: • **Add-Announcement-Audio** (TTS and json-uploaded-file) • **Dash-Text** (text) • **Display-Msg** (text) • **Email** (subject and text) • **Log-Text** (text) • **Webhook-Post** (POST command) For example, if the `data` element is defined as: `{ dtmf_code": "12345", "wait_flag": "1", "message": "A user-defined string", "display": { "dashboard": "A property of a user-defined object" } }` the `message` element can be referenced as `{{message}}` and the `dashboard` property of the display object can be referenced as `{{display.dashboard}}` in an action's Text field.

Executing API v2 Routines from a command prompt

Let's assume that we want to execute the Routine assigned to DTMF code 1111, which accepts an image to be used by one of the Actions. We will use the following form part, `data`:

```
{
   "dtmf_code": "1111",
   "wait_flag": "1",
   "images":
   {
      "circle": "circle"
   }
}
```

If we store the JSON string in a file, Request.json, we can initiate the Routine using `curl` and prefix the Request.json file with the "less than" symbol, <, which indicates that the contents of the file should be used for the `data` part:

```
curl.exe --ssl-no-revoke -H "Authorization: Bearer <apikey>" -F data=<Request.json -F
circle=@1920x1080circle.png https://<server>/routine/api2
```

Important: The < character indicates input redirection in both the Windows command prompt and most Linux command shells. To use it with curl.exe to indicate that the contents of a file should be passed as a form part (see https://curl.se/docs/manpage.html#-F), it must be escaped. In the Windows Command Line, prefix it with the caret symbol, ^. In Linux shells, prefix it with a backslash, \. To be platform agnostic, this guide will use neither, which works in a PowerShell environment, whether Windows or Linux.

Note: PowerShell has (unfortunately) defined an alias called "curl" that maps to the Invoke-WebRequest method. To avoid it, either specify "curl.exe" or remove the alias using the following command:

```
Remove-Alias -Name curl
```

Tip: If the Bogen CA has not been installed in the current environment, curl's `--insecure` parameter can be used for testing, but should not be used for production.

Using PowerShell v7 or higher (earlier versions can access multipart forms, but it is more complicated), use the Get-Content cmdlet to retrieve the contents of the JSON file for the `data` part (all parts are provided to the Form parameter in a hashtable):

```
Invoke-RestMethod -Uri https://<server>/routine/api2 `
   -Headers @{ Authorization = "Bearer <apikey>" } `
   -Method Post `
   -Form @{ data = (Get-Content -Path Request.json -Raw); circle = (Get-Item -Path 1920x1080circle.png) }
```

We can exclude the `dtmf_code` and/or `wait_flag` from the JSON file and specify one or both as form (-F) parameters with curl:

```
curl.exe --ssl-no-revoke -H "Authorization: Bearer <apikey>" -F dtmf_code=1111 -F wait_flag=1 -F
data=<Request.json -F circle=@1920x1080circle.png https://<server>/routine/api2
```

or as hashtable entries of the Invoke-RestMethod cmdlet's Form parameter in PowerShell:

```
Invoke-RestMethod -Uri https://<server>/routine/api2 `
   -Headers @{ Authorization = "Bearer <apikey>" }
   -Method Post `
   -Form @{ dtmf_code = "1111"; wait_flag = "1"; `
            data = (Get-Content -Path Request.json -Raw); circle = (Get-Item -Path 1920x1080circle.png) }
```

Alternatively, the `json` part, a file reference, can be specified instead of the `data` part. Using curl, the `json` part must be specified by prefixing the JSON file with the @ symbol, which indicates that the file, including the file name (i.e., not just the file contents), should be sent for the `json` part.

```
curl.exe --ssl-no-revoke -H "Authorization: Bearer <apikey>" -F json=@Request.json -F
circle=@1920x1080circle.png https://<server>/routine/api2
```

In PowerShell, `json` can be specified as a FileInfo object, such as by using Get-Item:

```
Invoke-RestMethod -Uri https://<server>/routine/api2 `
   -Headers @{ Authorization = "Bearer <apikey>" } `
   -Method Post `
   -Form @{ json = (Get-Item -Path Request.json); `
            circle = (Get-Item -Path 1920x1080circle.png) }
```

The JSON text can also be provided as literal text instead of as a file. This is fairly simple using PowerShell by surrounding the JSON text with single quotes:

```
Invoke-RestMethod -Uri https://<server>/routine/api2 `
   -Headers @{ Authorization = "Bearer <apikey>" } `
   -Method Post `
   -Form @{ data = '{ "dtmf_code": "1111", "wait_flag": "1", "images": {"circle":"circle"} }'; `
            circle = (Get-Item -Path 1920x1080circle.png) }
```

If executing curl in a shell that supports single-quotes, such as PowerShell or bash, simply wrap the JSON string in single-quotes:

```
curl.exe --ssl-no-revoke -H "Authorization: Bearer <apikey>" -F
data='{"dtmf_code":"1111","wait_flag":"1","images":{"circle":"circle"}}' -F circle=@1920x1080circle.png
https://<server>/routine/api2
```

The Windows Command Prompt, however, does not support single-quoted strings. All double quotes must be escaped:

```
curl.exe --ssl-no-revoke -H "Authorization: Bearer <apikey>" -F data="{ \"dtmf_code\":\"1111\",
\"wait_flag\":\"1\", \"images\": { \"circle\": \"circle\" } }" -F circle=@925x1040circle.png
https://<server>/routine/api2
```

Tip: Windows Command Prompt commands can be split across multiple lines by ending a line with a caret (^) and pressing Enter to continue on the next line. PowerShell uses the backtick character (`) similarly. This technique may be helpful when typing long commands.

For non-trivial JSON strings, escaping all double quotes can become onerous. As an alternative, the JSON string can be specified without escape characters using the echo command and redirecting to curl via either the `json=@-` or `data=<-` syntax to receive the redirected value from stdin (for details, see https://curl.se/docs/manpage.html#-F).

Note: Note that < is a special character within the Windows Command Prompt and must be escaped with a caret (^).

```
echo {"dtmf_code":"1111","wait_flag":"1","images":{"circle":"circle"}} | curl.exe --ssl-no-revoke -H
"Authorization: Bearer <apikey>" -F data=^<- -F circle=@1920x1080circle.png https://<server>/routine/api2
```

or

```
echo {"dtmf_code":"1111","wait_flag":"1","images":{"circle":"circle"}} | curl.exe --ssl-no-revoke -H
"Authorization: Bearer <apikey>" -F json=@- -F circle=@1920x1080circle.png https://<server>/routine/api2
```

The format of the `data` and `json` subparts are specified in *Table 129, "Routines API v2 data/json part JSON elements," on page 432*.

HTTP details of the `json` part

Unlike the `data` part, the multipart HTTP Content-Disposition header for the `json` part must include the `filename` parameter.

```
Content-Disposition: form-data; name="json"; filename="myfile.json"
```

With `curl`, this can accomplished by prefixing the name of the file containing the JSON-encoded data with the @ symbol, which indicates that a file is being sent, as in:

```
curl.exe --ssl-no-revoke -H "Authorization: Bearer <apikey>" -F json=@myfile.json
https://<server>/routine/api2
```

In PowerShell v7, define the `json` part of the Form parameter as a FileInfo object using Get-Item, as in:

```
Invoke-RestMethod -Uri https://192.168.90.10/routine/api2 -Method Post `
   -Headers @{ Authorization = "Bearer <apikey>" } `
   -Form @{ json = (Get-Item -Path myfile.json) }
```

Routines API v2 Request Format

The following shows an example of a complex JSON object, which demonstrates several features of the v2 API.

```
{
   "dtmf_code": "12345",
   "wait_flag": "1",
   "images": {
      "image01": "image01",
    "image02": "image02"
   },
   "audio": {
      "beep": "beep",
      "alarm": "alarm"
   },
   "routineApiParams": {
      "apiParam1": "Display on NQ-GA10PV devices using $apiParam1 in Display-Msg action",
      "apiParam2": "Display on NQ-S1810WBC devices using $apiParam2 in Display-Msg action",
      "apiParam3": "Display on the Nyquist Dashboard using $apiParam3 in Dash-Text action",
      "apiParam4": "Include in Email message body text using $apiParam4 in Email action",
      "apiParam5": "Log this text in Log using $apiParam5 in Log-Text action",
      "apiParam20": "Up to 20 $apiParam variables can be used: $apiParam1 thru $apiParam20"
   },
   "displayMsgParams": [
      {
         "name": "WBC Message-01",
         "zones": "10",
         "stations": "",
         "priority": "4",
         "text": "LOCKDOWN",
         "displayTime": "60",
         "wbcFlasherPattern": "fast",
         "wbcFlasherCycles": "10",
         "wbcFlasherColor": "blue"
      },
      {
         "name": "Image upload",
         "deviceTypeFilter": "1",
         "priority": "6",
         "imageType": "full"
      }
   ],
   "displayText": {
      "ga10pvText1": "Lockdown initiated, follow all lockdown procedures",
      "wbcText1": "LOCKDOWN",
      "dashboard": "Lockdown initiated"
   }
}
```

This sample JSON object specifies:

- the DTMF code used to initiate the routine (`dtmf_code`);
- the wait flag, which indicates whether or not to execute the routine synchronously (`wait_flag`);
- lists of images and audio files that can be referenced by actions within the routine (`images` and `audio`);
- a list of `apiParam#` variable definitions (`routineApiParams`);
- parameter overrides for the "WBC Message-01" and "Image upload" Display-Msg actions (`displayMsgParams`);
- and a custom object (`displayText`), the properties of which can be referenced within the routine's actions.

The properties of the `routineApiParams` object can be referenced from an Action's Condition and Text properties as `$apiParam<n>`, such as `$apiParam10`.

Important: The properties of the `routineApiParams` object are the only properties from the JSON object that can be used in a Condition property.

The parameters of a Routine's Action can be overridden by declaring an array within the JSON string with a name matching the camel case version of the Action type (i.e., remove all spaces and hyphens and capitalize the first letter of each word other than the first) with "Params" appended. Each object within the array indicates an Action name and the parameters to override for that Action. For example, to override the **Zone** parameter of the New-Announcement action named "Add my announcement," specify an object with `name` set to "Add my announcement" in the `newAnnouncementParams` array and define the `zone` action parameter as "Zone1":

```
{
   "dtmf_code": "12345",
   "wait_flag": "1",
   "newAnnouncementParams": [
      {
         "name": "Add my announcement",
         "zone": "Zone1"
      }
   ]
}
```

Image and audio files are passed to the Routines API as parts of the multipart/form-data HTTP request. Each is added to the request as a form part (at the same level as the `data` or `json` part described in *Table 129*), the name of which must match the name of the corresponding item in the `image` or `audio` object specified within the `data` or `json` part. For example, if the name of the form part is `image01`, the `json.images` (or `data.images`) element must contain the item: `"image01": "image01"`.

```
{
   "dtmf_code": "12345",
   "wait_flag": "1",
   "images":
   {
      "image01": "image01",
   },
   "audio":
   {
      "audio01": "audio01",
   }
}
```

Tip: Image and audio files are automatically deleted from the server immediately after they are used. As a result, they can only be used by one Action of a Routine. If an image or audio file must be used by multiple Actions within a Routine, include the same file multiple times (e.g., as `image01` and `image02`).

An audio or image file can be referenced within an Action by selecting **JSON-Uploaded-File** for **Audio Source Type** (for an Add-Announcement-Audio action)—or by selecting **JSON-Uploaded-Image** for **Message Type** (for a Display-Msg action)—and specifying the audio or image in the **Form Field Parameter Name** property as `<audioName>` or `<imageName>`. For the previous example, we would specify `image01` and `audio01`.

Important: The maximum size of each image or audio file is 5 MB (5×10^6 bytes).

Custom properties can be defined within the JSON object and referenced from an Action's Text property as `{{<property>}}`, such as `{{displayText}}`. Nested properties can also be defined and referenced as `{{<property>.<subproperty>}}`, such as `{{messages.wbcText1}}`.

```
{
   "dtmf_code": "12345",
   "wait_flag": "1",
   "displayText": "Welcome back",
   "messages":
   {
      "wbcText1": "Greetings",
   }
}
```

Example Routine and Routines API v2 invocation

Let's look at an example of a Routine designed to be invoked via the Routines API v2. The Actions and settings for this Routine and its Actions are summarized as follows.

	Setting	Value
Routine		
	Name	Routines API v2 Test
	Extension	(any)
	Enabled	Yes
	Allow DTMF	No

	Setting	Value
	Allow API	Yes
	DTMF Code	12345
Display-Msg		
	Name	Display Image
	Type	Display-Msg
	Message Type	JSON-Uploaded-Image
	Device Type Filter	GA10PV and DSC01/WBC
	Form Field Parameter Name	`logo`
Display-Msg		
	Name	Display WBC Message
	Type	Display-Msg
	Message Type	Text
	Device Type Filter	GA10PV and DSC01/WBC
	Text	Today's message is: `{{displayText.text}}`
Webhook-Post		
	Name	Post message
	Type	Webhook-Post
	Webhook POST Command	curl.exe -d "`{{displayText.text}}`" https://bogen.request-catcher.com
New-Announcement		
	Name	Create announcement
	Type	New-Announcement
Add-Announcement-Audio		
	Name	Add announcement
	Type	Add-Announcement-Audio
	Audio Source Type	JSON-Uploaded-File
	Form Field Parameter Name	`announcement`
Play-Announcement		
	Name	Play the announcement
	Condition	$apiParam3 == "Play"

The Routine includes a Display-Msg action called "Display Image" with a **Message Type** of JSON-Uploaded-Image and **Form Field Parameter Name** of `logo`, which will display the image specified by the `logo` part of the request.

The second Display-Msg is action called "Display WBC Message" with a **Message Type** of Text and a **Text** parameter of "*Today's message is: {{displayText.wbcText}}*", which will display the caller-specified text, `displayText.wbcText`.

This Routine's final Actions will create a new announcement with New-Announcement, add the caller-specified `announcement` audio file to the announcement with Add-Announcement-Audio, and play the announcement (if `$apiParam3` has a value of "Play") with Play-Announcement.

We now create a JSON file named `DTMF12345.json` that will be used to invoke the API:

```
{
   "dtmf_code": "12345",
   "wait_flag": "1",
   "images": {
      "logo": "logo",
   },
   "audio": {
      "announcement": "announcement"
   },
   "routineApiParams": {
      "apiParam3": "Play"
   },
   "displayMsgParams": [
      {
         "name": "Display WBC Message",
         "wbcFlasherPattern": "fast",
         "wbcFlasherCycles": "10",
         "wbcFlasherColor": "blue"
      }
   ],
   "displayText": {
      "text": "Hello world",
   }
}
```

This JSON file includes the `images.logo` element referenced in the "Display Image" Display-Msg action as `logo` and the audio file referenced as `announcement` in the Add-Announcement action. It also overrides the DSC01/WBC flasher settings (i.e., pattern, cycles, and color) of the Display-Msg action named "Display WBC Message", sets the `apiParam3` parameter to "Play", and defines the custom object `displayText` with its `text` property set to "Hello world."

To initiate the Routine, send a POST command to `https://<server>/routine/api2` that includes the form field, `data`, whose value is the contents of the MyTest.json file (defined above). The POST command includes another form field, `logo`, whose value is the image file that will replace the Routine's references to `logo` with the CompanyLogo.png file.

Using curl:

```
curl.exe --ssl-no-revoke -H "Authorization: Bearer <apikey>" -F data=<DTMF12345.json -F
logo=@CompanyLogo.png -F announcement=@Hello.mp3 https://<server>/routine/api2
```

Note: In the curl syntax, the @ symbol before the file name indicates that the subsequent value is a file name, and that the file (including the file name) should be sent as the value of the named form field. The < symbol before the file name indicates that only the contents of the file should be sent. For a more complete description, see the "*-F, --form <name=content>*" section of https://curl.se/docs/manpage.html.

Using PowerShell v7+:

```
Invoke-RestMethod -Uri https://<server>/routine/api2 -Headers @{ Authorization = "Bearer <apikey>" } `
   -Method Post -Form @{ data = (Get-Content -Path DTMF12345.json -Raw); `
   logo = (Get-Item -Path CompanyLogo.png); announcement = (Get-Item -Path Hello.mp3) }
```

The Routine will be activated on the C4000. It will display the CompanyLogo.png image, display the message "*Today's message is: Hello World*" while quickly flashing the WBC's blue LED 10 times, post the message "*Hello World*" to a webhook, and play the Hello.mp3 audio file as an announcement.

Note: The status returned by a Routines API call only indicates if the API was able to initiate the Routine; it does not indicate if the Routine executed successfully or encountered errors. The `api2_log` and `nyquist_routines.log` System Log files (see *Table 120, "System Logs," on page 360*) may be helpful when troubleshooting Routines API v2 calls.

Tip: The content of HTTP requests and responses can be viewed via the api2_log (see *"Viewing System Log Files" on page 361*).

Another way to view the content of the HTTP request is to initialize a subdomain at https://requestcatcher.com; browse to that subdomain; POST requests to `https://<subdomain>.requestcatcher.com/<tag>` from curl, PowerShell, or your application (<tag> will display in the output to help identify the request); and select the received request to examine the HTTP content. Other services, such as https://beeceptor.com, allow similar functionality with configurable return values.

Dynamically Modifying I/O Controller Contacts via Routines API v2

Using the Routines API v2, it is possible to programmatically enable or disable any I/O Controller contacts. Simply define a Routine that includes the Output-Contact-Open and/or Output-Contact-Close actions, then activate it via the Routines API v2 and override the IO Controller, Output Contacts, and/or Duration for one or both Actions via the `outputContactOpenParams` and/or `outputContactCloseParams` JSON structures.

As an example, let's define a Routine that includes both Output-Contact-* Actions.

	Setting	Value
Routine		
	Name	Manipulate IO Controller
	Extension	(any)
	Enabled	Yes
	Allow API	Yes
	DTMF Code	1010
Output-Contact-Open		
	Name	Open contacts
	Type	Output-Contact-Open
	IO Controller	API-Specified
	Output Contacts	API-Specified
Output-Contact-Close		
	Name	Close contacts

Setting	Value
Type	Output-Contact-Close
IO Controller	API-Specified
Output Contacts	API-Specified
Duration	0

This Routine includes an Output-Contact-Open action and an Output-Contact-Close action. The caller can specify which switches to open and which to close via the `outputContactOpenParams.output-Contacts` and `outputContactCloseParams.outputContacts` elements of the JSON structure, as shown in the following OpenCloseIOPorts.json file.

```
{
   "dtmf_code": "1010",
   "wait_flag": "1",
   "outputContactOpenParams": [
      {
         "name": "Open contacts",
         "ioController": "332",
         "outputContacts": "4"
      }
   ],
   "outputContactCloseParams": [
      {
         "name": "Close contacts",
         "ioController": "332",
         "outputContacts": "1,2,3",
         "duration": "0"
      }
   ]
}
```

This indicates that contact 4 of I/O Controller 332 will be opened, and contacts 1, 2, and 3 will be closed. (If we only want to open or close contacts, we only need to include the appropriate elements.)

The following curl command will initiate this Routine, opening and closing the specified contacts:

```
curl.exe --ssl-no-revoke -H "Authorization: Bearer <apikey>" -F data=<OpenCloseIOPorts.json
https://<server>/routine/api2
```

The following PowerShell v7 command will do the same:

```
Invoke-RestMethod -Uri https://<server>/routine/api2 -Headers @{ Authorization = "Bearer <apikey>" } `
   -Method Post -Form @{ data = (Get-Content -Path OpenCloseIOPorts.json -Raw) }
```

Routines API v1

Important: The Routines API v1 has been extended by the Routines API v2, but is supported for backward compatibility. We recommend using the v2 API for new development.

A routine can be invoked through the Routines API v1 by sending an HTTPS GET command to the server. The specific routine to execute and several parameters are passed as part of the URL (i.e., as query parameters).

The URL of a Routines API v1 web request must take the following form:

```
https://<server>/routine/api/<dtmf-code>/0/<wait-flag>/<p1>/<p2>
```

The hostname and path parameters are:

- `<server>`: The Nyquist server's IP address.
- `<dtmf-code>`: The DTMF code of the Routine to be executed.
- `<wait-flag>`: Can be 1 (ON) or 0 (OFF). A value of 1 returns to the caller after the routine finishes (i.e., a synchronous call), while a value of 0 returns immediately after the routine starts (i.e., an asynchronous call).
- `<p1>`: A value that will replace the `$apiParam1` variable in an action field.
- `<p2>`: A value that will replace the `$apiParam2` variable in an action field.

The parameters `<p1>` and `<p2>` are passed through the URL to the routine. That routine can reference these values by using the variables `$apiParam1` and `$apiParam2` within specific fields of the Routine Actions (as well as within Routine Action Condition fields). See *Table 130, "Routine Actions and Routines API parameters," on page 447* and *Table 2, "Routine Action Type-Specific Parameters," on page 588* for details about which fields of which Routine Actions can use the `$apiParam1` and `$apiParam2` variables.

Note: Values must be provided for both `<p1>` and `<p2>`. If either or both parameters will not be used, specify a value or values of "0" (zero).

To invoke a routine, submit an HTTPS web request to the server formatted as described in *"Invoking a Routine via the Routines API" on page 428*. For example, to execute a routine associated with DTMF code `3333` on server `192.168.0.1` with a Routines API Key of `1ed163a71c6695f42035ebade76f1968` and passing '`abc`' and '`xyz`' as parameters `p1` and `p2`, either of the following examples would work.

Example 1 (curl): At a command prompt, execute the following curl command:

```
curl.exe --ssl-no-revoke -H "Accept: application/json" -H "Content-Type: application/json" -H
"Authorization: Bearer 1ed163a71c6695f42035ebade76f1968"
https://192.168.90.1/routine/api/3333/0/1/abc/xyz
```

Response text:

```
{"status":"success","message":"Test routine. p1 = abc, p2 = xyz"}
```

Example 2 (PowerShell): At a PowerShell prompt, execute the following command:

```
Invoke-RestMethod -Uri https://192.168.90.1/routine/api/3333/0/1/abc/xyz -Method Get `
   -Headers @{ Authorization = "Bearer 1ed163a71c6695f42035ebade76f1968" }
```

Response object:

```
status  message
------  -------
success Test routine. p1 = abc, p2 = xyz
```

Tip: These examples can be useful for testing a newly developed Routine. They allow you to execute it from a command line without having to initiate the actual trigger. The Routines button on the Dashboard can also be used for testing, but does not provide the ability to specify parameters.

Important: Be aware that the variables available to the Routine when invoked through the Routines API may be different than when invoked through a trigger.

The status returned by a Routines API call only indicates if the API was able to initiate the Routine; it does not indicate if the Routine executed successfully or encountered errors. The `api_log` and `nyquist_routines.log` System Log files (see *Table 120, "System Logs," on page 360*) can be used for troubleshooting Routines API v1 errors.

Backward Compatible Passwords

For backward compatibility with earlier product releases, a Routine can also be initiated by specifying the password of the user associated with the Routine's extension as a path parameter (instead of providing using the following URL format:

```
https://<server>/routine/api/<dtmf-code>/<password>/<wait-flag>
```

This technique makes it possible to initiate a Routine using a browser. Note that this format does not support the `<p1>` or `<p2>` path parameters, and it is undefined which user's password is required if more than one user is associated with the Routine's extension.

Although this request format is still supported, it is not recommended, as it is significantly less secure and risks exposure of the user's login password.

Table 130. Routine Actions and Routines API parameters

Routine Action	Routine Action field(s) able to use `$apiParam1` and `$apiParam2`
Add-Announcement-Audio	Number Text-To-Speech
Change-Volume	Cut Level
Dash-Delete	Identifier
Dash-Text	Identifier Text
Display-Msg	Identifier Text
Display-Msg-Delete	Identifier

Table 130. Routine Actions and Routines API parameters (continued)

Routine Action	Routine Action field(s) able to use `$apiParam1` and `$apiParam2`
Email	Subject Text
Log-Text	Text to log
Webhook-Post	POST command

Viewing Routines

Selecting **Routines** from the navigation bar allows you to view and edit existing routines and to create new routines.

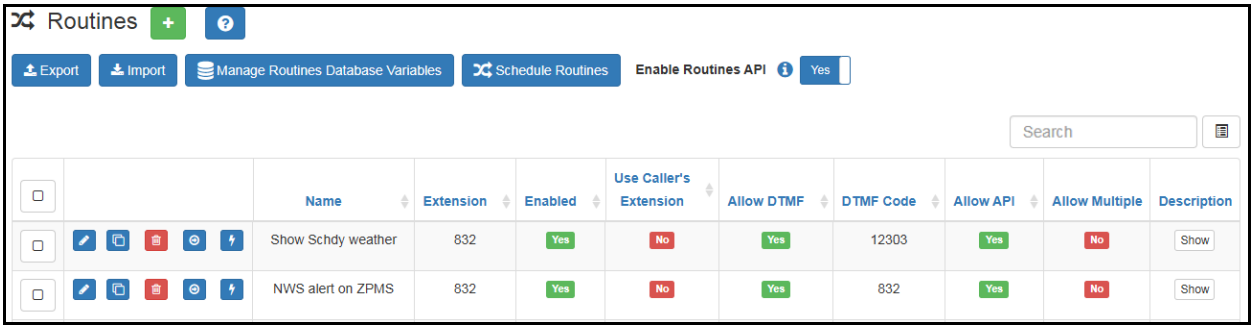


Figure 195. Routines

To view existing routines:

On the navigation bar, select **Routines**.

The Routines page includes several functions available at the top of the page, as described in *"Routines page commands" on page 448*:

Table 131. Routines page commands

Export button	Exports the selected Routines to an SQL file that can subsequently be imported to another System Controller (see *"Exporting a Routine" on page 494*).
Import button	Imports one or more Routines from a selected SQL file that was previously exported from this or another System Controller (*"Importing a Routine" on page 494*).
Manage Routines Database Variables button	Navigates to the *Manage Routines Database Variables* page (see *"Managing Routine Database Variables" on page 495*).

Table 131. Routines page commands (continued)

Schedule Routines button	Navigates to the *Schedule Routines* page (see *"Using the Schedule Routines Feature" on page 283*).
Enable Routines API	Toggle button that enables or disables ability of clients to activate routines by using a Routines API web request (see *"Invoking a Routine via the Routines API" on page 428*). *Note:* This is a system-wide setting, not specific to a routine.

The Routines page displays the following parameters for each routine:

Table 132. Routines Parameters

Triggers button	Click to select or add Triggers that will start the routine.
Actions button	Click to select or add Actions that will occur as part of the routine.
Name	Specifies the routine's name.
Extension	Specifies the station extension to use when granting CoS permissions and displaying Caller ID (e.g., the `$caller` variable). If **Use Caller's Extension** is specified, this field must be blank. *Note:* Either **Extension**, **Use Caller's Extension,** or **Allow API** must be specified. *Note:* If **Extension** is specified, the `$caller` variable will equal the **Extension** value, unless the Routine was triggered by another extension, such as via the Intercom-Call trigger, in which case `$caller` will equal the extension of the caller that placed the intercom call.
Enabled	Specifies if the routine is enabled. Routine is disabled by default.
Use Caller's Extension	Specifies that the caller's extension is to be used for granting CoS permissions and displaying Caller ID. This option may be appropriate when a routine is expected to be executed by a caller dialing a DTMF code or when a routine trigger is associated with an event that involves a caller (for example, All-Call, Zone Page) who has sufficient CoS permissions to execute the routine's actions. If either **Extension** or **Allow API** is specified, this field must not be set. This field is enabled by default. *Note:* Either **Extension**, **Use Callers Extension,** or **Allow API** must be specified.
Allow DTMF	Specifies if the routine can be manually started by dialing the routine's DTMF code from an Admin Phone. This field is disabled by default.

Tip:	It is typically safest to set **Allow DTMF** to No if **Allow API** is set to Yes and the Routines API v2 is being used to activate it, because $apiParam1 and $apiParam2 (i.e., Routines API v1 variables) are the only parameters that can be set via DTMF.

Table 132. Routines Parameters

DTMF Code	Specifies the number to use when manually starting the routine from an Admin Phone or via the Routines API. The number can have from 1 to 10 digits. You cannot assign the same DTMF code to multiple routines. A DTMF code is required if either **Allow DTMF** or **Allow API** is enabled.
Allow API	Specifies if the routine can be executed via the Routines API (see *"Using the Routines API" on page 428*). *Note:* Either **Extension**, **Use Callers Extension,** or **Allow API** must be specified.
Allow Multiple	Specifies if multiple instances of the routine can run at the same time. This field is disabled by default. When disabled, the system allows only one instance of the routine to execute at a time, regardless of how many times the routine might be triggered while already executing.
Routine Passcode	Specifies an optional four-digit passcode that, if specified, must be entered by the user at the keypad before the Routine can be executed. **Important:** This passcode is ignored when the Routine is executed via the Routines API.
Description	A description of the routine.

You can also select the **Triggers** button to select or add triggers to start the routine or select the **Actions** button to select or add **Actions** that will occur as part of the routine.

Adding a Routine

Adding a routine creates a **New Routine** on the *Routines* page. By default, this new routine is not enabled. It also has no **Triggers** or **Actions**.

To add a routine:

1. On the navigation bar, select **Routines**.
2. On the *Routines* page, select the **Add** icon.

The Edit Routine page appears (see *"Editing a Routine" on page 451*).

Note: When a Routine is added, edited, or deleted, all Admin phones will automatically be rebooted to update their **Routines** menu.

Editing a Routine

The Edit Routine page allows you to set other parameters for the routine (see *Table 132, "Routines Parameters," on page 449*).

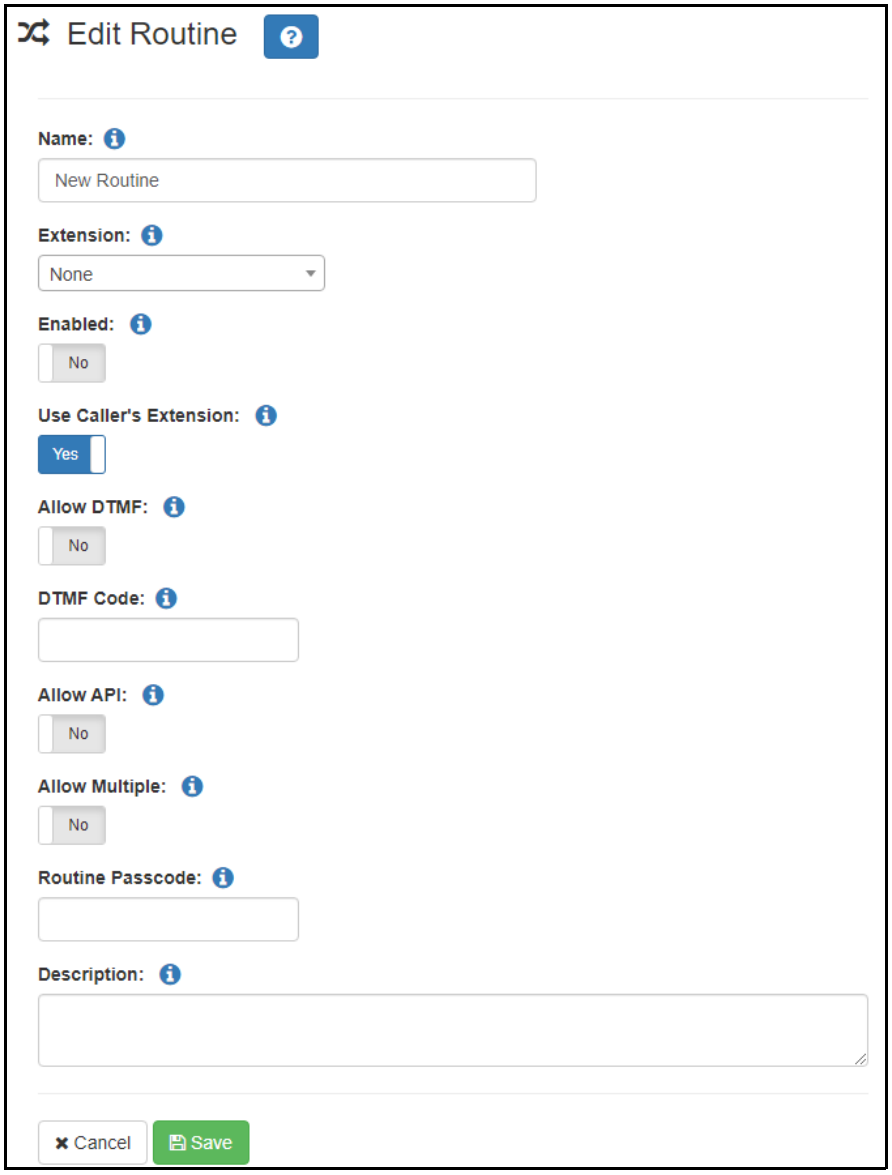


Figure 196. Edit Routine

To edit a routine:

1. On the navigation bar, select **Routines**.
2. On the *Routines* page, select the **Edit** icon.
3. Complete the changes for the parameters on the Edit Routines page (see *Table 132, "Routines Parameters," on page 449*).
4. Select **Save**.

Cloning a Routine

To clone a routine:

1. On the navigation bar, select **Routines**.
2. On the *Routines* page, select the **Clone** icon next to the routine that you want to clone.
3. A copy of the selected routine will be created with the following modifications:
   - The **Name** will have " clone" appended to it.
   - The **DTMF Code** will be blank.
   - The **Enabled** flag will be set to No (i.e., disabled).
4. Modify the cloned routine as desired.

Deleting a Routine

To delete a routine:

1. On the navigation bar, select **Routines**.
2. On the *Routines* page, select the **Delete** icon next to the routine that you want to delete.
3. When prompted, select **Delete**.

Creating and Executing Multi-Site Routines

The Routine action (see *Table 2, "Routine Action Type-Specific Parameters," on page 588*) allows a routine to initiate another routine. It also has the capability to initiate the routine at a remote facility, or even multiple remote facilities (see *"Configuring Facilities" on page 133*), by specifying a particular facility or **All Facilities** for the action's Facility parameter.

Tip: To execute a routine on multiple, but not all, facilities, specify a separate **Routine** action for each remote facility.

To execute a routine at a remote facility, specify the DTMF code of the routine to execute. A routine with that exact DTMF code should be defined at each remote facility. Furthermore, the **Use Caller's Extension** setting of that routine must be disabled, and the remote routine will not execute any calling or paging actions.

Tip: There will be a one-second delay between the execution of one **Routine** action and the next **Routine** action. For example, if you execute a multi-site routine for 10 sites, there will be 10-second delay between when the routine starts on the first facility and when it starts on the tenth facility. To eliminate this delay, you can select **All Facilities** and ensure that a routine with the specified DTMF does *not* exist on the sites that you do *not* want to run the routine (or define an empty routine with that DTMF code). If **All Facilities** is selected, the remote routines start at the same time.

Multi-Site Call Detail Records

Call Detail Records (CDRs) are created when a routine is started. When started on a local facility, the **Destination** field will show **Local Facility** and the **Type** field will show **Start Routine (<routine-DTMF-code>)**.

When a routine is started on a selected remote facility, the CDR will show the remote facility name in the **Destination** field and **Start Remote Routine (<routine-DTMF-code>)** in the **Type** field.

When a routine is started on all facilities, the CDR will show **All Facilities** in the **Destination** field and **Start Remote Routine (<routine-DTMF-code>)** in the **Type** field.

For more information about viewing CDRs, see *"Viewing Call Details Records" on page 363*.

Triggers

A trigger is an event that starts a routine. By default, when you create a routine, it has no trigger or actions.

A trigger can have up to two parameters. For example, you can create a trigger that uses a specific Announcement. The first parameter would be the **Announcement Type** (Number) and the second parameter would be the **Announcement**.

Viewing Triggers for a Routine

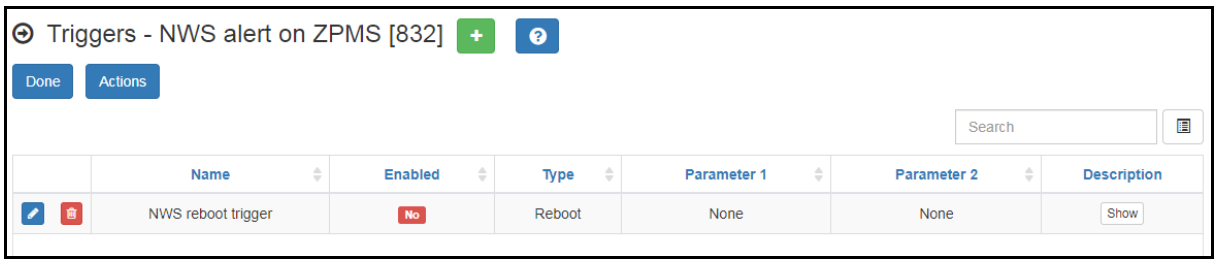


Figure 197. Triggers

To view triggers for a routine:

1. On the navigation bar, select **Routines**.
2. Select **Triggers** for the routine that you want to view triggers for.

   If a trigger has been added for the selected routine, information about the trigger appears (see *Table 133, "Triggers," on page 454*).

From the Triggers page, you can also add a trigger or select the **Actions** button to add actions that the selected routine will perform.

3 Select **Done** when finished viewing.

Table 133. Triggers

Name	Displays the user-provided name for the trigger.
Enabled	Specifies if the trigger is enabled. When enabled, the trigger will cause the routine to begin when the trigger event occurs.
Type	Displays the system event that triggers the routine. For the list of trigger types and their descriptions, see *Figure 27, "Failover Event Routine Triggers," on page 97* and *Figure 4, "Routine Trigger Types and Parameters," on page 615*.
Parameter 1	Displays the first parameter for the specified trigger if required. For example, if a trigger involves the closing of a contact on an I/O Controller, Parameter 1 is the name of the I/O Controller. For more information about Parameter 1 options, see *"Understanding Trigger Parameters" on page 456*.
Parameter 2	Displays the second parameter for the specified trigger if required. For example, if a trigger involves the closing of a contact on an I/O Controller, Parameter 2 is the specific contact or contacts of the device. For more information about Parameter 2 options, see *"Understanding Trigger Parameters" on page 456*.
Description	Displays the description entered by the user for the selected trigger.

Adding a Trigger

One or more triggers (i.e., events that start a routine) can be added to a routine. When adding a trigger, you can set up to two parameters for the trigger (see *"Understanding Trigger Parameters" on page 456*).

To add a trigger:

1. On the navigation bar, select **Routines**.
2. Select **Triggers** for the routine that you want to add a trigger for.
3. Select the **Add** icon.

   The Edit Trigger page appears.
4. Complete the parameters for the new trigger (see *"Editing a Trigger" on page 455*).
5. Select **Save**.

Editing a Trigger

The Edit Trigger page allows you to set the parameters for the trigger.

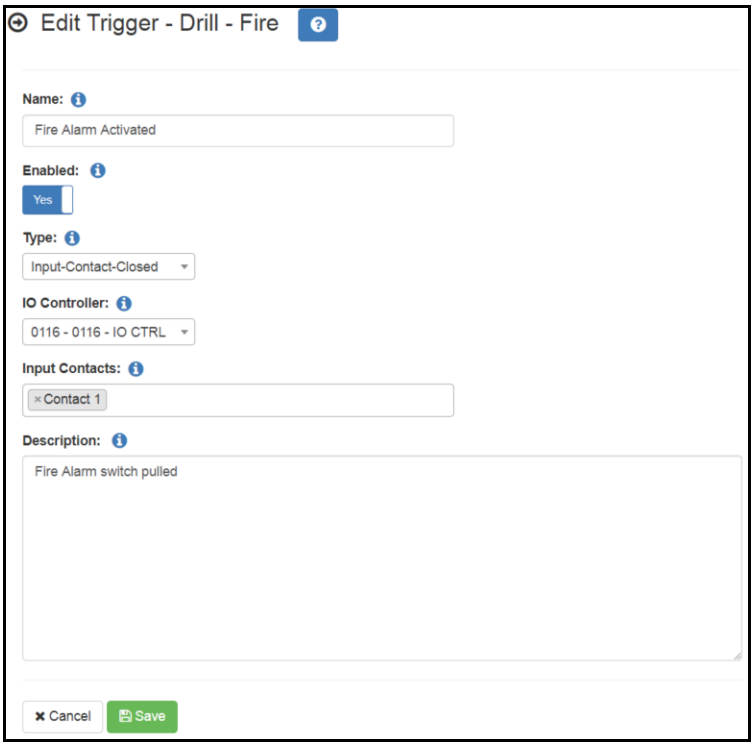


Figure 198. Edit Trigger

To edit a trigger:

1. On the navigation bar, select **Routines**.
2. Select **Triggers** for the routine that you want to edit a trigger for.
3. Select the **Edit** icon.
4. Complete parameters for the trigger. (See *Table 133, "Triggers," on page 454*.)

