

Zoom Configuration Guide: SIP Paging Server

Document Part # 931807A

CyberData Corporation
3 Justin Court
Monterey, CA 93940
(831) 373-2601

Zoom Configuration Guide: SIP Paging Server Document #931807A

COPYRIGHT NOTICE:

© 2020, CyberData Corporation, ALL RIGHTS RESERVED.

This configuration guide and related materials are the copyrighted property of CyberData Corporation. No part of this configuration guide or related materials may be reproduced or transmitted, in any form or by any means (except for internal use by licensed customers), without prior express written permission of CyberData Corporation. This configuration guide, and the products, software, firmware, and/or hardware described in this configuration guide are the property of CyberData Corporation, provided under the terms of an agreement between CyberData Corporation and recipient of this configuration guide, and their use is subject to that agreement and its terms.

DISCLAIMER: Except as expressly and specifically stated in a written agreement executed by CyberData Corporation, CyberData Corporation makes no representation or warranty, express or implied, including any warranty or merchantability or fitness for any purpose, with respect to this configuration guide or the products, software, firmware, and/or hardware described herein, and CyberData Corporation assumes no liability for damages or claims resulting from any use of this configuration guide or such products, software, firmware, and/or hardware. CyberData Corporation reserves the right to make changes, without notice, to this configuration guide and to any such product, software, firmware, and/or hardware.

OPEN SOURCE STATEMENT: Certain software components included in CyberData products are subject to the GNU General Public License (GPL) and Lesser GNU General Public License (LGPL) “open source” or “free software” licenses. Some of this Open Source Software may be owned by third parties. Open Source Software is not subject to the terms and conditions of the CyberData COPYRIGHT NOTICE or software licenses. Your right to copy, modify, and distribute any Open Source Software is determined by the terms of the GPL, LGPL, or third party, according to who licenses that software. Software or firmware developed by CyberData that is unrelated to Open Source Software is copyrighted by CyberData, subject to the terms of CyberData licenses, and may not be copied, modified, reverse-engineered, or otherwise altered without explicit written permission from CyberData Corporation.

TRADEMARK NOTICE: CyberData Corporation and the CyberData Corporation logos are trademarks of CyberData Corporation. Other product names, trademarks, and service marks may be the trademarks or registered trademarks of their respective owners.

Revision Information

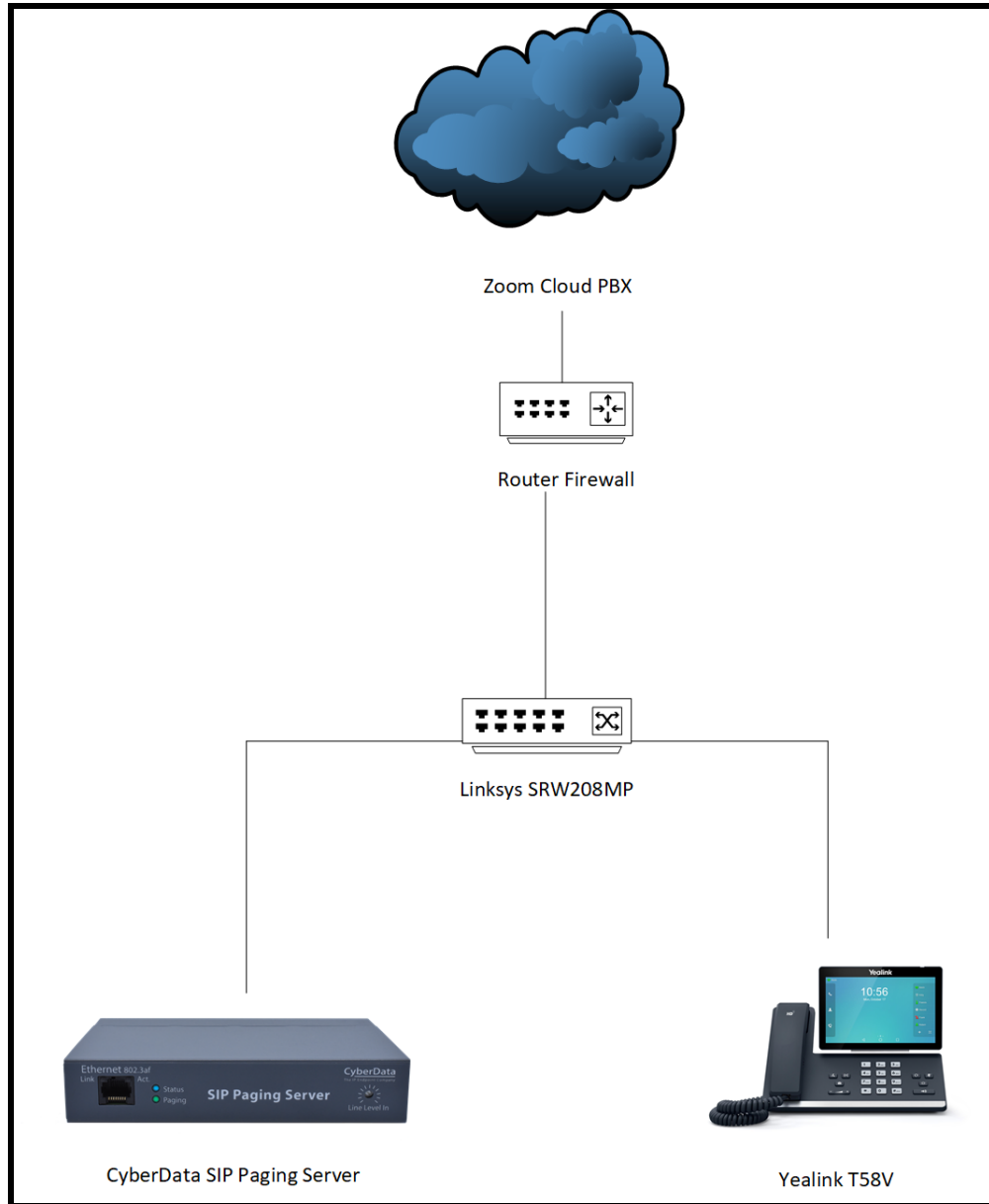
- 9-11-2020 Initial Release

Table of Contents

| | |
|--|----|
| 1.0 Setup Diagram..... | 4 |
| 2.0 Test Setup Equipment..... | 5 |
| 3.0 Before You Start | 6 |
| 4.0 Configuration Procedure: Common Area Phone | 7 |
| 5.0 Configuration Procedure: Setting up the Paging Extension | 14 |
| 6.0 Configuration Procedure: Setting up the Nightringer extension..... | 21 |
| 7.0 Using the CyberData SIP Paging Server in a Zoom system..... | 28 |
| 7.1 Creating a Call queue | 29 |
| 7.2 Multicast Paging..... | 34 |
| 7.2.1 Setting up Multicast Receive on other CyberData Products..... | 36 |
| 8.0 Contact CyberData Corporation..... | 38 |

1.0 Setup Diagram

Figure 1-1: Interoperability Test Infrastructure



2.0 Test Setup Equipment

This section describes the products used for interoperability testing with Zoom.

Table 2-1: Setup Equipment

| EQUIPMENT | MODEL or PART NUMBER | FIRMWARE VERSION |
|-----------------------------|----------------------|------------------|
| CYBERDATA SIP PAGING SERVER | 011146 | v12.2.0 |
| YEALINK | T58A | 58.83.3.6 |
| LINKSYS SWITCH | SRW208MP | --- |

3.0 Before You Start

This configuration guide documents the integration process of a CyberData SIP Paging Server.

Network Advisories

Zoom uses a Fully Qualified Domain Name (FQDN) for the SIP server and Outbound Proxy addresses. The CyberData SIP Paging Server needs to perform a DNS A query to resolve the IP address of Zoom's Outbound Proxy FQDN. It is necessary to ensure the configured DNS server(s) have an A record for the Outbound Proxy address.