5 Select **Save**.

Deleting a Trigger

To delete a trigger:

1 On the navigation bar, select **Routines**.
2 Select the Delete icon next to the trigger that you want to delete.
3 When prompted, select **Delete**.

Understanding Trigger Parameters

Each trigger can have a maximum of two parameters, depending on the selected trigger **Type**.

When viewing triggers, the parameters appear as **Parameter 1** and **Parameter 2**. On the *Edit Trigger* page, however, the parameter names and available selections change based on the **Type**. For example, if **Alarm** is selected as **Type**, a field called **Alarm** appears with a drop-down menu that shows all of the tones whose **Type** is set to **Alarm** on the Tones page (see *"Viewing Available Tones" on page 332*).

For some Announcement Types, additional information is needed. For instance, if you select **Normal-Zone** as the **Announcement Type** on the Edit Trigger page, the **Zone** field appears. From the Zone field, you can select **All Speakers**, **Any Zone**, or a specific zone.

Some triggers have no parameters. For example, if you select **Emerg-All-Call** for **Type**, no parameters are applicable.

For detailed descriptions of the available trigger types and their associated parameters, see *"Routine Trigger Types and Parameters" on page 615*.

Actions

An action is an activity or task that the system performs as the result of a trigger starting a routine. For example, a routine that uses a selected tone for the trigger could have audio distribution start as the action.

Viewing Actions for a Routine

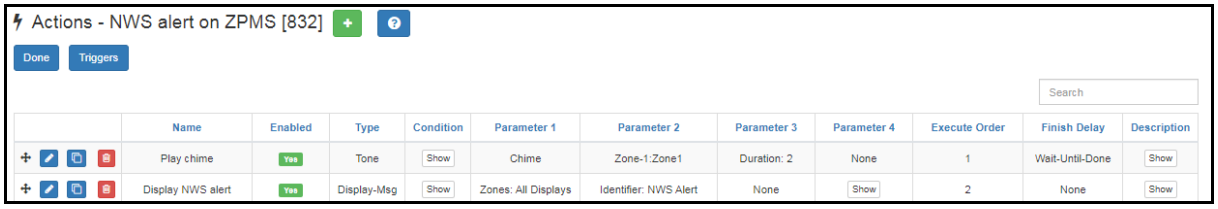


Figure 199. Actions

To view actions for a routine:

1. On the navigation bar, select **Routines**.
2. Select **Actions** for the routine that you want to view actions for.

   If an action has been added for the selected routine, information about the action appears (see *Table 134, "Actions," on page 457*).

   From the Actions page, you can also add an action or select the **Triggers** button to add triggers that the selected routine will perform.
3. Select **Done** when finished viewing.

Table 134. Actions

Name	Displays Name of the action.
Enabled	Indicates if the action is enabled. When adding or editing an Action, move the slider to **Yes** to enable the action.
Type *Note:* Depending on the Type, additional parameters may be set (see *"Understanding Action Parameters" on page 460*).	Displays the type of action. Type can be one of the following: • Add-Announcement-Audio • Alarm • All-Call • Announcement • Audio-Dist-Start (Audio Distribution Start) • Audio-Dist-Stop (Audio Distribution Stop) • Call-And-Announce • Change-Setting • Change-DSC01-Setting • Change-Volume • Change-WBC-Setting • Check-In • Check-intercom • Dash-Delete (Dashboard Text Delete) • Dash-Text (Dashboard Text) • Disable-Audio • Display-Msg (display NQ-GA10PV, NQ-DSC01, or NQ-S1810WBC message) • Display-Msg-Delete (delete NQ-GA10PV, NQ-DSC01, or NQ-S1810WBC message) • Enable-Audio • Email • Emergency-Call • Emerg-All-Call (Emergency All-Call) • Facility-Announcement • Facility-Page • Feature-Wait • Goto • Intercom-Call • Intercom-WaitLog-Text • Multi-Site-All-Call • Multi-Site-E-All-Call • New-Announcement • No-Action • Output-Contact-Close • Output-Contact-Open • Page-Exclusion • Pause • Play-Announcement • Play-Ringtone • Ring-Wait • Routine • Routine-Enable • Routine-Disable • SM-Disable-Zone • SM-Enable-Zone • SM-Scheduled-Ramp • SM-Set-Output-Gain • Stop-Announcement • Tone • Urgent-Call • Webhook-Post • Zone-Page

Table 134. Actions (continued)

Parameter 1	Displays the first parameter for the specified action type, if required. For example, if the action **Type** is **Routine**, then the DTMF Code for the routine appears as Parameter 1.
Parameter 2	Displays the second parameter for the specified action type, if required. For example, if **Routine** is selected as the action **Type**, then either **Local** or a specific facility appears as Parameter 2.
Parameter 3	Displays the third parameter for the specified action type, if required.
Parameter 4	Displays the fourth parameter for the specified action type, if required.
Execute Order	Displays the sequential order in which the action will be executed.
Finish Delay	Specifies if the routine should wait until this action is completed before starting the next action.
Description	Displays the user-provided description for the action.

Adding an Action

One or more actions can be added to a routine. When adding an action, you can set up to four parameters for the action (see *"Understanding Action Parameters" on page 460*).

To add a trigger:

1. On the navigation bar, select **Routines**.
2. Select **Actions** for the routine that you want to add an action for.
3. Select the **Add** icon.

   The Edit Action page appears.
4. Complete the parameters for the new action (see *Table 134, "Actions," on page 457*).
5. Select **Save**.

Editing an Action

The Edit Action page allows you to set the parameters for the action.

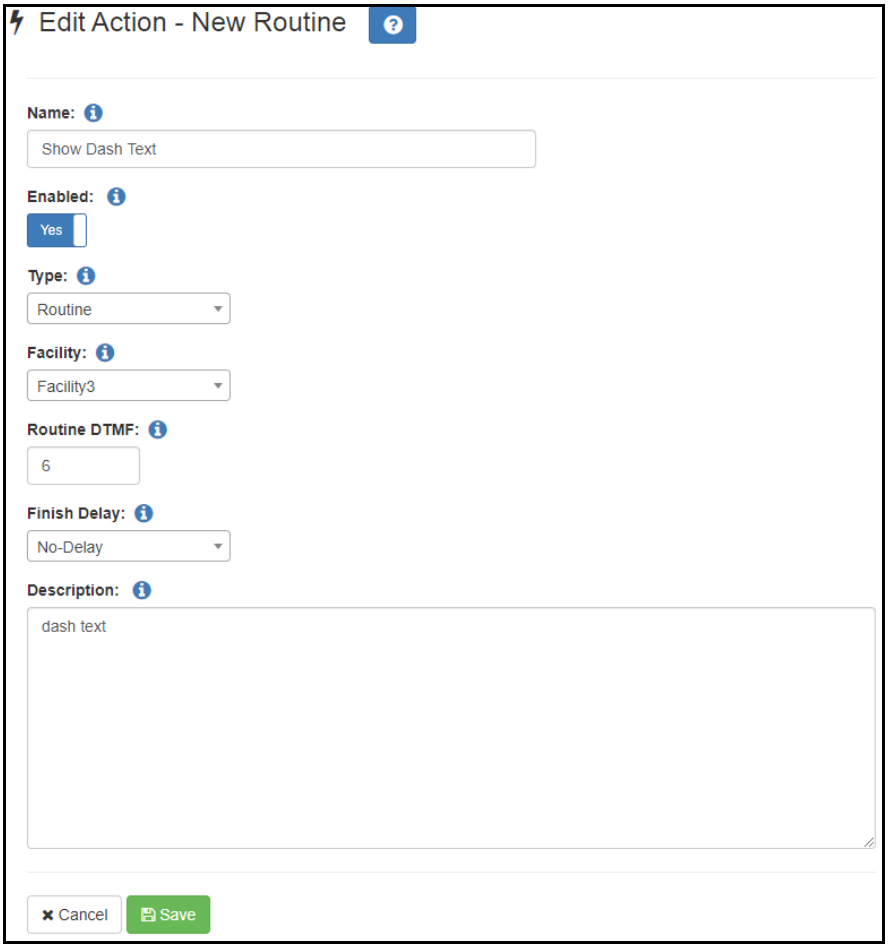


Figure 200. Edit Action

To edit an action:

1. On the navigation bar, select **Routines**.
2. Select **Actions** for the routine that you want to edit an action for.
3. Select the **Add** icon.

   The Edit Action page appears.
4. Complete the parameters for the action (see *Table 134, "Actions," on page 457*).
5. Select **Save**.

Cloning an Action

If an action is used more than once in a routine, you might want to clone the action rather than create a new action. Cloning an action creates a duplicate of the selected action and places the duplicate at the end of the action list.

You can edit a cloned action if you want to change any of the parameters.

To clone an action:

1. On the navigation bar, select **Routines**.
2. Select **Actions** for the routine that has the action you want to clone.
3. Select the **Clone** button ( ) for the action that you want to duplicate.

Understanding Action Parameters

In the list of Actions for a Routine, the parameters appear as **Parameter 1**, **Parameter 2**, **Parameter 3**, and **Parameter 4**. If the Action uses more than four parameters, **Parameter 4** will display a **Show** button that allows you to view the remaining parameters.

On the Edit Action page, however, the parameter names and available selections change based on the **Type**. For example, if **Alarm** is selected as **Type**, a field called **Alarm** appears with a drop-down menu that shows all of the tones with **Type** set to **Alarm** on the Tones page (see *"Viewing Available Tones" on page 332*). With this type of action, you can also set the **Duration**, which appears on the Actions page as **Parameter 3**. Parameters 2 and 4 are not used for this type of action, but you can set a **Finish Delay**, which establishes if the routine should wait until this action is completed before starting the next action.

Some actions have no parameters. For example, if you select **All-Call** for **Type**, no parameters are applicable.

Important: Each action can be made conditional, which means that it will only execute if its defined condition evaluates to true. To make an action conditional, enter a PHP expression in the **Condition** field for that action.

For more details about conditional actions, see *"Condition Statements" on page 478*.

For details about the available action Types and their applicable parameters, see *"Routine Action Types" on page 587*.

Using Email Action to Send Text Message

You can use the **Email** action **Type** to send a situation-specific message to an email address outside the Nyquist system and to send a text message to a cellphone. For text messages, the cellular server provider receives the email message and converts it to text.

The following table provides formats to use in the **Send Email To** field when creating or editing an **Email** action **Type** for some of the major cellular carriers:

Table 135. Email Address Formats for Cellular Carriers

Cellular Carrier	Email Address Format
AT&T	Not supported
Boost Mobile	<phone number>@sms.myboostmobile.com (SMS) <phone number>@myboostmobile.com (MMS)
C-Spire	<phone number>@cspire1.com
Consumer Cellular	<phone number>@mailmymobile.net
Cricket	<phone number>@sms.cricketwireless.net (SMS) <phone number>@mms.cricketwireless.net (MMS)
Google Fi (Project Fi)	<phone number>@msg.fi.google.com (SMS & MMS)
Metro PCS	<phone number>@mymetropcs.com (SMS & MMS)
Page Plus	<phone number>@vtext.com
Republic Wireless	<phone number>@text.republicwireless.com (SMS)
S. Cellular	<phone number>@email.uscc.net (SMS) <phone number>@mms.uscc.net (MMS)
Sprint	<phone number>@messaging.sprintpcs.com (SMS) <phone number>@pm.sprint.com (MMS)
T-Mobile	<phone number>@tmomail.net (SMS and MMS)
Ting	<phone number>@message.ting.com
Tracfone	<phone number>@mmst5.tracfone.com (MMS)
Verizon	Not supported
Virgin Mobile	<phone number>@vmobl.com (SMS) <phone number>@vmpix.com (MMS)
Xfinity Mobile	<phone number>@vtext.com (SMS) <phone number>@mypixmessages.com (MMS)

Tip: For other cellular carriers or to verify the email format (i.e., these may change over time), see the carrier's website. There are free services available (e.g., https://freecarrierlookup.com) that can help identify the carrier used by a cellular phone number.

How Actions Impact Other Actions

When creating a routine, you must take into account how an action impacts other actions in the routine. For example, if you want an announcement to play after an alarm, you want to ensure that the alarm ends before the announcement begins. Otherwise, the announcement may not be heard. In this scenario, you would want to ensure that the action to play an announcement waits until the alarm ends.

Check-Intercom, Intercom-Wait, Ring-Wait Action Types

If a routine's trigger **Type** is **Intercom-Call**, the routine's action **Type** could be **Check-Intercom**, **Intercom-Wait**, or **Ring-Wait**. Each of these action types depends on the status of the **Callers** – parameter 1 for the trigger (see *"Understanding Trigger Parameters" on page 456*).

The **Check-Intercom** action **Type** checks to see if the trigger caller is on an active intercom call. If the trigger caller is on an active intercom call, the routine executes subsequent actions. If the trigger caller is not on an active intercom call, the routine terminates and remaining actions will not be executed. You may want a routine to execute a **Check-Intercom** action **Type** before executing **Intercom-Wait** to ensure that the trigger caller is on an active intercom call.

The **Intercom-Wait** action **Type** waits for the trigger caller's call to finish. After the call finishes, the routine executes subsequent actions. If the call finishes before **Intercom-Wait** action **Type** is executed, the routine executes subsequent actions without delay.

The **Ring-Wait** action **Type** waits for the trigger caller's ringing to finish. After the ringing stage of a call ends, the routine executes subsequent actions. If the call is answered before the **Ring-Wait** action **Type** executes, the routine executes subsequent actions without delay.

A sample scenario using these three actions is a routine that is executed by the Intercom-Call trigger Type. The routine contains actions to be performed to indicate a ringing call The routine waits for the ring to finish (Ring-Wait action Type). When the ring finishes, the routine executes additional actions and then checks to see if the call was answered (Check-Intercom action Type). If the call was not answered (no active intercom call), the routine terminates. Otherwise, it executes additional actions before waiting for the call to finish (Intercom-Wait action Type), and then when the call is finished, the routine executes the remaining actions.

Note: The check and wait actions described in this section are always related to the caller that triggered the routine. The routine settings for **Extension** and **Use Caller's Extension** are not related to these wait actions; the check and wait actions will always be evaluated based on the trigger caller regardless of the routine's **Extension** or **User Caller's Extension** settings.

Check-In Action Type with Check-In Set to Wait

When the routine includes a **Check-In** action **Type** and **Check-In** (parameter 1) is **Wait**, the routine pauses the execution of subsequent actions until the check-in process is no longer active. When the check-in process is **Finished** or you select **Stop**, **Finish**, or **Reset**, the routine resumes executing actions

that follow a finished Check-In process such as: announcing Check-In completed to Admin Station speakers or displaying Check-in completion messages on web interface dashboards or GA10PV displays.

Check-In action **Type** with **Check-In** set to **Wait** does not differentiate between the Check-in process moving to the **Finished** state or having been manually stopped or finished.

Note: If you want to execute routine Actions after all stations have checked in (**Check-In** status is **Done**), create a routine with trigger **Type** set to **Check-In** and **Parameter 1** set to **Done**.

For more information about the Check-In process, see *"Manage Check-In" on page 523*.

Feature-Wait Action Type with 911

You may want to include the **Feature-Wait** action **Type** in a routine that is triggered by a 911 call to pause subsequent actions until the 911 call ends. In this scenario, set **Feature Wait** (parameter 1 of the **Feature-Wait** action **Type**) to **911**.

After the 911 call ends, the routine executes subsequent actions. The **911** trigger **Type** can execute routines when any caller dials 911, so multiple routines (one for each active 911 call) could execute.

Feature-Wait Action Type with Alarm

If you want to pause subsequent routine actions until the alarm finishes playing, use the **Feature-Wait** action **Type** with **Feature Wait** (parameter 1) set to **Alarm**. If no alarm is playing when the **Feature Wait** action executes, the routine does not wait for an alarm. Instead, it continues executing subsequent actions.

If you want to ensure that the routine includes an active alarm, use **Alarm** as the trigger **Type** (see *"Understanding Trigger Parameters" on page 456*).

If you do not need the routine to wait until the alarm finishes, you can still use **Feature-Wait** as the action **Type** and **Alarm** as **Feature Wait** and set **Maximum Wait Time** (action parameter 2) to the desired amount of time to wait.

Feature-Wait Action Type with Announcement

If you want all active Normal and Emergency announcements to complete before continue with subsequent routine actions, use the **Feature-Wait** action **Type** with **Feature Wait** (parameter 1) set to **Announcement**.

This action will not allow you to specify which announcement type or which announcement to wait for. The **Announcement** trigger **Type** does allow you to specify an announcement type or number (see *"Understanding Trigger Parameters" on page 456*). However, if the routine uses **Feature-Wait** action **Type** with **Feature Wait** set to **Announcement** and multiple announcements start, then the routine will pause until all announcements have completed.

Feature-Wait Action Type with All-Call

If you want a routine to pause until an active All-Call page completes, use the **Feature-Wait** action **Type** with **Feature Wait** (parameter 1) set to **All-Call**.

If no All-Call page is playing when the **Feature Wait** action executes, the routine does not wait for an All-Call page. Instead, it continues executing subsequent actions.

If you want to ensure that the routine includes an All-Call page, use **All-Call** as the trigger **Type**.

If you do not need the routine to wait until the All-Call page finishes, you can still use **Feature-Wait** as the action **Type** and **All-Call** as **Feature Wait** and set **Maximum Wait Time** (action parameter 2) to the desired amount of time to wait.

Feature-Wait Action Type with Disable-Audio

If you want a routine to pause until audio is re-enabled, use the F**eature-Wait** action **Type** with **Feature Wait** (parameter 1) set to **Disable-Audio**.

If audio is enabled when the **Feature Wait** action executes, the routine does not wait for audio to be disabled. Instead, it continues executing subsequent actions.

Feature-Wait Action Type with Emerg-All-Call

If you want a routine to pause until an active Emergency All-Call page completes, use the **Feature-Wait** action **Type** with **Feature Wait** (parameter 1) set to **Emerg-All-Call**.

If no Emergency-All-Call page is playing when the **Feature Wait** action executes, the routine does not wait for an Emergency-All-Call page. Instead, it continues executing subsequent actions.

If you want to ensure that the routine includes an Emergency-All-Call page, use **Emerg-All-Call** as the trigger **Type**.

If you do not need the routine to wait until the Emergency-All-Call page finishes, you can still use **Feature-Wait** as the action **Type** and **Emerg-All-Call** as **Feature Wait** and set **Maximum Wait Time** (action parameter 2) to the desired amount of time to wait.

Feature-Wait Action Type with Facility-Page

You can use the **Feature-Wait** action **Type** with **Feature Wait** (parameter 1) set to **Facility-Page** in a routine that is triggered by a facility page. The routine will pause subsequent actions until the facility page completes. If no facility page is playing when the Feature Wait action executes, the routine does not wait for a facility page. Instead, it continues executing subsequent actions.

Note: Only routines with the trigger **Type** set to **Facility Page** can use this action.

If you do not need the routine to wait until the facility page finishes, you can still use **Feature-Wait** as the action **Type** and **Facility Page** as **Feature Wait** and set **Maximum Wait Time** (action parameter 2) to the desired amount of time to wait.

Feature-Wait Action Type with Multi-Site-All-Call

If you want a routine to pause until a Multi-Site-All-Call page completes, use the **Feature-Wait** action **Type** with **Feature Wait** (parameter 1) set to **Multi-Site-All-Call**.

If no Multi-Site-All-Call page is playing when the **Feature Wait** action executes, the routine does not wait for a Multi-Site-All-Call page. Instead, it continues executing subsequent actions.

If you want to ensure that the routine includes a Multi-Site-All-Call page, use **Multi-Site-All-Call** as the trigger **Type**.

This action will only wait on a Nyquist system that starts the Multi-Site-All-Call. Remote sites that are included in a Multi-Site-All-Call only see a playing All-Call; they do not see it as a Multi-Site call. In this case, this action will have no effect.

If you do not need the routine to wait until the Multi-Site-All-Call page finishes, you can still use **Feature-Wait** as the action **Type** and **Multi-Site-All-Call** as **Feature Wait** and set **Maximum Wait Time** (action parameter 2) to the desired amount of time to wait.

Feature-Wait Action Type with Multi-Site-E-All-Call

If you want a routine to pause until a Multi-Site Emergency All-Call page completes, use the **Feature-Wait** action **Type** with **Feature Wait** (parameter 1) set to **Multi-Site-E-All-Call**.

If no Multi-Site Emergency All-Call page is playing when the **Feature Wait** action executes, the routine does not wait for a Multi-Site Emergency All-Call page. Instead, it continues executing subsequent actions.

If you want to ensure that the routine includes a Multi-Site Emergency All-Call page, use **Multi-Site-E-All-Call** as the trigger **Type**.

This action will only wait on a Nyquist system that starts the Multi-Site Emergency All-Call. Remote sites that are included in a Multi-Site Emergency All-Call only see a playing Emergency-All-Call; they do not see it as a Multi-Site Emergency All-Call. In this case, this action will have no effect.

If you do not need the routine to wait until the Multi-Site-Emergency-All-Call page finishes, you can still use **Feature-Wait** as the action **Type** and **Multi-Site-E-All-Call** as **Feature Wait** and set **Maximum Wait Time** (action parameter 2) to the desired amount of time to wait.

Feature-Wait Action Type with Tone

If you want a routine to pause until a tone finishes, use the **Feature-Wait** action **Type** with **Feature Wait** (parameter 1) set to **Tone**.

If no tone is playing when the **Feature Wait** action executes, the routine does not wait for a tone to start. Instead, it continues executing subsequent actions.

If you want to ensure that the routine includes the playing of a tone, use **Tone** as the trigger **Type**.

If you do not need the routine to wait until the tone finishes, you can still use **Feature-Wait** as the action **Type** and **Tone** as **Feature Wait** and set **Maximum Wait Time** (action parameter 2) to the desired amount of time to wait.

Feature-Wait Action Type with Zone

If you want all zone pages to complete before continuing with subsequent routine actions, use the **Feature-Wait** action **Type** with **Feature Wait** (parameter 1) set to **Zone**.

This action will not allow you to specify a zone. The **Announcement** trigger **Type** does allow you to specify a zone (see *"Understanding Trigger Parameters" on page 456*). However, if multiple routines triggered by a zone page use **Feature-Wait** action **Type** with **Feature Wait** set to **Zone** and multiple zone pages start, then all routines triggered by the start of a zone page will pause until the multiple zone pages have completed.

Zones and Stations Parameters for Deleting Display Messages

If you set Parameter 1 of **Display-Msg-Delete** action **Type** to **PARAM**, the options used for Zones and Stations determine which messages, if any, a routine automatically deletes from the dashboard and NG-GA10PV video displays. For example, if you leave **Zones** blank and set **Stations** to All, then messages that have no zones defined but do have stations defined will be deleted.

The following table describes how the combination of **Zones** and **Stations** settings are used to select messages for deletion:

Table 136. Selecting Messages for Deleting

Zones	Stations	Messages Selected for Deletion
<blank>	<blank>	No messages
<blank>	All	Messages that have no zones defined and any stations defined
Any	<blank>	Messages that have any zones defined and no stations defined

Table 136. Selecting Messages for Deleting

Zones	Stations	Messages Selected for Deletion
Any	All	All Messages
Selected zone or zones	<blank>	Messages that have specified zones defined and no stations defined
Selected zone or zones	All	Messages that have specified zones defined and any stations defined (including none)
Selected zone or zones	Selected station or stations	Messages that have specified zones defined and specified stations defined
<blank>	Selected station or stations	Messages that have no zones defined and specified stations defined
Any	Selected station or stations	Messages that have any zones defined (including none) and specified stations defined

Using Variables for Dashboard, NQ-GA10PV, NQ-DSC01, and NQ-S1810WBC Text Parameters

You can add variables to text messages for the Admin Web UI dashboard, the video display connected to the NQ-GA10PV, the NQ-DSC01 or NQ-S1810WBC LED display, and email messages. When a trigger starts a routine that includes a text message for display, the variable is replaced. For example, if the routine uses the variable $date1, that variable is replaced by the current date in the format YYYY-MM-DD when the routine is started.

The availability of specific variables is based on the trigger that started the routine (see *Table 138, "Variables, Definitions, and Availability," on page 468*).

When using variables, be sure to allow enough room for the message text, including the new text replaced by the variable.

- For dashboard messages, the maximum text that can be displayed is 255 characters per message.
- The character limit for the NQ-GA10PV display is 4096 characters, but the actual limit will vary due to font style and size.
- The NQ-S1810WBC LED display can display up to 64 characters, which will display as uppercase and will horizontally scroll text that exceeds the display width.
- The number of displayable characters on the NQ-DSC01 are dependent on the priority, as is the text colors and number of displayable messages (see *Table 137*).

Table 137. NQ-DSC01 Message Priorities

Priority	Simultaneous Messages	Max Characters (color specified per character)	Max Characters (default color of Red)
6	One (no clock)	64	639

Table 137. NQ-DSC01 Message Priorities

Priority	Simultaneous Messages	Max Characters (color specified per character)	Max Characters (default color of Red)
5	One (with optional clock)	64	639
0 to 4	One or two	64	639

You should test your display messages to ensure they fit into the available space.

The following variables (see *Table 138*) are available for text messages and related fields. Within the condition statement of a routine action, there are other variables available, as described in *Table 144, "Conditional Statement Variables," on page 488*.

Table 138. Variables, Definitions, and Availability

Variable	Definition	Available for Routines Triggered by:
$alerts(?,?)	When used in the **Text** field of a **Display-Msg**, NWS alerts will display on the video connected to the NQ-GA10PV (see *"Setting Variables for the Display Message" on page 548*).	Always available *Note:* The Reboot trigger is recommended to ensure the routine is always running.
$apiParam1 $apiParam2	Used only by the Routines API v1, these parameters can be specified as part of the Routines API URL and referenced by the Routine Action. For details, see *"Routines API v1" on page 445*.	Routines API v1
$apiParam1 ⋮ $apiParam20	Used only by the Routines API v2, these parameters can be specified within the `data` or `json` multipart form subpart and referenced by the Routine Actions and Conditions. For details, see *"Routines API v2" on page 429*.	Routines API v2
$autobgcolor	When appended to the end of text, the message's background color automatically appears as red for Emergency-Call, yellow for Urgent-Call, or the font color set in Display-Msg action for Intercom-Call. *Note:* Use only $autobgcolor or $autofontcolor, but not both.	• Emergency-Call • Intercom-Call • Urgent-Call

Table 138. Variables, Definitions, and Availability (continued)

Variable	Definition	Available for Routines Triggered by:
$autofontcolor	When appended to the end of text, the message's font color automatically appears as red for Emergency-Call, yellow for Urgent-Call, or the font color set in Display-Msg action for Intercom-Call. *Note:* Use only $autobgcolor or $autofontcolor, but not both.	• Emergency-Call • Intercom-Call • Urgent-Call
$autopriority(E,U,N)	When appended to the end of text field, the message's priority is changed where E is replaced by the priority for Emergency calls, U is replaced by the priority for Urgent calls, and N is replaced by the priority for Normal calls. For example, $autopriority(5,4,3) will set Emergency-Call–triggered Dash-Msg to priority 5, Urgent-Call–triggered Dash-Msg to priority 4, and Intercom-Call–triggered Dash-Msg to priority 4. If the (E,U,N) parameters are not present, the priorities will be 4,3,2.	• Emergency-Call • Intercom-Call • Urgent-Call
$auto_resize(N)	When used in the **Text** field of a **Display-Msg**, automatically resizes the display message by decreasing the font size, if needed, to better fit the message to the screen, but will keep the font size to at least N (see *"Setting Variables for the Display Message" on page 548*).	Always available

Table 138. Variables, Definitions, and Availability (continued)

Variable	Definition	Available for Routines Triggered by:
$caller	Extension number of caller that triggered execution of the routine; when calls are placed from outside the system, displays the phone number of the caller.	• Alarm • All-Call • Announcement • Check-In • Disable-Audio • Enabled-Audio • Emergency-Call • Emerg-All-Call • Facility-Page • Incoming-Call • Intercom-Call • Multi-Site-All-Call • Multi-Site-E-All-Call • Night-Ring • PBX-Incoming-Call • Tone • Urgent-Call • Zone-Page
$called	Extension number of called station.	• Emergency-Call • Intercom-Call • PBX-Incoming-Call • Urgent-Call
$calltypechar	Replaced by **E** for Emergency-Call, **U** for Urgent-Call, or left blank for Intercom-Call.	• Emergency-Call • Intercom-Call • Urgent-Call
$calltypelong	Replaced by **Emergency** for Emergency-Call, **Urgent** for Urgent-Call, or left blank for Intercom-Call.	• Emergency-Call • Intercom-Call • Urgent-Call
$calltypeshort	Replaced by **Emerg** for Emergency-Call, **Urg** for Urgent-Call, or left blank for Intercom-Call.	• Emergency-Call • Intercom-Call • Urgent-Call

Table 138. Variables, Definitions, and Availability (continued)

Variable	Definition	Available for Routines Triggered by:
$CAP_Alert_ <element_name>	Returns the value CAP message sub-element of the <alert> segment specified by <element_name>. See section 3.2.1 of the CAP protocol standard.	All triggered routines that include one of the following actions: • Add-Announcement_Audio • Display-Msg • Display-Msg-Delete • Dash-Text • Dash-Delete • Email • LogText • Webhook-Post
$CAP_Info_ <element_name>	Returns the value of the CAP message sub-element of the <info> segment specified by <element_name>. See section 3.2.2 of the CAP protocol standard.	

$CAP_EventCode_ <valueName>	Returns the value of the <value> sub-element of an <eventCode> structure having the specified <valueName> in the <info> segment of the specified CAP message.
	See section 3.2.2 of the CAP protocol standard.
	`<eventCode>`
	`  <valueName>valueName</valueName>`
	`  <value>value</value>`
	`</eventCode>`	

$CAP_Parameter_ <valueName>	Returns the value of the <value> sub-element of a <parameter> structure having the specified <valueName> in the <info> segment of the specified CAP message.
	See section 3.2.2 of the CAP protocol standard.
	`<parameter>`
	`  <valueName>valueName</valueName>`
	`  <value>value</value>`
	`</parameter>`	

$contact	I/O Controller's input contact number that triggered execution of the routine.	• Input-Contact-Closed • Input-Contact-Opened
$cputemp	Current temperature (in °C) of the CPU core with the highest temperature.	All triggered routines that include one of the following actions: • Dash-Text • Display-Msg • Email
$date1	Current date in YYYY-MM-DD format	Always available
$date2	Current date in MM-DD-YYYY format	Always available

Table 138. Variables, Definitions, and Availability (continued)

Variable	Definition	Available for Routines Triggered by:
$date3	Current date in DD-MM-YYYY format	Always available
$deviceMacAddr	MAC address for Nyquist appliance that went into protection mode.	The following actions of the Amp-Protection-Mode trigger: • Display-Msg • Dash-Text • Email • Log-Text Also available in the CODE: segments of the action's Condition statement.
$deviceName	Name of Nyquist appliance that went into protection mode.	The following actions of the Amp-Protection-Mode trigger: • Display-Msg • Dash-Text • Email • Log-Text Also available in the CODE: segments of the action's Condition statement.
$df-avail	Available disk space of the Nyquist server displayed in either M for megabytes or G for gigabytes.	All triggered routines that include one of the following actions: • Dash-Text • Display-Msg • Email
$eventid	Scheduled Event ID (integer)	• Scheduled-Event
$eventname	Scheduled Event Name	• Scheduled-Event
$facility	Name of facility that is being paged or for which the current status is being provided	• Facility-Page • Facility Status Down

Table 138. Variables, Definitions, and Availability (continued)

Variable	Definition	Available for Routines Triggered by:
$namecalled	Station name for caller that triggered execution of the routine	• Emergency-Call • Intercom-Call • PBX-Incoming-Call • Urgent-Call
$namecaller	Called station's name	• Alarm • All-Call • Announcement • Check-In • Disable-Audio • Enabled-Audio • Emergency-Call • Emerg-All-Call • Facility Page • Intercom-Call • Multi-Site-All-Call • Multi-Site-E-All-Call • Night-Ring • PBX-Incoming-Call • Tone • Urgent-Call • Zone-Page
$nwsAlertEvent $nwsAlertSeverity $nwsAlertCertainty $nwsAlertUrgency $nwsAlertResponse	The event, severity, certainty, urgency, and response of the NWS alert.	The following actions of the NWS-Alert trigger: • Add-Announcement-Audio (with *Text-to-Speech* Audio Source) • Dash-Text • Dash-Delete • Display-Msg • Display-Msg-Delete • Email • Log-Text • Webhook-Post

Table 138. Variables, Definitions, and Availability (continued)

Variable	Definition	Available for Routines Triggered by:
$schedParam1 $schedParam2	Used only by the Schedule Routines, these parameters can be specified via the Schedule Routine's Parameter 1 and Parameter 2 properties and referenced by the Routine Action (as well as Action Conditional CODE: segments). For details, see *"Using the Schedule Routines Feature" on page 283*.	Schedule Routines only: • Add-Announcement-Audio • Dash-Text • Dash-Text-Delete • Display-Msg • Display-Msg-Delete • Email Also available in the CODE: segments of the Action's Condition statement.
$schedulename	Activated schedule name	• Schedule-Activated
$station	Station, such as the I/O Controller, that triggered execution of the routine or for which the current status is being provided	• Input-Contact-Closed • Input-Contact-Opened • Station-Status-Up • Station-Status-Down
$time1	Current time in 12-hour format	Always available
$time2	Current time in 24-hour format	Always available
$toneid	Tone's identifier	• Scheduled-Tone
$tonename	Tone's name	• Scheduled-Tone
$uptime	Indicates how long the Nyquist server has been running, since the last reboot (e.g., "up 4 hours, 44 minutes")	All triggered routines that include one of the following actions: • Dash-Text • Display-Msg • Email

Table 138. Variables, Definitions, and Availability (continued)

Variable	Definition	Available for Routines Triggered by:
$user_var[1...10]	The values in this general-purpose array can be set and referenced within the Routine Condition CODE: segments and Actions of a single Routine. *Note:* The scope and lifetime of this variable corresponds to the execution of all actions and conditions of the current routine. If you need values to persist and be accessible across multiple executions or between different routines, you can store the values in database variables (see *"Managing Routine Database Variables" on page 495*).	Routine Action Condition fields can access this general purpose array. In addition, the following routine actions can access them via Text, Identifier, and Subject fields: • Dash-Text • Display-Msg • Email • Add-Announcement-Audio (TTS field) • Webhook-Post (POST Command field)
$weather	Displays current weather conditions as provided by the OpenWeather API service. For details, see *"The $weather variable and the OpenWeather API" on page 475*. *Tip:* If you want the weather to display at all times, use the Reboot trigger to display it upon startup.	All triggered routines that include one of the following actions: • Display-Msg
$zone	Announcement zone or page zone that triggered execution of the routine	• Announcement • Zone-Page
`{{object.property}}`	Custom objects can be defined with the `json` structure of a Routines API v2 call and referenced within the Actions. For details, see *"Routines API v2" on page 429*.	Routines API v2

The $weather variable and the OpenWeather API

The `$weather` variable, if used in a Display-Msg action message, will be replaced by the current weather conditions and displayed using the following format:

```
Temperature: ## F (feels like ##)
Humidity: ##%
Condition: <text description>
Wind: <direction> ## mph (gusts to ##)
```

To use the `$weather` variable, you must first acquire a free OpenWeather API key. For details on acquiring and using an API key, visit https://openweathermap.org/appid.

Important: This feature requires Internet access and the Nyquist system must be able to access https://api.openweathermap.org. The *Check Internet Site Access* tests will verify this (see *"Check Internet Site Access" on page 44*).

To enable the `$weather` variable, use the **Custom Configuration** button in *System Parameters* (see *"Custom Configuration" on page 46*) to set the following two variables in the *Actions and Custom Variables* section:

- `weather_api_key`
- `weather_zipcode`

In the *Actions and Custom Variables* text editor, uncomment the `#weather_api_key=` and `#weather_zipcode=` lines (i.e., remove the # symbols) and append your API key and the relevant ZIP code (respectively) after the equal signs. The `weather_api_key` specifies an API key from your OpenWeather account. The `weather_zipcode` indicates the 5-digit ZIP code whose weather conditions are to be retrieved. Note that this must be set, even if you intend to override the ZIP code using the `weather_zipcode_#####` parameter.

Tip: Due to the length of many OpenWeather descriptions, you may want to format the message using a smaller font size. For example, the following will display the text at 70% of normal size:

```
<span style="font-size:70%">$weather</span>
```

Override the forecast location

The target ZIP code specified by the `weather_zipcode` can be overridden in a Display-Msg action by specifying the `weather_zipcode_#####` parameter after the `$weather` variable, where `#####` is the target ZIP code. For example:

```
$weather weather_zipcode_12345
```

The Display-Msg action can also specify the forecast location via coordinates (i.e., latitude and longitude) instead of by ZIP code by specifying the `weather_latlon_<latitude>,<longitude>#` parameter after the `$weather` variable. For example:

```
$weather weather_latlon_42.833261,-74.058015#
```

These overrides allows you to display the weather conditions for multiple and/or alternate locations.

Tip: To display weather conditions for multiple locations at once, you should define a separate Action for each location, as only one location is allowed per Action.

Unit of measurement (Fahrenheit or Celsius)

Temperatures are displayed in degrees Fahrenheit by default. To display temperatures in degrees Celsius, specify `weather_units_metric` after the `$weather` variable. For example:

```
$weather weather_units_metric
```

or

```
$weather weather_latlon_42.833261,-74.058015# weather_units_metric
```

Update frequency

When using the `$weather` variable in a Display-Msg routine action, you will usually want to execute the Display-Msg action in a loop (e.g., by using the Goto action) and pause between executions (e.g., by using the Pause action). The length of the pause should be based on how timely you wish the information to be, while taking into consideration the access limits imposed by your OpenWeatherMap subscription.

As of this Nyquist release, a free OpenWeatherMap account allows 60 calls per minute with a monthly cap of 1,000,000 calls (paid subscriptions allow more). Executing the Display-Msg action once per minute is well within the limit and should not negatively impact Nyquist performance. We do not recommend executing the Display-Msg action more frequently than once every 15 seconds, especially if the GA10PV is being used to play audio distribution.

Tip: OpenWeather recommends calling their API no more than once every 10 minutes per location, as their forecast data is updated no more than once every 10 minutes.

Note: If you initiate a long-running routine like this via the Routines API, you will probably want to set the URL's `<delay_flag>` value to zero ("0") so the call will not block indefinitely, waiting for the routine to complete.

Using Variables in Dashboard and NQ-GA10PV Identifiers

You can use one or more variables in the **Identifier** field of **Display-Msg**, **Display-Msg-Delete**, **Dash-Text**, and **Dash-Delete** action types (see *Table 2, "Routine Action Type-Specific Parameters," on page 588* for the specific variables available). The value of the Identifier will be determined by the values of the specified variables.

An **Identifier** can have a maximum character length of 255 characters. When using variables, be sure the specified value, including the expanded values of the variables, does not exceed this maximum character length.

Tip: If you would like to verify the actual value of an Identifier that includes variables, you can create a LogText action, specifying the same value as used for **Identifier**, and view the resulting value in the System Logs (nyquist_routines.log). Keep in mind that the LogText message allows more characters, removes single and double quotes, and does not allow the $date# and $time# variables.

Using Variables in Display-Msg Text

Note: This section describes variables that are only available for use in the **Display-Msg** action type, and *only* if the routine trigger is **Intercom-Call**, **Urgent-Call**, or **Emergency-Call**.

The following variables can only be used in the **Text** field of the **Display-Msg** action type:

- $calltypechar
- $calltypeshort
- $calltypelong
- $autobgcolor
- $autofontcolor
- $autopriority(E,U,N)

These variables allow you to set the priority and appearance of the NQ-GA10PV and NQ-S1810WBC display messages for emergency, urgent, or intercom calls. For more information about these variables, see *"Using Variables for Dashboard, NQ-GA10PV, NQ-DSC01, and NQ-S1810WBC Text Parameters" on page 467*.

Reordering Actions

You can reorder actions in a routine but should exercise care. Some actions must be the last action in a routine (see *"Understanding Action Parameters" on page 460*).

To reorder an action:

1. On the navigation bar, select **Routines**.
2. Select **Actions** for the routine that you want to reorder actions for.
3. Click the Move icon (✣) next to the action that you want to move and drag the action to the desired location.

Condition Statements

An action's **Condition** property can be used to specify conditional execution of the Routine Action based on the supplied conditional statement. If the Condition field is not specified (i.e., left blank), the routine action will always be executed. If a condition is specified, the action will only be executed if the condition evaluates to true.