In addition, be sure to verify the following ports are available for the paging server to use:

- TCP 5060-5061, 5091 (SIP)
- UDP 10500 (RTP)

The paging server will need to traverse the public internet in order to operate with Zoom in the cloud.

The paging server's paging extension uses SIP port 5060 to receive SIP messages. The Nightringer extension uses SIP port 5061 to receive SIP messages. Both extensions will send SIP messages to port 5091, the port used by Zoom's Outbound Proxy.

SIP ports 5060-5061 and RTP port 10500 are the default values on all noted firmware levels.

Alternatively, SIP ports for the paging and Nightringer extension are configurable on the **SIP** page of the web interface.

The RTP port setting on the **SIP** page is used for both extensions.

The CyberData Discovery Utility can be used to locate CyberData devices on your network. You may download it from the following web address:

<https://www.cyberdata.net/pages/discovery>

Note: DHCP addressing mode is enabled on default on all noted firmware levels.

Product Documentation and Utilities

Before you start, download the Operation and Quick Start guides from the paging servers' product webpage:

SIP Paging Server ([011146](#))

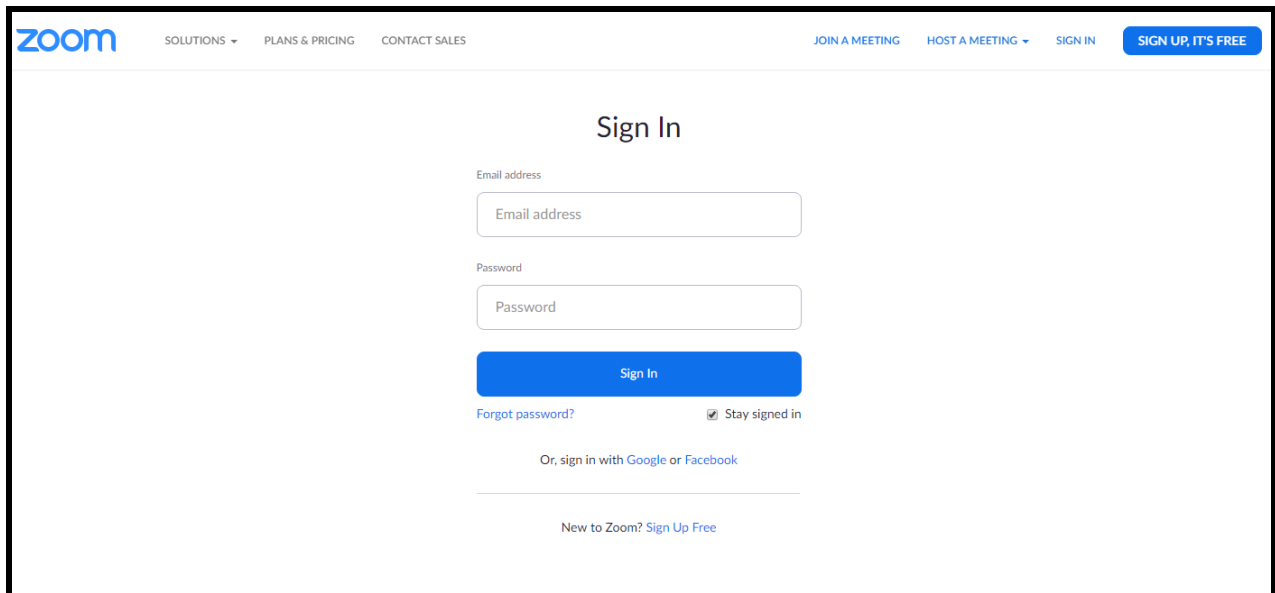
http://files.cyberdata.net/assets/011146/011146_931073K_SIP_Paging_Server_Operations_Guide.pdf

4.0 Configuration Procedure: Common Area Phone

There are several different extension types that can be used on the Zoom platform. This guide provides instructions to register the CyberData SIP Paging Server as a Common Area Phone. Registering in a different capacity may require creating a user profile and providing an email address. See Zoom documentation for more details.

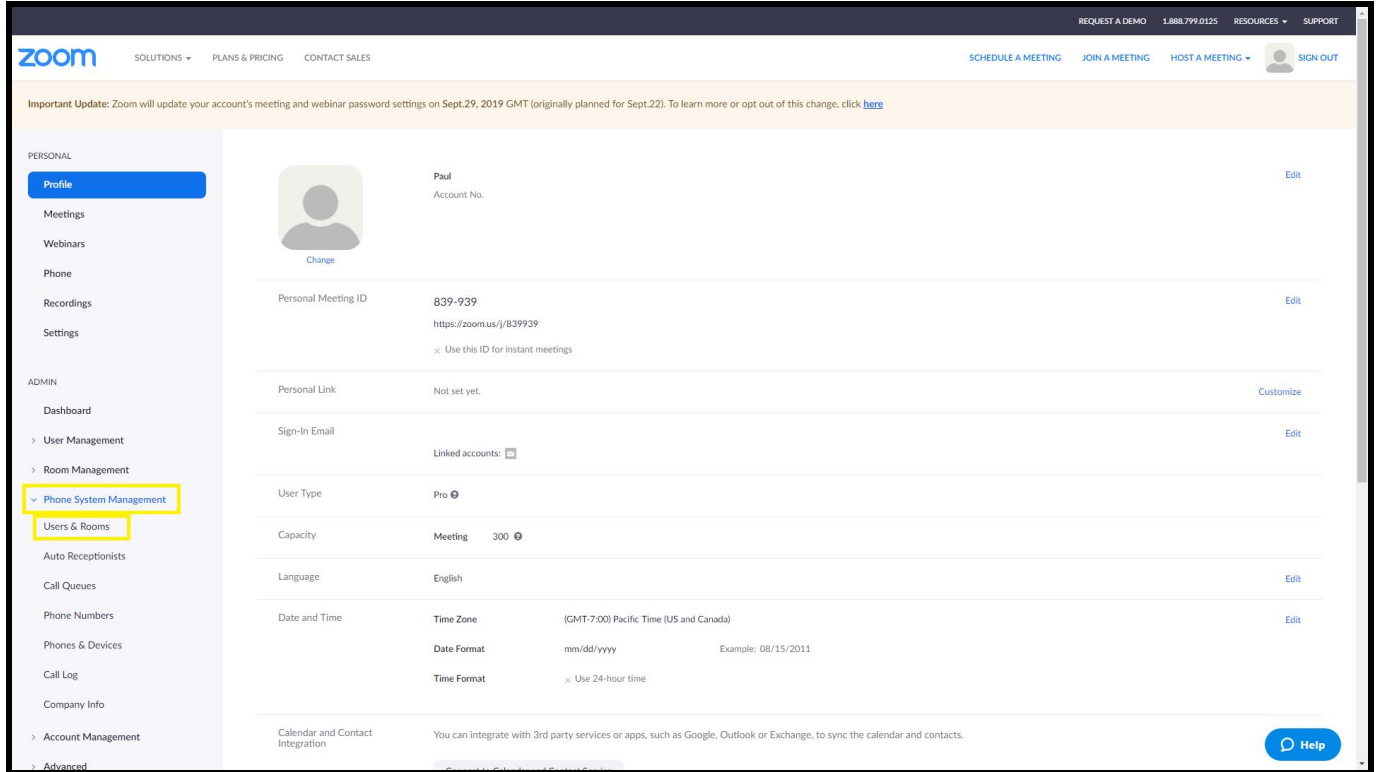
1. Log into Zoom. <https://zoom.us/signin>

Figure 4-1: Log into Zoom



- From the Profile page select the “Phone System Management” section and the ‘Users & Rooms’ subsection.