Conditional statement syntax must adhere to the PHP 7.4 programming language while using existing Nyquist variables, functions, and valid conditional logic. The Nyquist system will not attempt to validate

the statement syntax or the provided conditional logic, so please ensure that you thoroughly test your conditional statements.

Simple Conditions

A conditional statement can be a simple boolean PHP conditional statement, which evaluates to either true or false. The statement can include PHP and Nyquist variables (see *"Available Condition Variables" on page 487*) and functions (see *"Condition Statement Functions" on page 481*).

Simple Condition Examples

The following condition for an action will cause the action to execute only if the caller is 105:

```
$caller == "105"
```

The following condition for an action will cause the action to execute only if the caller is 105 and the called is 200:

```
($caller == "105") && ($called == "200")
```

The following condition for an action will cause the action to execute only if the caller is 100 or 101 and the called is 200 or 201:

```
(($caller == "100") || ($caller == "101")) && (($called == "200" || ($called == "201"))
```

The following condition for an action will cause the action to execute only if the caller starts with 10 (e.g. 100, 101, 102):

```
strpos($caller,"10") === 0
```

The following condition for an action will cause the action to execute only if the zone number is 123:

```
$zonenumber == "123"
```

The following condition for an action will cause the action to execute only if zone number is 4444 and its name is "Gym":

```
$zone == "Zone 4444 - Gym"
```

The following condition for an action will cause the action to execute only if the current time is between 8 a.m. and 5 p.m.:

```
(($curtime > "08:00:00") && ($curtime < "17:00:00"))
```

The following condition for an action will cause the action to execute only on Monday through Friday:

```
($weekday != "Sat") && ($weekday != "Sun")
```

The following condition for an action will cause the action to execute only if any Nyquist CPU core has a temperature higher than 85 C:

```
$cputemp > 85
```

Advanced Conditions

Advanced conditions begin with one of the following (including the colon):

- `STOP:`
- `CODE:`

Conditions that begin with `STOP:` will cause the Routine to stop executing actions and terminate if the condition is true.

For example, the following condition will cause the Routine to stop if today is Saturday or Sunday:

```
STOP:($weekday == "Sat") || ($weekday == "Sun");
```

Conditions that begin with `CODE:` will execute the provided code, which may assign values to user variables (which are accessible within the current routine) or database variables (which are accessible within *any* routine). If you also want the current action to execute, the following statement must be included:

```
$DOACTION=true;
```

If `$DOACTION=true;` is not included (or is not executed), the default behavior is to not execute the action.

A `return;` statement in the `CODE:` section can be used to exit the code section before all statements have been executed.

The Dash-Text, Display-Msg, Email, and Webhook-Post actions have access to ten user-supplied variables—`$user_var[1]` through `$user_var[10]`—which can be set with Action conditions.

The `CODE:` section can also be used to branch to ("go to") a specified action, using the `$gotoActionName` variable. For example, the following statement will cause a Routine to go to the Action named "Display Msg 2":

```
CODE:$gotoActionName = "Display Msg 2";
```

If you also want the current action to execute, use:

```
CODE:$DOACTION=true; $gotoActionName = "Display Msg 2";
```

After branching to—and executing—the specified action, the Routine will continue executing the actions that follow the one specified by `$gotoActionName`.

The `$gotoActionName` variable can be used to go to Actions that either follow *or precede* the current action. This enables loops within the actions of a Routine.

Caution If you create a loop within the routine by setting `$gotoActionName` to a preceding action of the routine, be aware that the routine may execute indefinitely (i.e., an infinite loop).

If you plan to use the `$gotoActionName` feature, make sure that all Action's have unique names. If more than one action has the same name, the first one found after the current action will be executed.

If you set `$gotoActionName` to a name that does not exist, the Routine will be terminated. This could be an issue if you accidentally specify the wrong name, but it can also be useful if you need to stop the

Routine based on conditions determined by your `CODE:` section. If you intend to use `$gotoActionName` to terminate a Routine, you could set `$gotoActionName` to `"TERMINATE"` or `"STOP"` and make sure you don't have an Action with that name.

Routines can be repeated (looped) by setting `$gotoActionName` to the first Action in the Routine. Routines can also be repeated by using a Goto Action to the name of the first Action in the Routine.

Instead of using the `$gotoActionName` variable, you can also use the Goto Action to branch to the name of the Action specified in the Goto Action. Goto Actions can also be conditionally executed based on the associated Condition. The `$gotoActionName` variable is typically used in `CODE:` sections for advanced use-case scenarios where the Goto Action would not be sufficient.

Advanced Condition Examples

The following condition for an action will cause the Routine to stop if the condition is true:

```
STOP:$caller == "105"
```

The `STOP:` keyword tells the system that you want to stop the Routine if the condition is true. When the Routine is stopped, subsequent actions will not be executed, and the Routine will be terminated.

The following condition for an action, if true, will set a user variable and cause the action to be executed:

```
CODE:if ($caller == "105") { $user_var[1] = "Bogen"; $DOACTION=true; }
```

The `$user_var[1]` variable can be used in the current or subsequent actions of type Dash-Text, Display-Msg, or Email (in the action Text fields and the Subject field for Email).

The following condition for an action will evaluate the `$cputemp` variable and set a user variable for use in a Dash-Text, Display-Msg, or Email action:

```
CODE:if ($cputemp > 85) { $user_var[1] = "CPU Temperature getting too hot: $cputemp"; } else { $user_var[1]
= "CPU Temperature is normal: $cputemp"; } $DOACTION=true;
```

Whitespace and comments can be used in the CODE: section to make it easier to read the code. For example, the above code could be the following instead:

```
CODE:
if ($cputemp > 85) {
   $user_var[1] = "CPU Temperature getting too hot: $cputemp";
} else {
   $user_var[1] = "CPU Temperature is normal: $cputemp";
}
$DOACTION=true;
```

Condition Statement Functions

There are several utility functions provided that are available within the condition statements of the Routine Actions.

Database Variable Functions

The database variable functions enable you to share data between the condition statements of any number of routines by storing key/value pairs in the Routines database.

Table 139. Routine Database Variable Functions

Function Name	Description
dbPut(<key>,<value>)	Stores the string <value> to a database, which can subsequently be retrieved using the <key> string. <key> is a variable-length string with a maximum of 64 characters. <value> is a variable-length string with a maximum of 4095 characters. For example: `dbPut("Test", "This is a test");` will store "This is a test" in a row referenced by "Test". Subsequent execution of `dbPut()` can be used to update the row; for example, `dbPut("Test", "Update my test string")` will update the value referenced by "Test" to the new value "Update my test string".

dbGet(<key>)	Retrieves the string value referenced by the <key> string.
	
	For example, after executing:
	`$value = dbGet("Test");`
	the `$value` variable will be set to "This is a test", the value referenced by "Test".
	
	Tip: To make the retrieved data available outside of the condition statements (e.g., for display by a Dash-Text or Display-Msg action) copy the retrieved value to the `$user_var` array. For example:
	`$user_var[1] = dbGet("Test");`
	This value can then be accessed (within the currently executing routine) via the `$user_var[1]` variable.

dbDelete(<key>)	Deletes the key/value pair referenced by the <key> string. Example: `$dbDelete("Test");` Will delete the database variable referenced by the "Test" key.
dbTruncate()	Deletes all database variables stored in the Routine database. **Warning** This operation cannot be reversed.

The routine database variable functions provide the ability to create named values (i.e., key/value pairs) that can be accessed from the condition statements of routines. This is similar to the functionality pro-

vided by the $user_var array, but allows values to be shared not only between the actions of one execution of a single routine, as with the $user_var array, but between multiple executions of all routines. It also provides named values, which makes for more readable code than indexed values, and a virtually unlimited number of values that can be stored.

Unlike the $user_var array, however, database variables cannot be programmatically accessed outside of condition statements (e.g., within the Text property of the Display-Msg action). If you want to access these values, however, simply assign the value of the database variable to an element of the $user_var array within a condition statement and then access the value from $user_var array outside of the condition statement.

Tip: Database variables can also be viewed, created, modified, and deleted via the *Routines Database Variables* view, accessible via the **Manage Routines Database Variables** button of the *Routines* page (see *"Managing Routine Database Variables" on page 495*). They can also be imported and exported to and from a CSV (comma-separated value) file, which allows the values to be defined and/or modified in an editor, script, or application (see *"Importing and Exporting Database Variables" on page 496*). This can be used for troubleshooting, maintenance, or even as a way to define and modify custom configuration settings for your routines.

As described in *Table 139*, dbPut(<key>) stores a value for <key>, dbGet(<key>) gets the stored value for <key>, dbDelete(<key>) deletes the value associated with <key>, and dbTruncate() deletes all key/value pairs in the database.

Example:

The following CODE segment can be added to a Routine Action Condition of a Routine that is triggered by All-Call to track the number of All-Call pages placed by the Nyquist system:

```
CODE:
$count = dbGet("All-Call Count");
if ($count == "") $count = 0;
$count++;
dbPut("All-Call Count", $count);
dbPut("Latest All-Call","$pDate2 - $pTime1");
```

The counter can then be viewed on the Routines Database Variables page. The Routine Action can be any action type, including No-Action, if you want to keep track of All-Call pages without performing any other actions.

Page Exclusion Functions

The isPageExcluded() function indicates whether a specified station extension is currently excluded from receiving pages.

Table 140. Page Exclusion Function

Function Name	Description
isPageExcluded(<station>)	Accepts a station extension string (e.g., "104") as a parameter and returns one (1) to indicate the station is currently excluded from receiving pages or zero (0) to indicate it is not excluded.

Example:

```
CODE:
if ( !isPageExcluded("104") ) {
   $DOACTION=true;
} else {
   $DOACTION=false
}
```

Logging Functions

Routine condition statements can log entries to the `nyquist_routines.log` file (see *"Routines Log" on page 492*) by calling the `logText(<text>)` function from within a routine action condition's CODE segment. The `<text>` value can be a string literal (e.g., "Problem detected") or a previously set variable (e.g., `$loggingMessage`).

Table 141. Routine Logging Functions

Function Name	Description
logText(<text>)	Logs the specified `<text>` value to the `nyquist_routines.log` file (see *"Viewing System Log Files" on page 361*). *Note:* This function mirrors the capabilities of the Log-Text action, as described in *"Routine Action Types" on page 587*.

The `logText()` function logs the user-supplied text to the log file in the following format:

```
<date time> <pid> [<routine-name>] <text>
```

where `<date time>` is replaced with the date and time at which the log entry was created, `<pid>` is replaced with the routine's process ID (to facilitate correlation of log entries), `<routine-name>` is replaced with the routine's name, and `<text>` is replaced with the user-supplied text.

For example, the following action condition CODE segment will cause a `nyquist_routines.log` log entry to be created with the text "`<date time> <pid> [<routine-name] This is a test`".

```
CODE:
logText("This is a test");
$DOACTION=true;
```

Note: The `$DOACTION=true` statement has nothing to do with the logging. It is included to make sure the routine action is executed.

Example using a variable:

```
CODE:
$logText = "This is a test";
logText($logText);
$DOACTION=true;
```

Tip: Any variable available in a CODE segment (limited by trigger type) can be used when creating the text to be logged. For details, see *Table 138, "Variables, Definitions, and Availability," on page 468*.

Tip: It is best practice to avoid using parentheses or quotation characters in the `<text>` string to be logged, as these can cause syntax errors.

Important: To protect the Nyquist system from running out of disk space, the system will only allow the user to log up to 500 MB of log messages per day before refusing to log additional messages. The Routines feature will continue logging Routine start/finish entries without a limit; only user-generated messages are limited. This user limit provides enough logging capacity for approximately 6200 bytes of log data per second during an entire day. The Routines log files are rotated every day, while making the last 31 days available. If the log files reached their maximum capacity every day for 31 days in a row, the maximum total storage used would be 16 GB; but it is very likely that the actual space used would be far less because rotated log files are compressed.

Webhook Functions

The Webhook-Post routine action invokes a webhook. The data returned by that webhook can be accessed within a Routine Action condition using the `getWebhookReturnValue` and `getWebhookReturnData` functions.

Table 142. Webhook Functions

Function Name	Description

getWebhookReturnValue(<format>)	This function returns a string based on the specified HTML-compatible format string, in which JSON elements from the response to the most recent Webhook-Post routine action are specified using JSON dot-notation within double curly-bracket pairs, as shown in this example:
	`"<b>Employee name:</b> {{employee.fName}} {{employee.lName}}"`
	Alternatively, the format string can specify the name of a single JSON property from the response without curly brackets. The first occurrence (based on a depth-first transversal) of a JSON element with the specified property name will be returned.
	`"fName"`

getWebhookReturnData()	The `getWebhookReturnData()` function returns a string containing the entire HTTP body of the response returned by the last Webhook-POST action. This is typically used for debugging purposes, but can also be used to access a non-JSON response.

Example

Assume the following JSON data returned by the POST command of a Webhook-POST action:

```
{
  "employee": {
    "id":"12345678",
    "fName":"John",
    "lName":"Doe"
  }
}
```

and assume the following Routine Condition CODE segment:

```
CODE:
$user_var[1] = getWebhookReturnValue("id");
$user_var[2] = getWebhookReturnValue(
   "<i>Employee $user_var[1] name:</i> {{employee.fName}} {{employee.lName}}" );
logText( getWebhookReturnData() );
```

The `id` value from the JSON data, "12345678", is assigned to `$user_var[1]`, and the string, "*Employee 12345678 name*: John Doe", is assigned to `$user_var[2]`. These variables can be used subsequently, such as in the **Text** property of a Display-Msg action or a `logText` function.

The `logText` line from the example logs the entire HTTP response body of the Webhook-POST action to the `nyquist_routines.log` file (see *"Logging Functions" on page 484*).

CAP Message Functions

Several condition functions can access properties of the Common Alerting Protocol (CAP) alert specified via the `xml` parameter of a Routine initiated via the Routines API v2 (see *"Routines API v2" on page 429*).

Table 143. CAP Message Functions

Function Name	Description

getCapAlertElement (<element_name>)	Retrieves the value of the specified sub-element of the <alert> segment of the current CAP message. Valid values are:
	• identifier • status • scope • note
	• sender • msgType • restriction • references
	• sent • source • code • incidents
	
	Example Condition text:
	`CODE:`
	`$user_var[1] = getCapAlertElement("msgType");`
	`if ("$user_var[1]" == "Alert") {`
	`  $DOACTION=true;`
	`} else {`
	`  $DOACTION=false;`
	`}`

getCapInfoElement (<element_name>)	Retrieves the value of the specified sub-element of the alert's <info> segment of the current CAP message. Valid values are: • language • responseType • certainty • onset • category • urgency • audience • expires • event • severity • effective • senderName
isPointInCapArea (<lat>,<long>)	Returns true if the specified latitude and longitude values are within the geographic area specified by the current CAP message; otherwise, it returns false.

Available Condition Variables

The following variables are available for use in the conditional statement. Their availability depends on the trigger that started the Routine (and, in some cases, the Action being executed).

Important: Condition statements use PHP syntax (for a PHP tutorial, see https://www.w3schools.com/php/default.asp). PHP variable names are case-sensitive, so ensure all variables use the appropriate uppercase and lowercase letters.

Note: Remember that these variables can be used *only* within an action's condition statement. For variables that can be used within other fields (e.g., Text, Text to Log, etc.), see *Table 138, "Variables, Definitions, and Availability," on page 468*.

Table 144. Conditional Statement Variables

Trigger	Variables

All Triggers	`$caller`
	Station extension or DID Caller ID Number
	`$callerName`
	`$called`
	Station extension
	`$calledName`
	`$cputemp`
	Current temperature (in °C) of the CPU core with the highest temperature.
	`$curtime`
	Current time in 24-hour format: HH:MM:SS
	`$DOACTION`
	In a CODE: segment, setting this variable to true indicates that the current action should be executed, otherwise the current action will not be executed (default is false, don't execute). When using a CODE: segment, you must include the `$DOACTION` variable to indicate if the current Action should be executed or not.
	If `$gotoActionName` is also set, and `$DOACTION` is set to true, the current Action will be executed before branching to the eventAction specified by `$gotoActionName`.
	`$gotoActionName`
	Assigning the name of an Action to this variable will cause the Routine to branch to that Action.
	`$origCaller`
	Station extension or DID Caller ID Number
	`$schedParam1 and $schedParam2`
	Parameters passed via a Schedule Routine.
	`$trigger`
	Trigger type name in all lowercase characters, e.g. "facility-page"

Table 144. Conditional Statement Variables

Trigger	Variables
	`$user_var[1…10]` The values in this general purpose array can be set and/or referenced within the Routine Condition CODE: segments and Actions of the current Routine.
	Tip: The database variable functions (see *"Database Variable Functions" on page 482*) can also be used within conditional statements and provide similar functionality to the `$user_var` array, but allow values to be accessible across routines. Unlike the `$user_var` array, however, the database variable functions cannot be used outside of action condition statements. To use the database variables from within an Action's Text property, for example, assign the value to an element of the `$user_var` array (e.g., `$user_var[1]=dbGet("key1")`) and reference that `$user_var` element within the Text field.
	`$weekday` Three-letter textual representation of current day: "Mon", "Tue", "Wed", "Thu", "Fri", "Sat", "Sun"
Actions: • Display-Msg	`$ga10pvExt` This variable can be assigned an integer value to specify the station extension of the NQ-GA10PV or NQ-S1810WBC station on which the message should be displayed.
Actions: • Display-Msg	`$autoDeleteDisplayMsgsUponExit` Setting this variable to true causes Display Messages created by the Routine to be removed when the Routine exits.
	`$autoDeleteDashMsgsUponExit` Setting this variable to true causes Dashboard Messages to be removed when the Routine exits.
	`$mergeDelete` Setting this variable to true merges Display-Msg-Delete and subsequent Display-Msg actions into one operation to improve performance for GA10PV displays. See *"Merging Display Message Delete with new Display Message Create" on page 492* for a detailed explanation.

Routines API v1	`$apiParam1`
	`$apiParam2`
	Query parameters specified in the URL of a Routines API v1 call. See *"Routines API v1" on page 445* for further details.

Table 144. Conditional Statement Variables

Trigger	Variables
Routines API v2	`$apiParam1, $apiParam2, ..., $apiParam20` Up to 20 parameter values—specified via the `routineApiParams` element of the API call's `data` or `json` element—can be referenced as `$apiParam1` through `$apiParam20`. See *"Routines API v2" on page 429* for further details.
Alarm	`$alarmDtmfCode` `$alarmName`
Amp-Protection-Mode	`$deviceMacAddr` `$deviceName`

Announcement	`$announceType`
	"Emergency", "Normal"
	`$announceDtmfCode`
	`$zoneNumber`
	`$zoneName`
	Format for regular playlist, sound machine and radio:
	`Zone <zone-number> - <zone-name>`
	Format for Line-Input:
	`<amplifier/matrix-mixer name>  - Ext: <ext-number> Ch: Channel <# (#)>`
	Note: There must be two spaces before "`- Ext:`"

Audio-Dist	`$audioDistCmd`
	"start" or "stop"
	`$audioDistName`

Facility-Page
Facility-Status-Down
Facility-Status-Up
	`$facilityPageNumber`
	`$facilityName`
	Note: The Facility-Page trigger will be fired once for each paged facility. The local facility, however, will fire the All-Call trigger instead of Facility-Page,

Input-Contact-Closed
Input-Contact-Opened
	`$ioContactStation`
	`$ioContactNumber`
	`$ioContactAction`
	"Closed" or "Opened"

NWS-Alert	`$nwsAlertEvent`
	`$nwsAlertSeverity`
	`$nwsAlertCertainty`
	`$nwsAlertUrgency`
	`$nwsAlertResponse`
	Note: See *"Alert Filters Configuration" on page 535* for possible values of these variables.

Table 144. Conditional Statement Variables

Trigger	Variables
Sched-Event	`$eventId` `$eventName`

Schedule-Activated	`$scheduleId`
	`$scheduleName`
	Schedule's name or "Holiday" for any holiday

Scheduled-Routine	`$schedParam1`
	`$schedParam2`
	`$zoneNumber` (if Zone provided)
	`$zoneName` (if Zone provided)

Scheduled-Tone **Tone**	`$toneDtmfCode` `$toneName`

Station-Status-Down
Station-Status-Up
	`$station`
	Station extension
	`$stationStatus`
	"Down" or "Up"

Zone-Page	`$zoneName`
	Format: "Zone <zone-number> - <zone-name>"
	`$zoneNumber`

When doing comparisons with variables that contain station extension numbers (e.g. $caller, $station), make sure to surround the numeric constants with quotes. For example, when comparing $caller to 105, use the following statement:

```
$caller == "105"
```

This is important because if station extension numbers begin with one or more zeros, numeric comparisons will not work properly. For example, when comparing $caller to 0105, use the following statement:

```
$caller == "0105"
```

Automatic Deletion of GA10PV Display Messages and Web Interface Dashboard Messages Upon Exit

The following variables can be set to true in a CODE: section to cause Display Messages or Dashboard Messages created by the Routine to be automatically deleted upon the Routines exit:

```
$autoDeleteDisplayMsgsUponExit
$autoDeleteDashMsgsUponExit
```

For example, in a CODE: section, including the following statement will cause all Display Messages created by the Routine to be automatically deleted upon routine exit:

```
CODE:$autoDeleteDisplayMsgsUponExit=true;
```

Using a <Parameter#> to change the target GA10PV Display

When a routine is executed via DTMF dialing, one of the supplied parameters can be used to change the target GA10PV Display for a Display-Msg Routine Action.

In the Condition field of a Display-Msg routine action, a CODE: segment can be used to change the GA10PV Display to a GA10PV extension specified in `<Parameter1>` or `<Parameter2>` of the dialed DTMF digits.

For example, if the user dials, `*94<routine-DTMF-code>*105`, the following CODE: segment, placed in the Condition field of a Display-Msg Action, will cause the GA10PV with extension 105 to be used:

```
CODE:
$ga10pvExt=$cmdParam1;
$DOACTION=true;
```

Merging Display Message Delete with new Display Message Create

If your routine is executing in a loop and contains actions that create a new display message on a GA10PV, waits for some time or event, deletes the display message, and then immediately creates a new display message, you can use the conditional variable `$mergeDelete` to have the Display-Msg-Delete and subsequent Display-Msg create actions merged to prevent the GA10PV from being notified/updated twice. Using this variable in this way will help improve performance for GA10PV displays, especially if audio is being played to the GA10PV.

To use the `$mergeDelete` conditional variable, add the following to the **Conditional** field for the Display-Msg-Delete action:

```
CODE:$mergeDelete=TRUE;$DOACTION=TRUE;
```

Note: When you use `$mergeDelete`, make sure you have a Display-Msg action that will be immediately executed after the Display-Msg-Delete, otherwise you may notice that the deleted message is not being removed from the GA10PV display. The deleted message will be removed as soon as the new display message is created. Proper testing of your routine can ensure that you get the intended results.

Routines Log

The Routines feature logs the start and finish of routines to the `nyquist_routines.log` log file (see *Table 120, "System Logs," on page 360*) using the following format:

```
<date time> <pid> [<routine-name>] <status> (<routine-initiator>)
```

where <date time> is replaced with the date and time for the status event, <pid> is replaced with the routine's process ID (to facilitate correlation of log entries), <routine-name> is replaced with the routine's name, <routine-initiator> is replaced with the routine trigger type that started the routine, and <status> is replaced with either Started, Not started, Finished, Stopped, or Exited (see below for more details).

When routines are started, a log entry is added to the nyquist_routines.log file using the following format:

```
<date time> <pid> [<routine-name>] Started (<routine-initiator>)
```

In this and other entries, the value of <routine-initiator> is based on how the routine was initiated.

- In most cases, <routine-initiator> is replaced with the name of the trigger that started the routine.
- If a routine is started via the routines API, <routine-initiator> is set to "API".
- If a routine is started via Dashboard or IP Phone via DTMF, <routine-initiator> is set to "DTMF/System".
- If a routine is started by the Nyquist system, <routine-initiator> is set to "DTMF/System".
- If a routine is started by a reboot trigger, <routine-initiator> is set to "reboot".

When routines finish, a log entry is added to the nyquist_routines.log file using the following format:

```
<date time> <pid> [<routine-name>] Finished (<routine-initiator>)
```

If a routine finishes but no Actions were enabled, a log entry is added to the nyquist_routines.log file using the following format:

```
<date time> <pid> [<routine-name>] Finished - no actions (<routine-initiator>)
```

When a routine is terminated, a log entry is added to the nyquist_routines.log file using the following format:

```
<date time> <pid> [<routine-name>] Exited - terminated (<routine-initiator>)
```

Routines may be terminated by the user via the Web Interface dashboard Routines Manager or when the Nyquist system is restarted by the user.

If a routine fails to start, a log entry is added to the nyquist_routines.log file using the following format:

```
<date time> <pid> [<routine-name>] Not started - disabled (<trigger-type>)
<date time> <pid> [<routine-name>] Not started - already running (<trigger-type>)
```

where <trigger-type> is replaced with the Routine Trigger type that attempted to start the Routine.

If a routine receives an invalid parameter value, a log entry is added to the nyquist_routines.log file. Invalid parameter *names*, however, are simply ignored by the API and are not logged.

If a routine using $alerts() with REPEAT_# is disabled by the user or by another routine while it is already running, a log entry is added to the nyquist_routines.log file using the following format:

```
<date time> <pid> [<routine-name>] Stopped - disabled (<routine-initiator>)
```

If a routine is terminated due to a CODE segment error, the following entry will be logged:

```
<date time> <pid> [<routine-name>] Exited - terminated due to CODE segment error (<routine-initiator>)
```

Exporting a Routine

You can export routines to share with Bogen Technical Support for debugging issues or to later import them to other servers.

To export a routine:

1. On the navigation bar, select **Routines**.
2. Select the routine or routines that you want to export.
3. Select **Export**.

   The SQL files (one file for each exported routine) will be saved to the **Downloads** folder on the server and can then be copied to a shared directory or to removable media.

Important: To export multiple routines at once, you may first need to configure your browser to allow pop-ups and redirects in the Nyquist server's site settings.

To allow pop-ups for this server:

1. Click the lock icon to the left of the server address in the browser URL bar.
2. On Chrome, select **Site Settings**.
3. Set "Pop-ups and redirects" to **Allow**.

Importing a Routine

You can import a routine that was created from other Nyquist server to your Nyquist server.

Note: After importing a routine, you must ensure that parameters are correct for the server since the server that created the routine will not have the same station, zone, or audio files as the server to which you are importing the routine. Imported routines must be enabled and the DTMF code will need to be changed if the same code is already being used on the server.

Caution **Form Field Parameter Name** values that reference image files (i.e., Display-Msg actions with JSON-Uploaded-Image message types) are not exported or imported. Manually specify this value for all relevant Actions after importing any Routine that uses this feature.

To import a routine:

1. On the navigation bar, select **Routines**.
2. Select **Import**.

3 From the Import popup window that appears, select **Choose file**.

4 Use the browser window to select the routine that you want to import.

5 Select **Import**.

Managing Routine Database Variables

The C4000 provides database variables that can be accessed within Routine Action condition statements (see *"Condition Statement Functions" on page 481*). You can view, insert, delete, or modify these database variables, not only through Nyquist functions, but also via the web interface.

To view the database variables:

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

2 Select Manage Routines Database Variables

3 The key, value, and most recent routine to access each variable are displayed.

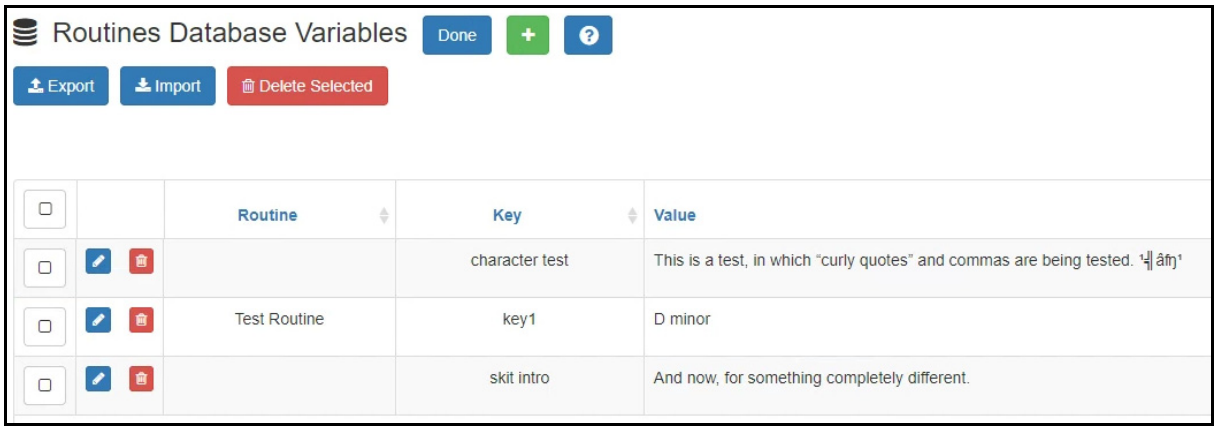


Figure 201. Routines Database Variables

To add a database variable:

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

2 Select Manage Routines Database Variables

3 Click **Add**.

4 Enter a unique **Key** name (maximum of 64 characters) and a **Value** (maximum of 4095 characters).

5 Click **Save**.

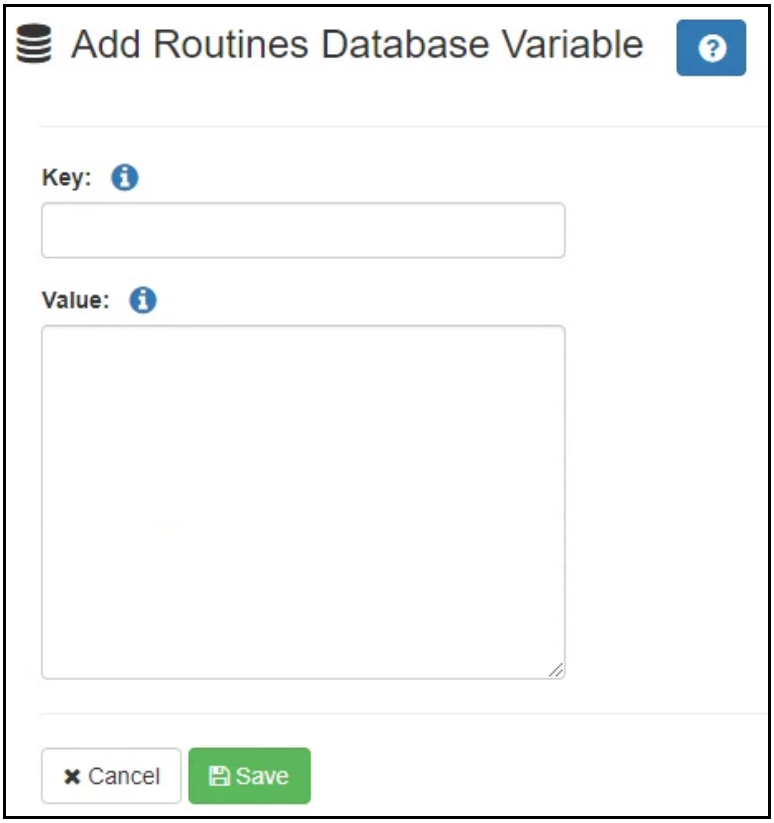


Figure 202. Add Routines Database Variable

To edit a database variable:

1. On the navigation bar, select **Routines**.
2. Select Manage Routines Database Variables
3. Click the **Edit** button next to the variable to be edited.
4. Update the Key and/or Value for the variable.
5. Click **Save**.

To delete one or more database variables:

1. On the navigation bar, select **Routines**.
2. Select Manage Routines Database Variables
3. Click the **Delete** button for a specific variable, or
4. Select one or more variables (via checkboxes) to delete.
5. Click **Delete Selected** and confirm the deletion.

Importing and Exporting Database Variables

Database variables are backed up and restored as part of the normal system backups (see *"Backing Up Your Nyquist System and Files" on page 349*); however, it can sometimes be helpful to export and import database variables to and from a CSV (comma-separated value) text file, such as to transfer variables between systems or to create and/or edit variables in another application (e.g., a spreadsheet).

To export the current database variables:

1. On the navigation bar, select **Routines**.
2. Select **Manage Routines Database Variables**
3. Select (via checkboxes) one or more variables to export.
4. Click the **Export** button
5. The `routine_db.csv` file will be downloaded to your browser's download directory.

Each row of the exported CSV file contains four comma-separated columns:

- For future use. When importing, this column should always contain a zero (0).
- Routine ID (enclosed in double quotes)

  In an exported file, this may contain the routine ID that last accessed the variable. When importing, this column can contain a "0" (zero) or the previously exported value.
- Variable name (enclosed in double quotes)
- Variable value (enclosed in double quotes)

To import database variables from a CSV file:

1. On the navigation bar, select **Routines**.
2. Select **Manage Routines Database Variables**
3. Click the **Import** button
4. On the *Import Routines Database Variables* page:
   a) Click the **Choose file** button and select the CSV file to import.
   b) If you want to delete all existing database variables before importing, set **Delete all data before importing** to Yes.
   c) Select whether you want to **Replace** or **Ignore** keys that already exist, whether defined prior to importing or defined multiple times within the CSV file.
   d) Press the **Import** button.
5. The database variables defined in the CSV will be imported into the database and will be displayed on the *Routines Database Variables* page.

Managing Display Messages

It is possible to display messages and images on NQ-GA10PV devices and messages on NQ-S1810WBC and NQ-DSC01 devices, either manually or through a triggered Routine. Messages containing text and sent manually can be defined and sent as needed. To send messages using triggered Routines or to define messages that can be used at a later time, you can create *message templates* (see *"Viewing Message Templates" on page 511*). If a message is to include an image, whether to be sent immediately or within a template, you must first define a *message image* (see *"Viewing Message Images" on page 513*), which can then be used in the message or message template.

Tip: It is possible to programmatically display an image, without predefining a message image, by using the Routines API v2 (see *"Routines API v2" on page 429*).

The **Display Message** option allows you to create impromptu messages that will display on NQ-S1810WBC and NQ-DSC01 devices and monitors connected to NQ-GA10PV devices in a selected zone, in multiple zones, or to specific devices. When creating the message, you can set several options, including when and how long the message is displayed and the appearance of the message. You can also remove messages from the message queue.

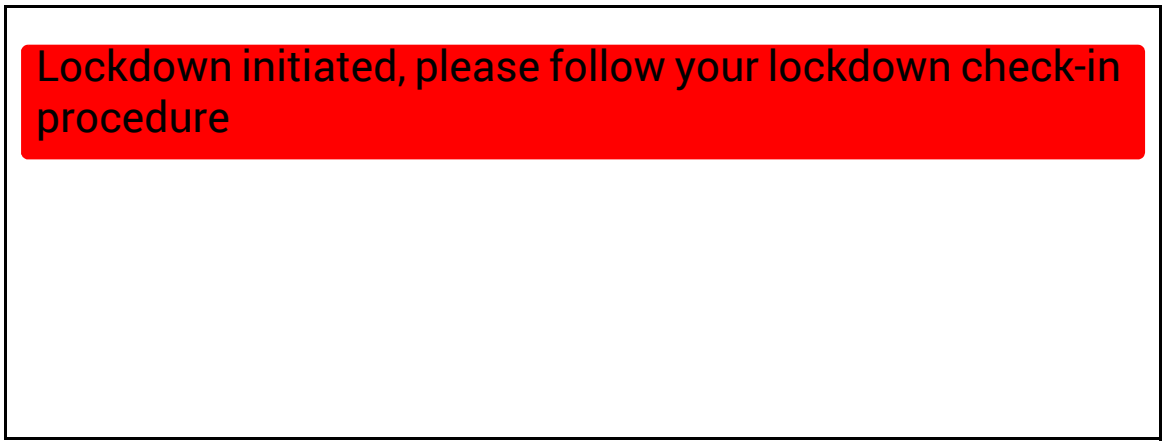


Figure 203. Example of NQ-GA10PV Message with Fullscreen Priority

The station's **Display Configuration** option controls the overall appearance of the display (e.g., what type of clock appears, whether an event or the date appears, and the background color of the screen). For information about setting the display configuration for an NQ-GA10PV, see *"Configuring Intercom HDMI Module Display Options" on page 176*.

The **Message Templates** option allows you to create and save messages in advance, which can be easily sent later. Sending a **Message Template** simply fills in a form with the saved message data. You must specify the zone and/or stations where the message will appear, override any other properties from the **Message Template** (if desired), and send it.

Saved **Message Templates** can also be used in **Routines** (see *"Using Routines" on page 425*), which allows messages to be sent automatically in response to various system events. When used this way, the Routine definition specifies the zone and/or stations where the message will appear and can optionally override other template properties.

Note: This discussion refers to GA10PV, S1810WBC, and DSC01 Display Messages, not the Messages section shown at the top of the Dashboard. For information on these Dashboard Messages, see *"Dashboard Messages" on page 367*.

Message Priorities and Precedence

Multiple simultaneous messages (with or without an image) can be displayed on an NQ-GA10PV, and the NQ-DSC01 can display two simultaneous messages, while the NQ-S1810WBC can only display one message at a time. It is possible, however, to queue up more messages than can be displayed at a time. To determine which messages to display first, we need to determine a message's precedence. Messages with a higher precedence are displayed before messages with lower precedence, and can even override and interrupt a lower precedence message.

Note: The term *priority*, as used here, refers to a numeric value assigned to a message. The term *precedence* refers to the determination of which message will be displayed over another message after evaluation of the assigned message priorities and other related factors, as described below.

There are several factors that affect the precedence and display of a message.

The first factor is the message **Priority**. This is a number from zero (0) through six (6), where zero is the lowest priority and six the highest.

The second factor is the **Image Priority**, which applies only to messages of type **Image**, and is applied when two messages have the same message priority. This is either **Text Over Image** or **Image Over Text**. The first implies that text messages have precedence over this image message, while the second implies this image message has precedence over text messages.

Note: As the NQ-DSC01 and NQ-S1810WBC cannot display message images, **Image Priority** only applies to the NQ-GA10PV.

The third factor does not actually affect the precedence, but is relevant in that it determines where an image is displayed, which can affect whether or not other messages can be seen. The **Image Type** of a message can be either **Right**, **Left**, or **Full Screen**. **Right** and **Left** specify on which half of the screen the image will be displayed, while **Full Screen** specifies that the image will cover the entire screen. Since text messages display on the right side of the screen, an image displayed on the left side can show both messages simultaneously, while an image displayed on the right side or full screen will be subject to the precedence rules.

Message Precedence Rules

The following set of rules determine which messages have precedence and how they are to be displayed:

- **Text** messages are sorted in descending order by priority, and then in the order they were sent.

- If two messages of the same type (**Image** or **Text**) have the same priority, the newer one has precedence.
- If an image message and a text message have the same priority, the Image message's **Image Priority** property determines which has precedence:
  - **Text Over Image**: Text message has precedence.
  - **Image Over Text**: Image message has precedence.
- **Full Screen** image messages take precedence over everything except another Full Screen image message, for which normal rules of precedence are applied.
- Priority **5 (Exclusive)** messages always display alone, which prevents all lower precedence messages from being displayed.
- For Analog Clock view:
  - An image message can display simultaneously on the left while another message is displayed on the right. Multiple image messages are prioritized according to normal rules. If there are no image messages displayed on the left, the clock will be displayed.
  - Image messages displayed on the right along with text messages based on normal rules of precedence.
- For multi-column and Digital Clock views:
  - Only **Text** or **Full Screen** image messages are displayed.

Note: Even when a message is not visible, usually due to a higher priority message being displayed, its expiration timer is still ticking, so it may display for shorter than the intended duration or not at all.

Creating a Display Message via the Dashboard

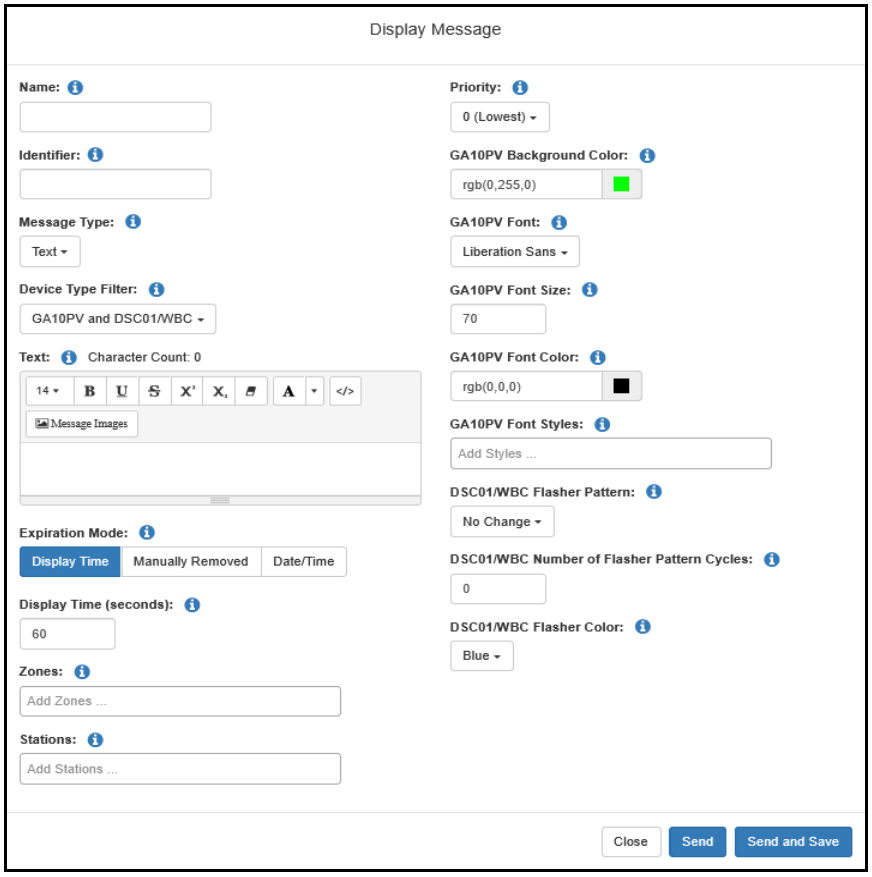


Figure 204. Display Message

Note: You also can add display messages through routine actions (see *"Adding an Action" on page 458*.)

To create a display message:

1. If not already on your dashboard, select **Dashboard** from the navigation bar.
2. Under **Tones/Announcements**, select **Display Message.**
3. On the Display Message page, complete the options for the new message.
4. To save the message as a Message Template and send it immediately, select **Send and Save**. The **Name** field must be specified to save a message.

Note: When saved as a Message Templates, an **Expiration Mode** of **Date/Time** will be converted to a **Display Time** of 60 seconds and an **Expiration Mode** of **Manually Removed** will be converted to a **Display Time** of zero (0) seconds.

---

5. To send the message immediately without saving it, select **Send**.

Note: The options set through the Display Message page are for the message only. If you want to change how the clock, date, or other display features appear, you must set configuration options for the NQ-GA10PV station (see *"Configuring Intercom HDMI Module Display Options" on page 176*).

Table 145. Display Message Options

Name	Specifies a name for this message. This is used if the message is to be saved.
Identifier	Used to identify the message so it can be deleted by a Routine action.
Message Type	Select the type of message to be sent: • **Text**: A text message will be displayed. • **Image**: An image will be displayed. *Note:* Selecting **Image** disables the **Priority** "5 (Exclusive)" option, sets **Priority** to "0 (Lowest)," sets **Device Type Filter** to "GA10PV Only," and disables NQ-DSC01 and NQ-S1810WBC (DSC01/WBC) options.
Device Type Filter	Select the device type(s) to which the message will be sent. Valid values are: • **GA10PV and DSC01/WBC** • **GA10PV Only** • **DSC01/WBC Only**
Text	Type the message that is to appear on the display monitor. You can format text using basic HTML tags, such as: • **bold** • *italic* • <u>underline</u> • styled text *Note:* Be aware that entering a new line, even within HTML tags, will create a new line in the final message.

Important: For further details about the Text field, including how to display images within a Text-type Display Message, see *Table 149, "Add/Edit Message Template Parameters," on page 517*.

Table 145. Display Message Options (continued)

Expiration Mode	Select the mode for setting the message's expiration. Options are: • **Display Time**: Uses **Display Time (seconds)** to set the expiration. • **Manually Removed**: Sets the expiration time to Never. You must use the **Remove Message** button to remove a message from the message queue, or the message can be removed by a Routine Action using the display message **Identifier**. • **Date/Time**: By default, the current date and time appear in the **Date/Time** field.
Display Time (seconds)	Appears only if **Expiration Mode** is set to **Display Time**. Sets the length of time for the message to be displayed before it expires. The specified value can range from 1 to 99999 seconds.
Expiration Date/Time	Appears only if **Expiration Mode** is set to **Date/Time**. By default, is set to the current date and time. To change the date, select the calendar and pick the date and time.
Zones	Select the zone or zones. Messages will be sent to the display devices in the selected zones.
Stations	The message is sent to the specified stations and any stations that belong to the specified zones.
Priority	Select the message priority, which can range from **0 (Lowest)** to **6 (Fullscreen)**. Priority **6 (Fullscreen)** is the highest priority, and when a message is assigned this priority, only the messages with this priority appear on the display with the Scheduled Event Name and Date being temporarily removed. If Priority **5 (Exclusive)** is selected, the Scheduled Event Name and Date remain on the display, but all other messages with lower priorities are removed. *Note:* Priority **5 (Exclusive)** is disabled for Image messages and enabled for Text messages.
Image Type	If the Type field was set to **Image**, select one of the following values to specify how the image will be displayed: • **Full Screen (1920x1080)**: Image will be displayed full screen. • **Left (925x1040)**: Image will be displayed on the left side of the screen. • **Right (925x1040)**: Image will be displayed on the right side of the screen.
Image Priority	Select the image priority for this message, which determines precedence when an Image message and Text message have the same message priority: • **Text Over Image**: Text message will be given precedence. • **Image Over Text**: Image message will be given precedence.

Table 145. Display Message Options (continued)

Message Image	The name of the saved **Message Image** to be displayed. For more information, see *"Create or Edit a Message Image" on page 514*. *Tip:* The predefined **Solid-Black** image can be used to clear the device's screen, *Note:* The dimensions of this image (which are displayed in parentheses after the image name) must match the dimensions implied by the **Image Type**. The list of images can contain *any* valid Image Type (i.e., 1920×1080 or 925×1040), but the specified image must match the selected **Image Type** size before saving the message template.
GA10PV Background Color	Select the color for the message background. You can select a color by: • Using the color picker • Entering a hex color (for example: #000000, for black) • Entering an RGB color (for example: rgb(0,0,0) for black) • Entering a color alias name (for example: red, blue, etc.) For more information, see *"Using Color in Display Messages" on page 505*.
GA10PV Font	Select the down arrow to view a list of available fonts and then select the desired font for the message text. Available fonts are: Comic-Relief Courier-Prime Gelasio Liberation Sans Linux Libertine
GA10PV Font Size	Enter the desired font size.
GA10PV Font Color	Select the color for the message text. You can select a color by: • Using the color picker • Entering a hex color (for example: #000000, for black) • Entering an RGB color (for example: rgb(0,0,0) for black) • Entering a color alias name (for example: red, blue, etc.) For more information, see *"Using Color in Display Messages" on page 505*.
GA10PV Font Styles	Place your cursor in the **Add Styles** box to select **Bold** or **Italic**. Otherwise, the **Font Style** remains at Regular.

Table 145. Display Message Options (continued)

DSC01/WBC Flasher Pattern	Specifies the on/off pattern the flasher will display. Valid values are: • **No Change**: The message will not cause the selected flasher to change from its current flasher setting. • **Off**: The selected flasher will be turned off unless a higher priority message is using the flasher. When the flasher is turned off, it will remain off until another message is sent with a new flasher setting. • **Slow**: The selected flasher will blink at a rate of once per second for the duration of the message. • **Fast**: The selected flasher will blink at a rate of twice per second for the duration of the message. • **Double**: Flash two (2) times within one second with a 1-second pause and repeat. • **Triple**: Flash three (3) times within 1.5 seconds with a 1-second pause and repeat. • **Quad**: Flash four (4) times within two seconds with a 1-second pause and repeat.
DSC01/WBC Number of Flasher Pattern Cycles	Specifies the number of times that the flasher pattern will repeat. Valid values are 1 through 65536 or zero (0) to flash continuously for the duration of the message.
DSC01/WBC Flasher Color	Specifies the color of the LED flasher. Valid values are: • **Amber** • **Blue** • **Green** • **Orange** • **Red** • **Violet** • **White** • **Yellow**

Using Color in Display Messages

You can select colors for display messages three different ways:

- Background, text, and time colors via GA10PV **Display Configuration** (see *"Configuring Intercom HDMI Module Display Options" on page 176*)
- Background and font colors for individual messages by selecting **Display Message** from the dashboard (see *"Creating a Display Message via the Dashboard" on page 501*)
- Background and font colors for individual messages via the **Display-Msg** routine action **Type** (see *Table 2, "Routine Action Type-Specific Parameters," on page 588*).

You can select colors by:

- Using the color picker
- Entering a hex color (for example: #000000, for black)
- Entering an RGB color (for example: rgb(0,0,0) for black)
- Entering a color alias name (for example: red, blue, etc.)

  When using a color alias name, the corresponding hex color code appears in the text portion of the color field and the swatch (i.e., color box) portion changes to the selected color. When entering a color alias, you cannot use spaces, and the system only accepts the default color alias listed in the following table:

Table 146. Default Color Alias

Color Alias	Corresponding Hex Code	Color Alias	Corresponding Hex Code
aliceblue	f0f8ff	antiquewhite	faebd7
aqua	00ffff	aquamarine	7fffd4
azure	f0ffff	beige	f5f5dc
bisque	ffe4c4	black	000000
blanchedalmond	ffebcd	blue	0000ff
blueviolet	8a2be2	brown	a52a2a
burlywood	deb887	cadetblue	5f9ea0
chartreuse	7fff00	chocolate	d2691e
coral	ff7f50	cornflowerblue	6495ed
cornsilk	fff8dc	crimson	dc143c
cyan	00ffff	darkblue	00008b
darkcyan	008b8b	darkgoldenrod	b8860b
darkgray	a9a9a9	darkgreen	006400
darkkhaki	bdb76b	darkmagenta	8b008b
darkolivegreen	556b2f	darkorange	ff8c00
darkorchid	9932cc	darkred	8b0000
darksalmon	e9967a	darkseagreen	8fbc8f
darkslateblue	483d8b	darkslategray	2f4f4f
darkturquoise	00ced1	darkviolet	9400d3
deeppink	ff1493	deepskyblue	00bfff
dimgray	696969	dodgerblue	1e90ff
firebrick	b22222	floralwhite	fffaf0
forestgreen	228b22	fuchsia	ff00ff
gainsboro	dcdcdc	ghostwhite	f8f8ff

Table 146. Default Color Alias (continued)

Color Alias	Corresponding Hex Code	Color Alias	Corresponding Hex Code
gold	ffd700	goldenrod	daa520
gray	808080	green	00ff00
greenyellow	adff2f	honeydew	f0fff0
hotpink	ff69b4	indianred	cd5c5c
indigo	4b0082	ivory	fffff0
khaki	f0e68c	lavender	e6e6fa
lavenderblush	fff0f5	lawngreen	7cfc00
lemonchiffon	fffacd	lightblue	add8e6
lightcoral	f08080	lightcyan	e0ffff
lightgoldenrodyellow	fafad2	lightgreen	90ee90
lightgrey	d3d3d3	lightpink	ffb6c1
lightsalmon	ffa07a	lightseagreen	20b2aa
lightskyblue	87cefa	lightslategray	778899
lightsteelblue	b0c4de	lightyellow	ffffe0
lime	00ff00	limegreen	32cd32
linen	faf0e6	magenta	ff00ff
maroon	800000	mediumaquamarine	66cdaa
mediumblue	0000cd	mediumorchid	ba55d3
mediumpurple	9370d8	mediumseagreen	3cb371
mediumslateblue	7b68ee	mediumspringgreen	00fa9a
mediumturquoise	48d1cc	mediumvioletred	c71585
midnightblue	191970	mintcream	f5fffa
mistyrose	ffe4e1	moccasin	ffe4b5
navajowhite	ffdead	navy	000080
oldlace	fdf5e6	olive	808000
olivedrab	6b8e23	orange	ffa500
orangered	ff4500	orchid	da70d6
palegoldenrod	eee8aa	palegreen	98fb98
paleturquoise	afeeee	palevioletred	d87093
papayawhip	ffefd5	peachpuff	ffdab9
peru	cd853f	pink	ffc0cb
plum	dda0dd	powderblue	b0e0e6
purple	800080	red	ff0000
rosybrown	bc8f8f	royalblue	4169e1
saddlebrown	8b4513	salmon	fa8072
sandybrown	f4a460	seagreen	2e8b57
seashell	fff5ee	sienna	a0522d
silver	c0c0c0	skyblue	87ceeb
slateblue	6a5acd	slategray	708090
snow	fffafa	springgreen	00ff7f
steelblue	4682b4	tan	d2b48c

Table 146. Default Color Alias (continued)

Color Alias	Corresponding Hex Code	Color Alias	Corresponding Hex Code
teal	008080	thistle	d8bfd8
tomato	ff6347	transparent	transparent
turquoise	40e0d0	violet	ee82ee
wheat	f5deb3	white	ffffff
whitesmoke	f5f5f5	yellow	ffff00
yellowgreen	9acd32		

Removing Display Messages via the Dashboard

The **Remove Message** window allows you to remove one or more messages from the display message queue. It can also expire a message that was created using **Manually Removed** as the **Expiration Mode**.

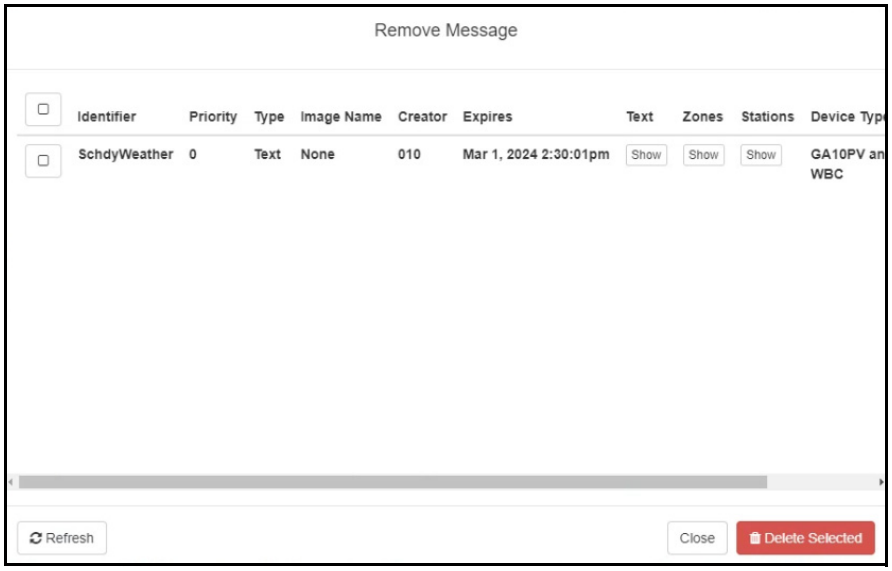


Figure 205. Remove Message

To remove one or more messages via the Remove Message button:

1. If not already on your dashboard, select **Dashboard** from the navigation bar.
2. Select the **Remove Message** button from the *Tones/Announcements* section.
3. Select one or more messages to be removed.
4. Select the **Delete Selected** button.
5. Optionally select **Refresh** to update the list of pending messages.
6. Optionally repeat the previous steps to remove more messages.
7. Select **Close** to close the window.

Tip: Removing all messages from the NQ-GA10PV does not necessarily clear the display, which may still show other messages and a clock. To completely clear the display and ensure that it will not display a message or the clock (i.e., completely black), show the **Solid-Black** image at the highest priority.

Table 147. Remove Message

Identifier	Indicates the identifier of the message, by which the message can be deleted by a Routine action.
Priority	Indicates the message priority, which can range from **0 (Lowest)** to **6 (Fullscreen)**.
Type	Indicates the type of message: • **Text**: A text message will be displayed. • **Image**: An image will be displayed.
Image Name	Indicates the name of the **Message Image** being displayed, or **None** if the **Type** is **Text**.
Creator	Displays the extension of the user that displayed this message.
Expires	Displays the date and time when the message will expire.
Text	Displays the message that appears on the display monitor.
Zones	Displays the zones within which the message has been sent.
Stations	Indicates the stations at which the message is displayed.
Device Type Filter	Indicates the device type(s) to which the message has been sent. Valid values are: • **GA10PV and DSC01/WBC** • **GA10PV Only** • **DSC01/WBC Only**

Table 147. Remove Message

Flasher

Indicates the flasher pattern, pattern cycles, and flasher color displayed on NQ-S1810WBC devices.

Flasher Pattern

Specifies the on/off pattern the flasher will display.

Valid values are:

- **No Change**: The message will not cause the selected flasher to change from its current flasher setting.
- **Off**: The selected flasher will be turned off unless a higher priority message is using the flasher. When the flasher is turned off, it will remain off until another message is sent with a new flasher setting.
- **Slow**: The selected flasher will blink at a rate of once per second for the duration of the message.
- **Fast**: The selected flasher will blink at a rate of twice per second for the duration of the message.
- **Double**: Flash two (2) times within one second with a 1-second pause and repeat.
- **Triple**: Flash three (3) times within 1.5 seconds with a 1-second pause and repeat.
- **Quad**: Flash four (4) times within two seconds with a 1-second pause and repeat.

Pattern Cycles

Specifies the number of times that the flasher pattern will repeat.

Valid values are 1 through 65536 or specify zero (0) to flash continuously for the duration of the message.

Flasher Color

Specifies the color of the LED flasher. Valid values are:

- **Amber**
- **Blue**
- **Green**
- **Orange**
- **Red**
- **Violet**
- **White**
- **Yellow**

Table 147. Remove Message

Refresh	Refreshes the list of current messages.
Delete Selected	Removes the selected messages from the devices on which they are displayed.

Removing an Event Name from a Display

If you create a scheduled event with **Display Event Name** enabled, the event remains on the display that is connected to an NQ-GA10PV until the next scheduled event replaces it.

To clear the event name from the display, create another scheduled event with the **Name** set to **No-Event**.

For information on creating scheduled events, see *"Adding an Event" on page 270*.

Viewing Message Templates

The **Message Templates** page allows you to quickly view saved message details; create a message to be added to the database; and edit, delete, or send a message. Messages appearing on the **Message Templates** page also include messages that were started using the **Send and Save** button on the Display Message popup (see *"Creating a Display Message via the Dashboard" on page 501*).

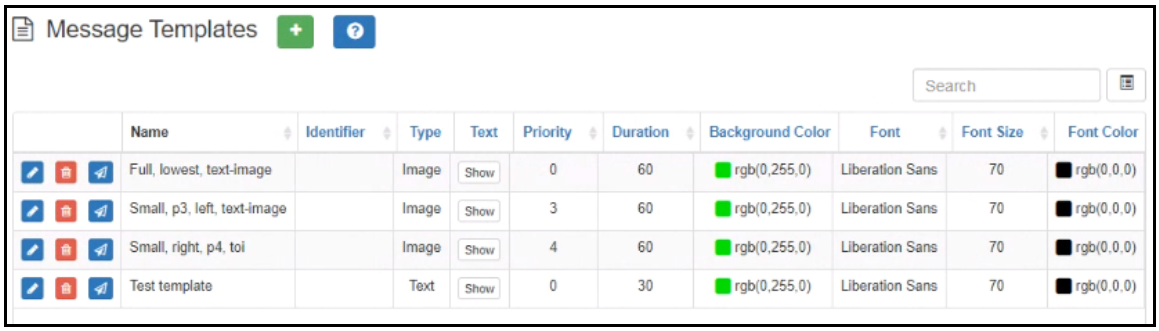


Figure 206. Message Templates

To view saved message templates:

1 From the navigation bar, select **Messages** then **Message Templates**.

The **Message Templates** page displays the following fields for each saved message:

Table 148. Message Templates

Edit button	Edits the message template.
Delete button	Deletes the message template.

Table 148. Message Templates

Send button	Displays the Display Message page, from which a message can be sent (see *"Display Message Options" on page 502* for further details). *Note:* The Display Message page will be initialized with the settings from the selected message template and can be modified for the message to be sent, but the template will not be altered unless the **Send and Save** button is selected.
Name	Specifies a name for this message.
Identifier	Used to identify the message so it can be deleted by a Routine action.
Message Type	Displays the type of message: • **Text**: A text message will be displayed. • **Image**: An image will be displayed.
Text	Place the mouse over the **Show** icon to view the text message that is to appear on the display monitor. For Image messages, this does nothing.
Priority	Displays the message priority, which can range from **0 (Lowest)** to **6 (Fullscreen)**. Priority **6 (Fullscreen)** is the highest priority, and when a message is assigned this priority, only the messages with this priority appear on the display with the Scheduled Event Name and Date being temporarily removed. If Priority **5 (Exclusive)** is selected, the Scheduled Event Name and Date remain on the display, but all other messages with lower priorities are removed. *Note:* Priority **5 (Exclusive)** is disabled for Image messages and enabled for Text messages.
Duration	Sets the length of time in seconds for the message to be displayed before it expires. Time can range from 1 to 99999.
Background Color	Displays the color for the message background. For more information, see *"Using Color in Display Messages" on page 505*.
Font	Specifies the font for the message text.
Font Size	Specifies the font size for the message text.
Font Color	Displays the color for the message text. For more information, see *"Using Color in Display Messages" on page 505*.
Font Styles	Displays the style (bold, italic) for the text. If blank, the message will use the regular style.
Image Type	If the Type field was set to Image, displays one of the following values to specify how the image will be displayed: • **Full**: Image will be displayed full screen. This value is also shown for text message templates. • **Left**: Image will be displayed on the left side of the screen. • **Right**: Image will be displayed on the right side of the screen.

Table 148. Message Templates

Message Image	For text message templates, "**None**" is shown. For image templates, the Name of the saved Message Image to be displayed.

Tip: The predefined **Solid-Black** image can be used to clear the device's screen,

Image Priority	Displays the image priority for this message, which determines precedence when an Image message and Text message have the same message priority: • **Text Over Image**: Text message will be given precedence. • **Image Over Text**: Image message will be given precedence.

Viewing Message Images

The **Message Images** page allows you to quickly view message image details; view the full-sized message image (by clicking on the thumbnail); add a message image to the database; edit or delete a message image; or copy the URL of a message image to the clipboard.

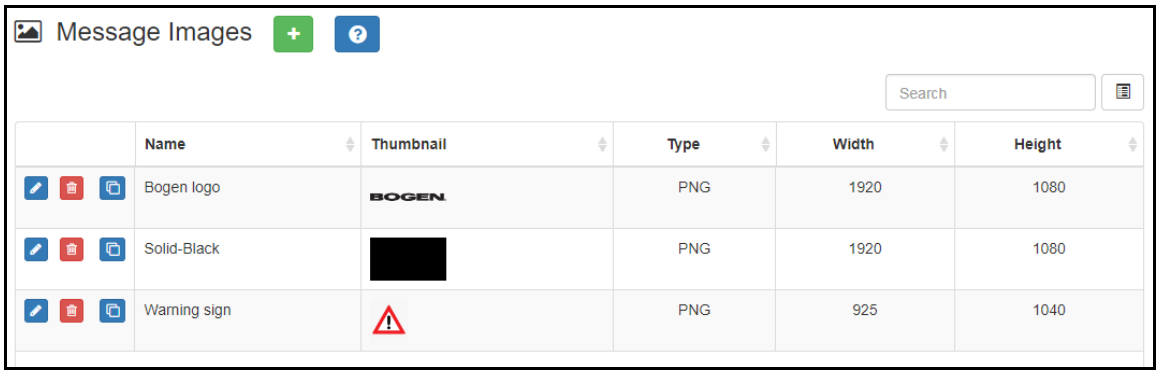


Figure 207. Message Images

To view saved message images:

1 From the navigation bar, select **Messages** then **Message Images**.

Tip: The **Solid-Black** image is available by default. This is a 1920×1080 black PNG image that can be used to "turn off" an NQ-GA10PV display, such that it will not display a message or the clock (i.e., completely black).

The **Message Images** page displays the following fields for each saved image:

Figure 208. Message Images properties

Edit button	Edits the message image.
Delete button	Deletes the message image.
Copy URL button	Copies the image URL to the clipboard.

Figure 208. Message Images properties

Name	Name of the message image.
Thumbnail	Displays a thumbnail of the message image. Placing the mouse over the image will display a URL at which the image can be accessed from the Nyquist server. When clicked, the full image is displayed in a new browser tab.
Type	Format of the image. Allowed image formats include: • PNG • JPEG
Width	Image width (in pixels).
Height	Image height (in pixels).

Creating a Message Template via the Message Templates Page

You can create messages in advance which can be easily selected for use when needed. Selecting a saved message fills in a form with the message data. Information about which zones or stations will receive the message, though, is not included in this form. You specify the zone or station when you send the message.

These saved messages can also be used in Routines (see *"Using the Routines API" on page 428*).

Create or Edit a Message Image

If the message is to display an image, you must first define one or more Message Images. An image can be used by one or more message templates, or even by an ad-hoc Display Message command.

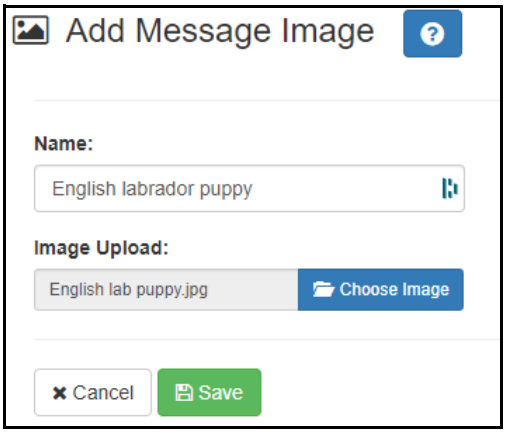


Figure 209. Add Message Image

To create (or edit) a message image:

1. On the navigation bar, select **Messages**, then **Message Images**.
2. Select the **Add** icon (or the Edit icon next to an existing **Message Image**).
3. Assign a name for this image.
4. Select the **Choose Image** button and select an image file to upload.

Note: An image to be used in a message must be in the PNG or JPEG format. The PNG format has the advantage of supporting transparency, which allows the background to display through the image.

Note: If this image will be used as part of an Image-type message (as opposed to being embedded as an `<img>` HTML element in a Text-type message), the image must have dimensions of either 925x1040 or 1920x1080, depending on whether it will be used full screen (1920x1080) or half screen (925x1040).

---

5. Select **Save**.

Create or Edit a Message Template

A Message Template predefines a message and all of its properties so that it can easily be sent at a later time, whether manually or from a triggered Action in a Routine.

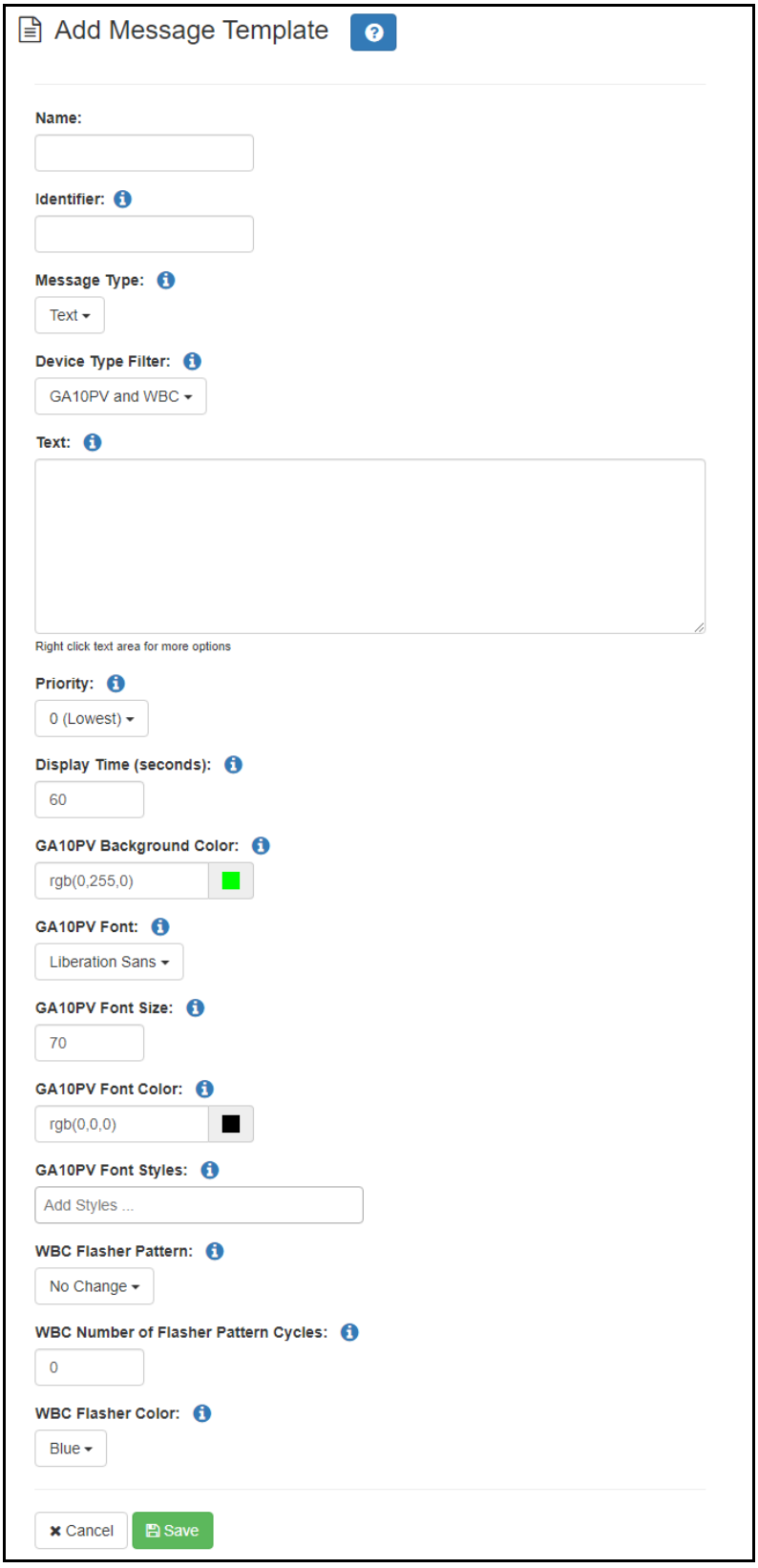


Figure 210. Add Message Template

To create (or edit) a message template:

1. On the navigation bar, select **Messages**, then **Message Templates**.
2. Select the **Add** icon (or the Edit icon next to an existing **Message Template)**.

3 Provide a descriptive **Name** for the image.

4 Complete the options on the **Add Message Template** page.

5 Select **Save**.

Note: You can edit saved messages, but if the message is called by a routine, it won't be dynamically updated when the routine starts.

Table 149. Add/Edit Message Template Parameters

Name	Specifies a name for this message. This is used if the message is to be saved.
Identifier	Used to identify the message so it can be deleted by a Routine action.
Message Type	Select the type of message to be sent: • **Text**: A text message will be displayed. • **Image**: An image will be displayed. *Note:* Selecting **Image** disables the **Priority** "5 (Exclusive)" option, sets **Priority** to "0 (Lowest)," sets **Device Type Filter** to "GA10PV Only," and disables NQ-DSC01 and NQ-S1810WBC (DSC01/WBC) options. This value will determine which of several following parameters will be displayed.
Device Type Filter	Select the device type(s) to which the message will be sent: • **GA10PV and DSC01/WBC** • **GA10PV Only** • **DSC01/WBC Only**

Table 149. Add/Edit Message Template Parameters

Text

Type the message that is to appear on the display monitor.

Tip: Click and drag the bottom-right corner to adjust the size of the edit box.

You can format text using basic HTML tags, such as:

- `<b>bold</b>`
- `<i>italic</i>`
- `<u>underline</u>`
- `<span style="color:blue; border: 2px solid red">styled text</span>`

Note: Be aware that entering a new line, even within HTML tags, will create a new line in the final message.

As shown in the `<span>` example, above, HTML elements can also include CSS style definitions to modify their positioning and appearance. (For details on CSS, see https://www.w3schools.com/css.)

Tip: The edit box menu provides basic HTML font formatting options. Press the **</>** button to toggle between the formatted preview and the raw HTML Code View.

You can also use the `<img>` HTML tag to display an image. For example:

```
<img src="https://bogen.com/themes/bogen/logo.png" width="250"
height="48">
```

An image displayed using this mechanism is not restricted to the standard image sizes to which Image-type messages are restricted, but may require more detailed specification of attributes and style to ensure it appears correctly on the screen.

Note: If the `<img>` HTML tag is used, verify that the GA10PV devices on which this message will be displayed has network/internet access to the specified URL.

Tip: You can easily insert an `<img>` HTML tag for a previously uploaded Message Image to the message (see *"Create or Edit a Message Image" on page 514*) by clicking the edit box's **Message Images** button, selecting an image from the list of defined Message Images, and clicking the **Insert Image** button. You can edit the generated HTML tag (using Code View) to adjust the displayed image's appearance as needed.

Table 149. Add/Edit Message Template Parameters

Priority	Select the message priority, which can range from **0 (Lowest)** to **6 (Fullscreen)**. Priority **6 (Fullscreen)** is the highest priority, and when a message is assigned this priority, only the messages with this priority appear on the display with the Scheduled Event Name and Date being temporarily removed. If Priority **5 (Exclusive)** is selected, the Scheduled Event Name and Date remain on the display, but all other messages with lower priorities are removed. *Note:* Priority **5 (Exclusive)** is disabled for Image messages and enabled for Text messages.
Display Time (seconds)	Sets the length of time for the message to be displayed before it expires. This value can range from 0 to 99999 seconds. A value of zero (0) indicates that the message will display indefinitely (i.e., until the device has been restarted or the message is removed by a Display-Msg-Delete action or via the Dashboard's **Remove Message** button).
Image Type	Select the image type to specify the image dimensions and how the image will be displayed: • **Full Screen (1920x1080)**: Image will be displayed full screen. • **Left (925x1040)**: Image will be displayed on the left side of the screen. • **Right (925x1040)**: Image will be displayed on the right side of the screen.
Image Priority	Select the image priority for this message, which determines precedence when an Image message and Text message have the same message priority: • **Text Over Image**: Text message will be given precedence. • **Image Over Text**: Image message will be given precedence.
Message Image	Select the image to be displayed for this message from the list of **Message Images**. *Tip:* The predefined **Solid-Black** image can be used to clear the device's screen, *Note:* The dimensions of this image (which are displayed in parentheses after the image name) must match the dimensions implied by the **Image Type**. The list of images is restricted to those with dimensions compatible with *any* valid Image Type (i.e., 1920×1080 or 925×1040), but must match the selected **Image Type** size before saving the message template.

Table 149. Add/Edit Message Template Parameters

GA10PV Background Color	Select the color for the message background. You can select a color by: • Using the color picker • Entering a hex color (for example: #000000, for black) • Entering an RGB color (for example: rgb(0,0,0) for black) • Entering a color alias name (for example: red, blue, etc.) For more information, see *"Using Color in Display Messages" on page 505*.
GA10PV Font	Select the down arrow to view a list of available fonts and then select the desired font for the message text. Available fonts are: Comic-Relief Courier-Prime Gelasio Liberation Sans Linux Libertine
GA10PV Font Size	Enter the desired font size.
GA10PV Font Color	Select the color for the message text. You can select a color by: • Using the color picker • Entering a hex color (for example: #000000, for black) • Entering an RGB color (for example: rgb(0,0,0) for black) • Entering a color alias name (for example: red, blue, etc.) For more information, see *"Using Color in Display Messages" on page 505*.
GA10PV Font Styles	Place your cursor in the **Add Styles** box to select **Bold** or **Italic**. Otherwise, the **Font Style** remains at Regular.

Table 149. Add/Edit Message Template Parameters

DSC01/WBC Flasher Pattern	Specifies the on/off pattern the flasher will display. Valid values are: • **No Change**: The message will not cause the selected flasher to change from its current flasher setting. • **Off**: The selected flasher will be turned off unless a higher priority message is using the flasher. When the flasher is turned off, it will remain off until another message is sent with a new flasher setting. • **Slow**: The selected flasher will blink at a rate of once per second for the duration of the message. • **Fast**: The selected flasher will blink at a rate of twice per second for the duration of the message. • **Double**: Flash two (2) times within one second with a 1-second pause and repeat. • **Triple**: Flash three (3) times within 1.5 seconds with a 1-second pause and repeat. • **Quad**: Flash four (4) times within two seconds with a 1-second pause and repeat.
DSC01/WBC Number of Flasher Pattern Cycles	Specifies the number of times that the flasher pattern will repeat. Valid values are 1 through 65536 or specify zero (0) to flash continuously for the duration of the message.
DSC01/WBC Flasher Color	Specifies the color of the LED flasher. Valid values are: • **Amber** • **Blue** • **Green** • **Orange** • **Red** • **Violet** • **White** • **Yellow**

Displaying a Message from the Message Templates Page

You can display a message based on a previously created Message Template from the ***Message Templates*** page.

To display a message based on a previously created Message Template:

1 On the navigation bar, select **Messages,** then **Message Templates**.

2 Select the **Send** icon next to the Message Template on which you want the new message to be based.

3 On the *Display Message* popup, select the zones or stations at which you want the message to be displayed.

Note: The selected zones and station will not be saved.

---

4 Make changes to the message options as needed (see *Table 145, "Display Message Options," on page 502*).

5 Select **Send**, or if you have made changes and want those changes to be saved to the Message Template, select **Send and Save**.

Deleting a Saved Message Template

To delete a saved Message Template:

1 On the navigation bar, select **Message Templates**.

2 Select the **Delete** icon next to the Message Template that you want to delete.

3 When prompted, select **Delete**.

Manage Check-In

A check-in event is a request for a person at each station (other than those explicitly or implicitly excluded) to report in, typically to indicate that they are aware of a current situation and/or are safe.

Examples of check-in events include:

- Weather-related shelter in place
- Safety-related lockdown
- Fire evacuation (staff member performs check-in to indicate room has been evacuated)
- Room occupancy (staff member checks room in with start of each class period)

Manage Check-In allows you to quickly obtain the check-in status of specific areas within a facility—such as conference rooms, offices, or break rooms—during a check-in event. During a check-in event, users check in by initiating a Normal call to their assigned Admin Station, such as the front office, using either their Nyquist phone (by dialing zero), a digital or analog call switch associated with their intercom speaker or station, or any other station whose **Check-in as Station Extension** is assigned to their assigned station (see *Table 43, "View, Add, or Edit Station Configuration Parameters," on page 143*).

During check-in, a Normal call initiated by a station to the Admin Station places the station in checked-in status. Subsequent calls made following a check-in are processed as Normal calls to the Admin Station.

You can also elect to enable audio feedback that tells the staff member they have successfully checked in.

Calls placed to perform a check-in are not applied towards the system's Current Call Count. Urgent and Emergency calls can still be placed by stations and are not included as part of Manage Check-In.

As long as Privacy Mode is not enabled and a room's device allows two-way transmission, you can select to use Spy Mode to listen to the room (see *"Using Spy Mode" on page 528*).

Managing Check-In Status

For administrators, the Manage Check-In feature provides a color-coded view of which rooms have checked in, which rooms or stations are not part of the check-in process, and which should check-in but have not yet done so.

Note: You can also use the Maps feature to view check-in status. For more information, see *"Using Maps for Check-In" on page 421*.

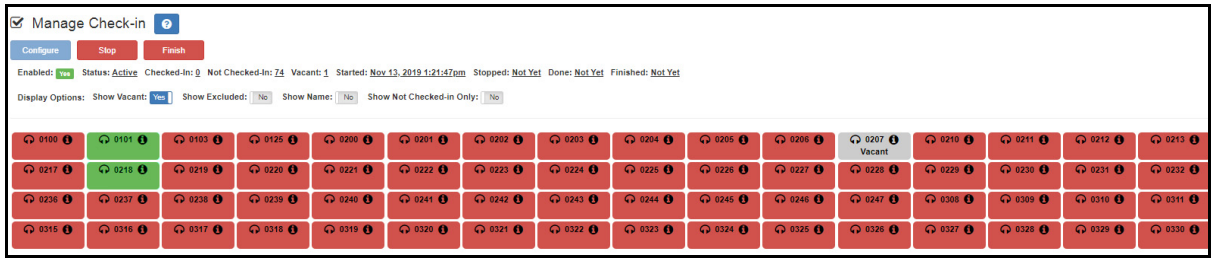


Figure 211. Manage Check-In

To view check-in status:

1 If not already on your dashboard, select **Dashboard** from the navigation bar.

2 Under *Calling/Paging*, select **Manage Check-In**.

A separate tab appears so that you can toggle the dashboard and Manage Check-In views.

The status of each station appears in a color-coded box. *Table 150, "Color-coded Check-In Status," on page 524* explains the use of colors to describe status:

Table 150. Color-coded Check-In Status

Color	Status
Green	Checked in
Red	Not checked in
Gray	Check-in is not expected because the station is either on the vacant or excluded lists.