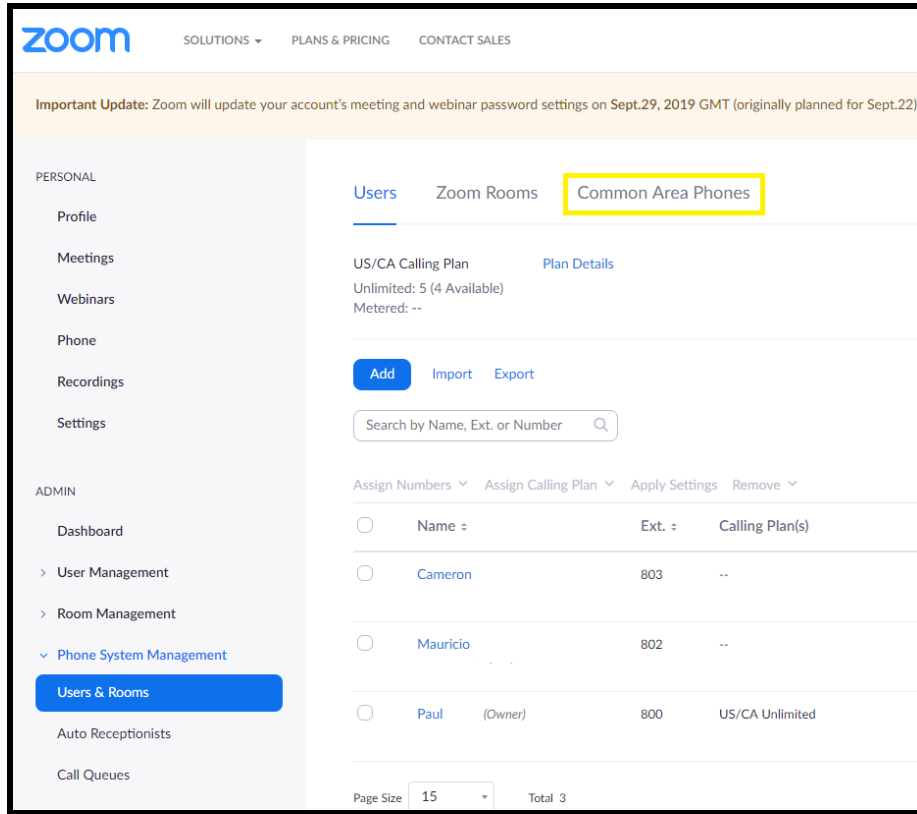
Figure 4-2: Profile Landing Page



Note: Some text from the profile page has been hidden to protect sensitive information.

- From the “Users & Rooms” page select ‘Common Area Phones’.

Figure 4-3: Phone System Management

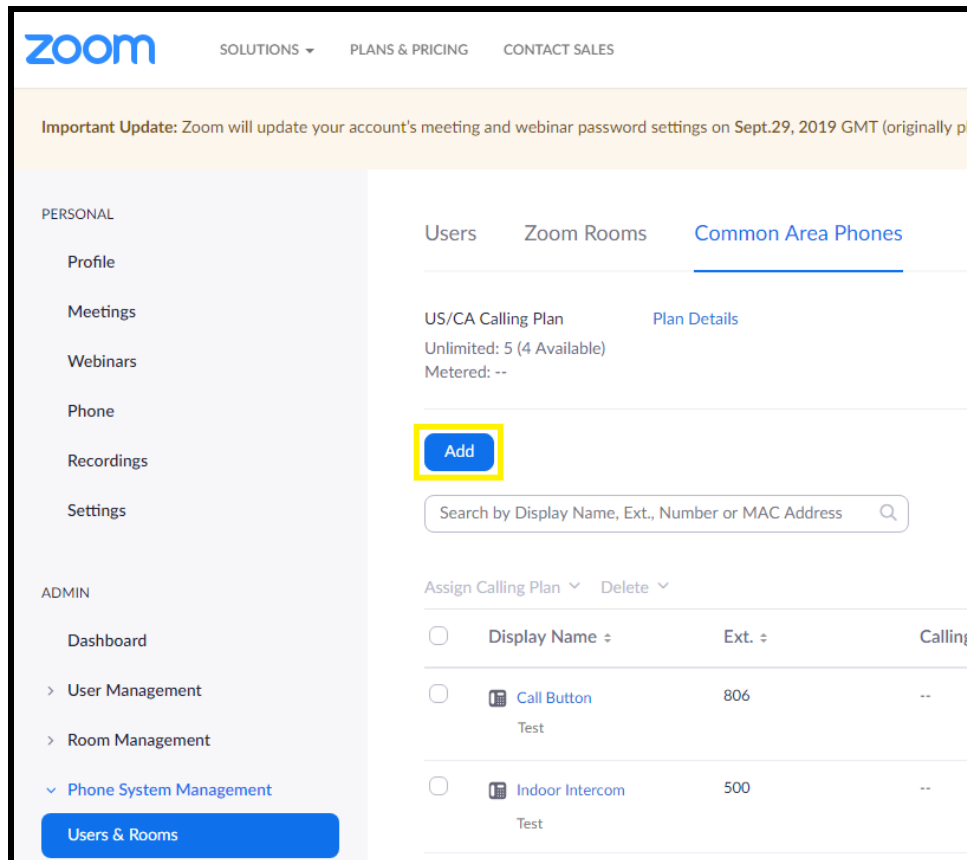


Note: Some text from this page has been hidden to protect sensitive information.

4. From the “Common Area Phones” press the ‘Add’ Button to create a new common area phone to be used by the device.

Note: The MAC address of the paging server will be required to create the common area phone.

Figure 4-4: Common Area Phones



5. After clicking the Add button a Pop-up will appear that allows extension creation.

Figure 4-5: Common Area Phone Pop-up

The screenshot shows a form titled "Add Common Area Phone". It has the following fields and values:

- Display Name: |
- Description (Optional):
- Extension Number: 809
- MAC Address:
- Device Type: Select Brand (dropdown), Select Model (dropdown)

Buttons: Cancel, Save

6. Set the **Display name** of the extension. This will be the main Identifier on the Common Area Phones page.
7. Set the **description**.
8. The **extension number** will be auto generated but can be changed if desired.
9. Set the **MAC address** of the device.

Figure 4-6: Common Area Phone Pop-up – Filled

The screenshot shows the "Add Common Area Phone" form filled with the following data:

- Display Name: CyberData SIP Paging Server
- Description (Optional): Bell Scheduler
- Extension Number: 828
- Country: United States of America (+1)
- Time Zone: (GMT-7:00) Pacific Time (US and Canada)
- MAC Address: 00:20:f7:03:30:1e
- Device Type: Algo/Cyberdata (dropdown), Paging&Intercom (dropdown)