You also can select the following **Display Options**:

Table 151. Check-In Display Options

Show Vacant	When enabled, stations in the **Vacancy List** appear in the color-coded display.
Show Excluded	When enabled, stations in the **Exclusion List** appear in the color-coded display.
Show Name	When enabled, the station's name appears along with the station's extension number. Displaying the name is useful if you are not sure where a station is located when only the extension number is displayed.
Show Not Checked In Only	*Note:* **Show Vacant** and **Show Excluded** options are disabled when this option is selected. When enabled, only the stations that have not checked in are listed. This option may be preferable if a large number of stations are managed by your Nyquist server, and you want to quickly view which stations have not checked in.

Additional information that appears on the Manage Check-In window includes:

- Status of check-in process such as **Active**

- Number of stations that have checked in
- Number of stations that have not yet checked in
- Number of vacant stations
- Date and time check-in started
- If check-in has been manually stopped or is done.

Manage Check-in also allows you to use Spy Mode on a station or room, provided the privacy feature has not been activated and the station device allows two-way transmission.

Stations typically excluded from the check-in process would include stations assigned to hallway speakers or amplifiers or areas that were scheduled to be vacant when the check-in procedure began. For more information, see *"Managing Exclusion and Vacancy Lists" on page 530*.

View Check-In Status on NQ-GA10PV display

You can also display Check-In status on NQ-GA10PV displays, which will indicate the start and stop time for the Check-In process as well as the check-in status for each station. For information, see *"Configuring Intercom HDMI Module Display Options" on page 176*.

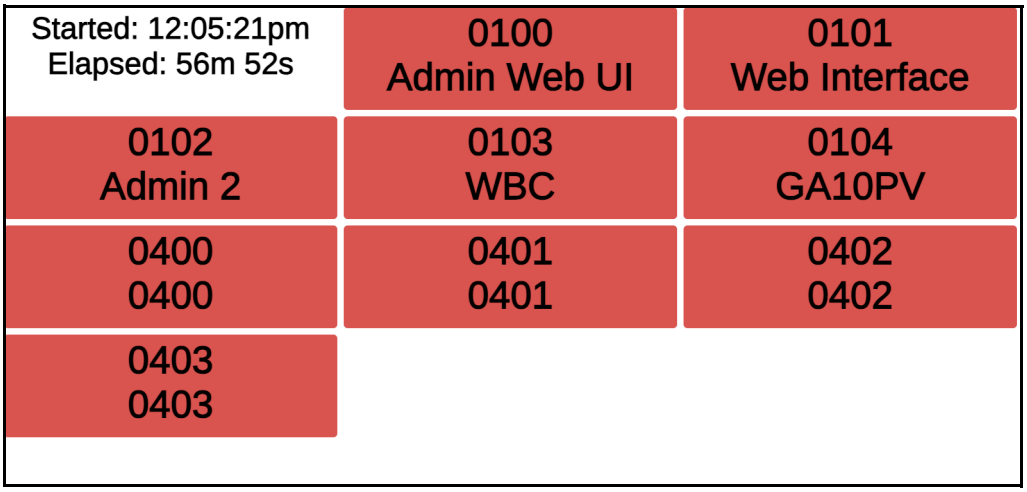


Figure 212. Check-In Status on NQ-GA10PV display

Starting Check-In

You can manually start the Check-In procedure from the Admin Web UI. Check-In can also be started via the Routines feature (see *"Using Routines" on page 425*.)

Check-In does not play any audio instruction announcements or send any text instructions to web interface stations or GA10PV display stations. If you want audio instruction announcements or text instructions on web interface stations or GA10PV display stations, set up a routine that includes audio instructions in an announcement or text instructions to be sent to web interface dashboards and

GA10PV displays. The routine can be triggered by a Check-in **Start**, or the Check-in can be started by the routine.

Figure 213. Manage Check-In When Idle

To manually start Check-In:

1. If not already on your dashboard, select **Dashboard** from the navigation bar.
2. Under *Calling/Paging*, select **Manage Check-In**.
3. On the *Manage Check-In* page, select **Start**.

When Check-In starts, the **Start** button changes to a **Stop** button and the red squares that represent occupied rooms or areas change to green squares as staff members check in.

Station Check-In

During Check-In, a Normal call placed by a station to the Admin Station marks the calling station or the station assigned to it's **Check-in as Station Extension** setting as Checked-in.

After a station has successfully checked in, additional Normal calls will go through as normal calls to the Admin station. Stations can still place Urgent or Emergency calls during the Check-in process, even if the station has not checked in.

If audio prompt feedback is enabled and a station checks in, the caller hears a confirmation prompt. If audio feedback is disabled, stations checking in with digital call switches will still see a ringing status (flashing green) for about two seconds while checking in. Stations checking in with IP phones will notice a call lasting about two seconds before automatic hang up.

A **VoIP Speaker Only** station that does not have a call switch can still participate in the check-in process if an I/O controller Input contact is connected to a switch present in the room that contains the **VoIP Speaker Only** station. In this case, the I/O controller Input contact closure can trigger a Routine that performs a check-in.

In this scenario, the Routine's Trigger **Type** is set to **Input-Contact-Closed** (see *"Understanding Trigger Parameters" on page 456*) and the Routine's Action **Type** is set to **Check-In** with **Station** set to the **VoIP Speaker Only** station extension (see *"Understanding Action Parameters" on page 460*).

If a station is configured (via the Call-In Level of its CoS configuration) to only place Emergency calls, the station cannot participate in the check-in process. Station's configured with a Call-In Level of **Emergency-Only** will, upon initiation of the check-in process, be automatically added to the Check-In Exclusion List (see *"Managing Exclusion and Vacancy Lists" on page 530*). If you wish to include the station in the check-in process, the station's CoS Call-In Level configuration should be changed to **Normal+Emergency** or **Urgent+Emergency** (see *"Editing CoS Parameters for a Station" on page 104*).

Ending the Check-In Process

There are two different ways to end the check-in process: *stop or finish*. *Finish* implies that every station has checked in. *Stop* implies that someone decided to cancel the check-in process before every station had checked in.

After all stations included in the check-in process have checked in, the check-in Status will automatically change to **Done.** Since stations that were not expected to check in may do so, the check-in is not considered complete until you explicitly set the status to **Finish**.

> The behavioral difference between *finishing* and *stopping* a check-in is largely determined by how you configure your system. You can define different Actions for your system to perform for the Check-In trigger based on the Stop or Finish values of the Check In property. The primary built-in differences are:
>
> - The elapsed time for the check-in process is calculated after the process is *finished*.
> - *Stopping* sets check-in Status to Idle and updates Stopped time, while *finishing* sets check-in Status to Finished and updates Finished time.

Completing the Check-In

You can complete an active check-in process by selecting the **Stop** or **Finish** button on the *Manage Check-In* view. An active check-in process can also be stopped or finished via a Routine action by using the **Check-In** Action **Type** with the **Check In** option set to **Stop** or **Finish** (see *"Understanding Action Parameters" on page 460*).

Stopping or finishing the check-in will trigger those routines that use **Check-In** as the trigger **Type** and either **Stop** or **Finish** as **Check In** (see *"Understanding Trigger Parameters" on page 456* for more information).

After the check-in process has been stopped or finished, all Normal station calls resume as normal calls to the Admin Station, and the check-in process **Status** becomes either **Idle** (if stopped) or **Finished** (if finished).

Resetting the Check-In Process

Once a check-in process has completed, the check-in status should *always* be reset, typically via the **Reset** button on the *Manage Check-In* view. This will clear all check-in statuses, allow non-Admin–to–Admin Station calls to resume, and restore all GA10PV displays back to their normal operational states. Until reset, the GA10PV displays will show check-in statuses.

You can also reset the check-in process with a Routine action. When resetting check-in via a routine, the Action **Type** is **Check-In** and the **Check In** option is **Reset** (see *"Understanding Action Parameters" on page 460*).

Using Spy Mode

You can use Spy Mode to listen to a station as long as Privacy Mode is not enabled and the station device allows two-way transmission.

This feature adds a step toward verifying that the room's occupants are safe.

Figure 214. Listen In, or Spy Mode, Button

To activate Spy Mode:

1. If not already on your dashboard, select **Dashboard** from the navigation bar.
2. Under *Calling/Paging*, select **Manage Check-In**.
3. On the *Manage Check-In* page, select the **Listen In** icon for the station you want to monitor.

To activate Spy Mode using a DTMF code (regardless of Check-In process):

1. If not already on your dashboard, select **Dashboard** from the navigation bar.
2. Under *Calling/Paging*, select **Dial Pad**.
3. When the dial pad appears, dial `978{station-extension}` and press **Send** (see *"Monitoring/Recording" on page 580*).

Note: Spy Mode monitoring cannot be used on a station that has been set to Privacy Mode.

Configuring Check-In

To use the check-in process, the user must have appropriate permissions assigned (see *"Assigning and Editing Permissions" on page 248*).

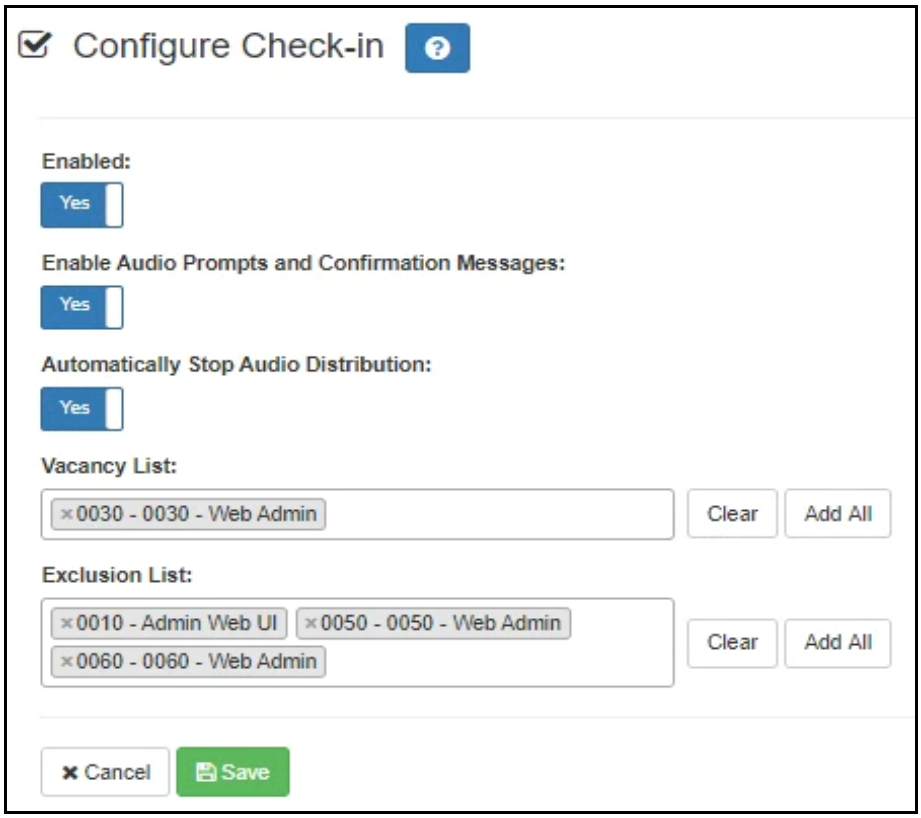


Figure 215. Configure Check-in

To configure check-in options:

1. If not already on your dashboard, select **Dashboard** from the navigation bar.
2. Under **Calling/Paging**, select **Manage Check-In**.
3. On the *Manage Check-In* page, select **Configure**.
4. Complete the configuration options (see *Table 152, "Check-In Configuration Options," on page 529*).
5. Select **Save**.

Table 152. Check-In Configuration Options

Enabled	Specifies if Manage Check-In can be used. If disabled, you can configure *Manage Check-In* options, but you cannot start the check-in process.
Enable Audio Prompts and Confirmation Messages	Specifies if audio files will be used as part of Manage Check-In. When enabled, audio prompts and audio feedback play at stations when the stations perform check-in. If disabled, no audio prompts or audio feedback are played on the station. When feedback is disabled, stations checking in with digital call switches will see a ringing status (flashing green) for about two seconds while checking in. Stations checking in with IP phones will notice a call lasting about two seconds.

Table 152. Check-In Configuration Options

Automatically Stop Audio Distribution	When enabled, all currently playing audio distributions will be stopped when a check-in process is started.
Vacancy List	Specifies the stations to be added to the Vacancy List (see *"Managing Exclusion and Vacancy Lists" on page 530*).
Exclusion List	Specifies the stations to be added to the Exclusion List (see *"Managing Exclusion and Vacancy Lists" on page 530*). *Note:* Stations configured with a Call-In Level of Emergency-Only (via the station's CoS configuration) will automatically be added to the Exclusion List upon initiation of the check-in process.

Managing Exclusion and Vacancy Lists

A station added to the Vacancy List and a station added to the Exclusion List both appear gray on the Admin Station's Check-In page if the *Manage Check-In* page is configured to display these lists (see *"Configuring Check-In" on page 528*). The difference between the two lists, though, is that stations on the Exclusion List should always be excluded from the check-in process. Those on the Vacancy List are stations (rooms or areas) that normally would be checking in, but may be vacant when the check-in process is started.

Important: A station on the vacancy list can still check in. This could occur during an emergency situation where a normally vacant room becomes the closest temporary shelter. An occupant could perform a check-in to let administrators know that the room is occupied and secure.

Excluded stations should include stations not physically located in a room, such as speakers located in a hallway; and stations assigned to appliances, such as power amplifiers and MMPAs. Stations that have **Check-in as Station Extension** assigned to another station (see *Table 43, "View, Add, or Edit Station Configuration Parameters," on page 143*) are automatically added to the exclusion list and are only removed from the list when they are unassigned.

Stations whose CoS is configured as *Emergency-Only* at the time the Check-In process is initiated (based on the Station's currently active CoS configuration) will be automatically added to the Check-in Exclusion List. These stations will appear in the `checkin` log with a status of **Exclude Add (Auto)** and will remain in the Check-in Exclusion list until the **Reset** button is pressed (stations manually added to the Exclusion list remain in that list until explicitly removed).

You can add or delete a station to or from the Exclusion or Vacancy Lists by:

- Using **Manage Check-In** via the Admin Web UI
- Using the **Routines** feature

To add a station to the Exclusion List via the Admin Web UI:

1 If not already on your dashboard, select **Dashboard** from the navigation bar.

2 Under **Calling/Paging**, select **Manage Check-In**.
3 On the *Manage Check-In* page, select **Configure**.
4 Add desired station or stations to the **Exclusion List**.
5 Select **Save**.

To add a station to the Exclusion List via a routine:

1 Add or edit a routine that has a **Check-In** action (see *"Actions" on page 456*).
2 For **Check In**, select **Exclude-Add**.
3 For **Stations**, select the stations that you want to exclude from *Manage Check-In*.
4 Select **Save**.

To remove a station from the Exclusion List via the Admin Web UI:

1 If not already on your dashboard, select **Dashboard** from the navigation bar.
2 Under **Calling/Paging**, select **Manage Check-In**.
3 On the *Manage Check-In* page, select **Configure**.
4 Remove the desired station or stations from the **Exclusion List**.
5 Select **Save**.

To remove a station from the Exclusion List via a routine:

1 Edit a routine that has a **Check-In** action (see *"Actions" on page 456*).
2 For **Check In**, select **Exclude-Delete**.
3 For **Stations**, select the stations that you want to remove from **Manage Check-In Exclusion List**.
4 Select **Save**.

To add a station to the Vacancy List via the Admin Web UI:

1 If not already on your dashboard, select **Dashboard** from the navigation bar.
2 Under **Calling/Paging**, select **Manage Check-In**.
3 On the *Manage Check-In* page, select **Configure**.
4 Add desired station or stations to the **Exclusion List**.
5 Select **Save**.

To add a station to the Vacancy List via a routine:

1 Add or edit a routine that has a **Check-In** action (see *"Actions" on page 456*).
2 For **Check In**, select **Vacancy-Add**.
3 For **Stations**, select the stations that are expected to be vacant.
4 Select **Save**.

To delete a station from the Vacancy List via the Admin Web UI:

1 If not already on your dashboard, select **Dashboard** from the navigation bar.
2 Under **Calling/Paging**, select **Manage Check-In**.

3 On the *Manage Check-In* page, select **Configure**.

4 Select the stations that you want to remove from the **Vacancy List**.

5 Select **Save**.

To delete a station from the Vacancy List via a routine:

1 Edit a routine that has a **Check-In** action (see *"Actions" on page 456*).

2 For **Check In**, select **Vacancy-Delete**.

3 For **Stations**, select the stations you want to remove from the **Vacancy List**.

4 Select **Save**.

Check-In Routine Actions and Triggers

You will typically define Routines that perform check-in actions (see the Check-In action in *Table 2, "Routine Action Type-Specific Parameters," on page 588*) and/or that are triggered by check-in events (see the Check-In trigger in *Table 4, "Routine Trigger Types and Parameters," on page 615*). This allows a great deal of flexibility and customization over the various check-in processes and types of check-in scenarios that you will implement.

Creating and Using Multiple Check-In Routines

You can create check-in routines for multiple purposes and to ensure that the vacancy and exclusion lists are accurate.

You should create separate routines for drills and each type of emergency check-in. For example, a fire drill could use audio explaining that it was a drill and would not include an actual 911 call, while a routine used for evacuation during an actual fire would probably include a 911 call.

Tip: In the drill scenario, the word "drill" should appear in the name.

If you want to create routines for accurate exclusion and vacancy lists, use descriptive names such as "Fire Drill Period 1." Each routine should include a **Check-In** action that uses **Vacancy-Add** and a separate **Check-In** action that uses **Vacancy-Delete**.

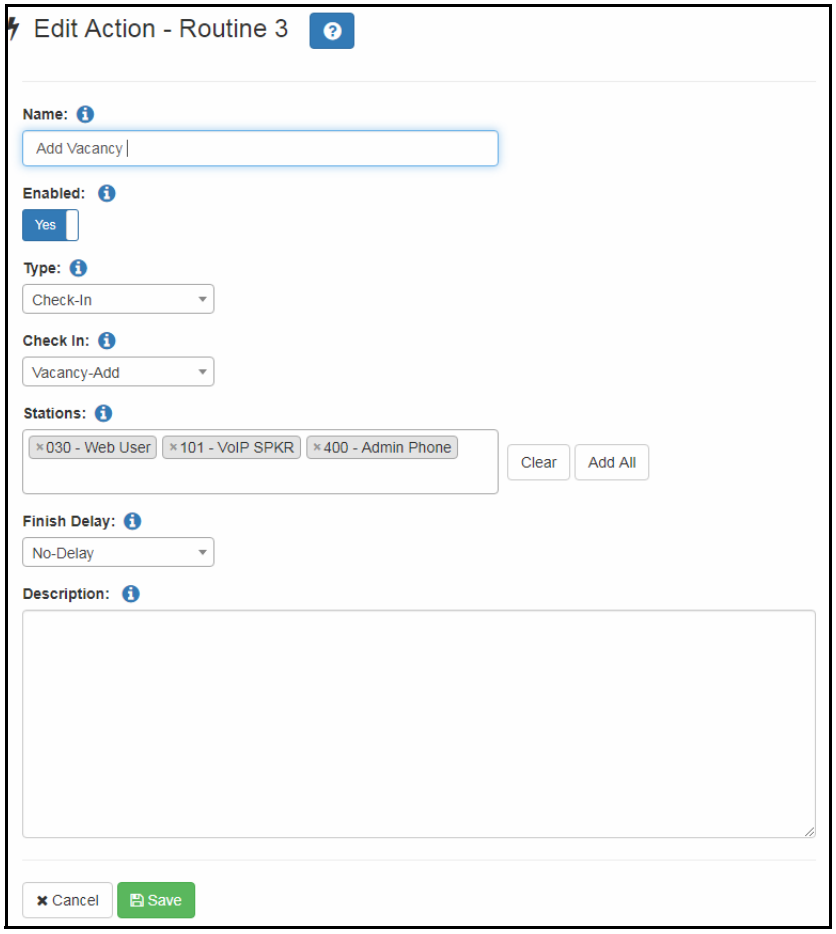


Figure 216. Example of Check-In Routine Action

Check-In Log and Call Detail Records

Manage Check-In writes data to the `checkin` log file (see *"Using System Log Files" on page 359*) and also creates a Call Detail Record (see *"Viewing Call Details Records" on page 363*). You can export the `checkin` log file using the **Export** button (see *"Exporting and Printing a Call Log" on page 363*). You can also copy the displayed log file information and paste it into another application.

Each logged event includes a date-and-time stamp, a hyphen, the station extension that created the event, the check-in event type, and optional event-related information. For example:

```
2026-02-24 15:28:17 - 010 Start, Verify: Off Feedback: On
```

The following event types are logged:

- Start
- Check-in
- Stop
- Reset
- Finished

- Vacancy Add
- Vacancy Delete
- Exclude Add
- Exclude Delete

The **Finished** event indicates the elapsed time for the Check-in process (amount of time between Check-in **Start** and **Finished**). For example:

```
2026-03-02 10:59:22 - 010 Finished (elapsed time: 0d:0h:1m:20s)
```

On the Call Detail Records, the detail record **Type** is set to **Check in** when a station checks in.

Managing Weather Alerts

The National Weather Service (NWS) provides an Alerts Web Service to issue watches, warnings, advisories, and other alerts (for details, see https://www.weather.gov/documentation/services-web-alerts) for both weather-related and non-weather-related events. The C4000 can subscribe to this service and respond to these alerts by displaying the alerts, issuing announcements, or other custom actions.

Administrators can configure Alert Filters, which specify which events will be displayed and which Announcement will be made for each alert type. The events can be further filtered by event Severity, Certainty, Urgency, and Response criteria. Events that occur and meet the specified criteria can be displayed on NQ-GA10PV, NQ-T1100, and NQ-ZPMS devices; play an Announcement; or trigger a custom Routine Action.

Note: The Nyquist server must have an Internet connection and access to the necessary websites (see *"Whitelisted Web Addresses" on page 3*) to detect and respond to NWS alerts..

To display NWS events:

1. Determine which NWS alerts you want to monitor and enable filters for those alerts based on an alert's Event Type, Severity, Certainty, Urgency, and Response criteria (see *"Alert Filters Configuration" on page 535*).
2. Create a Routine to handle NWS alerts.

   The recommended method is via the *NWS Alert* page (see *"NWS Alert Routines" on page 539*), which provides a graphical interface to the NWS Alert options.

   Alternatively, a Routine can be explicitly created containing a Display-Msg action that displays the `$alerts` variable. This method is more complex to create and maintain, but may allow greater flexibility for advanced processing (see *"Display NWS Alerts Using a Routine" on page 547*).

Alert Filters Configuration

The Common Alerting Protocol (CAP) is an international standard format for emergency alerting and public warning. It is designed for all hazards related to weather events, earthquakes, tsunami, volcanoes, public health, power outages, and many other emergencies.

CAP elements and values are used when configuring alert filters for your Nyquist system. Further details regarding CAP and the data it provides can be found at:

https://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.html

---

Note: You must have **Edit** permissions to enable and set Alert Filters Configuration. For more information, refer to *"Assigning and Editing Permissions" on page 248*.

The Alert Filters Configuration page allows administrators to specify which alerts the C4000 will monitor and which Announcements will be played when they occur.

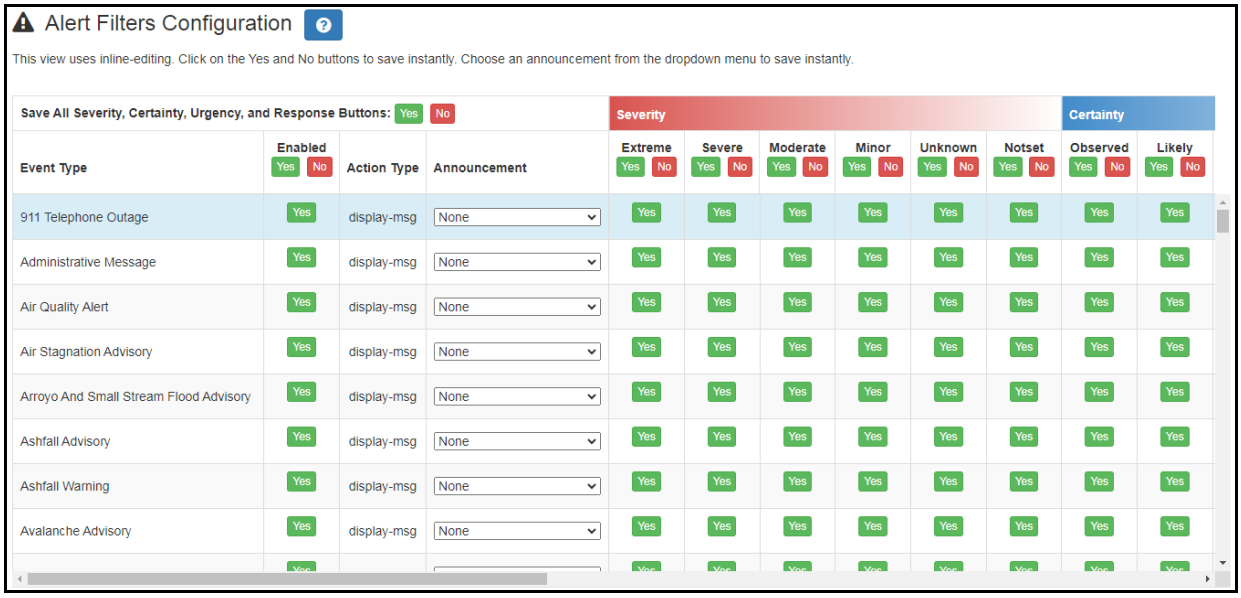


Figure 217. Alert Filters Configuration

Events can be filtered not only by the Event Type (i.e., what happened), but also by the alert conditions: Severity, Certainty, Urgency, and Response. If all of an arriving alert's conditions are enabled (i.e., set to **Yes**), the alert will be detected. In other words, if any of the conditions of an arriving alert are disabled (i.e., set to **No**), the alert will be ignored.

The **Announcement** to play for a detected alerts can be configured for each Event Type, but it will only play if the NWS Alert Routine's **Announcement by Event** option is set to **Yes** (see *Table 155, "Add/Edit NWS Alert options," on page 541*) or the `ANNOUNCEMENT_BY_EVENT` option of the `$alerts` variable is specified (see *"ANNOUNCEMENT_BY_EVENT" on page 551*).

If the **Announcement** for an Event Type is unspecified, the Announcement to play when an alert of that type is detected can be specified for the NWS Alert Routine via its **Event Announcement Default** setting or the `ANNOUNCEMENT_DEFAULT_DTMF_<dtmf-code>` option of the `$alerts` variable (see *"ANNOUNCEMENT_DEFAULT_DTMF_<dtmf-code>" on page 551*). A Routine can also override Event Type-specific Announcements completely by specifying an Announcement to play for all enabled events via the NWS Alert Routine's **Announcement** setting (see *Table 155, "Add/Edit NWS Alert options," on page 541*) or the `ANNOUNCEMENT_DTMF_<dtmf-code>` option of the `$alerts` variable (see *"ANNOUNCEMENT_DTMF_<dtmf-code>" on page 551*).

To configure alert filters:

1. On the navigation bar, select **Alert Filters**.
2. For each **Event Type** (i.e., weather watch, warning, advisory, etc.), indicate that you want to display alert events by toggling the **Enabled** column button to **Yes**. Toggle it to **No** to disable the **Event Type**.

   To enable or disable all **Event Types**, select the **Yes** or **No** button in the **Enabled** header.
3. For each **Event Type**, indicate which **Announcement**, if any, that you want to play for this alert event if the ANNOUNCEMENT_BY_EVENT parameter (see *"ANNOUNCEMENT_BY_EVENT" on page 551*) or **Announcement by Event** (see *Table 155, "Add/Edit NWS Alert options," on page 541*) is enabled.

Important: Although the Announcement to play is specified here, it will not actually play unless a Routine is monitoring the alerts.

4 For each enabled **Event Type**, specify Yes for the Severity, Certainty, Urgency, and Response values of alert events that you want to display. If an alert matches *any* of the specified criteria, it will be displayed.

To enable or disable an alert type for *all* **Event Types**, select Yes or No for that alert type (e.g., Extreme, Severe, Moderate, etc.). To enable or disable *all* alert types for *all* **Event Types**, select Yes or No for **Save All Severity, Certainty, Urgency, and Response Buttons**.

See *"CAP Elements and Values" on page 538* for descriptions of the CAP elements (e.g., Severity, Certainty, Urgency, and Response).

For descriptions of weather-related event types, refer to the following website:

https://www.weather.gov/lwx/WarningsDefined

For descriptions of non-weather-related event types, refer to the following website:

https://www.weather.gov/meg/nonwxrelatedemergmesg

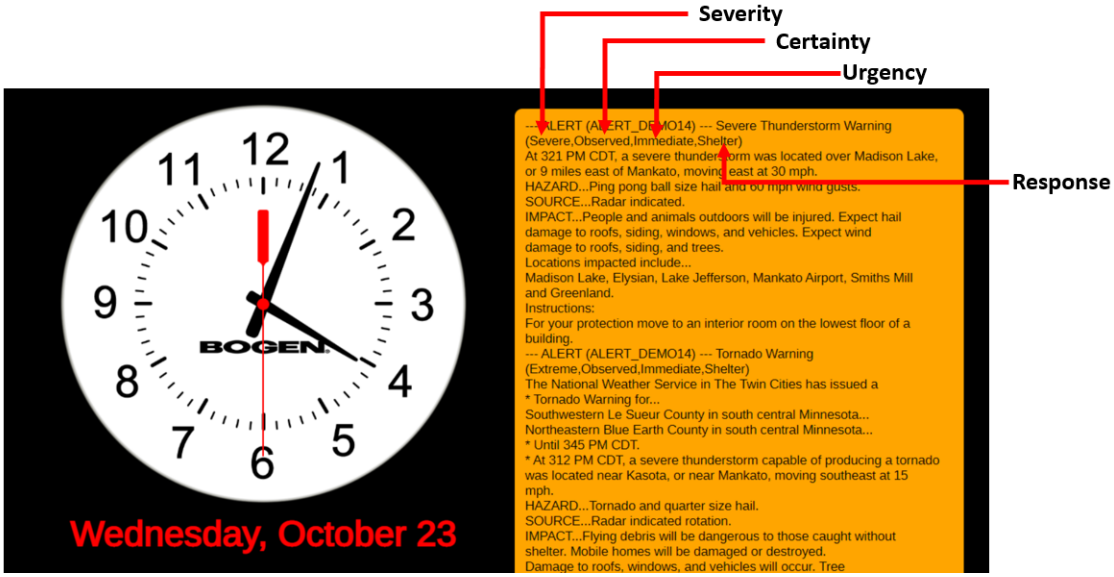


Figure 218. Sample Alert With Elements Defined

Elements and their values are described in the following table:

Table 153. CAP Elements and Values

Element	*Available Values*
Severity Denotes the severity of the event.	**Extreme:** Extraordinary threat to life or property. **Severe:** Significant threat to life or property. **Moderate:** Possible threat to life or property. **Minor:** Minimal to no known threat to life or property. **Unknown:** Severity unknown. **Notset:** Severity was not provided in the alert received by the NWS.
Certainty Denotes the certainty of the event.	**Observed:** Determined to have occurred or to be ongoing. **Likely:** Probability is greater than or equal to 50%. **Possible:** Probability is less than 50%. **Unlikely:** Not expected to occur. **Unknown:** Certainty unknown. **Notset:** Certainty was not provided in the alert received by the NWS.
Urgency Denotes the urgency of the event.	**Immediate:** Responsive action should be taken immediately. **Expected:** Responsive action should be taken soon (within next hour). **Future:** Responsive action should be taken in the near future. **Past:** Responsive action is no longer required. **Unknown:** Urgency unknown. **Notset:** Urgency was not provided in the alert received by the NWS.
Response Denotes the action recommended for the target audience.	**Shelter:** Take shelter in place or per instruction. **Evacuate:** Relocate as instructed in the instruction. **Prepare:** Make preparations per the instruction. **Execute:** Execute a preplanned activity identified in instruction. **Avoid:** Avoid the subject event as per the instruction. **Monitor:** Attend to information sources as described in instruction. **Assess:** Evaluate the information in this message. **Allclear:** The subject event no longer poses a threat or concern and any follow-on action is described in the instructions. **None:** No action is recommended. **Notset:** Response was not provided in the alert received by the NWS.

Note: The Severity, Certainty Urgency, and Response values only appear in the Alert message if the INCLUDES_CODES option is included in the $alerts parameters list (see *"Setting Variables for the Display Message" on page 548*).

NWS Alert Routines

To receive National Weather Service (NWS) alerts, a Routine must be created with a Display-Msg Action that includes the `$alerts` variable and its properties in the Action's Text field. Designing this Routine and configuring the `$alerts` variable (as described in *"Display NWS Alerts Using a Routine" on page 547* and *"Setting Variables for the Display Message" on page 548*) can be fairly involved and potentially error-prone.

To simplify this process, the C4000 provides the *NWS Alerts* page, which provides a simplified mechanism for creating, configuring, and manipulating Routines to handle NWS alerts.

Tip: NWS Alert Routines can be configured using either the *NWS Alerts* page or the *Routines* page. Unless the extended functionality of a Routine is required, we strongly recommend using the *NWS Alerts* page. It simplifies many of the interdependencies between various alert settings and helps minimize configuration and runtime errors.

View NWS Alert Routines

To view a list of existing NWS Alert Routines:

1. On the navigation bar, select **NWS Alerts**.
2. From the *NWS Alerts* page, NWS Alert Routines can be monitored, created, enabled, disabled, started, stopped, or edited, and the Routines that handle the alerts can be edited.

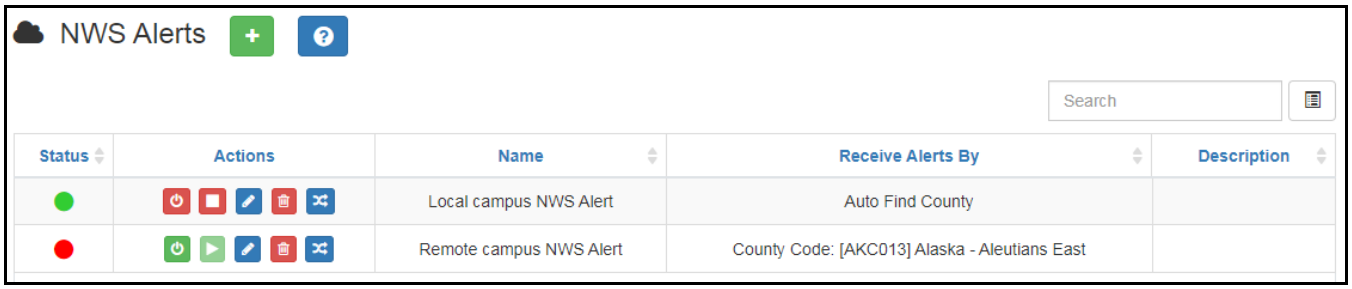


Figure 219. View NWS Alerts

Table 154. NWS Alerts parameters

Status	A green circle indicates that the associated Routine is executing, while a red circle indicates that the associated Routine is not executing.
Actions	Several buttons that perform operations on the NWS Alert Routine.

Table 154. NWS Alerts parameters

Enable/Disable	Enables or disables the Routine associated with this NWS Alert Routine.
Start/Stop	Starts or stops the Routine associated with this NWS Alert Routine.
Edit Alert	Edits this NWS Alert Routine, which displays the *Edit NWS Alert* page (see *"Add or Edit an NWS Alert Routine" on page 540*).
Delete Alert	Deletes the Routine associated with this NWS Alert.
	Warning Before deleting, ensure that it is safe to delete all actions, triggers, and other settings associated with this Routine.
Edit Routine	Edits the Routine associated with this NWS Alert (see *"Editing a Routine" on page 451*).
Name	The name of the Routine associated with this NWS Alert.
Receive Alerts By	Indicates the **Receive Alerts By** setting for the NWS Alert.
Description	Indicates the **Description** of the Routine associated with this NWS Alert.

Add or Edit an NWS Alert Routine

To create or edit an NWS Alert Routine:

1. On the navigation bar, select **NWS Alerts**.
2. Select the **Add** button to create a new NWS Alert Routine, or select the **Edit** button in the Actions column of an existing NWS Alert Routine.
3. The **Add NWS Alert** or **Edit NWS Alert** page will be displayed (see *Figure 220, "Add NWS Alert," on page 541*).
4. Specify the options for the NWS Alert Routine, as described in *Table 155, "Add/Edit NWS Alert options," on page 541*.
5. Select the **Configure Display Options** button to configure the display options for the NWS Alert Routine (see *Table 156, "NWS Alert Display Options," on page 545*).
6. When all settings have been configured, select the **Save NWS Alert** button.

Note: As an alternative, a standard Routine can be created to monitor and display NWS Alerts. For details, see *"Display NWS Alerts Using a Routine" on page 547*.

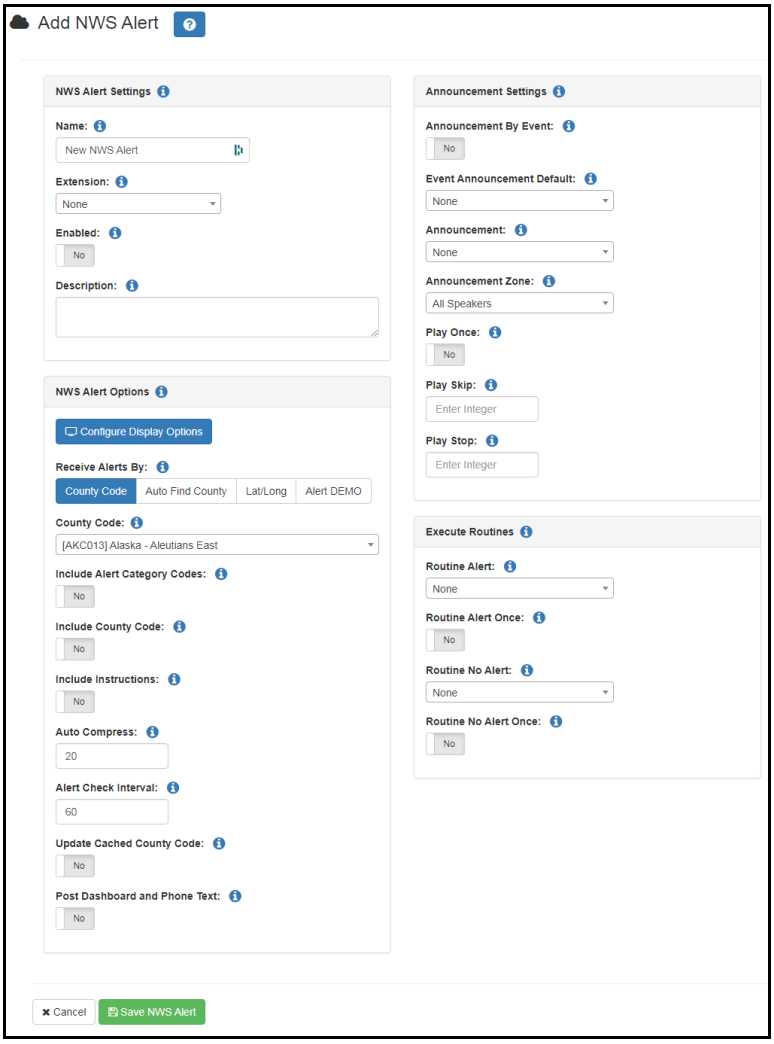


Figure 220. Add NWS Alert

The following table describes the options available when configuring an NWS Alert.

Table 155. Add/Edit NWS Alert options

Name	Specify a name for the NWS Alert.
Extension	Specify the user extension to be used for granting permissions.
Enabled	Enable or disable the NWS Alert. Valid values are **Yes** or **No**.
Description	Specify a description of the NWS Alert.
Configure Display Options	This button displays the **Display Options** popup (see *"NWS Alert Display Options" on page 545*), which provides options regarding how to display the alert on NQ-S1810WBC and/or NQ-GA10PV devices.

Table 155. Add/Edit NWS Alert options (continued)

Receive Alerts By	Specifies how the system will determine which zones will be monitored for NWS alerts. **County Code:** Zone specified by County Code. **Auto Find County:** The Nyquist server will automatically determine the zone. If this is used, For details, see *"AUTO_FIND_COUNTY" on page 552*. **Lat/Long:** The zone is specified by latitude and longitude. **Alert DEMO:** A simulated demonstration alert will be sent
County Code	Select which county code (i.e., location code) will be monitored for NWS alerts. For details, see *"<location-code>" on page 550*. *Note:* This parameter is only available if **Receive Alerts By** is set to **County Code**.
Latitude **Longitude**	Specify the geographic coordinates (as latitude and longitude) that will be monitored for NWS alerts. For details, see *"LATLON:<latitude>_<longitude>" on page 555*. *Tip:* Right-clicking a location on Google Maps or Bing Maps shows the coordinates for that location. Clicking the coordinates copies the coordinates to the clipboard. *Note:* These parameters are only available if **Receive Alerts By** is set to **Lat/Long**.
Alert DEMO	Select the demonstration alert to use for generating test alerts. For details, see *"Demonstration Alerts" on page 551*. *Note:* This parameter is only available if **Receive Alerts By** is set to **Alert DEMO**.
Include Alert Category Codes	Specifies whether or not to include Severity, Certainty, Urgency, and Response codes in the header of each weather alert. Valid values are **Yes** or **No**. For details, see *"INCLUDE_CODES" on page 553*.
Include County Code	Specifies whether or not to include the county code in each weather alert. Valid values are **Yes** or **No**. For details, see *"INCLUDE_COUNTY" on page 554*.
Include Instructions	Specifies whether or not instructions that are included as part of the alert are displayed. Valid values are **Yes** or **No**. For details, see *"INCLUDE_INSTRUCTIONS" on page 554*.

Table 155. Add/Edit NWS Alert options (continued)

Auto Compress	If the number of lines in the alert message exceeds this number, the message will be compressed by replacing end-of-line characters with spaces. For details, see *"AUTO_COMPRESS_<integer>" on page 553*.
Alert Check Interval	Specifies the interval, in seconds, before the system repeats the process and checks for another alert. This must be an integer with a value of 30 or higher. For details, see *"REPEAT_<integer>" on page 558*.
Update Cached County Code	If **Yes**, the C4000 updates the cached value of the county code to the value determined by the system when **Receive Alerts By** was set to **Auto Find County**. Valid values are **Yes** or **No**. For details, see *"UPDATE_CACHE" on page 559*.
Post Dashboard and Phone Text	Specifies whether or not single-line NWS weather alert notices will be displayed on the Nyquist Dashboard and NQ-T1100 devices, and full-text notices will be viewable on the NQ-T1100 and NQ-ZPMS devices. Valid values are **Yes** or **No**. For details, see *"POST_DASH_PHONE_TEXT" on page 556*.
Announcement by Event	If **Yes**, the system will play the announcement associated with the alert event's Event Type (see *"Alert Filters Configuration" on page 535*). If this option is **Yes**, the **Announcement** option will be unavailable. Valid values are **Yes** or **No**. For details, see *"ANNOUNCEMENT_BY_EVENT" on page 551*.
Event Announcement Default	Specifies which Announcement to play if an Announcement is not configured for the alert's Event Type. For details, see *"ANNOUNCEMENT_DEFAULT_DTMF_<dtmf-code>" on page 551*.
Announcement	Specifies the Announcement to play for all alert events. If this option is specified, **Announcement by Event** and **Event Announcement Default** are unavailable. For details, see *"ANNOUNCEMENT_DTMF_<dtmf-code>" on page 551*.

Table 155. Add/Edit NWS Alert options (continued)

Announcement Zone	The paging zone to which alert announcements will be played. If **Defined by Announcement** is selected, the announcement will play to the zone specified in the *Alert Filters Configuration* for the event's Event Type (see *"Alert Filters Configuration" on page 535*). **Caution** Unless **Event Announcement Default** is defined, **Defined by Announcement** requires that **Play to Zone** be defined (see *Table 103, "Add Announcement Page Parameters," on page 324*) for every Announcement specified for any Event Type of the Alert Filters Configuration. If **All Speakers** is selected, the announcement will play to all speakers. If a specific zone is selected, the announcement will play to speakers in the selected zone. For details, see *"ANNOUNCEMENT_ZONE_<zone>" on page 552*.
Play Once	If **Announcement** is specified, setting **Play Once** to **Yes** indicates that the alert Announcement will only play once, when the alert event first occurs. Valid values are **Yes** or **No**. For details, see *"PLAY_ONCE" on page 555*.
Play Skip	If **Announcement** is specified and **Alert Check Interval** is non-zero, setting **Play Skip** to an integer, *n*, indicates that the alert Announcement will be skipped *n* intervals for each interval that it plays. For details, see *"PLAY_SKIP_<integer>" on page 555*.
Play Stop	If **Announcement** is specified and **Alert Check Interval** is non-zero, setting **Play Stop** to an integer, *n*, indicates that the Announcement should only play *n* times before stopping. For details, see *"PLAY_STOP_<integer>" on page 556*.
Routine Alert	Executes the specified Routine when an alert event is received. For details, see *"ROUTINE_ALERT_DTMF_<dtmf-code>" on page 559*.
Routine Alert Once	If **Routine Alert** is specified, the Routine will only be executed once during the alert event's lifetime. Valid values are **Yes** or **No**. For details, see *"ROUTINE_ALERT_ONCE" on page 559*.

Table 155. Add/Edit NWS Alert options (continued)

Routine No Alert	Executes the specified when *no* alert event has been received. For details, see *"ROUTINE_NOALERT_DTMF_<dtmf-code>" on page 559*.
Routine No Alert Once	If **Routine No Alert** is specified, the Routine will only be executed once when no alert events are present. Valid values are **Yes** or **No**. For details, see *"ROUTINE_NOALERT_ONCE" on page 559*.

When the **Configure Display Options** button is selected, the following options regarding how to display the alert on NQ-S1810WBC, NQ-DSC01, and/or NQ-GA10PV devices are displayed:

Table 156. NWS Alert Display Options

Device Type Filter	Select the device type(s) to which the message will be sent. This determines which display options will be available. Valid values are: • **GA10PV and DSC01/WBC** • **GA10PV Only** • **DSC01/WBC Only**
Display Time (seconds)	Sets the length of time for the message to be displayed before it expires. The specified value can range from 1 to 99999 seconds.
Zones	Messages will be displayed on devices in the selected zones.
Stations	The messages will be sent to the specified stations and any stations that belong to the specified Zones.
Priority	Select the message priority, which can range from **0 (Lowest)** to **6 (Fullscreen)**. Priority **6 (Fullscreen)** is the highest priority, and when a message is assigned this priority, only the messages with this priority appear on the display with the Scheduled Event Name and Date being temporarily removed. If Priority **5 (Exclusive)** is selected, the Scheduled Event Name and Date remain on the display, but all other messages with lower priorities are removed. *Note:* Priority **5 (Exclusive)** is disabled for Image messages and enabled for Text messages.

Table 156. NWS Alert Display Options

GA10PV Background Color	Select the color for the message background. You can select a color by: • Using the color picker • Entering a hex color (for example: #000000, for black) • Entering an RGB color (for example: rgb(0,0,0) for black) • Entering a color alias name (for example: red, blue, etc.) For more information, see *"Using Color in Display Messages" on page 505*.
GA10PV Font	Select the down arrow to view a list of available fonts and then select the desired font for the message text. Available fonts are: Comic-Relief Courier-Prime Gelasio Liberation Sans Linux Libertine
GA10PV Font Size	Specify the desired font size.
GA10PV Auto Resize Font	Specify the minimum point size to which the font will be resized to fit the NWS Alert on the screen.
GA10PV Font Color	Select the color for the message text. You can select a color by: • Using the color picker • Entering a hex color (for example: #000000, for black) • Entering an RGB color (for example: rgb(0,0,0) for black) • Entering a color alias name (for example: red, blue, etc.) For more information, see *"Using Color in Display Messages" on page 505*.
GA10PV Font Styles	Place your cursor in the **Add Styles** box to select **Bold** and/or **Italic**. Otherwise, the **Font Style** remains at Regular.

Table 156. NWS Alert Display Options

DSC01/WBC Flasher Pattern	Specifies the on/off pattern the flasher will display. Valid values are: • **No Change**: The message will not cause the selected flasher to change from its current flasher setting. • **Off**: The selected flasher will be turned off unless a higher priority message is using the flasher. When the flasher is turned off, it will remain off until another message is sent with a new flasher setting. • **Slow**: The selected flasher will blink at a rate of once per second for the duration of the message. • **Fast**: The selected flasher will blink at a rate of twice per second for the duration of the message. • **Double**: Flash two (2) times within one second with a 1-second pause and repeat. • **Triple**: Flash three (3) times within 1.5 seconds with a 1-second pause and repeat. • **Quad**: Flash four (4) times within two seconds with a 1-second pause and repeat.
DSC01/WBC Number of Flasher Pattern Cycles	Specifies the number of times that the flasher pattern will repeat. Valid values are 1 through 65536 or specify zero (0) to flash continuously for the duration of the message.
DSC01/WBC Flasher Color	Specifies the color of the LED flasher. Valid values are: • **Amber** • **Blue** • **Green** • **Orange** • **Red** • **Violet** • **White** • **Yellow**

Display NWS Alerts Using a Routine

An NWS Alert Routine (*"View NWS Alert Routines" on page 539*) is actually an optimized view of a regular Routine that monitors and displays NWS alerts. Although an NWS Alert Routine is much easier to create and maintain, using a regular Routine and explicitly configuring how NWS alerts will be handled can sometimes provide extra flexibility.

To display NWS events using a standard Routine:

1. Decide which alerts you want to monitor and enable filters for those Event Types, filtering them by various criteria, such as the events' severity, certainty, urgency, and response (see *"Alert Filters Configuration" on page 535*).
2. Create a routine (see *"Adding a Routine" on page 450*).
3. Set the routine's **Allow Multiple** field to No (default).
4. *Optional*: If you will be using the Dashboard's **Routines** button to test this routine, set **Allow DTMF** to Yes and assign a value to **DTMF Code**.
5. Create an action for the routine that uses **Display-Msg** for the action **Type** (see *"Actions" on page 456*). Ensure the Text for the **Display-Msg** action contains the `$alerts()` variable, and specify its properties to customize which alerts you want to display, how they will be formatted, and how the alerts will be monitored (see *"Setting Variables for the Display Message" on page 548*).

   For example:

   ```
   $alerts(FLC095,INCLUDE_CODES,AUTO_COMPRESS_15,REPEAT_60)
   ```
6. Create a trigger of type **Reboot** to start the routine.

Note: The **Reboot** trigger type may not seem intuitive, but the *trigger* is what starts the *monitoring* of NWS events, not the NWS event itself. Other trigger types can be used, but **Reboot** best ensures the system is always monitoring for NWS events.

Tip: To test your Alerts routine, use a demonstration alert code (see *"Demonstration Alerts" on page 551*) for the $alerts variable's <location-code> parameter (see *"Setting Variables for the Display Message" on page 548*) and execute the routine using the Dashboard's Routines button. To initiate the routine this way, Allow DTMF must be enabled for the routine. Be sure to change the <location-code> back to its normal value after testing is complete.

Setting Variables for the Display Message

You can use the following variables in the **Text** field of a **Display-Msg** to have NWS alerts automatically appear on the video display connected to the NQ-GA10PV:

- `$auto_resize`

  Indicates that the font will be automatically resized (to a specified minimum) as needed to fit the NWS alert on the screen.

- `$alerts`

  Specifies the details of how to respond to an NWS alert, such as: for which county to receive alerts, what information to display, what announcement to play, and more.

$auto_resize Parameters

The `$auto_resize` variable must be immediately followed by a number in parentheses, for example, `$auto_resize(20)`. In this example, Nyquist automatically resizes the display message by decreasing the font size, if needed, to better fit the message to the screen, but will keep the font size to at least 20.

The font size will automatically resize to 20 if the Alert message has these following parameters:

- Priority is smaller than 6.
- Text length is longer than 1500 characters.
- The text has more than 500 capital letter characters.

The font size also automatically resizes to 20, if needed, even if the `$auto_resize` variable is not specified.

$alerts Parameters

The `$alerts` variable is immediately followed by one or more parameters in parentheses, as in the following example:

```
$alerts(FLC095,INCLUDE_CODES,AUTO_COMPRESS_15,REPEAT_60)
```

The first parameter should specify the location, either as a location code (see *"<location-code>" on page 550*), coordinates (see *"LATLON:<latitude>_<longitude>" on page 555*), auto-find location (see *"AUTO_FIND_COUNTY" on page 552*), or as a demonstration location for testing (see *"Demonstration Alerts" on page 551*).

When designing a Routine to process alerts, it is important to understand how alerts are detected and processed. It can be helpful to think of `$alerts` as a function which waits for the arrival of an event and then processes the event by displaying text, playing announcements, etc. The next time the `$alerts` function is called (i.e., either the Action is executed again or the `REPEAT_<integer>` parameter was specified with the `$alerts` variable, causing it to execute repeatedly), it again waits for an event to arrive and repeats the process. If the previous alert is still pending, the previously processed event can be detected and processed again. If the `REPEAT_<integer>` parameter is specified, several other parameters can be specified to minimize or prevent duplicate processing of the same alert:

- PLAY_ONCE
- PLAY_SKIP_<integer>
- PLAY_STOP_<integer>
- REPEAT_ONCE
- ROUTINE_ALERT_ONCE
- ROUTINE_NOALERT_ONCE

The available parameters are described in the following sections.

<location-code>

Displays weather alerts for the zone that corresponds to the specified Universal Geographic Code (UGC), as described in the NWS Common Alerting (CAP) documentation:

https://vlab.noaa.gov/web/nws-common-alerting-protocol/cap-documentation#geocode

The UGC is a 6-character value that can be specified using either county zone (`ssCnnn`) or public zone (`ssZnnn`) formats. (Specific Area Message Encoding [SAME] codes are not supported.)

For example, the UGC for Orange County, Florida is can be specified as either FLC095 (county zone) or FLZ045 (public zone).

```
$alerts(FLC095,...)
$alerts(FLZ045,...)
```

The NWS API web service is used to retrieve weather data. Details about the service are available at:

https://www.weather.gov/documentation/services-web-api

Note: Only UGCs of type `county` or `public` should be used as the <location-code>.

Identifying a Target UGC

The list of valid UGCs (i.e., county and demo codes) can be found in the **NWS Alert Options** section of the *Add NWS Alert* page (see *"Add or Edit an NWS Alert Routine" on page 540*).

An alternate (though less accurate) method to determine which UGC to use is to enable the AUTO_FIND_COUNTY parameter (see *"AUTO_FIND_COUNTY" on page 552*), which attempts to use the IP address of the C4000 to determine the approximate coordinates and thus the UGC to use (see *"AUTO_FIND_COUNTY" on page 552* and *"UPDATE_CACHE" on page 559*).

Important: Bogen recommends the use of the LATLON variable, which specifies the alert location via latitude and longitude coordinates (see *"LATLON:<latitude>_<longitude>" on page 555*), over the `<location-code>` and `AUTO_FIND_COUNTY` $alert parameters. This is to ensure receipt of all relevant alerts for the specified location.

The following document explains how NWS uses different methodologies to geolocate watch, warning, and advisory alerts and how use of zone-based codes can potentially result in missed alerts.

https://www.weather.gov/media/documentation/docs/NWS_Geolocation.pdf

Specifying a latitude/longitude point or a county-based code (ssCnnn) ensures all county- and zone-based alerts are received, while a zone-based code (ssZnnn) may not include all county-based alerts.

Demonstration Alerts

Several demonstration/sample Alerts are available for demonstrations or testing. These samples represent typical alerts sent by the NWS for various alert types.

You can access these by replacing `<location-code>`, `LATLON:<lat>_<long>`, or `AUTO_FIND_COUNTY` with `ALERT_DEMO<integer>`, where `<integer>` is replaced with a number between 1 and 20 (for example, `ALERT_DEMO1` or `ALERT_DEMO20`). Bogen recommends that you test each demonstration alert to help you get familiar with the alert format, the available `$alerts` options, and font sizing.

ANNOUNCEMENT_BY_EVENT

Whenever an alert is active, the system will play the announcement associated with the **Event Type**, as defined in the *Alert Filters Configuration* view (see *"Alert Filters Configuration" on page 535*).

If `ANNOUNCEMENT_ZONE_<zone>` is defined, the announcement will be played to the specified zone; if not, it will be played to the zone specified by the Announcement associated with the **Event Type**.

ANNOUNCEMENT_DEFAULT_DTMF_<dtmf-code>

When combined with ANNOUNCEMENT_BY_EVENT, this defines the default announcement to use if the **Announcement** for the current alert **Event Type** is set to **None**. This parameter should usually be included in combination with ANNOUNCEMENT_BY_EVENT; if not, alerts that occur with **Event Type** set to **None** will not play any announcement.

Example:

```
$alerts(FLC127,INCLUDE_CODES,INCLUDE_COUNTY,AUTO_COMPRESS_25,ANNOUNCEMENT_BY_EV
ENT,ANNOUNCEMENT_DEFAULT_DTMF_411,ANNOUNCEMENT_ZONE_10,PLAY_SKIP_59,POST_DASH_P
HONE_TEXT,REPEAT_60) $auto_resize(20)
```

ANNOUNCEMENT_DTMF_<dtmf-code>

Plays the announcement with the DTMF code specified by `<dtmf-code>`. For example, including `ANNOUNCEMENT_DTMF_12` will cause the routine action to play the announcement that has a DTMF code equal to 12. When specifying an `ANNOUNCEMENT_DTMF_<dtmf-code>`, the `<dtmf-code>` is replaced by the desired announcement's DTMF code.

The announcement to be played must have **Play To Zone** set to the desired playback zone, or the `ANNOUNCEMENT_ZONE_<zone>` variable must be included to specify the zone to play to. If **Play To Zone** is not set and `ANNOUNCEMENT_ZONE_<zone>` is not included, the announcement will not play

The announcement will only be played if an actual alert exists and the alert text is sent to a GA10PV display. If an alert does not exist when the action executes, the announcement will not be played.

If the `$alerts()` variable contains a `REPEAT_<integer>` parameter, the announcement's **Times to Play** should be considered, because the `REPEAT_<integer>` parameter will automatically cause the announcement to repeat at the interval specified by the `REPEAT_<integer>` parameter. If **Times to Play** is set to

zero (0), meaning continuous, the user will need to manually stop the Announcement once it has started.

The extension of a routine that includes the `$alerts()` variable and `ANNOUNCEMENT_DTMF_<dtmf-code>` parameter must have permission to start announcements.

Note: A generic National Weather Service alert announcement entitled "NWS Alert" is available for use. Under the Announcements view, look for the "NWS Alert" announcement and use the DTMF code associated with it.

Warning If you change the DTMF code of an announcement that is used in a Routine Action via the `$alerts()` `ANNOUNCEMENT_DTMF_<dtmf-code>` parameter, you will need to manually update the DTMF code for the `ANNOUNCEMENT_DTMF_<dtmf-code>` parameter. Nyquist will not automatically make the change.

ANNOUNCEMENT_ZONE_<zone>

Indicates the zone to which the announcement will be played—where `<zone>` specifies a valid zone number—when either the `ANNOUNCEMENT_DTMF_<dtmf-code>` or ANNOUNCEMENT_BY_EVENT variable has been specified. If `ANNOUNCEMENT_ZONE_<zone>` is not specified, the announcement will be played to All Speakers.

Note: This parameter is only applicable when using the `ANNOUNCEMENT_DTMF_<dtmf-code>` or `ANNOUNCEMENT_BY_EVENT` parameters.

Important: If `ANNOUNCEMENT_ZONE_<zone>` is not specified, the announcement will be played to the zone specified in the *Alert Filters Configuration* for the event's Event Type (see *"Alert Filters Configuration" on page 535*). Unless `ANNOUNCEMENT_DEFAULT_DTMF_<dtmf-code>` is specified, this requires that **Play to Zone** must be defined for every Announcement specified for an Event Type of the Alert Filters Configuration.

AUTO_FIND_COUNTY

Automatically discovers the county code (see *"<location-code>" on page 550*) associated with the Nyquist server's public IP address.

Important: The C4000 will only discover the county code once, then cache it for subsequent operations. To force it to rediscover the county code, use the UPDATE_CACHE option (see *"UPDATE_CACHE" on page 559*).

Caution This option is approximate and is not recommended if the server's physical location is in a different county from your facility, if your server resides in the cloud, or if you are tracking alerts for multiple facilities and those facilities are not in the same county. Instead, find and use your county code.

Tip: The value of the cached county code can be viewed in the output of **Check Server Status** (see *"Check Server Status" on page 44*).

Important: Bogen recommends the use of the LATLON variable, which specifies the alert location via latitude and longitude coordinates (see *"LATLON:<latitude>_<longitude>" on page 555*), over the `<location-code>` and `AUTO_FIND_COUNTY` $alert parameters. This is to ensure receipt of all relevant alerts for the specified location.

AUTO_COMPRESS_<integer>

Automatically compresses the display message if the number of lines in the message exceeds the `<integer>` value. For example, `AUTO_COMPRESS_15` will cause messages that contain more than 15 lines to be compressed by removing end-of-line characters (lines will run together, separated by a space instead of end-of-line). The resulting message will perhaps be more difficult to read than the original. Use this option if you want to ensure that messages will fit on the screen. You may need to experiment to determine a suitable value for <integer>. You can combine this option with the `$auto_resize` variable.

Note: Font sizes are set in the Display Message options (see *"Creating a Display Message via the Dashboard" on page 501*). For weather alerts, the following settings are recommended for the Liberation Sans font:

30: When not using the `AUTO_COMPRESS_<integer>` option of the `$alerts` variable and not using the `$auto_resize` variable. A font size of 30 will ensure that the actual lines from the NWS will fit on each line displayed.

65: When using `AUTO_COMPRESS_15` and `$auto_resize(25)` variable.

40: When using `AUTO_COMPRESS_25` and `$auto_resize(25)` variable.

70: When using `AUTO_COMPRESS_<integer>` and `$auto_resize` variable with display message priority of six (6).

Tip: If you are not going to use NQ-GA10PV displays to view NWS Alerts, then do not include the AUTO_COMPRESS_# parameter in the Display-Msg action `$alerts()` parameter list. Inclusion of the `AUTO_COMPRESS_#` parameter is designed to help fit alerts onto the NQ-GA10PV message display when the alerts contain a lot of text, but as a result of compression, they will also display compressed in the National Weather Service Alerts window of the Nyquist dashboard display and on the NQ-T1100 or NQ-ZPMS NWS Alerts display.

If your primary method for viewing alert details is via NQ-GA10PV displays, then inclusion of the `AUTO_COMPRESS_#` parameter is recommended.

INCLUDE_CODES

Displays the Severity, Certainty, Urgency, and Response codes on the Alerts header for each alert (see *Figure 218, "Sample Alert With Elements Defined," on page 537*).

Note: This parameter is also applicable to the NQ-T1100, NQ-ZPMS, and dashboard when using the `POST_DASH_PHONE_TEXT` parameter.

INCLUDE_COUNTY

Displays the county code on the Alerts headers. This is useful if you have several Alert-related routines that use different county codes.

Note: This parameter is also applicable to the NQ-T1100, NQ-ZPMS, and dashboard when using the `POST_DASH_PHONE_TEXT` parameter.

INCLUDE_INSTRUCTIONS

Displays instructions that came with the weather alerts. If you want to display the exact instructions provided by the NWS, then add the `INCLUDE_INSTRUCTIONS` option. Instructions are usually obvious (like seek shelter, stay indoors, stay hydrated). However, instructions can be verbose and, while they can provide valuable information, verbose instructions could cause the messages to be too large to display properly.

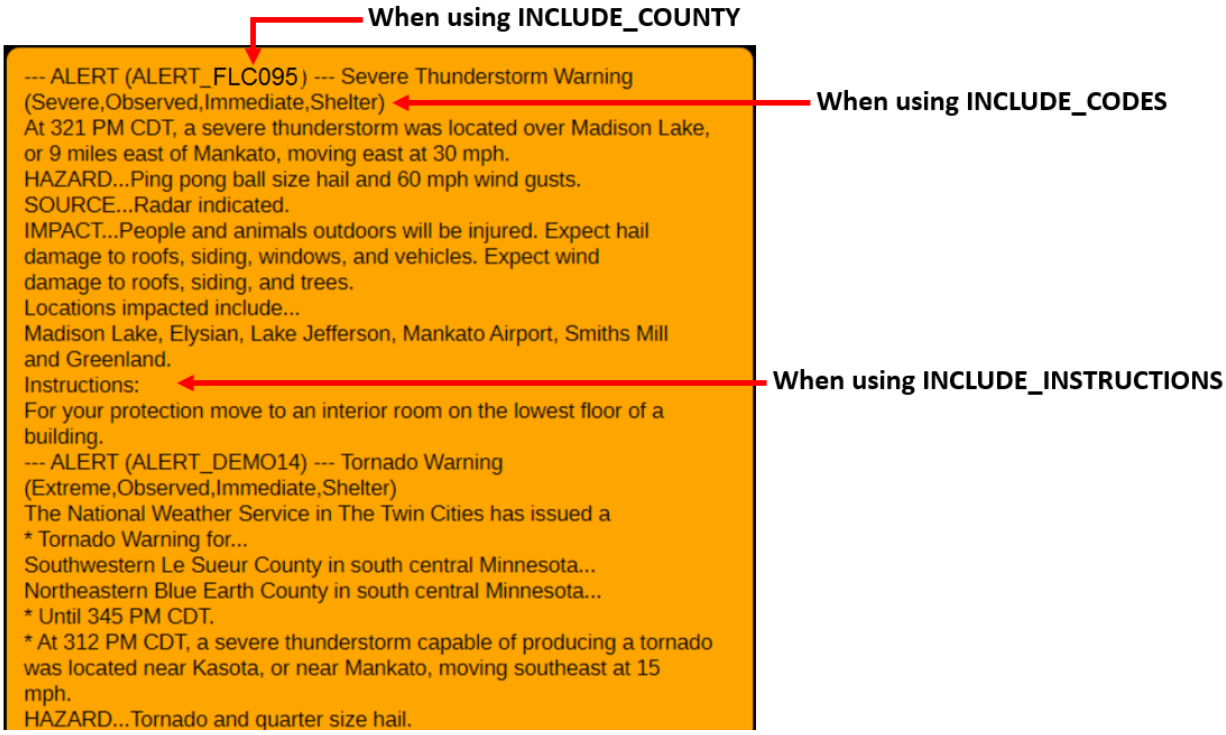


Figure 221. How Parameters Affect Display

A sample alert string is:

```
$alerts(FLC095,INCLUDE_COUNTY,INCLUDE_CODES,INCLUDE_INSTRUCTIONS,REPEAT_60)
```

This sample alert string will display alerts for county FLC095 (Orange County, Florida) every 60 seconds including alert instructions and the Severity, Certainty, Urgency, and Response codes (see *Figure 221, "How Parameters Affect Display," on page 554*).

LATLON:<latitude>_<longitude>

Displays weather alerts for the specified coordinates (i.e., latitude and longitude). The coordinates are specified as two decimal numbers separated by an underscore character.

```
$alerts(LATLON:<latitude>_<longitude>, ...)
```

For example, to specify coordinates 28.6064, −81.2210:

```
$alerts(LATLON:28.6064_-81.2210, ...)
```

Tip: Right-clicking a location on Google Maps or Bing Maps shows the coordinates for that location. Clicking the coordinates copies the coordinates to the clipboard. Coordinates can also be found using the NOAA's NWS GIS Viewer.

If the INCLUDE_COUNTY option has been specified (see *"INCLUDE_COUNTY" on page 554*), use the ZONE_DISPLAY_NAME option (see *"ZONE_DISPLAY_NAME_<text_to_display>" on page 560*) to specify what name to display (e.g., a city or county) in place of the coordinates.

Important: The location code variable can optionally be used instead of the latitude and longitude coordinates to specify the alert location (see *"<location-code>" on page 550* or *"AUTO_FIND_COUNTY" on page 552*), but use of latitude and longitude coordinates is strongly recommended.

PLAY_ONCE

Because the `REPEAT_<integer>` parameter will cause the announcement to repeat until an alert is no longer active, you can include `PLAY_ONCE` in the `$alerts()` parameter list if you want the announcement to play only once, when the alert first appears.

Note: This parameter is only applicable when using the `ANNOUNCEMENT_DTMF_<dtmf-code>` parameter.

Caution If `PLAY_ONCE` is included and an existing alert is immediately replaced by a new alert during a repeat cycle, the announcement will not play for the new alert. At least one repeat cycle must have no alerts present before the play count is reset and subsequent announcements are allowed to play.

PLAY_SKIP_<integer>

Because the `REPEAT_<integer>` parameter will cause the announcement to repeat during each repeat cycle until an alert no is longer active, you can include `PLAY_SKIP_<integer>` in the `$alerts()` parameter list if you only want the announcement to repeat periodically during an alert. When `PLAY_SKIP_<integer>` is included, the announcement playback will be skipped the number of times specified by `<inte-`

ger>. For example, if PLAY_SKIP_4 is included in the parameter list, the announcement will be played every five minutes (by skipping the announcement playback four times).

Note: This parameter is only applicable when using the ANNOUNCEMENT_DTMF_<dtmf-code> parameter.

Caution If PLAY_SKIP_<integer> is included and an existing alert is immediately replaced by a new alert during a repeat cycle, the announcement will not immediately play for the new alert. The announcement will play after the specified number of skips has transpired.

PLAY_STOP_<integer>

While an alert is pending and an ANNOUNCEMENT_DTMF_<integer> is specified, the PLAY_STOP_<integer> parameter can be used to control how many times the announcement is played while an alert is still pending. The <integer> specifies how many times to play before stopping. Since alerts can last several hours, this parameter can be used to control how many times to play the announcement during the alert before stopping.

Note: This parameter is only applicable when using the ANNOUNCEMENT_DTMF_<dtmf-code> parameter.

Caution If an existing alert is immediately replaced by a new alert during a repeat cycle, the announcement will not start playing again until at least one repeat cycle has no alerts present.

POST_DASH_PHONE_TEXT

Single-line NWS weather alert notices can be posted on the Nyquist Dashboard and NQ-T1100 Admin phones, and full-text NWS weather alert notices can be viewed on the NQ-T1100 Admin Phone and NQ-ZPMS Zone Paging Microphone Station screens.

To activate this feature, include the POST_DASH_PHONE_TEXT parameter in the $alerts() parameter list of a routine's Display-Msg action.

Tip: This feature can be used even if you do not have a NQ-GA10PV or NQ-T1100 device in your network (e.g., to display weather alert notices to the Dashboard). When configuring the Display-Msg action, set the Zones field to "All Displays."

If the POST_DASH_PHONE_TEXT parameter is included in the $alerts() variable parameter list, a single-line alert notice will be displayed on the Nyquist Dashboard (for admin users) and on NQ-ZPMS and NQ-T1100 Admin phone idle screens whenever there is an active alert.

The Nyquist Dashboard notice will include date/time, "--- ALERT ---", alert type, and optionally the county and codes (based on inclusion of INCLUDE_COUNTY and INCLUDE_CODES parameters in $alerts() parameter list).

The Admin Phone notice will omit the date/time and "--- ALERT ---" text to conserve space.

Important: The POST_DASH_PHONE_TEXT parameter requires the use of the REPEAT_## parameter. Without it, the weather alert will not be displayed on NQ-T1100 or NQ-ZPMS devices and dashboards.

The following is an example of a Dashboard notice using the POST_DASH_PHONE_TEXT parameter:

2021-04-22 10:15:20 --- ALERT --- Tornado Warning

The next example was achieved by adding INCLUDE_CODES in the $alerts() parameter list:

2021-04-22 10:15:20 --- ALERT --- Tornado Warning (Extreme,Possible,Future,Monitor)

The next example was achieved by adding INCLUDE_CODES and INCLUDE_COUNTY in the $alerts() parameter list:

2021-04-22 10:15:20 --- ALERT (FLC095) --- Tornado Warning (Extreme,Possible,Future,Monitor)

The following examples are comparable idle-screen notices on the NQ-T1100 Admin Phone:

>Tornado Warning

>(FLC095) Tornado Warning

If multiple routines are executing that contain a Display-Msg action with the $alerts() variable using different counties, alerts will be displayed for all counties that have active alerts. If you plan to display alerts for multiple counties, we recommend adding the INCLUDE_COUNTY parameter in the $alerts() parameter list to help distinguish between the counties that may be simultaneously displayed.

Note: In the phone images below, ALERT_DEMO2 and ALERT_DEMO4 are demonstration county codes.

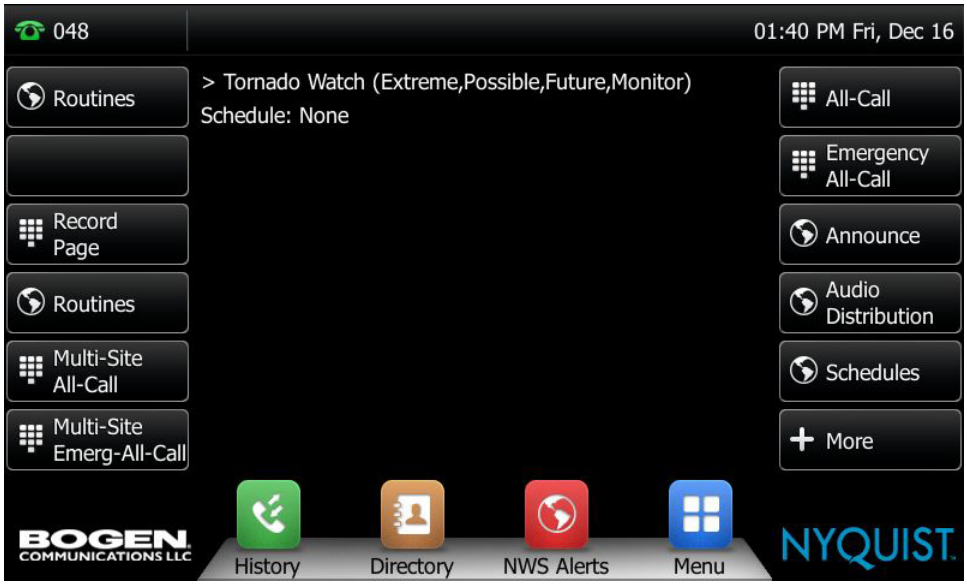


Figure 222. POST_DASH_PHONE_TEXT with ALERT_DEMO4

Figure 223. POST_DASH_PHONE_TEXT with ALERT_DEMO4 and ALERT_DEMO2

Important: For details on how to view the full alerts on the NQ-T1100 and NQ-ZPMS, see *"Viewing NWS Alerts on NQ-ZPMS Admin Phone" on page 560* and *"Viewing NWS Alerts on NQ-T1100 Admin Phone" on page 562*.

REPEAT_<integer>

Automatically repeats the alert processing and re-displays any resulting alerts every `<integer>` seconds with a minimum of 30 seconds. Previous alerts are automatically removed from displays. This option provides a convenient way to check for and display alerts at a regular interval without having to create a routine loop and without having to worry about deleting previous or expired alerts.

Important: This option is required when using the `POST_DASH_PHONE_TEXT` parameter to display NWS alerts on phone devices and/or the C4000 dashboard.

Warning When this option is used in a routine, subsequent actions of that routine will never be executed.

Tip: If you would like to monitor multiple locations for NWS alerts while using this option, create multiple routines, one for each location to be monitored.

Since alert processing requires Internet access processing, Bogen recommends a minimum `<integer>` value of 60 seconds. Using less than 60 seconds may significantly impact your network and Nyquist server processing utilization.

ROUTINE_ALERT_DTMF_<dtmf-code>

Executes the routine with the DTMF code specified by `<dtmf-code>` when an alert is present.

For example, including `ROUTINE_ALERT_DTMF_555` will cause the routine with a DTMF code of 555 to be executed, which might execute a routine that closes an I/O controller output contact which, in turn, might turn on an external light or buzzer.

Tip: If the `REPEAT_<integer>` parameter is present in `$alerts()` and alerts are present, the routine will be executed at each repeat cycle. For example, if `REPEAT_60` is included, the routine will be executed every 60 seconds. You can use `ROUTINE_ALERT_ONCE` to force the routine to only execute once while alerts are present.

ROUTINE_ALERT_ONCE

If this parameter is included with `ROUTINE_ALERT_DTMF_<dtmf-code>`, the specified routine will only be executed once during the alert lifetime.

ROUTINE_NOALERT_DTMF_<dtmf-code>

Executes the routine with the DTMF code specified by `<dtmf-code>` if no alerts are present.

For example, including `ROUTINE_NOALERT_DTMF_600` will cause the routine with DTMF code of 600 to be executed if *no alerts* exist. For example, this might execute a routine that opens an I/O controller output contact that, in turn, might turn off an external light or buzzer.

Tip: If the `REPEAT_<integer>` parameter is present in `$alerts()` and *no alerts* exist, the routine will be executed at each repeat cycle. For example, if `REPEAT_60` is included in the parameter list but no alerts exist, the routine will be executed every 60 seconds. You can use `ROUTINE_NOALERT_ONCE` to force the Routine to only be executed once while alerts do not exist.

ROUTINE_NOALERT_ONCE

If this parameter is included with `ROUTINE_NOALERT_DTMF_<dtmf-code>`, the specified routine will only be executed once if *no alerts* are present.

Tip: The `ROUTINE_ALERT_DTMF_<dtmf-code>` and `ROUTINE_NOALERT_DTMF_<dtmf-code>` parameters can be used together to toggle the state of an I/O Controller output contact. They could also be used together to add and/or delete Dashboard messages via Routine Actions.

UPDATE_CACHE

When using the `AUTO_FIND_COUNTY` option, Nyquist caches the county code found so the system does not have to search more than once. If your county code changes, however, include the `UPDATE_CACHE`

option along with AUTO_FIND_COUNTY to have the system rediscover the county code and cache the new value.

Important: You should remove the UPDATE_CACHE option after the first use (i.e., execute the Routine once, remove the UPDATE_CACHE option from the Routine Action, then restart the Routine); otherwise, the Nyquist system searches for the county code every time alerts are retrieved.

ZONE_DISPLAY_NAME_<text_to_display>

When the INCLUDE_COUNTY option (see *"INCLUDE_COUNTY" on page 554*) is used in the parameters list in combination with coordinate-based alerts (see *"LATLON:<latitude>_<longitude>" on page 555*), use ZONE_DISPLAY_NAME_<text_to_display> to change the name to be displayed in place of the county code. For example, to display "Orlando Florida" in place of the county code, specify:

ZONE_DISPLAY_NAME_Orlando_Florida

Note: Underscore characters in the <*text_to_display*> will be replaced by spaces on the display. For example, Orlando_Florida will be displayed as "Orlando Florida."

Caution Only alphanumeric characters are supported within <*text_to_display*>. Do not use special characters other than the underscore to indicate where spaces should be displayed.

Viewing National Weather Service Alerts

NWS Alerts will display automatically on some devices, but they are not as easily visible on NQ-ZPMS and NQ-T1100 Admin Phones.

NWS Glossary

NWS Alerts use a lot of abbreviations and technical terminology. The NWS provides a glossary of many of the terms they use, which can be found at:

https://forecast.weather.gov/glossary.php

It is also available in JSON format for programmatic access at:

https://api.weather.gov/glossary

Viewing NWS Alerts on NQ-ZPMS Admin Phone

National Weather Service (NWS) alerts can be viewed on the NQ-ZPMS display. To enable this, use the Nyquist server to customize one of this station's Line Keys with a **Type** of **NWS Alerts**. This will create a

Line Key on the NQ-ZPMS (i.e., the **NWS Alerts** button on the Line Keys screen) that can be used to view pending NWS alert messages.

Tip: To notify NQ-ZPMS users about an active NWS alert, we suggest triggering an announcement over the NQ-ZPMS station's associated Speaker Extension, triggering strobe lights via an I/O Controller, or displaying the NWS alerts on a highly visible NQ-GA10PV display. One or more of these actions can be initiated by triggering a routine via the `ROUTINE_ALERT_DTMF_<dtmf-code>` `$alerts` parameter, specifying the DTMF code of a routine containing one or more actions that notify users of the NWS alert.

To view the text of the active National Weather Service Alerts, press the **NWS Alerts** Line Key.