Buttons: Cancel, Save

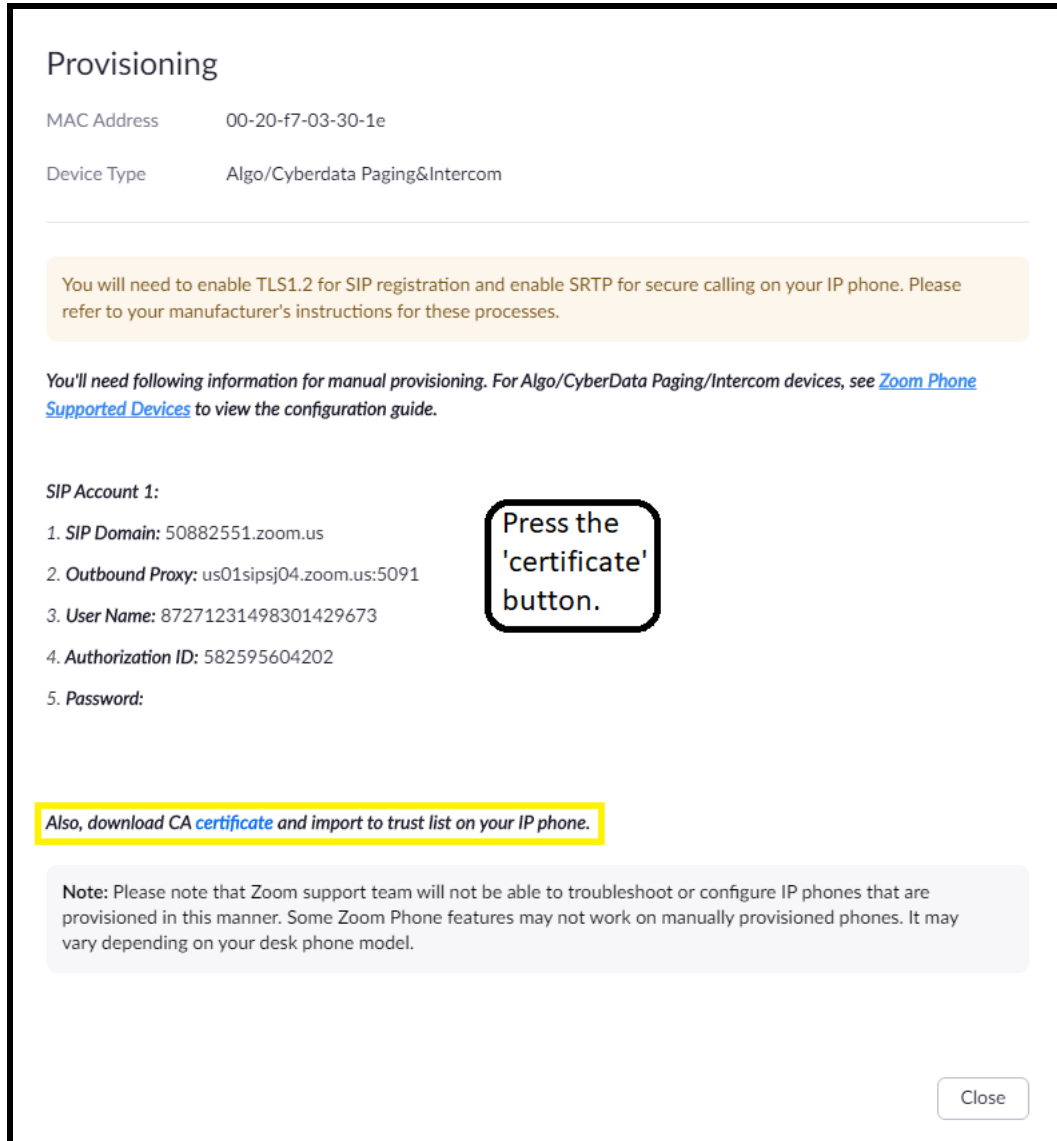
- 10. Click the **Save** button to create the Common Area Phone.
- 11. Once created the new extension will appear in the list.

Figure 4-7: Common Area Phone list

| | Display Name | Ext. | Calling Plan(s) | Number(s) | Hot Desking (Signed In) | Device Type | MAC Address | IP Address | Provision Template | Status | |
|-----------------------|---|------|-----------------|-----------|-------------------------|--------------------------------|-------------------|------------|--------------------|----------------------|-------------------------|
| <input type="radio"/> | CyberData Intercom Intercom | 809 | -- | -- | Unsupported | Other | 00-20-f7-02-bf-11 | -- | Unsupported | Offline Provision | Assign Calling Plan ... |
| <input type="radio"/> | CyberData SIP Call Button Front Office | 815 | -- | -- | Unsupported | Other | 00-20-f7-04-13-5c | -- | Unsupported | Offline Provision | Assign Calling Plan ... |
| <input type="radio"/> | CyberData SIP IP66 Outdoor Horn Warehouse | 813 | -- | -- | Unsupported | Other | 00-20-f7-03-a3-2f | -- | Unsupported | Offline Provision | Assign Calling Plan ... |
| <input type="radio"/> | CyberData SIP Paging Server Bell Scheduler | 828 | -- | -- | Unsupported | Algo/Cyberdata Paging&Intercom | 00-20-f7-03-30-1e | -- | Unsupported | Offline Provision | Assign Calling Plan ... |

- 12. Press the “Provision” button on the extension that was just created.

Figure 4-7: Provisioning Pop-up



13. A popup will appear with manual provisioning information to setup the CyberData Paging Server. Keep this popup open.

14. Make sure to download the “CA Certificate,” which will be needed for device configuration.

5.0 Configuration Procedure: Setting up the Paging Extension

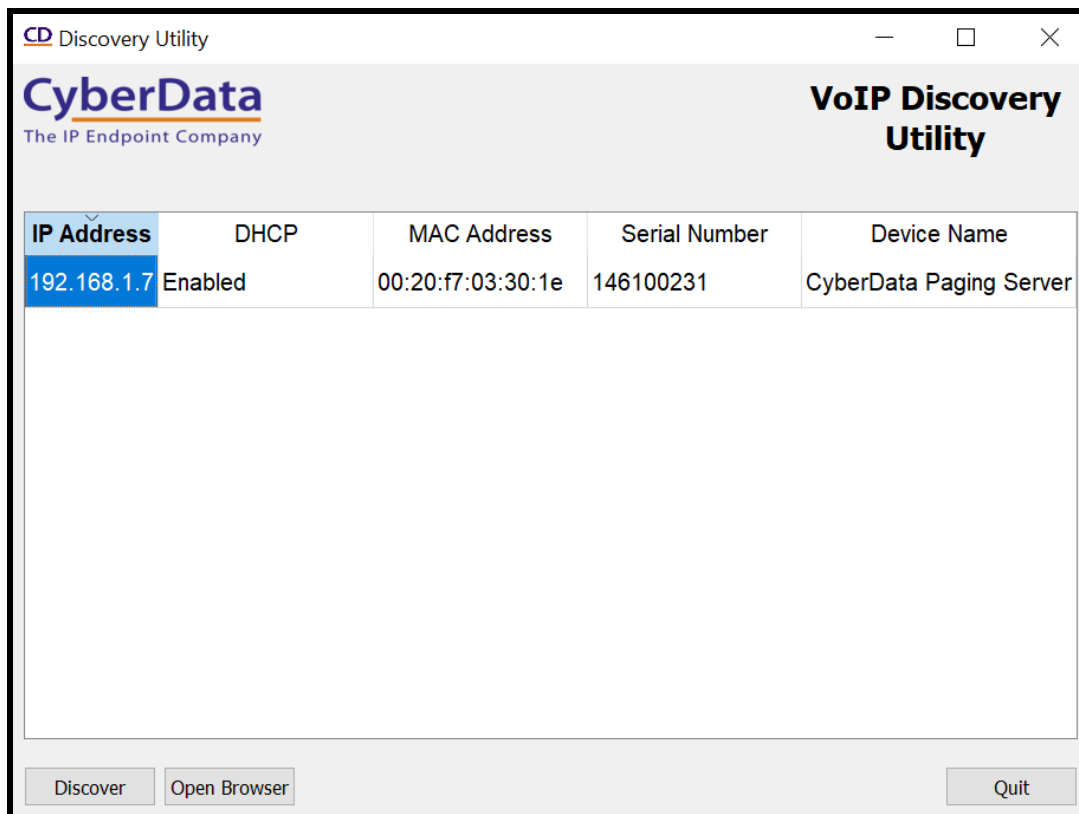
If you are configuring through the web interface, use the following steps to login to the web interface of your CyberData device.

Table 5-1: Setting Name correlation

| CyberData Setting | Zoom Provisioning Pop-up |
|---------------------------------------|--------------------------|
| Primary SIP Server | SIP Domain |
| Outbound Proxy Outbound Proxy Port | Outbound Proxy |
| Primary SIP User ID | User Name |
| Primary SIP Auth ID | Authorization ID |
| Primary SIP Auth Password | Password |

1. Click **Open Browser** from the CyberData Discovery Utility or point your browser to the CyberData device’s IP address to access the Home Page of the web interface.