If no NWS alerts are active, the display will show "No alerts":

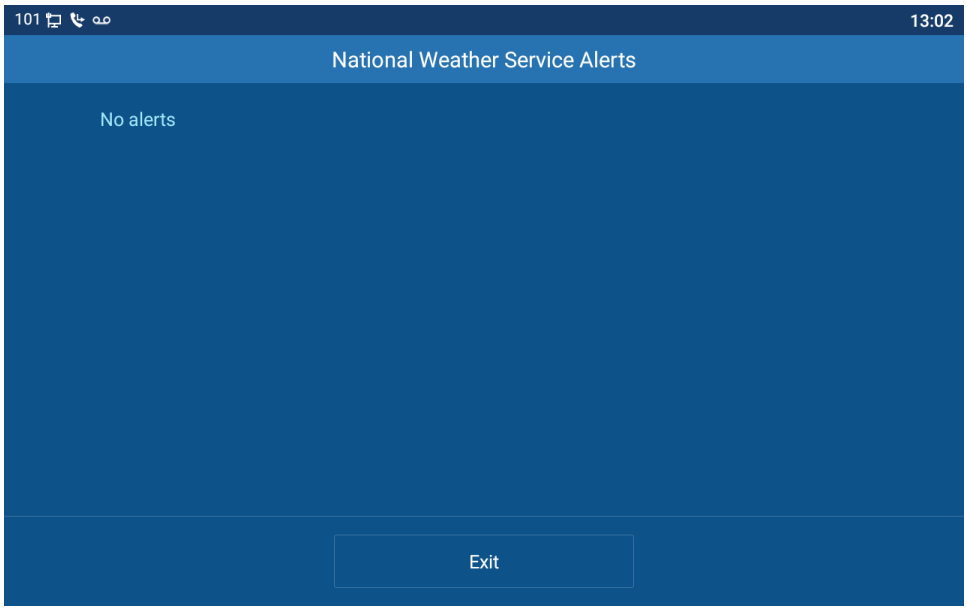


Figure 224. NWS with No Alerts

Note: "No alerts" can also indicate that there are no NWS Alert Routines executing to process NWS alerts.

Important: For NWS alerts to be displayed on the NQ-ZPMS, the Nyquist server must execute an NWS Alert Routine with **Post Dashboard and Phone Text** enabled (or that includes the `POST_DASH_PHONE_TEXT` parameter of the `$alerts` variable). For details, see "NWS Alert Routines" in the *Nyquist System Administrator Guide*.

When NWS alerts are active, a scrollable text window will display the text of active alerts:

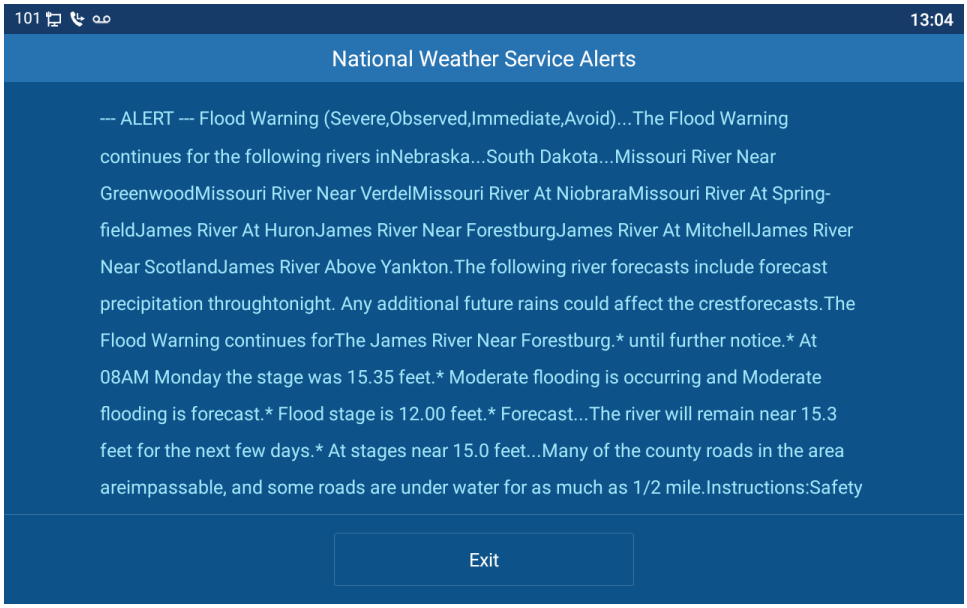


Figure 225. NWS with scrollable window

Touch and drag the screen to advance through the alert text pages. Press the Exit button to go back to the phone's main screen. While displaying the alerts, if there is no scrolling activity for 45 seconds, the phone will automatically return to the idle screen. If a call rings on the phone while the alerts are being displayed, the phone will automatically switch to the incoming call display.

Important: The alerts display is limited to 2000 characters. If the active alerts contain more than 2000 characters of text, "-TRUNCATED" will be appended to the end of the alert text to indicate that the remaining alert text has been truncated. To reduce the number of characters taken up by alerts, consider excluding the `INCLUDE_INSTRUCTIONS` `$alerts()` parameter.

Viewing NWS Alerts on NQ-T1100 Admin Phone

National Weather Server Alerts text can be viewed on the NQ-T1100 Admin Phone display. To view the text of all active National Weather Service Alerts, press the NWS Alerts softkey found on the bottom of the NQ-T1100 Admin phone display:

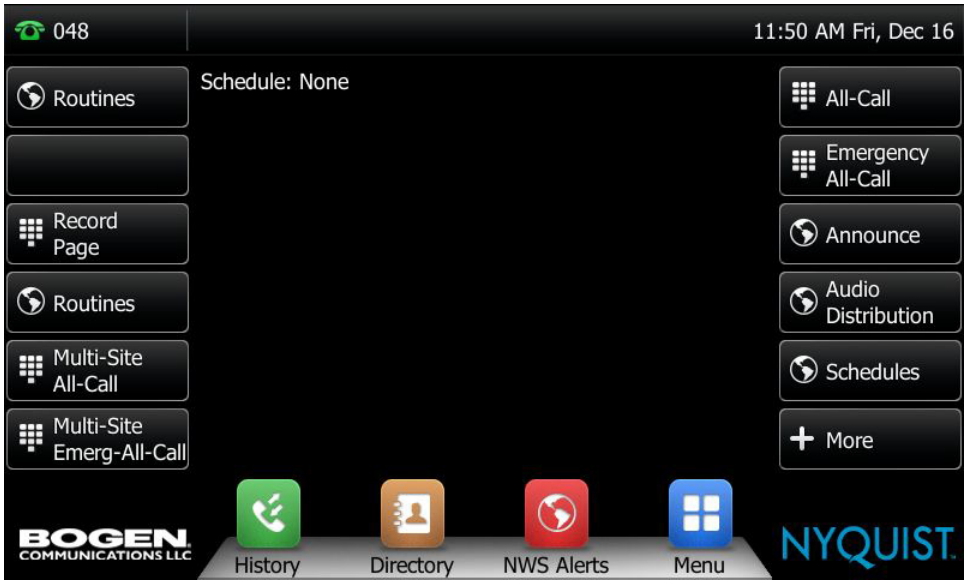


Figure 226. NWS Alerts softkey

If no NWS alerts are active, the display will show "No alerts":

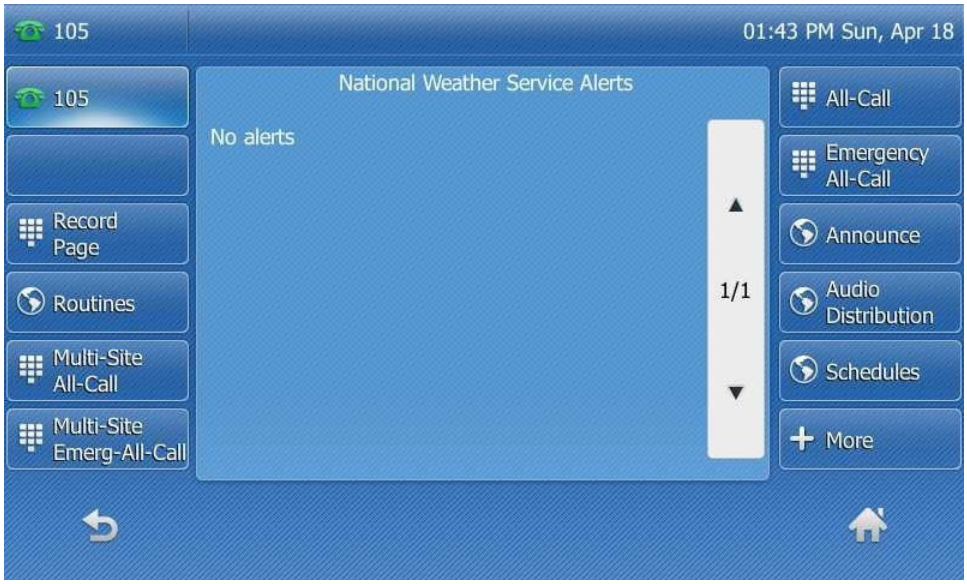


Figure 227. NWS with No Alerts

Note: "No alerts" can also indicate that there are no NWS Alert Routines executing to process NWS alerts.

Important: For NWS alerts to be displayed on the NQ-T1100, the Nyquist server must execute an NWS Alert Routine with **Post Dashboard and Phone Text** enabled (or that includes the `POST_DASH_-PHONE_TEXT` parameter of the `$alerts` variable). For details, see "NWS Alert Routines" in the *Nyquist System Administrator Guide*.

When NWS alerts are active, a scrollable text window will open in the center of the phone's screen to display the text of active alerts:

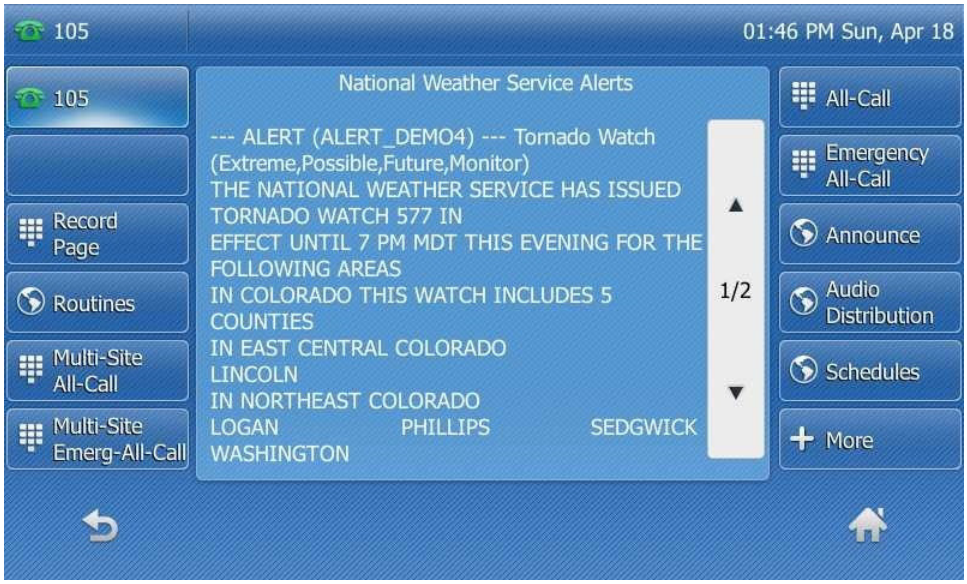


Figure 228. NWS with scrollable window

Use the scrollbar to advance through the alert text pages. Press the back button (on the bottom left) to go back to the phone's Idle screen. While displaying the alerts, if there is no scrolling activity for 45 seconds, the phone will automatically return to the Idle screen. If a call rings on the phone while the alerts are being displayed, the phone will automatically switch to the incoming call display.

Note: The alerts display is limited to 2000 characters. If the active alerts contain more than 2000 characters of text, the end of the display will show "-TRUNCATED" to inform you that the remaining alert text has been truncated. To help reduce the number of characters taken up by alerts, consider not using the `INCLUDE_INSTRUCTIONS $alerts()` parameter.

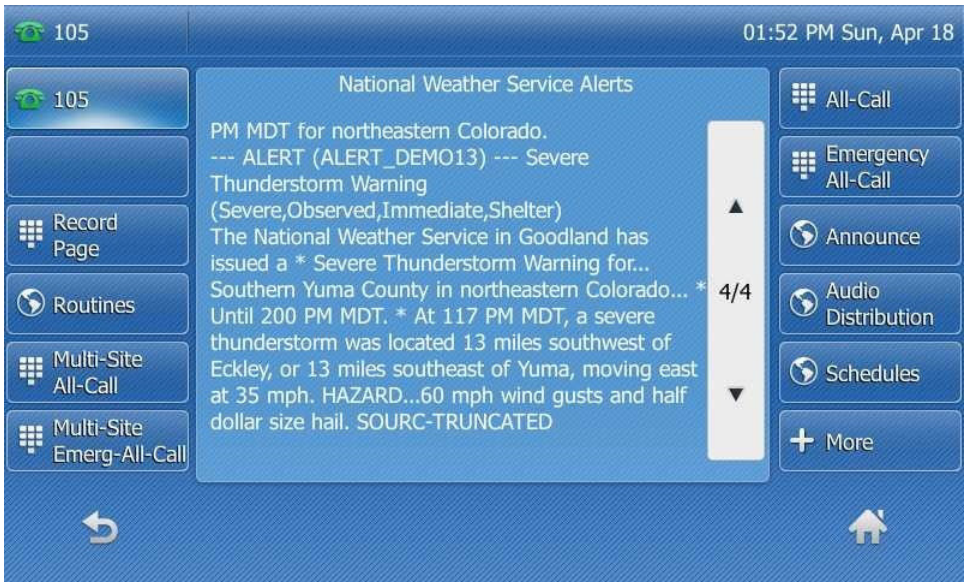


Figure 229. NWS without INCLUDE_INSTRUCTIONS

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

Appendix B: Acronyms and Abbreviations

A

AD	Active Directory
ANS	Ambient Noise Sensor
API	Application Programming Interface
ATA	Analog Telephone Adapter
Auth	Authorization

B

BTN	Billing Telephone Number

C

CA	Certification Authority
CAN	Controller Area Network
CAP	Common Alerting Protocol
CDR	Call Detail Record
codec	Coder-Decoder
CoS	Class of Service
CPU	Central Processing Unit

D

DCS	Digital Call Switch
DHCP	Dynamic Host Configuration Protocol
DID	Direct Inward Dial
DISA	Direct Inward System Access
DN	Distinguished Name
DNS	Domain Name System
DSC	Double-Sided Combo
DSP	Digital Signal Processing
DTMF	Dual Tone Multi-Frequency

DUNDI	Distributed Universal Number Discovery

E

EAS	Emergency Alert System
ECC	Error Correcting Code

F

FXO	Foreign Exchange Office
FXS	Foreign Exchange Subscriber

G

GND	Ground
GUI	Graphical User Interface

H

HDMI	High-Definition Multimedia Interface
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure

I

I/O	Input/Output
ICE	Interactive Connectivity Establishment
iOS	iPhone Operating System
IP	Internet Protocol
IRS	Internet Radio Services
IT	Information Technology
ITSP	Internet Telephony Service Provider

J

JSON	JavaScript Object Notation

K

L

LAK	License Activation Key
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LED	Light Emitting Diode
LLDP	Link Layer Discovery Protocol

M

MAC	Media Access Control
MGCP	Media Gateway Control Protocol
MMPA	Matrix Mixer Pre-Amp

N

NAS	Network Attached Storage
NAT	Network Address Translation
NFS	Network File System
NIC	Network Interface Card
NTP	Network Time Protocol
NTS	Network Time Server
NWS	National Weather Service

O

OS	Operating System

P

PBX	Private Branch Exchange
PC	Personal Computer
PCI	Peripheral Component Interconnect
PCIe	PCI Express
PIN	Personal Identity Number
PoE	Power over Ethernet

PSTN	Public Switched Telephone Network
PTT	Push-To-Talk

Q

R

RAID	Redundant Array of Independent Disks
REST	Representational State Transfer
RGB	Red-Green-Blue
RTP	Real-time Transport Protocol

S

SAN	Storage Area Network
SIP	Session Initiation Protocol
SMART	Self-Monitoring, Analysis, and Reporting Technology
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SRTP	Secure Real-time Transport Protocol
SSD	Solid State Drive
SSL	Secure Sockets Layer
STUN	Session Traversal Utilities for Network Address Translation (NAT)

T

TCP	Transport Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
TURN	Traversal Using Relays around Network Address Translation (NAT)

U

UDP	User Datagram Protocol
UI	User Interface
URL	Uniform Resource Locators

USB	Universal Serial Bus

V

VCTRL	Volume Controller
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol

W

WAN	Wide Area Network
WBC	Wall Baffle Combo Speaker with Integrated LED Message Display and Flasher (NQ-S1810WBC)

X

XML	Extensible Markup Language

Y

Z

ZPMS	Zone Paging Microphone Station

Appendix C: Nyquist DTMF Feature Dialing Codes

Most features of the Nyquist system can be accessed via DTMF dial codes entered from a station's keypad. The availability of a particular feature dial code is determined and restricted by the DTMF code's required CoS and the station's CoS assignments.

- "Alarm/Tone Activation" on page 575
- "Announcements" on page 576
- "Calling" on page 577
- "Call Forwarding" on page 578
- "Call Parking/Call Pickup" on page 578
- "Call Transfer" on page 579
- "Conferencing" on page 579
- "Monitoring/Recording" on page 580
- "Paging" on page 581
- "Voicemail" on page 582
- "Walking CoS" on page 583
- "Dial Codes Used for Simulating Calls to Admin Station from Station Call Switches" on page 583
- "Routines" on page 584
- "Audio Distribution" on page 584
- "Miscellaneous Dial Codes" on page 585

For a list of alternatives to some of the DTMF codes listed here (e.g., codes that do not use the pound/hashtag symbol, #), see:

- "Alternate Dialing Codes" on page 586

Note: DTMF codes marked with [a] support terminating the DTMF code with a # symbol to avoid the 5-second delay while the DISA application waits for additional digits to be entered.

Alarm/Tone Activation

Description	DTMF Code	Required CoS
Start Alarm specified by {DTMF-code}	`*91{DTMF-code}`[a]	Activate Alarm Signals
	`0000091` *Note:* You will be prompted to enter the Alarm's DTMF code.	Activate Alarm Signals
Start Tone specified by {DTMF-code}, play to {zone} *Note:* *{zone} is optional.	`*96{DTMF-code}*{zone}`[a]	Manually Activate Tone Signals
	`0000096{DTMF-code}*{zone}`	Manually Activate Tone Signals
Start Tone specified by {DTMF-code}	`*96{DTMF-code}`	Manually Activate Tone Signals
Prompts user to enter a tone number and tone parameters (e.g., times to play) and starts the tone at all Time-type zones	`*96`	Manually Activate Tone Signals

a. The DTMF code can be terminated with a # symbol to avoid the 5-second delay while the DISA application waits for additional digits to be entered.

Announcements

Description	DTMF Code	Required CoS
Start Announcement specified by {DTMF-code} to station's configured "Announcement Zone" *Note:* If "Announcement Zone" is not configured, the caller will be prompted to enter a zone number.	*92{DTMF-code}	All-Call Page
	0000092{DTMF-code}	All-Call Page
Start Announcement specified by {DTMF-code}, play to {zone}	*92{DTMF-code}*{zone}[a]	Zone Paging
	0000092{DTMF-code}*{zone}	Zone Paging
Start Announcement specified by {DTMF-code} to all Facilities (including local facility)	*97{DTMF-code}#0	Multi-Site Paging Inter-Facility Call/Page
Start Announcement specified by {DTMF-code} to Facility specified by {facility-page-number}	*97{DTMF-code}#{facility-page-number}	Inter-Facility Call/Page
Start Announcement specified by {DTMF-code} to dialed Facilities *Note:* Use "0" for {facility-page-number} to include the local facility. *Note:* The number of dialed digits cannot exceed 70 digits.	*97{DTMF-code}#{facility-page-number}*{facility-page-number}	Multi-Site Paging Inter-Facility Call/Page
Stop Announcement currently playing to {zone-number}	*93{zone-number}[a]	(none)
	0000093{zone-number}	(none)

a. The DTMF code can be terminated with a # symbol to avoid the 5-second delay while the DISA application waits for additional digits to be entered.

Calling

Description	DTMF Code	Required CoS
Call {extension} speaker (intercom, auto-answer)	`{extension}`	Call Any Station
Call {extension} ringer (telephonic, ringing)	`*{extension}`	Call Any Station
Join conversation at {extension}	`*#{extension}`	Join Conversation
Call {extension} at {facility-page-number}	`##*{facility-page-number}*{extension}`	Inter-Facility Call/Page
Place long distance call with area code (AAA = Area code, NNNNNNN = number)	`981AAANNNNNNN`	Outside Access rights
Place local ten-digit call with area code	`98AAANNNNNNN`	Outside Access rights
Place local seven-digit call	`98NNNNNNN`	Outside Access rights
Place 911 emergency call *Note:* Based on Station's **911 Route** setting, call may be directed to Admin Station, PSTN-based 911, or denied.	`911` `98911`	(none) (none)
Place Emergency call to designated Admin station	`****`	(none)
Place call to PBX system (via SIP Trunk) by dialing {DTMF-codes} *Note:* {DTMF-codes} can be as simple as an extension number on the attached PBX system.	`***{DTMF-codes}`	Outside Access rights

Call Forwarding

Description	DTMF Code	Required CoS
Call Forwarding Menu	`970`[a]	Call Forwarding
All-Calls (CFALL)	`971{extension}`	Call Forwarding
When Busy (CFBS)	`972{extension}`	Call Forwarding
When No Answer (CFNA)	`973{extension}`	Call Forwarding
When Busy or No Answer (CNBN)	`974{extension}`	Call Forwarding
Cancel Call Forwarding	`975`	Call Forwarding
Call Forwarding Status (Caller only)	`976`	Call Forwarding
Call Forwarding Status (All users)	`977`	Call Forwarding

a. The DTMF code can be terminated with a # symbol to avoid the 5-second delay while the DISA application waits for additional digits to be entered.

Call Parking/Call Pickup

Description	DTMF Code	Required CoS
Park call (during call)	`#72`	(none)
Note: To pick up a parked call, dial the parked call's extension (by default, extensions 21-29) that was provided when the call was parked using #72. The parking lot extensions can be changed at the Admin Web UI through **System Parameters**.		
Call pickup {extension} when ringing	`7*{extension}`[a]	Remote Pickup

a. The DTMF code can be terminated with a # symbol to avoid the 5-second delay while the DISA application waits for additional digits to be entered.

Call Transfer

Description	DTMF Code	Required CoS
Blind transfer (during call)	`#1{extension}`	Call Transfer
Attended transfer (during call)	`*1{extension}`	Call Transfer
Complete attended transfer, dropping out of call	`*2`	Call Transfer
Complete attended transfer, but stay in the call	`*3`[a]	Call Transfer
Swap to the other party (during attended transfer)	`*4`	Call Transfer
Transfer (drop) call from Speaker to associated Phone	`*3`[a]	Call Transfer
Transfer (drop) call from Speaker to associated Phone	`####`	Call Transfer
Transfer call from Phone to associated Speaker	`#1{speaker-extension}`	Call Transfer

a. The DTMF code can be terminated with a # symbol to avoid the 5-second delay while the DISA application waits for additional digits to be entered.

Conferencing

Description	DTMF Code	Required CoS
Create/Enter Dynamic Conference {number}	**{number}	Conference Admin Conference User
Note: If the conference owner enters 0000 as the password, the conference will be deleted. If an Admin station user type enters 0000 as the password but is not the conference owner, the user will be prompted for the system password. If the correct system password is entered, the conference will be deleted.		
Start system playback of list of created conferences that includes the conference number and the extension that created the conference	**0	(none)

Monitoring/Recording

Description	DTMF Code	Required CoS
Monitor call or location at {extension} *Note:* Spy Mode monitoring cannot be used on a station that has been set to Privacy Mode.	978{extension}[a]	Monitor Calls/Locations
Enable "spy mode" (MUTE) during call monitoring	4	(none)
Enable "whisper mode" during call monitoring	5	(none)
Enable "barge mode" during call monitoring	6	(none)
Record Message (Announcement)	*990[a]	All-Call Paging
Note: When you record an announcement by dialing *990 or by selecting **Record Announcement** on the Admin phone's **Announce** menu, the initial DTMF Code for the recorded and saved announcement will be set to the announcement's row ID. You can change the DTMF Code after the announcement is saved by editing the announcement in the web interface **Announcements** view. The saved announcement has **Play to Zone** set to blank (no zone selected). This means that when you play an announcement via an IP phone **Announcement** menu selection, you will be asked to enter a zone number (where 0 = All Speakers). You can define a permanent zone number for the saved announcement by updating **Play to Zone** after the recorded announcement has been saved.		
Playback recorded calls **MENU**: 1–Emergency, 2–Monitored, 3–Urgent, 4–Standard	999	Manage Recordings
Start/Stop recording (DTMF used during a call)	*3	Record Calls

a. The DTMF code can be terminated with a # symbol to avoid the 5-second delay while the DISA application waits for additional digits to be entered.

Paging

Note: The "##" prefix is used to indicate multi-facility paging operations.

Description	DTMF Code	Required CoS
Multi-Site Emergency All-Call Page	##0911[a]	Emergency All-Call Multi-Site Paging
Multi-Site All Call Page	##0	All-Call Paging Multi-Site Paging
Emergency All-Call Page	#0911[a]	Emergency All-Call
Multi-Facility Emergency All-Call Page	##0912{facility-page-number}*{facility-page-number}...	Emergency All-Call Multi-Site Paging
Emergency All-Call Page	951	Emergency All-Call
All-Call Page	#0[a]	All-Call Paging
	#00	All-Call Paging
	0000000	All-Call Paging
Real-time All-Call Page that belongs to a queue	#0*[a]	All-Call Paging
	0000001[a]	All-Call Paging
Page to {zone}	#{zone}[a]	Zone Paging
	0000099{zone}[a]	Zone Paging
Real-time Page to {zone} that belongs to a queue	#{zone}*[a]	Zone Paging
All-Call Page to {facility-page-number}	##{facility-page-number}	Inter-Facility Call/Page

Paging (Continued)

Note: The "##" prefix is used to indicate multi-facility paging operations.

Description	DTMF Code	Required CoS
Multi-Facility All-Call Page	##{facility-page-number}*{facility-page-number}...	Inter-Facility Call/Page
Zone Page to {zone-number} at {facility-page-number}	##{facility-page-number}#{zone-number}	Inter-Facility Call/Page
Real-time page to {zone-number} that belongs to a queue at {facility-page-number}	##{facility-page-number}#{zone-number}*	Inter-Facility Call/Page
Record page; system will prompt for Zone Number	*991	Zone Paging
Record page for {zone-number}	*991*{zone-number}[a]	Zone Paging
Cancel Recorded Page *Note:* Only works if made from the same extension that created the recorded page.	*992	Zone Paging
Cancel Recorded Page for {zone-number} *Note:* Only works if made from the same extension that created the recorded page.	*992*{zone-number}[a]	Zone Paging

a. The DTMF code can be terminated with a # symbol to avoid the 5-second delay while the DISA application waits for additional digits to be entered.

Voicemail

Description	DTMF Code	Required CoS
Voicemail for current caller	900	Voicemail
Voicemail for specified {extension}	904{extension}	Voicemail
Leave voicemail for specified {extension}	904{extension}*	Voicemail

Walking CoS

Description	DTMF Code	Required CoS
Current phone or station temporarily uses the CoS settings of the specified {extension} For {auth-code}, specify the Auth Code configured for {extension} or, if that is 0000, the Auth Code configured via the System Parameters. *Note:* If **Auth Code** is set to 0000 in the Admin Web UI's **System Parameters**, this feature is disabled.	`3*{auth-code}*{extension}`	Walking Class of Service

Dial Codes Used for Simulating Calls to Admin Station from Station Call Switches

Description	DTMF Code	Required CoS
Normal call to admin *Note:* During the Check-In process, a Normal call starts the check-in process for a station.	`0`	(none)
Emergency call to admin	`*0`	(none)
Urgent call to admin	`*00`	(none)
Outside line calling in (uses night-ring logic)	`*000`	(none)

Routines

Description	DTMF Code	Required CoS
Execute Routine with {routine-DTMF-code} *Note:* Only routines with **Allow DTMF** can be executed from the Admin Phone.	`*94{routine-DTMF-code}`[a]	Execute Routines
	`0000094{routine-DTMF-code}`	Execute Routines
Execute Routine with {routine-DTMF-code} specifying values for parameters `$cmdParam1` and `$cmdParam2`. *Note:* Only routines with **Allow DTMF** can be executed from the Admin Phone.	`*94{routine-DTMF-code}*{cmdParam1}*{cmdParam2}`	Execute Routine
	`0000094{routine-DTMF-code}*{cmdParam1}*{cmdParam2}`	Execute Routine
Stop Routine with {routine-DTMF-code} *Note:* If the **Allow DTMF** parameter for the specified routine is set to **No**, you will be prompted to enter the system password.	`*95{routine-DTMF-code}`[a]	Execute Routines
	`0000095{routine-DTMF-code}`	Execute Routines

a. The DTMF code can be terminated with a # symbol to avoid the 5-second delay while the DISA application waits for additional digits to be entered.

Audio Distribution

Description	DTMF Code	Required CoS
Start Audio Distribution where {DTMF-code} is the DTMF code for the desired Audio Distribution	`987*{DTMF-code}`[a]	Audio Distribution
	`00000987{DTMF-code}`	Audio Distribution
Stop Audio Distribution where {DTMF-code} is the DTMF code for the desired Audio Distribution	`980*{DTMF-code}`[a]	Audio Distribution
	`00000980{DTMF-code}`	Audio Distribution
Stop ALL Scheduled Audio	`920`	Audio Distribution

a. The DTMF code can be terminated with a # symbol to avoid the 5-second delay while the DISA application waits for additional digits to be entered.

Miscellaneous Dial Codes

Description	DTMF Code	Required CoS
Restart Nyquist system server *Note:* User is prompted for System Password.	`#*349`	(none)
Toggle Audio Distribution to associated speaker	`*9`[a]	(none)
Disable Audio	`0000097`[a]	Disable Audio
Enable Audio	`0000098`[a]	Enable Audio
Stop Scheduled Audio	`920`	Audio Distribution
Close {contact-number} on I/O Controller {extension} *Note:* For example, dialing 942#120#1 closes contact number 1 on I/O Controller 120.	`942#{extension}#{contact-number}`	Manage Output Contacts
Open {contact-number} on I/O Controller {extension} *Note:* For example, dialing 943#120#1 opens contact number 1 on I/O Controller 120.	`943#{extension}#{contact-number}`	Manage Output Contacts
Request a callback during a call	`*7`	Call Any Station
Cancel a callback request during a call	`*8`	Call Any Station
Request a callback from a specific extension	`*7{extension}`[a]	Call Any Station
Cancel a callback request from a specific extension	`*8{extension}`[a]	Call Any Station
Start Nyquist Features on Remote Facilities	`##*{facility-page-number}*{feature-DTMF-digits}`	Inter-Facility Features
Examples:		(none)
Start Announcement 1 on Facility 1	`##*1*00000921`	(none)
Start Audio Distribution 6 on Facility 5	`##*5*000009876`	(none)
Execute Routine 5 on Facility 10	`##*10*00000945`	(none)

a. The DTMF code can be terminated with a # symbol to avoid the 5-second delay while the DISA application waits for additional digits to be entered.

Alternate Dialing Codes

If a PBX is not able to pass through the pound sign (or hashtag), #, in the dialing digits, alternative dialing codes may be used to replace Nyquist extensions that start with #.

Nyquist Feature	Dial Code	Alternative Dial Code
All-Call Page	`#0`	`0000000`
Emergency All-Call Page	`#0911`	`951`
Zone Page	`#{zone}`	`0000099{zone}`
Start Alarm	`*91{DTMF-code}`[a]	`0000091{DTMF-code}`
Start Tone to zone	`*96{DTMF-code}*{zone}`[a]	`0000096{DTMF-code}*{zone}`
Start Tone to all Time-type zones	`*96{DTMF-code}`	`0000096{DTMF-code}`
Start Announcement	`*92{DTMF-code}`	`0000092{DTMF-code}`
Start Announcement to zone	`*92{DTMF-code}*{zone}`[a]	`0000092{DTMF-code}*{zone}`
Stop Announcement	`*93{zone}`[a]	`0000093{zone}`
Start Audio Distribution	`987*{DTMF-code}`	`00000987{DTMF-code}`
Stop Audio Distribution	`980*{DTMF-code}`	`00000980{DTMF-code}`
Start Routine	`*94{DTMF-code}`	`0000094{DTMF-code}`
Start Routine with parameters	`*94{DTMF-code}*` `{cmdParam1}*{cmdParam2}`	`0000094{DTMF-code}*` `{cmdParam1}*{cmdParam2}`
Stop Routine	`*95{DTMF-code}`	`0000095{DTMF-code}`
Restart Nyquist system server *Note:* User is prompted for System Password.	`#*349`	`00000349`

a. The DTMF code can be terminated with a # symbol to avoid the 5-second delay while the DISA application waits for additional digits to be entered.

Appendix D: Routine Action Types

Routine Action Parameter Descriptions

All Action types include the following parameters:

Table 1. Routine Common Parameters

Parameter	Description
Name	User-supplied name for the action.
Enabled	This action can only be executed if **Enabled** is **Yes**.
Type	The routine action to execute.
Condition	Optional boolean condition statement (using PHP syntax) that determines whether or not the action should be executed. Blank always evaluates to True. See *"Condition Statements"* for further details.
Description	User-supplied description of the action.

The following table describes the Routine Action Types and any Action-specific parameters.

Note: Parameters that can be overridden for Routines API calls via the `<action>Params` elements are described in *Table 3, "Routine Action Parameter Overrides via Routines API v2"*.

Table 2. Routine Action Type-Specific Parameters

Routine Action Type	Parameter 1	Parameter 2	Parameter 3	Parameter 4
Add-Announcement-Audio Adds audio to a temporary announcement. This must be preceded by a **New-Announcement** action followed by zero or more **Add-Announcement-Audio** actions and finally a **Play-Announcement** action. The following variables can be used for Number or Text-to-Speech announcements: $apiParam1 $apiParam2 $caller $called $contact $schedParam1 $schedParam2 $station	**Audio Source Type**	**Announcement to play** (depends on Audio Source Type)		
	• Announcement	**Announcement** • Selected announcement (announcement type in parentheses)		
	• Number	**Number** • Numeric value • Variable	**Force Announcement of Fraction** (used only when Audio Source Type is Number) • No • Yes	**Announce number as** (used only when Audio Source Type is Number): • Numeric • Digits
	• Text-to-Speech	**Text-to-Speech (TTS)** Text, with optional variables and TTS formatting (see *"Using SSML for Text-to-Speech Entries"*)		
	• JSON-Uploaded-File	**Form-Field Parameter Name** Name of the Routines API v2 parameter that specifies the audio file (mp3 or wav) to use See *"Routines API v2"* for details.		

Table 2. Routine Action Type-Specific Parameters (Continued)

Routine Action Type	Parameter 1	Parameter 2	Parameter 3	Parameter 4
Alarm	**Alarm** • Selected alarm	None	**Duration** • Number of seconds for action to continue; default is 86400 seconds (24 hours)	**None**
All-Call *Note:* All-Call must be the last action in a routine.	None	None	None	None
Announcement	**Announcement** • Selected announcement (announcement type in parentheses)	**Zone** • All speakers • Selected zone	**Duration** • Number of seconds for action to continue; default is 86400 seconds (24 hours) *Note:* The announcement will stop when the duration length is reached, regardless of the length of the announcement.	None
Audio-Dist-Start	**Audio Distribution** • Selected Audio Distribution	None	None	None
Audio-Dist-Stop	**Audio Distribution** • Selected Audio Distribution • All	None	None	None

Table 2. Routine Action Type-Specific Parameters (Continued)

Routine Action Type	Parameter 1	Parameter 2	Parameter 3	Parameter 4
Call-And-Announce	**Number to Call** • 911 • <extension>: A station **Extension** • *<extension>: Do not allow the station to auto-answer, forcing the station's phone to ring. • A local 7-digit phone number prefixed with 98 • A local 10-digit phone number prefixed with 98 • A long-distance 10-digit phone number prefixed with 981 • 0 (zero): Simultaneously calls all admin stations of the **Admin Group** associated with the routine's **Extension** *Note:* If the specified number to call is not a station extension, then at least one outgoing SIP trunk or Outside Line DAHDI port must be available, and the CoS of the Routine extension must match the extension defined by the SIP trunk or Outside Line DAHDI port.	**Announcement to Play** • Selected announcement	**Play Count** • Continuous Play • Number of times to play *Note:* If left blank or set to zero (0), the announcement plays continuously until the called number hangs up. If you are playing the announcement to a station that cannot disconnect the call (such as a speaker), specify the number of times to play the announcement.	None

Table 2. Routine Action Type-Specific Parameters (Continued)

<table>
<tr><th>Routine Action Type</th><th>Parameter 1</th><th>Parameter 2</th><th>Parameter 3</th><th>Parameter 4</th></tr>
<tr><td>Change-DSC01-Setting</td><td>Stations
• All Displays
• List of DSC01 station extension numbers</td><td>Field to change
• Enable Clock Display
• Clock Time Format
• Show Clock Seconds
• Enable Flasher Use
• Message LED Brightness
• Flasher LED Brightness
• Clock Position
• Clock Color‡</td><td>New Value
The new value for the specified Field to Change.</td><td>None</td></tr>
<tr><td colspan="4">Tip: The DSC01 settings can be changed during the day by executing a routine as part of a “bell” schedule, and/or can be executed via the Schedule Routines page. For example, by changing the “Message LED Brightness”, a scheduled Routine could turn off all DSC01 LED displays after hours (Message LED Brightness = Off) and turn the DSC01 LED displays back on when the next day starts (Message LED Brightness = Low, Medium, or High).

‡ Supported colors are amber, blue, blue-violet, cyan, deep-pink, green, indigo, lime, magenta, ocean, orange, pink, red, spring-green, turquoise, violet, white , yellow, and yellow-green.</td></tr>
<tr><td>Change-Setting</td><td>Selected Setting
• Disable Emergency All-Call and Intercom when Audio Disabled
• Enable Callback Request Indicator
• Night Ring Admin
• Night Ring Enabled</td><td>New Value
The new value for the Selected Setting.</td><td>None</td><td>None</td></tr>
</table>

Table 2. Routine Action Type-Specific Parameters (Continued)

Routine Action Type	Parameter 1	Parameter 2	Parameter 3	Parameter 4
Change-Volume *Tip:* To change the cut level for multiple Audio Types and/or Zones in a Routine, add a Change-Volume action for each. *Tip:* To change the cut level at a specific time (or on a recurring schedule), create a Scheduled Routine that calls the Change-Volume action.	**Audio Type** • All-Call • Audio Distribution • Emergency-All-Call • Zone Paging	**Zone** (available options determined by specified Audio Type) • All Speakers • All Speakers • One of a list of Audio zones • All Speakers • One of a list of Paging and Time-type zones	**Cut Level (dB)** A value between −42 and 0 dB. If a Cut Level Type of "Cut Level" is specified, the cut level value is specified (in dB) via a slide control. If a Cut Level Type of "API Value" is specified, select either: • $apiParam1 or • $apiParam2. The actual cut level (in dB) will be determined by the value of the selected variable when this action is executed via a Routines API call.	None
Change-WBC-Setting	**Stations** • All Displays • List of WBC station extension numbers	**Field to change** • Enable Clock Display • Clock Time Format • Show Clock Seconds • Enable Flasher Use • Message LED Brightness • Flasher LED Brightness	**New value for specified field** Select a new value for the specified *Field to change*. Available values are determined by the selected field.	None
	Tip: WBC settings can be changed during the day to satisfy different daytime requirements by executing a routine as part of a "bell" schedule and/or via the Schedule Routines page. For example, a scheduled Routine could turn off all WBC LED displays after hours (Message LED Brightness = Off) and turn them back on when the next day starts (Message LED Brightness = Low, Medium, or High).			

Table 2. Routine Action Type-Specific Parameters (Continued)

Routine Action Type	Parameter 1	Parameter 2	Parameter 3	Parameter 4
Check-In	**Check In** • Start • Stop • Done • Finish • Wait (see *"Check-In Action Type with Check-In Set to Wait"*) • Station • Vacancy-Add • Vacancy-Delete • Reset • Exclude-Add • Exclude-Delete	**Stations** • Selected Stations *Note:* Used when Parameter 1 (Check In) is Station, Vacancy-Add, Vacancy-Delete, Exclude-Add, or Exclude-Delete.	**Finish Delay** • No-Delay • Wait-Until-Done No-Delay means the next action will execute immediately. Wait-Until-Done means the next action will not execute until this action has completed.	None
Check-Intercom	None	None	None	None

Table 2. Routine Action Type-Specific Parameters (Continued)

Routine Action Type	Parameter 1	Parameter 2	Parameter 3	Parameter 4
Dash-Delete This action type is for deleting messages from the web interface dashboard. The number used for Number is based on the order the message was created; the third message created would be identified as number 3.	**Dash Delete**			
	• LIFO (Last In, First Out)	None	None	None
	• FIFO (First In, First Out)	None	None	None
	• IDENT	**Identifier** The following variables can be used: $apiParam1 $apiParam2 $caller $called $contact $deviceMacAddr $facility $eventid $eventname $schedParam1 $schedParam2 $scheduleid $station $toneid $tonename $user_var[1...10] $zone	None	None
	• Number	**Number**	None	None

Table 2. Routine Action Type-Specific Parameters (Continued)

Routine Action Type	Parameter 1	Parameter 2	Parameter 3	Parameter 4
Dash-Text This action type is for adding messages to web interface dashboards.	**Style** • Basic • Danger • Info • Success • Warning	**Identifier** The following variables can be used: $apiParam1 $apiParam2 $caller $called $contact $deviceMacAddr $facility $eventid $eventname $namecalled $namecaller $schedParam1 $schedParam2 $scheduleid $station $toneid $tonename $user_var[1...10] $zone *Note:* This parameter is optional and is used to identify a message for deletion.	**Scope** • All • Admin	**Text** The following variables can be used: $apiParam1 $apiParam2 $schedParam1 $schedParam2 $caller $called $contact $cputemp $date1 $date2 $date3 $deviceMacAddr $deviceName $df-avail $facility $eventid $eventname $namecaller $namecalled $scheduleid $schedulename $toneid $tonename $station $time1,$time2 $uptime $user_var[1...10] $zone
	Note: When specifying the text to display, you can use variables, such as $caller. When $caller is used in the Text parameter for dashboard and NQ-GA10PV display messages, the variable is replaced by the ID of the caller that triggered the routine. When calls are placed from outside the system, it displays the phone number of the caller.			
Disable Audio *Note:* In addition to the parameters, you can also set a **Finish Delay**, of either **No-Delay** or **Wait-Until-Done**	None	None	None	None

Table 2. Routine Action Type-Specific Parameters (Continued)

Routine Action Type	Parameter 1	Parameter 2	Parameter 3	Parameter 4
Display-Msg Display a message on the NQ-GA10PV and/or NQ-S1810WBC display.	**Zones** • All Displays • Selected zone or zones	**Identifier** *Note:* This parameter is optional and is used to identify a message for deletion. The following variables can be used as part of the identifier value: $apiParam1 $apiParam2 $caller $called $contact $deviceMacAddr $toneid $tonename $facility $eventid $eventname $schedParam1 $schedParam2 $scheduleid $station $user_var[1...10] $zone	**Stations** • Selected NQ-GA10PV or NQ-S1810WBC station • $called • $caller *Note:* Using the $called variable allows a single Intercom-call triggered routine to handle all NQ-GA10PV and NQ-S1810WBC displays.	**Device Type Filter** • GA10PV and WBC • GA10PV Only • WBC Only *Note:* To display weather alert notices on NQ-ZPMS devices, specify any Device Type Filter value and include the POST_DASH_PHONE_TEXT parameter in the $alerts function (see *"POST_DASH_PHONE_TEXT"*). **Text** (see description below) **Priority** • 6 = Fullscreen on GA10PV • 5 = Exclusive on GA10PV • 1–4 • 0 = Lowest **Display Time (seconds)** 0–99999 **Message Type** • Text • Image • JSON-Uploaded-Image **JSON-Uploaded-Image** indicates that the JSON field specified in **Form Field Parameter Name** will provide the image to display. See *"Overriding Routine Action Parameters via Routines API v2"* for details.

Table 2. Routine Action Type-Specific Parameters (Continued)

Routine Action Type	Parameter 1	Parameter 2	Parameter 3	Parameter 4
Display-Msg (cont'd)				**Device Type Filter** • GA10PV and WBC • GA10PV Only • WBC Only To display weather alert notices on NQ-ZPMS devices, specify any Device Type Filter value and include the POST_-DASH_PHONE_TEXT parameter in the $alerts function (see *"POST_DASH_PHONE_TEXT"*). **GA10PV Background Color** **GA10PV Font** **GA10PV Font Size** **GA10PV Font Color** **GA10PV Font Styles** **WBC Flasher Pattern** • No Change • Off • Slow • Fast • Double • Triple • Quad **WBC Number of Flasher Pattern Cycles** Zero (0) turns the flasher on for the duration of the message.

Table 2. Routine Action Type-Specific Parameters (Continued)

Routine Action Type	Parameter 1	Parameter 2	Parameter 3	Parameter 4
Display-Msg (cont'd)				**WBC Flasher Color** • Amber • Blue • Green • Orange • Red • Violet • White • Yellow **Image Priority** • Text Over Image • Image Over Text **Form Field Parameter Name** The name of the Routines API v2 HTTP POST element containing the image to be displayed. (Only available if **Message Type** is **JSON-Uploaded-Image**.)

Table 2. Routine Action Type-Specific Parameters (Continued)

Routine Action Type	Parameter 1	Parameter 2	Parameter 3	Parameter 4
Display-Msg (cont'd)	The **Display-Msg** Action Type allows you to set the message text or image, display time (in seconds), priority, style settings (e.g., background color, font, font size, font color, font styles), and more. For further information about message settings, see *"Using Color in Display Messages"*. You also have the option to select a **Message Template**, which will initialize many of the **Display-Msg** parameters with preset values to use as a starting point for your message. The template selected can be of type Text or Image. For further information about defining and using Message Templates, see *"Managing Display Messages"*. **Caution** Be aware that specifying a **Message Template** does not associate the current action with that template (and will not be persisted as part of the action), but is only used to *initialize* the settings for this action. This also means that selecting a template can override settings that you may have already specified, such as the Text or Identifier properties (among others). Use caution when selecting a **Message Template** for a previously defined action. *Tip:* You can use this **Action Type** to create a routine for displaying emergency alerts from the National Weather Service (NWS). See *"Setting Variables for the Display Message"* for descriptions about the variables used in an Alerts routine. *Note:* Be aware that the **Display Time (seconds)** setting causes the message to display for that length of time, but the action completes immediately and the routine proceeds to the next action. You can use the Pause action if you want the routine to pause for a specified duration. If you plan to use **Display-Msg-Delete** to explicitly delete a displayed message, set **Display Time (seconds)** to 0 (i.e., do not automatically delete message). To specify Display-Msg parameters via the Routines API v2, see *"Overriding Routine Action Parameters via Routines API v2"*.			

Table 2. Routine Action Type-Specific Parameters (Continued)

<table>
<tr><th>Routine Action Type</th><th>Parameter 1</th><th>Parameter 2</th><th>Parameter 3</th><th>Parameter 4</th></tr>
<tr><td>Display-Msg (cont'd)</td><td colspan="4">
When entering the text to display, you can use variables, such as $caller. When $caller is used in the Text parameter for dashboard and NQ-GA10PV or NQ-S1810WBC display messages, the variable is replaced by the ID of the caller that triggered the routine. When calls are placed from outside the system, it displays the phone number of the caller.

On the NQ-GA10PV, you can also use basic HTML tags, such as:
• for bold
• for italic
• <u> for underline </u>

Includes the following fields, which were entered when the Action was created:
• Display Time
• +Priority
• Text to display
• Text style settings
• Message type
• Image type
• Image priority
• Message image

+ Priority of 5 (Exclusive) is disabled when Message Type is Image.

The Text field may use any of the following variables (availability determined by initiating trigger):

$alerts
$apiParam1
$apiParam2
*$autobgcolor
*$autofontcolor
$autopriority
$auto_resize
$caller
$called
*$calltypechar
*$calltypeshort
*$calltypelong
$contact
$cputemp
$date1
$date2
$date3
$deviceMacAddr
$deviceName
$df-avail
$eventid
$eventname
$facility
$namecalled
$namecaller
$schedParam1
$schedParam2
$scheduleid
$schedulename
$station
$time1
$time2
$toneid
$tonename
$uptime
$user_var[1…10]
$weather
$zone

* Available only for emergency-call and urgent-call triggers

Tip: To completely blank out an NQ-GA10PV screen, display a message using the Solid-Black (1920×1080) image, which is available by default. This can be used to "turn off" an NQ-GA10PV display such that it will not display a message or the clock (i.e., completely black). The Image Type must be set to Full Screen. To ensure no other messages will display during this message duration, specify a Priority of 6 (Fullscreen on GA10PV).
</td></tr>
</table>

Table 2. Routine Action Type-Specific Parameters (Continued)

Routine Action Type	Parameter 1	Parameter 2	Parameter 3	Parameter 4
Display-Msg-Delete *Note:* NQ-GA10PV and NQ-S1810WBC Display Messages created by a Routine that expires during the Routine's execution remain in the undeleted messages list until deleted with a Display-Msg-Delete action. When using **LIFO**, **FIFO**, or **NUMBER** to delete display messages, you will still need to execute a Display-Msg-Delete command for any display messages that have expired during the Routine's execution.	**Display Message Delete**			
	• LIFO	None	None	None
	• FIFO	None	None	None
	• IDENT	**Identifier** The following variables can be used: $apiParam1 $apiParam2 $caller $called $contact $deviceMacAddr $facility $eventid $eventname $schedParam1 $schedParam2 $scheduleid $station $toneid $tonename $user_var[1...10] $zone	None	None
	• PARAM	**Zones** *Note:* This field is optional.	**Stations** *Note:* This field is optional.	None
	• NUMBER	**Number**	None	None

Table 2. Routine Action Type-Specific Parameters (Continued)

Routine Action Type	Parameter 1	Parameter 2	Parameter 3	Parameter 4
Email *Note:* In addition to the parameters, you can also set a **Finish Delay**, of either **No-Delay** or **Wait-Until-Done**.	**Send Email To** Specifies a comma-delimited list of email addresses. Maximum length of string is 2048 characters. *Note:* To use this parameter to send a text message to a cell-phone, see *"Using Email Action to Send Text Message"*.	**Subject** The following variables can be used: $apiParam1 $apiParam2 $caller $called $contact $cputemp $date1 $date2 $date3 $deviceMacAddr $deviceName $df-avail $facility $eventid $eventname $namecaller $namecalled $schedParam1 $schedParam2 $schedulename $station $time1 $time2 $toneid $tonename $uptime $user_var[1...10] $zone *Note:* The availability of variables is based on the trigger type.	**Text** The following variables can be used: $apiParam1 $apiParam2 $caller $called $contact $cputemp $date1 $date2 $date3 $deviceMacAddr $deviceName $df-avail $facility $eventid $eventname $namecaller $namecalled $schedParam1 $schedParam2 $schedulename $station $time1 $time2 $toneid $tonename $uptime $user_var[1...10] $zone *Note:* The availability of variables is based on the trigger type.	None
Emergency-Call	**Placed by** • Calling Station • Selected Station *Note:* If Calling Station is used, this action must be the last action in the routine and must be executed via DTMF code.	None	None	None

Table 2. Routine Action Type-Specific Parameters (Continued)

Routine Action Type	Parameter 1	Parameter 2	Parameter 3	Parameter 4
Emerg-All-Call *Note:* This action must be the last action in a routine.	None	None	None	None
Enable-Audio *Note:* You can set a **Finish Delay**, of either **No-Delay** or **Wait-Until-Done**.	None	None	None	None
Facility-Announcement	**Announcement** • Non-continuous announcement to be played (announcement type in parentheses)	**Facilities** • One or more facilities at which the announcement will be played	None	None
Facility-Page *Note:* This action must be the last action in a routine.	**Facilities** • Facilities to be paged (maximum of 25)	None	None	None

Table 2. Routine Action Type-Specific Parameters (Continued)

Routine Action Type	Parameter 1	Parameter 2	Parameter 3	Parameter 4
Feature-Wait	**Feature Wait** • 911 *Note:* 911 waits for the specific caller to disconnect. • Alarm • Announcement • All-Call • Disable-Audio • Emerg-All-Call • Facility-Page *Note:* Facility-Page should only be used when the trigger is also Facility-Page. • Multi-Site-All-Call • Multi-Site-E-All-Call • Tone • Zone-Page	**Maximum Wait Time** • Number of seconds to wait for feature to complete; default is 86400 seconds (24 hours) *Note:* A value of 0 means to wait until the feature has completed regardless of the time it takes to complete. *Note:* If the feature is not active, the routine continues to the next action.	None	None
Goto	**Routine Action**			
	The Goto action can be used to change the flow of Action execution in a Routine. The Goto action can also be used to cause the Routine to repeat (loop) by adding a Goto Action at the end of the Routine and selecting the first Action in the Routine as the Routine Action to go to. The Condition field of the Goto action can be used to conditionally execute the Goto. **Caution** If you create a loop that causes the Routine to repeat all Actions until the Routine is stopped, please ensure that the loop does not put too much burden on the Nyquist server by aggressively repeating actions that are time consuming. If several aggressive Routines are started on the server, they could negatively impact system and audio performance. If Routines aggressively send Display messages to GA10PV devices, audio performance on the GA10PV could be negatively impacted.			

Table 2. Routine Action Type-Specific Parameters (Continued)

Routine Action Type	Parameter 1	Parameter 2	Parameter 3	Parameter 4
Intercom-Call	**Placed by** • Calling Station • Selected station *Note:* If Calling Station is used, this action must be the last action in the routine and must be executed via DTMF code.	**Received by** • Station that received the call	None	None
Intercom-Wait *Note:* This action can be used to wait for an Intercom Call to be disconnected or for the end of a Real-Time (not queued) Zone Page by caller.	None	None	None	None
Log-Text This action can be used to log user-supplied text to the Routines log file: `nyquist_routines.log`. This file can be viewed via System Logs under the *Nyquist C4000* category. *Note:* Similar functionality is also available via the `logText()` function, for use within CODE: segments (see *"Logging Functions"*).	**Text to log** The text supplied in the **Text** field will be logged. The text can include the same variables that are available to the **Dash-Text** action's Text field (excluding the `$date#` and `$time#` variables, as log entries already contain a timestamp). A maximum of 4095 characters can be entered as text to log. *Note:* Single-quote and double-quote characters are automatically removed and not included in the log output.	None	None	None

Table 2. Routine Action Type-Specific Parameters (Continued)

Routine Action Type	Parameter 1	Parameter 2	Parameter 3	Parameter 4
Multi-Site-All-Call *Note:* This must be the last action in a routine.	None	None	None	None
Multi-Site-E-All-Call *Note:* This must be the last action in a routine.	None	None	None	None
New-Announcement Creates a temporary announcement to be played by the routine. This must be followed by at least one **Add-Announcement-Audio** actions and a **Play-Announcement** action.	**Announcement Type** • Emergency • Normal	**Zone** • Selected zone number • All speakers (0)	**Number of times to play announcement** • Number of times to play (1–60)	**Silence time between repeats (seconds)** • Decimal number between 0.5 and 10.0
No-Action	None	None	None	None
Output-Contact-Close	**IO Controller** • Selected IO Controller • API-Specified *Note:* A selected I/O controller can be overridden by the API but will be used if the API call does not specify.	**Output Contacts** • Selected output contact or contacts • API-Specified *Note:* The selected contacts can be overridden by the API but will be used if the API call does not specify.	**Duration** • Number of seconds for action to continue *Note:* Duration of zero (0) will cause the contact or contacts to momentarily close. Leaving Duration blank will cause the contact to stay closed; use **Output-Contact-Open** to reopen the contact.	None
Output-Contact-Open	**IO Controller** • Selected IO Controller • API-Specified	**Output Contacts** • Selected output contact or contacts • API-Specified	None	None

Table 2. Routine Action Type-Specific Parameters (Continued)

Routine Action Type	Parameter 1	Parameter 2	Parameter 3	Parameter 4
Page-Exclusion	**Page Exclusion** • Add • Delete	**Stations** • Selected station or stations	None	None
Pause *Note:* If pausing is used in a DTMF-based routine that ends with paging, the page will not start until all pauses have been executed. If a DTMF-based routine does not end in a page, the call will not disconnect until all pauses have been executed.	**Duration** • Number of seconds to pause	None	None	None
Play-Announcement *Note:* This must be preceded by a **New-Announcement** action and at least one **Add-Announcement-Audio** actions.	None	None	None	None
Play-Ringtone *Note:* Using this action type will not trigger a routine that has a night-ring trigger.	**Action** • Start • Stop	**Zones** • All speakers • Selected zone	**Timeout (seconds)** *Note:* Blank or 0 means no timeout.	
Ring-Wait *Note:* Waits for caller's ring to end.	None	None	None	None

Table 2. Routine Action Type-Specific Parameters (Continued)

Routine Action Type	Parameter 1	Parameter 2	Parameter 3	Parameter 4
Routine *Note:* In addition to the parameters, you can also set a **Finish Delay**, of either **No-Delay** or **Wait-Until-Done**. All trigger parameters and trigger types from the selected routine pass to the new routine so both routines have the same trigger context.	**Routine** • Selected Routine	**Facility** • Local	None	None
	Routine DTMF • DTMF of Routine to execute on remote Facilities	**Facility** • Selected Facility • All Facilities		
Routine-Disable *Note:* If the routine that invokes this action does not execute for any reason (e.g., the server is down), the selected routine will *not* be disabled, even after the server resumes.	**Routine** • Selected routine	None	None	None
Routine-Enable *Note:* If the routine that invokes this action does not execute for any reason (e.g., the server is down), the selected routine will *not* be enabled, even after the server resumes.	**Routine** • Selected routine	None	None	None
SM-Disable-Zone	**Sound Masking Zone** • All Sound Masking Zones • Selected zone	None	None	None
SM-Enable-Zone	**Sound Masking Zone** • All Sound Masking Zones • Selected zone	None	None	None

Table 2. Routine Action Type-Specific Parameters (Continued)

Routine Action Type	Parameter 1	Parameter 2	Parameter 3	Parameter 4
SM-Scheduled-Ramp	**Sound Masking Zone** • All Sound Masking Zones • Selected zone	**Volume Adjustment** • Down • Up	**Ramp Duration (minutes)** • 60 • 120	**Range (dB)** • 5 • 10
SM-Set-Output-Gain	**Sound Masking Zone** • All Sound Masking Zones • Selected zone	**Output Gain (dB)** A value between −30 and 0 dB.	None	None
Stop-Announcement	**Zone** • All Speakers (stop an announcement that is playing to All Speakers) • Selected zone	None	None	None
Tone *Note:* In addition to the parameters, you can also set a **Finish Delay**, of either **No-Delay** or **Wait-Until-Done**.	**Tone** • Selected tone	**Zone** • Selected zone All zones of type Time	**Duration** • Number of seconds for action to continue; default is 86400 seconds (24 hours)	None
Urgent-Call	**Placed by** • Calling Station • Selected Station *Note:* If Calling Station is used, this action must be the last action in the routine and must be executed via DTMF code.	None	None	None

Table 2. Routine Action Type-Specific Parameters (Continued)

<table>
<tr><th>Routine Action Type</th><th>Parameter 1</th><th>Parameter 2</th><th>Parameter 3</th><th>Parameter 4</th></tr>
<tr><td>Webhook-Post

Sends an HTTP(S) POST request to a specified URL via a specified <code>curl</code> (or <code>wget</code>) command.

Note: The specified value can execute only the <code>curl</code> and <code>wget</code> commands.</td><td>POST command

The <code>curl</code> (or <code>wget</code>) POST request to be executed by this action.</td><td>None</td><td>None</td><td>None</td></tr>
<tr><td colspan="5">The Webhook-Post Routine Action can be used to execute actions and procedures on external systems that support incoming HTTPS POST requests. The external system defines the actions that will be taken when a specified HTTP POST is made to a specified URL with specified data. The target URL address and any related data is specified by the external system. The defined information can then be used via the Nyquist Webhook-Post action to cause the Nyquist system to send the HTTPS POST request to the external system for whatever purpose, as defined by the external system. The Nyquist system uses the <code>curl</code> command to generate the HTTP POST request that is sent to the external system.

The following example sends an HTTP POST request to a <code>webhook.site</code> service. (Visit <code>https://webhook.site</code> to generate your own unique webhook URL that can be used to receive and view requests):

<code>curl --request POST -H "Content-Type: application/json" --data '{"header": "Bogen Nyquist Alert", "title": "Lockdown", "body": "A lockdown has been initiated."}' -H "x-api-key: <service-api-key>" https://webhook.site/7afca716-551a-4b37-9e4c-bb08b9c4fa09</code>

The following example will execute the Nyquist routine configured for DTMF 15 via the Routine API on server <code><server></code>:

<code>curl --cacert /etc/apache2/ssl/bogenCA.crt --ssl-no-revoke -H "Accept: application/json" -H "Content-Type: application/json" -H "Authorization: Bearer 24f78e9392d4754138555c2470575a5e" https://<server>/routine/api/15/0/1/0/0</code>

Note: If the command will access the Nyquist Routine API, the requisite Bogen Certification Authority (CA) certificate file can be accessed on the Nyquist server at:

<code>/etc/apache2/ssl/bogenCA.crt.</code>

Important: The specified <code>curl</code> or <code>wget</code> command will execute on the Nyquist system and, therefore, must comply with the Debian syntax and implementation of the command. For details, see:

• https://manpages.debian.org/buster/curl/curl.1
• https://manpages.debian.org/buster/wget/wget.1

Tip: If testing curl commands using a Windows Command Prompt, be aware that it uses different syntax from Debian Linux Bash, such as different quoting rules. You may want to use the Windows Subsystem for Linux (WSL) to test compatibility. Alternatively, use a PowerShell command prompt which, although not identical, is more similar to Bash (e.g., it supports single-quoted strings, as shown in the previous examples).</td></tr>
</table>

Table 2. Routine Action Type-Specific Parameters (Continued)

Routine Action Type	Parameter 1	Parameter 2	Parameter 3	Parameter 4
Zone-Page *Note:* This must be the last action of the routine. Dashboard messages created during the routine will be deleted when the user disconnects the call.	**Zone** • Selected zone	None	None	None

Overriding Routine Action Parameters via Routines API v2

Some Routine Action parameters can be specified or overridden via the Routines API v2. The following table indicates the names and values that can be used to override Action parameters. For details on specific actions or parameters, see *Table 2, "Routine Action Type-Specific Parameters"*. For information about using the API, see *"Routines API v2"*.

Note: To indicate which Action is being overridden, the JSON object must specify the Action's name via the object's `name` property, which corresponds to the Name of the Action being overridden. Because the Name is not actually overridden, it is not specified here.

Table 3. Routine Action Parameter Overrides via Routines API v2

Action(s)	Action Field Name Label	JSON Field Name	Valid Values
Alarm		alarmParams	
	Alarm	alarmDTMF or alarmName	DTMF or Name from Tones list
	Duration (seconds)	duration	

Table 3. Routine Action Parameter Overrides via Routines API v2

Action(s)	Action Field Name Label	JSON Field Name	Valid Values
Announcement		announcementParams	
	Announcement	announcementDTMF or announcementName	DTMF or Name from Announcements list
	Zone	announcementZone	0 = All speakers # = Number from list of Zones that include Paging zone type
	Duration (seconds)	duration	
Display-Msg		displayMsgParams	
	Zones	zones	
	Stations	stations	
	Device Type Filter	deviceTypeFilter	0 = GA10PV and WBC 1 = GA10PV Only 2 = WBC Only
	Text	text	
	Priority	priority	0–6 5 = Exclusive on GA10PV 6 = Fullscreen on GA10PV
	Display Time (seconds)	displayTime	0–99999
	Image Type	imageType	• full • left • right
	Image Priority	imagePriority	• text • image

Table 3. Routine Action Parameter Overrides via Routines API v2

Action(s)	Action Field Name Label	JSON Field Name	Valid Values
	WBC Flasher Pattern	wbcFlasherPattern	• no-change • off • slow • fast • double • triple • quad
	WBC Number of Flasher Pattern Cycles	wbcFlasherCycles	0–99999 0 = keep flasher on
	WBC Flasher Color	wbcFlasherColor	• amber • blue • green • orange • red • violet
Emergency-Call		emergencyCAllParams	
	Placed By	placedBy	
Intercom-Call		intercomCallParams	
	Placed By	placedBy	
	Received By	receivedBy	
New-Announcement		newAnnouncementParams	
	Announcement Type	type	• normal • emergency
	Zone	zone	Number from Zones web page
	Number of Times to Play Announcement	numTimesToPlay	1–99
	Times Between Repeats (seconds)	timeBetweenRepeats	1–10

Table 3. Routine Action Parameter Overrides via Routines API v2

Action(s)	Action Field Name Label	JSON Field Name	Valid Values
Output-Contact-Close and **Output-Contact-Open**		outputContactCloseParams and outputContactOpenParams	
	IO Controller	ioController	
	Output Contacts	outputContacts	
	Duration (milliseconds) (Output-Contact-Close only)	duration	0 = momentary closure blank = stay closed
Tone		toneParams	
	Tone	toneName or toneDTMF	
	Zone	toneZone	0 = All Time Zones 1–99999
	Duration (seconds)	duration	
Urgent-Call		urgentCallParams	
	Placed By	placedBy	

Appendix E: Routine Trigger Types and Parameters

The following table describes each **Trigger Type** and its applicable parameters.

Table 4. Routine Trigger Types and Parameters

Routine Trigger Type	Parameter 1	Parameter 2
911	None	None
AF-Primary-* For details, see Table 27, “Failover Event Routine Triggers”.	None	None
AF-Secondary-* For details, see Table 27, “Failover Event Routine Triggers”.	None	None
Alarm	Alarm • Selected alarm • Any	None
All-Call	None	None
Amp-Protection-Mode Routines with this trigger will execute whenever a selected amplifier device goes into protection mode.	Selected device(s) • Any • Selected device(s) *Note:* Up to 19 devices may be selected. If more are needed, create additional triggers for the addition devices.	None

Table 4. Routine Trigger Types and Parameters (Continued)

Routine Trigger Type	Parameter 1	Parameter 2
Announcement	Announcement type	
	• Any	None
	• Number	Announcement
	• Normal-Any	None
	• Normal-Zone	Zone • All Speakers • Any Zone • Selected Zone
	• Emergency-Any	None
	• Emergency-Zone	Zone • All Speakers • Any Zone • Selected Zone
Audio-Dist *Note:* The routine must have an extension defined and **Use Caller's Extension** must be set to **No**. *Tip:* If you want to trigger on a Scheduled Audio that uses a playlist, make the playlist an Audio Distribution selection and then schedule the Audio Distribution instead of the playlist.	Audio Distribution Command • Start • Stop	Audio Distribution Selection • Any • Selected Audio Distribution
Audio-Disabled	None	None
Audio-Enabled	None	None

Table 4. Routine Trigger Types and Parameters (Continued)

Routine Trigger Type	Parameter 1	Parameter 2
Check-In *Note:* **Done** indicates that all stations that were expected to check in have done so. **Finished** indicates that the check-in process was manually finished by an admin user at the completion of check-in.	Check In • Start • Stop • Done • Finished • Reset	Stations • Any • Selected station or stations
Emergency-Call *Note:* When both Callers and Called are specified, the trigger occurs when an intercom call involves a specified caller OR a specified called party.	Callers • Any • Selected station or stations	Called • Any • Selected station or stations
Emerg-All-Call	None	None
Facility-Page	Facility • Any • Selected facility number(s) *Note:* A maximum of 25 facilities may be selected.	None
Facility Status Down *Note:* The routine must have an extension defined and **Use Caller's Extension** must be set to No. *Note:* If displaying messages, delete messages first using IDENT, then create messages with IDENT set. **Warning** Routines will be triggered every 60 seconds. Make sure that repeating actions make sense.	Facility • Any • Selected facility number	None

Table 4. Routine Trigger Types and Parameters (Continued)

Routine Trigger Type	Parameter 1	Parameter 2
Facility Status Up *Note:* This trigger fires when a facility that was previously down comes back up. After a Nyquist server reboot, it will fire for each Facility that has registered with the Nyquist server. *Note:* The routine must have an extension defined and **Use Caller's Extension** must be set to No. *Note:* If displaying messages, delete messages first using IDENT, then create messages with IDENT set. **Warning** Routines will be triggered every 60 seconds. Make sure that repeating actions make sense.	Facility • Any • Selected facility number	None
Incoming-Call *Note:* Incoming-Call triggers on incoming calls from the PSTN (from SIP or DAHDI trunks) that are received by an Admin station. (The Admin station rings and the call must be answered). Incoming-Call does not trigger on incoming DISA or Security DISA calls.	None	None
Input-Contact-Closed *Note:* If it is possible for the input contact to be repeatedly closed or opened in a very short time frame, consider setting **Allow Multiple** to **No** so the routine prevents multiple invocations from simultaneously occurring.	IO Controller • Selected IO Controller	Input Contacts • Selected input contact or contacts
Input-Contact-Opened *Note:* If it is possible for the input contact to be repeatedly closed or opened in a very short time frame, consider setting **Allow Multiple** to **No** so the routine prevents multiple invocations from simultaneously occurring. *Note:* This trigger is not generated for input contacts that have **Stop On** set to **Manual Control**.	IO Controller • Selected IO Controller	Input Contacts • Selected input contact or contacts

Table 4. Routine Trigger Types and Parameters (Continued)

Routine Trigger Type	Parameter 1	Parameter 2
Intercom-Call	Callers • Any • Selected station or stations	Called • Any • Selected station or stations
Multi-Site-All-Call	None	None
Multi-Site-E-All-Call	None	None
NWS-Alert *Note:* The Event and Severity parameters can be used to filter the execution of Routines via the trigger. *Note:* This trigger requires at least one Routine running with a Display-Msg action that includes the $alerts variable.	Event • Any • Selected event type	Severity • Any • Extreme • Severe • Moderate • Minor • Unknown
Night-Ring *Note:* Use the Action **Ring-Wait** to detect when a call has been answered or disconnected. See *"Understanding Action Parameters"* for more information. *Note:* The routine must have **Use Caller's Extension** disabled and an assigned Extension with the proper CoS.	None	None

Table 4. Routine Trigger Types and Parameters (Continued)

Routine Trigger Type	Parameter 1	Parameter 2
PBX-Incoming-Call This trigger is evaluated on all incoming calls from *PBX Connection* types. *Note:* This trigger does not apply to incoming calls from PSTN (use the Incoming-Call trigger for these).	Caller ID Allowed values (one of the following): • Comma-separated list of caller ID extensions to match (e.g., *100,101*) • Partial caller ID number followed by a percent sign (%) indicating a wildcard that matches one or more subsequent digits • Leave blank to match any caller ID number	Called Extension Allowed values (one of the following): • Comma-separated list of station or feature extensions (e.g., *100,#0911,*94111,*94222*) • Partial caller ID number followed by a percent sign (%) indicating a wildcard that matches one or more subsequent digits • Leave blank to match any caller ID number
Reboot Routines with this trigger will execute whenever the Nyquist server reboots or is restarted via Restart Server. Routines with this trigger will also be executed after a System Update is performed on the Nyquist server. To use this trigger, the routine must have an extension defined and disable **Use Caller's Extension**.	None	None
Schedule-Activated This trigger will start an associated routine every day at midnight when the schedule defined by parameter 1 is activated for the day, or when the schedule defined in parameter 1 is manually activated via the Admin web interface or Admin Phone. *Note:* When schedules are edited via the Nyquist web interface, this trigger is generated for all active schedules after changes have been saved.	Holiday or Schedule Name	None

Table 4. Routine Trigger Types and Parameters (Continued)

Routine Trigger Type	Parameter 1	Parameter 2
Sched-Event	Scheduled Event • Any • Selected event	None
Scheduled-Tone *Note:* The routine must have an extension defined and "Use Callers Extension" must be set to "No".	Tone • Any • Selected tone	None
Station-Status-Up *Note:* The routine must have an extension defined and **Use Caller's Extension** must be set to **No**. *Note:* Station Supervision must be enabled in System Parameters.	Stations • Any • Selected station or stations	None
Station-Status-Down *Note:* The routine must have an extension defined and **Use Caller's Extension** must be set to **No**. *Note:* Station Supervision must be enabled in System Parameters.	Stations • Any • Selected station or stations	None
Tone	Tone • Any • Selected tone	None
Urgent-Call *Note:* When Callers and Called are both specified, the trigger occurs when intercom call involves a specified caller OR a specified called party	Callers • Any • Selected station or stations	Called • Any • Selected station or stations
Zone-Page	Zone • Any • Selected zone	None

Appendix F: C4000 Software Licenses

This appendix describes the software licenses available for the C4000 series.

Note: Nyquist C4000 software licenses do not expire and no annual license renewal fees are charged. However, a Software Update Subscription (SUS) is required to receive future Nyquist software updates and new feature releases. All C4000 software license bundles include an initial 3-year subscription to software updates. A SUS expiration warning notice will appear on the Admin Station dashboard 90 days prior to expiration. If the SUS expires, the Nyquist system will continue to operate, but software updates will not be allowed until the SUS is updated via purchase and activation of a 3-year Extended System Software Update license (NQ-C4SWUP3YRBx, where "x" indicates the applicable C4000 system license bundle).

Nodelocked License Activation Key

A Nodelocked License Activation Key (LAK) is preloaded on the Nyquist System Controller, and if a customer prefers to install the Nyquist C4000 application software on his or her own server, he or she must obtain a Nodelocked LAK from Bogen Technical Support and install it as part of the Nyquist C4000 server setup. The format for this LAK is **NXXX-XXXX-XXXX-XXXX-XXXX**.

Note: LAKs use the 0 character representing the number zero; they do *not* use the letter O.

Product License Activation Key (NQ-C4000-B1, B2, B3, B4)

C4000 Product LAKs begin with the letters PC followed by a two digit numeric designation that denotes a specific C4000 product bundle (01 - 04). The C4000 Product LAK activates the C4000 bundle. The format for this LAK is PC##-XXXX-XXXX-XXXX-XXXX. The ## is a numerical value of 01 through 04 and represents the bundle purchased. The Product LAK must be entered before entering any Feature LAKs.

When the Product LAK is first activated, the SUS expiration date is automatically set to 3 years from the date of activation. Re-activating the Product LAK will not reset this expiration date. However, 3-year Extended System Software Update licenses can be purchased and installed (for example, NQ-C4SWUP3YRBx, where "x" indicates the applicable C4000 system license bundle). See “System Software Update Subscriptions (NQ-C4SWUP3YRB1, B2, B3, B4)” on page 623.

Feature License Activation Keys

Feature LAKs begin with the letters **FC** followed by a two character alpha-numeric designation that denotes the specific system feature or option.

Concurrent Call License Expansion Package (NQ-C4000CCLX)

This LAK uses the format FCC0-XXXX-XXXX-XXXX-XXXX.

Concurrent Call Licenses are sold in expansion packs of 10.

The following items each require and consume one or more Concurrent Call Licenses:

- All Call (1)
- Emergency All Call (1)
- Multi-Site All Call (1)
- Multi-Site Emergency All Call (1)
- Multi-Facility Pages (1)
- Multi-Facility Announcements (1)
- Zone Page (1)
- Intercom Call (1)
- Station-to-Station Call (1)
- Recording an announcement (1)
- Recorded Page (2)
- Retrieving a vmail message (1)
- Scheduled Events (for example, Tones or Announcements) (1 per active event)
- Audio Distribution (1 to start or stop the audio distribution; once the audio is streaming, no associated call count is consumed)
- Call Monitoring/Recording (1 in addition to the 1 for the call itself)
- DISA Station Monitoring (2)
- Executing routine via DTMF (1)

Note: If the routine ends with a call type, it does not consume an additional call. In this case, starting the routine consumes a call, but the call action takes over the call at the end of the routine.

- Executing routine on remote facilities (2)

System Software Update Subscriptions (NQ-C4SWUP3YRB1, B2, B3, B4)

This LAK uses the format FCDX-XXXX-XXXX-XXXX-XXXX.

There are four available 3-Year SUS Extension licenses–one for each C4000 software license bundle type. For example: if the system's current SUS expiration is 3/31/2022, the NQ-C4SWUP3YRB1 license extends the SUS expiration date of a Bundle-1 system until 3/31/2025.

SUSs encompass bug fixes, feature enhancements, and all standard new features introduced in subsequent releases of the product.

Any hardware that may be associated with a new feature is excluded and must to be purchased separately.

Intercom Call License (NQ-C4000ICL)

This LAK uses the format FCIX-XXXX-XXXX-XXXX-XXXX.

This license adds talkback, or intercom, capability to a system on a concurrent intercom call basis (i.e., one license for each concurrent intercom call).

Intercom calling is disabled by default on every C4000 system. Installing this license enables intercom calling (that is, talkback operation) between any two applicable Nyquist devices (VoIP phones, VoIP speakers, VoIP Intercom Modules, Web UI dashboard, etc.). Each NQ-C4000ICL license key installed and added to a system incrementally increases the concurrent Intercom Call limit by 1. For example, installing 3 NQ-C4000ICL licenses will permit up to 3 concurrent intercom calls on a system.

Note: The Intercom Call limit can never exceed the system's maximum Concurrent Call limit. **Intercom Call Limit** and **Intercom Call Count** are displayed on the Product License page (see "Product License Activation Key (NQ-C4000-B1, B2, B3, B4)" on page 622).

Map-Based Paging License (NQ-C4000MBP)

This LAK uses the format FCMX-XXXX-XXXX-XXXX-XXXX.

This is a one-time, system-wide license required to enable interactive Map-Based Paging in a C4000 system.

Paging Zone License Expansion Package (NQ-C4000PZX)

This LAK uses the format FCZX-XXXX-XXXX-XXXX-XXXX.

This license increases the zone count of any Bundle-1, Bundle-2, or Bundle-3 system by 3 zones. This allows any of these systems to be grown or expanded in 3-zone increments (For example, if a Bundle-2 system's current zone count is 9, installing this upgrade will increase it to 12 zones).

The licensed number of Page Zones (**Maximum Zone Limit)** and **Current Zone Count** are displayed on the Product License page (see "Product License Activation Key (NQ-C4000-B1, B2, B3, B4)" on page 622).

Queued Paging/Page Stacking License (NQ-C4000QPL)

This LAK uses the format FCQX-XXXX-XXXX-XXXX-XXXX.

Queued Paging/Page Stacking is disabled by default on every C4000 system. Queue Paging allows multiple users to simultaneously page to the same zone or zones and is an effective way to eliminate feedback in areas where a paging device (phone, microphone, etc.) may be in close proximity to speakers receiving the page. Installing this license enables Queued Paging/Page Stacking on the system and allows the user to create one page stacking queue. Each NQ-C4000QPL license key installed and added to a system incrementally increases the page stacking queue limit by 1. For example, installing 3 NQ-C4000QPL licenses will permit up to 3 separate page stacking queues to be created on a system.

The Page Queuing feature emulates the functions of the BOMDMU and Digital Feedback Terminator (DFT) in legacy PCM2000 and UTI1/UTI312 analog paging applications.

The licensed number of paging queues (**Maximum Page Stacking Queues)** and **Queue Count** are displayed on the Product License page (see “Product License Activation Key (NQ-C4000-B1, B2, B3, B4)” on page 622.)

Text-To-Speech License (NQ-C4000TTS)

This LAK uses the format FCTX-XXXX-XXXX-XXXX-XXXX.

This is a one-time, system-wide license required to enable TTS-based announcements and messaging in a C4000 system.

Automatic Failover License (NQ-C4000AFL)

This LAK uses the format PCAF-XXXX-XXXX-XXXX-XXXX.

This license is required to enable the Automatic Failover (AF) capability of the Nyquist server in an C4000 system. The AF feature requires customers to purchase a secondary standby System Controller (or server) on which to install this S/W license. An AF S/W license is not required to be purchased for the Nyquist system's primary server.

Sound Masking License (NQ-C4000SML)

This LAK uses the format FCSM-XXXX-XXXX-XXXX-XXXX.

This license is required to enable the Sound Masking feature.

System Software License Bundle Upgrades

These system upgrade LAKs use the format FCU#-XXXX-XXXX-XXXX-XXXX, where # indicates the number of the software bundle the system configuration will be upgraded to–for example, from Bundle-1 to Bundle-2.

NQ-C4000-B12UP Nyquist C4000 Series System Software License Bundle Upgrade - B1-B2

- Upgrades a Bundle-1 system to a Bundle-2 configuration by increasing the current zone count of the Bundle-1 system by 6 zones. For example, if a Bundle-1 system's current zone count is 3, installing this upgrade will increase it by 6 to 9 zones).
- Extends the current SUS expiration date by 1 year. For example, if the system's current SUS expiration is 3/31/2024, installing this upgrade will extend it to 3/31/2025.

NQ-C4000-B23UP Nyquist C4000 Series System Software License Bundle Upgrade - B2-B3

- Upgrades a Bundle-2 system to a Bundle-3 configuration by increasing the current zone count of the Bundle-2 system by 15 zones. For example, if a Bundle-2 system's current zone count is 9, installing this upgrade will increase it by 15 to 24 zones.
- Extends the current SUS expiration date by 1 year. For example, if the system's current SUS expiration is 3/31/2024, installing this upgrade will extend it to 3/31/2025.

Nyquist C4000 Series System Software License Bundle Upgrade - B3-B4

- Upgrades a Bundle-3 system to a Bundle-4 configuration by increasing the current zone count of the Bundle-3 system to virtually unlimited zones. For example, if a Bundle-3 system's current zone count is 24, installing this upgrade will enable it to support a virtually unlimited number of zones.
- Extends the current SUS expiration date by 1 year. For example, if the system's current SUS expiration is 3/31/2024, installing this upgrade will extend it to 3/31/2025.