Figure 5-1: CyberData Discovery Utility



2. Enter the default credentials when prompted and click the **Log In** button.

Username: admin

Password: admin

Figure 5-2: Web Interface Login



3. From the Home tab press the 'Device' Tab.

Figure 5-3: Device Tab

The screenshot displays the configuration page for the CyberData v3.1 Paging Server, specifically the Device Tab. The page has a navigation bar at the top with tabs for Home, Device, Network, SIP, PGROUPS, SSL, Schedules, Fault, Audiofiles, Events, Autopro, and Firmware. The main content area is titled "CyberData v3.1 Paging Server" and contains several configuration sections:

- Line-in Settings:** Includes checkboxes for "Enable Line-in to Line-out Loopback", "Enable Line-in to Multicast", and "Detect Line-in Silence". It also has input fields for "Multicast Address" (224.1.2.3) and "Multicast Port" (2000).
- Relay Settings:** Includes a checkbox for "Activate Relay on Local Audio".
- Clock Settings (highlighted with a yellow box):** Includes a checked checkbox for "Set Time with NTP server on boot", an "NTP Server" field (north-america.pool.ntp.org), a "Posix Timezone String" field (PST8PDT,M3.2.0/2:00:00,M11.1.0), a checked checkbox for "Periodically sync time with server", a "Time update period (in hours)" field (1), and a "Current Time" field (15:17:44).
- Misc Settings:** Includes a "Device Name" field (CyberData Paging Server), a "Bypass DTMF" checkbox, a "DTMF Duration" field (500), "Beep on Init" and "Beep on Page" checkboxes, an "Enable Polycom Paging on Multicast" checkbox, a "Polycom Transmit Channel" dropdown (1), and a "Disable HTTPS (NOT recommended)" checkbox.

At the bottom of the page, there are buttons for "Save" (highlighted with a yellow box), "Reboot", "Test Audio", "Test Multicast", "Test Relay", and "Toggle Help".

1. Check the box for “Set Time with NTP Server on Boot”.
2. Change the **NTP server** if necessary.
3. Set the **Posix Timezone String** to the local area.

Note: See the operations manual for other time zone strings.

4. Check the box for “Periodically sync time with server”.
5. Set the “Time update period (in hours)” to 1
6. **Save.**
7. Go to the SIP Tab.

Figure 5-4: SIP Tab

CyberData v3.1 Paging Server

SIP Settings

Enable SIP operation:

SIP Transport Protocol: TLS NTP enabled

TLS Version: 1.2 only (recommended)

Verify Server Certificate:

Register with a SIP Server:

Use Cisco SRST:

Primary SIP Server: 50882551.zoom.us

Primary SIP User ID: 87271231498301429673

Primary SIP Auth ID: 582595604202

Primary SIP Auth Password:

Backup SIP Server 1:

Backup SIP User ID 1:

Backup SIP Auth ID 1:

Backup SIP Auth Password 1:

Backup SIP Server 2:

Backup SIP User ID 2:

Backup SIP Auth ID 2:

Backup SIP Auth Password 2:

Remote SIP Port: 5060

Local SIP Port: 5060

Outbound Proxy: us01sipsj04.zoom.us

Outbound Proxy Port: 5091

Disable rport Discovery:

Buffer SIP Calls:

Re-registration Interval (in seconds): 360

Unregister on Boot:

Keep Alive Period: 10000

Nightringer Settings

Enable Nightringer:

SIP Server: 10.0.0.253

Remote SIP Port: 5060

Local SIP Port: 5061

Outbound Proxy:

Outbound Proxy Port: 0

User ID: 241

Authenticate ID: 241

Authenticate Password:

Re-registration Interval (in seconds): 360

Relay rings to multicast:

Multicast Address: 224.1.2.32

Multicast Port: 2020

Call Disconnection

Terminate Call after delay: 0

Codec Selection

Force Selected Codec:

Codec: PCMU (G.711, u-law)

RTP Settings

RTP Port (even): 10500

Jitter Buffer: 50

SRTP: Enabled

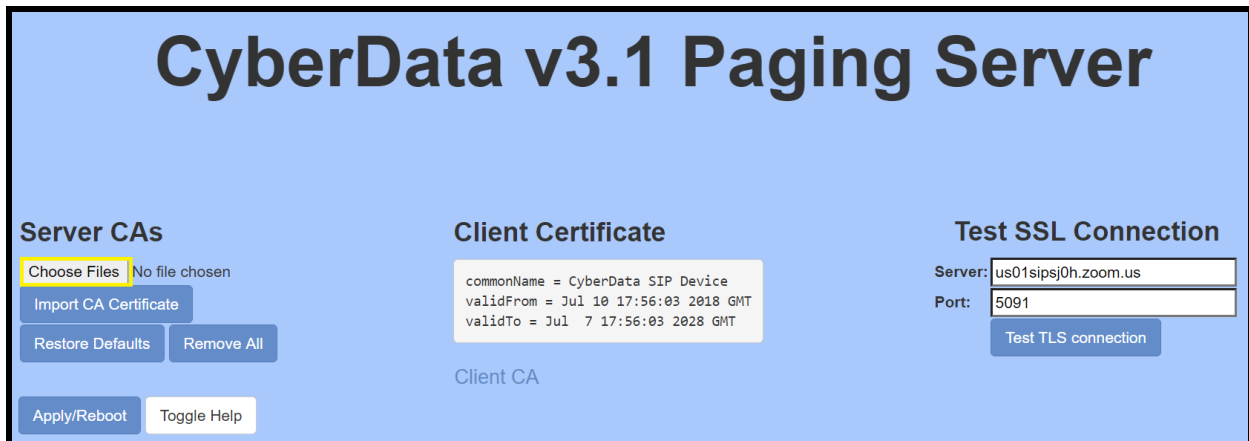
Save Reboot Toggle Help

8. Set the ‘SIP Transport Protocol’ to **TLS**.
9. Keep TLS version set to “**1.2 Only (Recommended)**”.
10. Check the box for “**Verify Server Certificate**”.
11. Set the **Primary SIP Server** to the SIP Domain from the configuration Popup.
12. Set the **Primary SIP User ID** to the Username from the configuration Popup.
13. Set the **Primary SIP Auth ID** to the Authorization ID from the configuration Popup.
14. Set the **Primary SIP Auth Password** to the password provided in the configuration popup.
15. Set the **Outbound proxy** and **Outbound Proxy port** to the address provided in the configuration popup.

Note: Make sure to separate the port from the outbound proxy information provided by zoom.

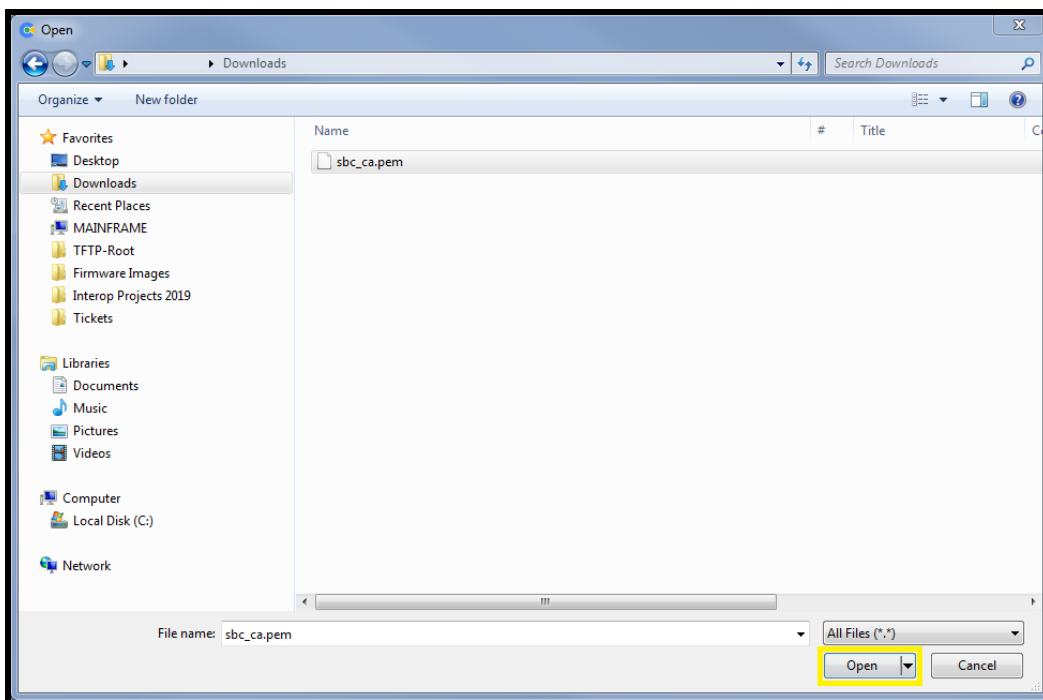
16. Check the box for “**Force Selected Codec**”.
17. Set SRTP to **Enabled**.
18. **Save**.
19. Go to the ‘**SSL**’ Tab.

Figure 5-5: SSL Tab



20. Press the ‘Choose Files’ button.

Figure 5-6: Choose file Pop-up



21. Select the “sbc_ca.pem” file and press the Open button.

22. Press the “Import CA Certificate” button to load the cert.

Figure 5-7: Import CA Certificate



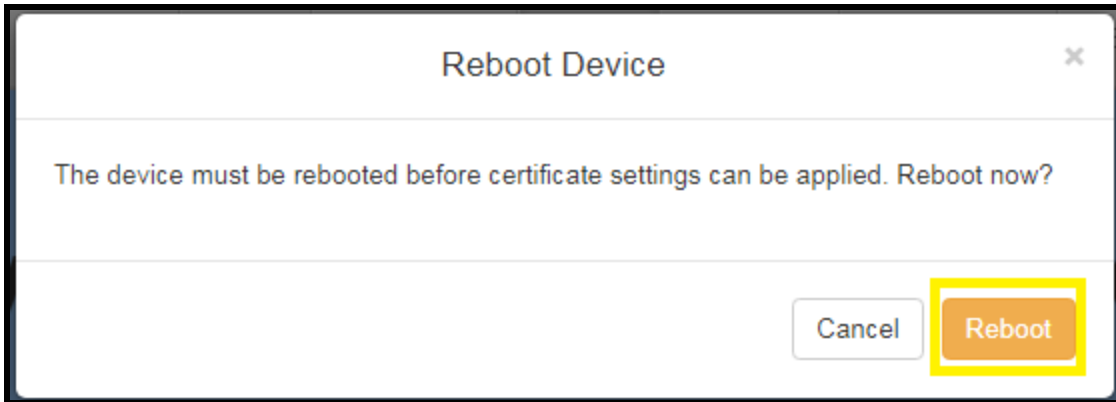
23. Once imported, confirm the file is listed with the other certificates.

Figure 5-8: Certificate List



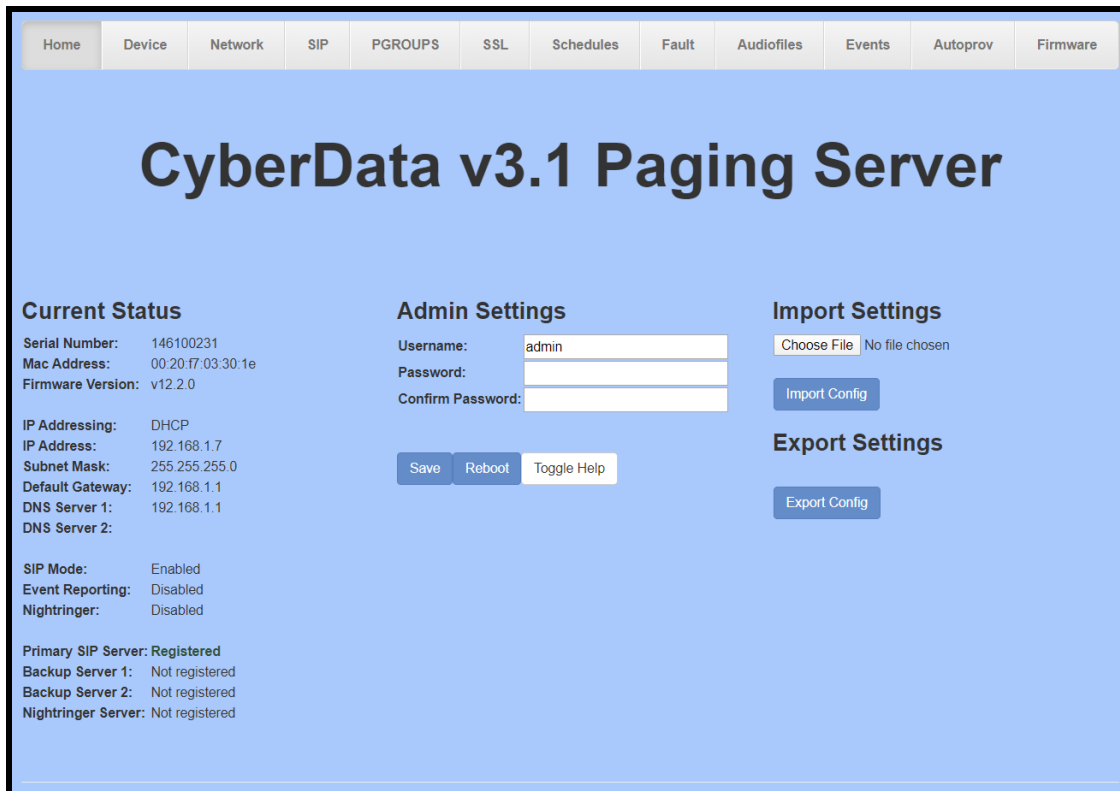
24. Once the certificate is loaded a reboot will be required to make the changes take effect
Use the “Apply/Reboot Button.”
25. Click Reboot in the Popup.

Figure 5-9: Apply/Reboot Popup



Once rebooted, “Registered” will appear in green on the Home page.

Figure 5-10: Home page – Registered



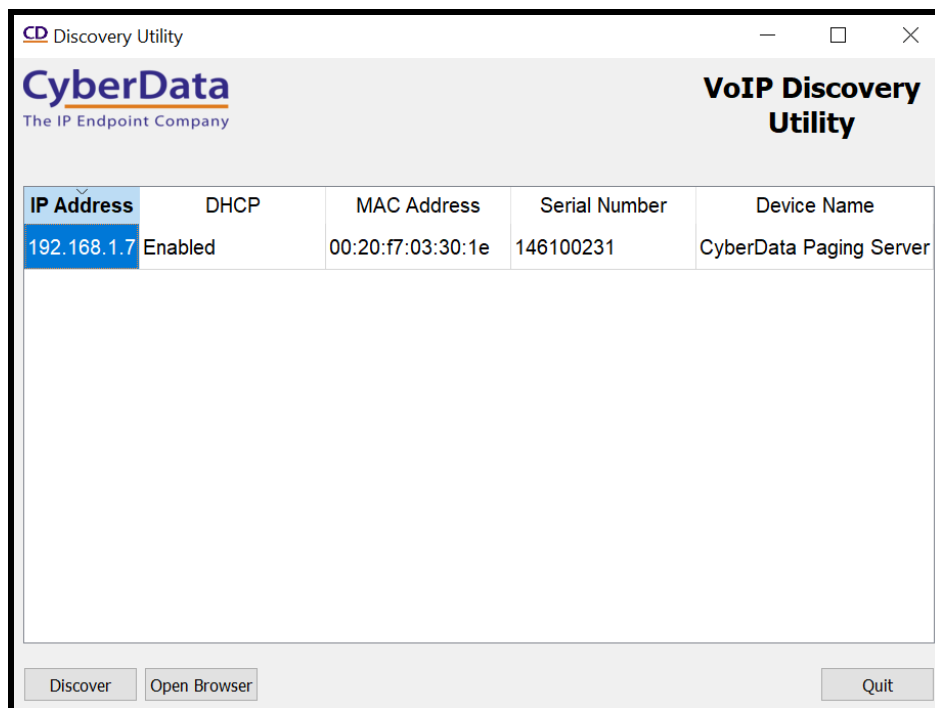
6.0 Configuration Procedure: Setting up the Nightringer extension

Table 6-1: Setting Name correlation

| CyberData Setting | Zoom Provisioning Pop-up |
|---------------------------------------|--------------------------|
| SIP Server | SIP Domain |
| Outbound Proxy Outbound Proxy Port | Outbound Proxy |
| User ID | User Name |
| Authenticate ID | Authorization ID |
| Authenticate Password | Password |

1. Click **Launch Browser** from the CyberData Discovery Utility or point your browser to the CyberData device’s IP address to access the Home Page of the web interface.

Figure 5-1: CyberData Discovery Utility



2. Enter the default credentials when prompted and click the **Log In** button.

Username: admin

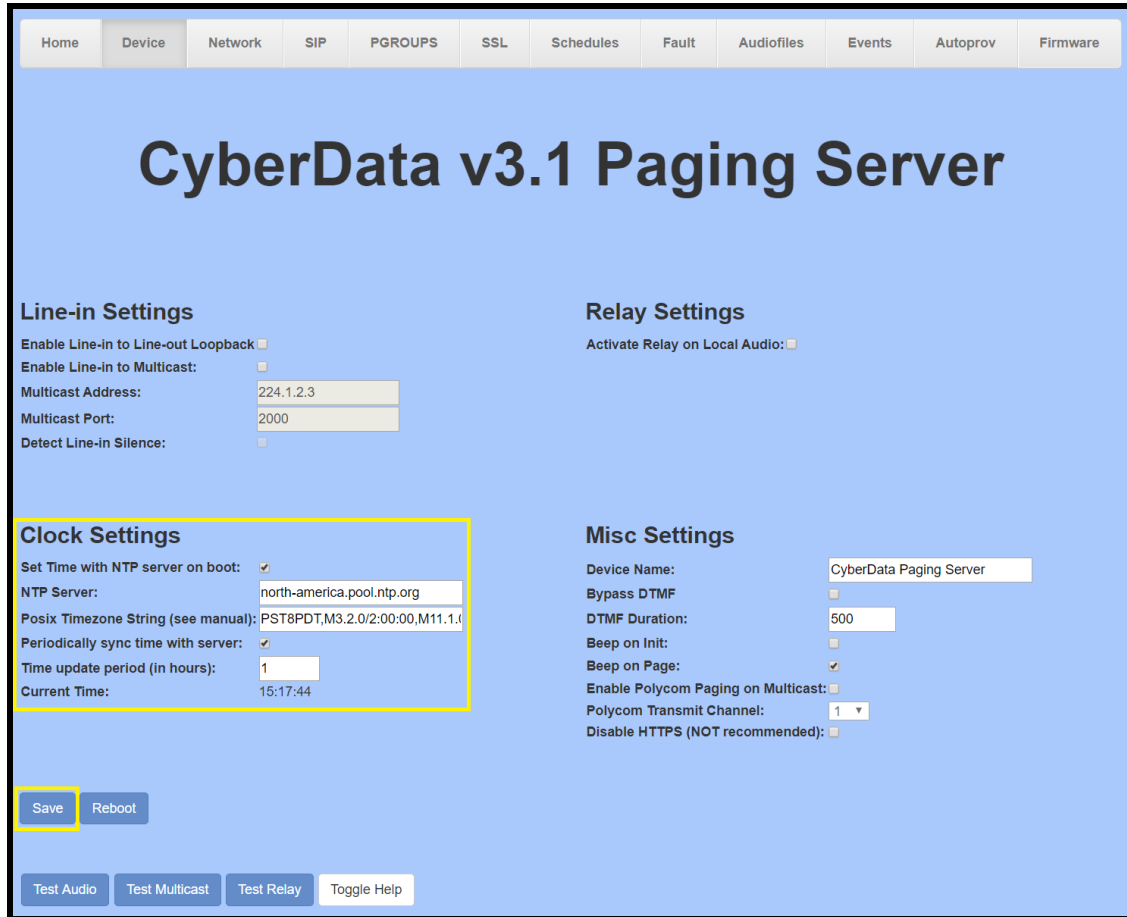
Password: admin

Figure 5-2: Web Interface Login



3. From the Home tab press the 'Device' Tab.

Figure 5-3: Device Tab



4. Check the box for “**Set Time with NTP Server on Boot**”.
5. Change the **NTP server** if necessary.
6. Set the **Posix Timezone String** to the local area.

Note: See the operations manual for other time zone strings.

7. Check the box for “**Periodically sync time with server**”.
8. Set the “**Time update period (in hours)**” to 1.
9. **Save.**
10. Go to the SIP Tab.

Figure 5-4: SIP Tab

The screenshot displays the configuration interface for the CyberData v3.1 Paging Server. It is divided into several sections:

- SIP Settings:** Includes checkboxes for 'Enable SIP operation', 'Verify Server Certificate', and 'Register with a SIP Server'. It features dropdown menus for 'SIP Transport Protocol' (set to TLS) and 'TLS Version' (set to 1.2 only). Text input fields are provided for 'Primary SIP Server', 'Primary SIP User ID', 'Primary SIP Auth ID', and 'Primary SIP Auth Password'. There are also fields for backup servers and ports.
- Nightringer Settings:** Includes a checkbox for 'Enable Nightringer'. It contains text input fields for 'SIP Server', 'Remote SIP Port', 'Local SIP Port', 'Outbound Proxy', 'Outbound Proxy Port', 'User ID', 'Authenticate ID', 'Authenticate Password', and 'Re-registration Interval (in seconds)'. There are also fields for 'Relay rings to multicast', 'Multicast Address', and 'Multicast Port'.
- Call Disconnection:** A text input field for 'Terminate Call after delay'.
- Codec Selection:** A checkbox for 'Force Selected Codec' and a dropdown menu for 'Codec' (set to PCMU (G.711, u-law)).
- RTP Settings:** Text input fields for 'RTP Port (even)', 'Jitter Buffer', and a dropdown for 'SRTP' (set to Disabled).

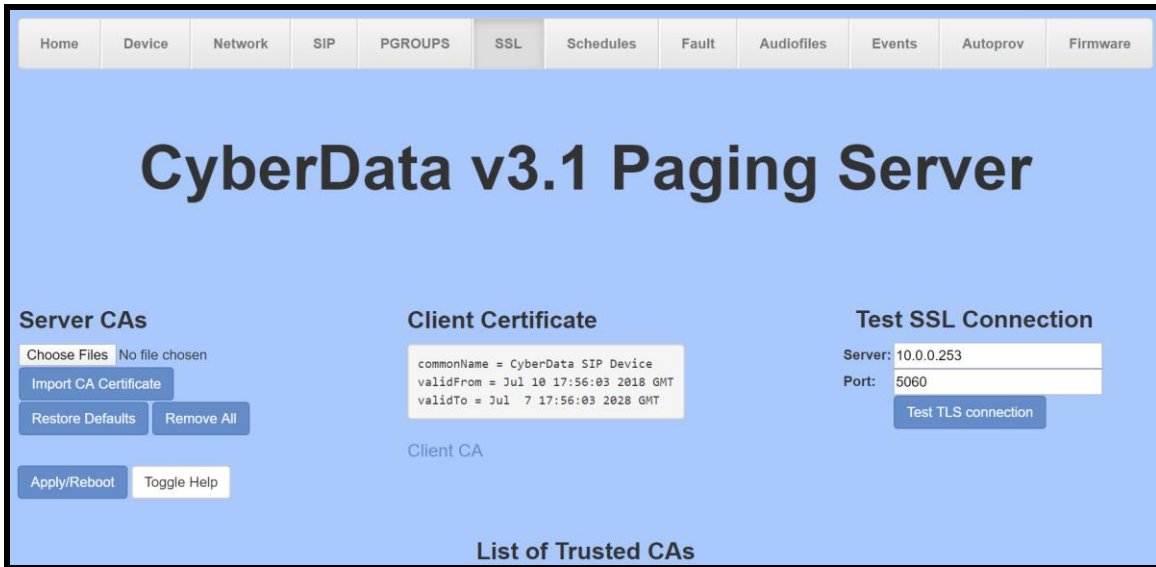
At the bottom right, there are buttons for 'Save', 'Reboot', and 'Toggle Help'.

11. Set the ‘SIP Transport Protocol’ to **TLS**.
12. Keep TLS version set to “**1.2 Only (Recommended)**”.
13. Check the box for “**Verify Server Certificate**”.
14. Set the **SIP Server** to the SIP Domain from the configuration popup.
15. Set the **User ID** to the Username from the configuration popup.
16. Set the **Authenticate ID** to the Authorization ID from the configuration popup.
17. Set the **Authenticate Password** to the password provided in the configuration popup.
18. Set the **Outbound proxy** and **Outbound Proxy port** to the address provided in the configuration Popup.

Note: Make sure to separate the port from the outbound proxy information provided by Zoom.

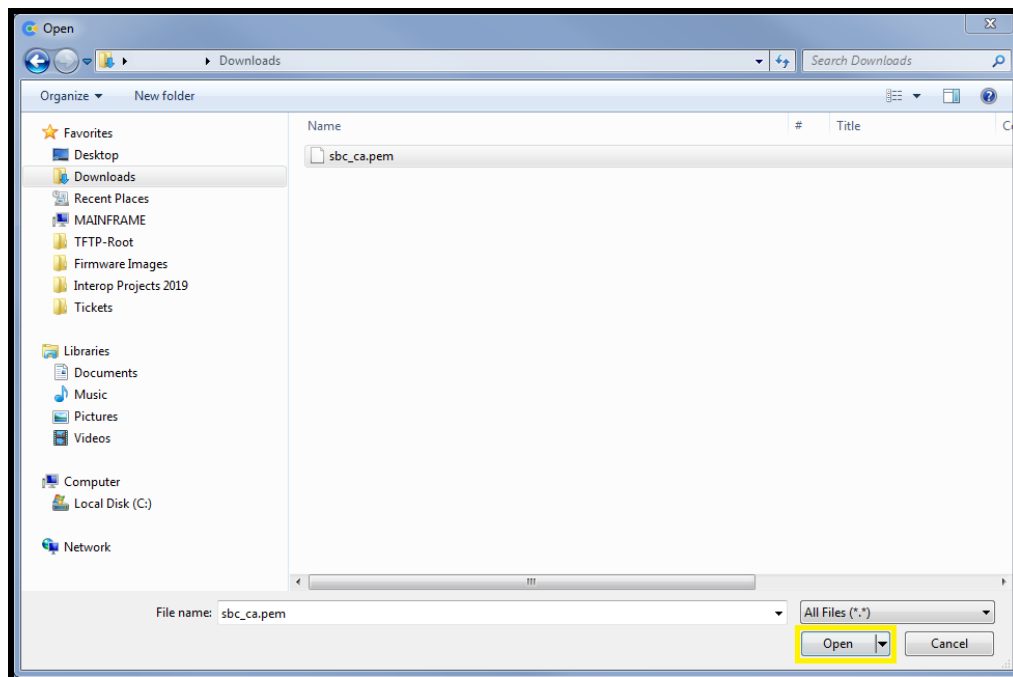
19. Check the box for “Force Selected Codec”.
20. **Save.**
21. Go to the ‘SSL’ Tab.

Figure 5-5: SSL Tab



22. Press the ‘Choose Files’ button.

Figure 5-6: Choose file Pop-up



23. Select the “sbc_ca.pem” file and press the Open button.
24. Press the “Import CA Certificate” button to load the cert.

Figure 5-7: Import CA Certificate



25. Once imported, confirm the file is listed with the other certificates.

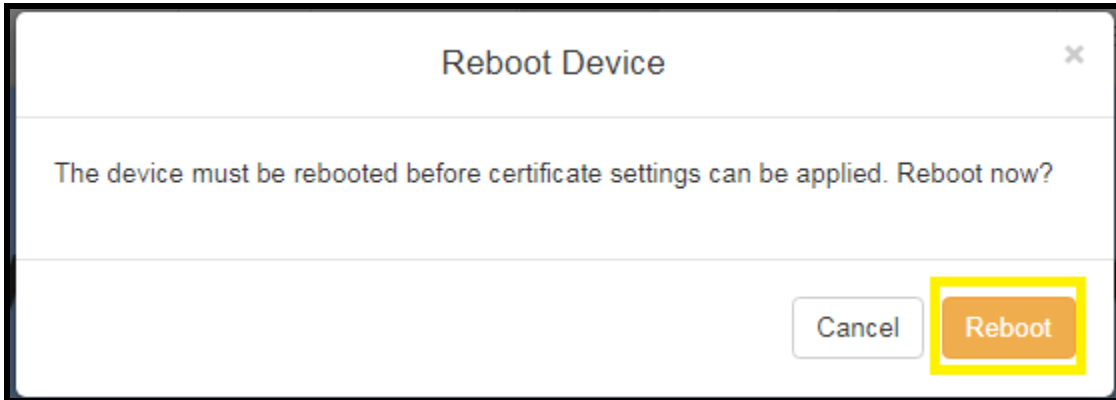
Figure 5-8: Certificate List

| | | | |
|----|--|------|--------|
| 22 | ISRG_Root_X1.crt | Info | Remove |
| 23 | VeriSign_Class_3_Public_Primary_Certification_Authority_-_G4.crt | Info | Remove |
| 24 | VeriSign_Class_3_Public_Primary_Certification_Authority_-_G5.crt | Info | Remove |
| 25 | VeriSign_Universal_Root_Certification_Authority.crt | Info | Remove |
| 26 | Verisign_Class_1_Public_Primary_Certification_Authority.crt | Info | Remove |
| 27 | Verisign_Class_1_Public_Primary_Certification_Authority_-_G3.crt | Info | Remove |
| 28 | Verisign_Class_2_Public_Primary_Certification_Authority_-_G2.crt | Info | Remove |
| 29 | Verisign_Class_2_Public_Primary_Certification_Authority_-_G3.crt | Info | Remove |
| 30 | Verisign_Class_3_Public_Primary_Certification_Authority.crt | Info | Remove |
| 31 | Verisign_Class_3_Public_Primary_Certification_Authority_-_G3.crt | Info | Remove |
| 32 | sbc_ca.pem | Info | Remove |
| 33 | thawte_Primary_Root_CA.crt | Info | Remove |
| 34 | thawte_Primary_Root_CA_-_G2.crt | Info | Remove |
| 35 | thawte_Primary_Root_CA_-_G3.crt | Info | Remove |

1. Once the certificate is loaded a reboot will be required to make the changes take effect Use the “Apply/Reboot Button.

2. Click Reboot in the popup.

Figure 5-9: Apply/Reboot Popup



Once rebooted, “Registered” will appear in green in the “Status” section of the Home page.

Figure 5-10: Home page – Registered



7.0 Using the CyberData SIP Paging Server in a Zoom system

Once the paging server is registered with Zoom, it can be used in several ways. The unit can be directly called by dialing the extension number of the unit. It is also possible to add the unit to a call queue to reach multiple endpoints simultaneously. Keep in mind that with a call queue, multiple devices will ring, but only one device may answer. Due to this operation it is not possible to page to multiple devices at once.

Please reference our [Connecting to Compatible Analog Amplifiers](#) page for wiring diagrams for many different amplifiers that can be used with the paging server.

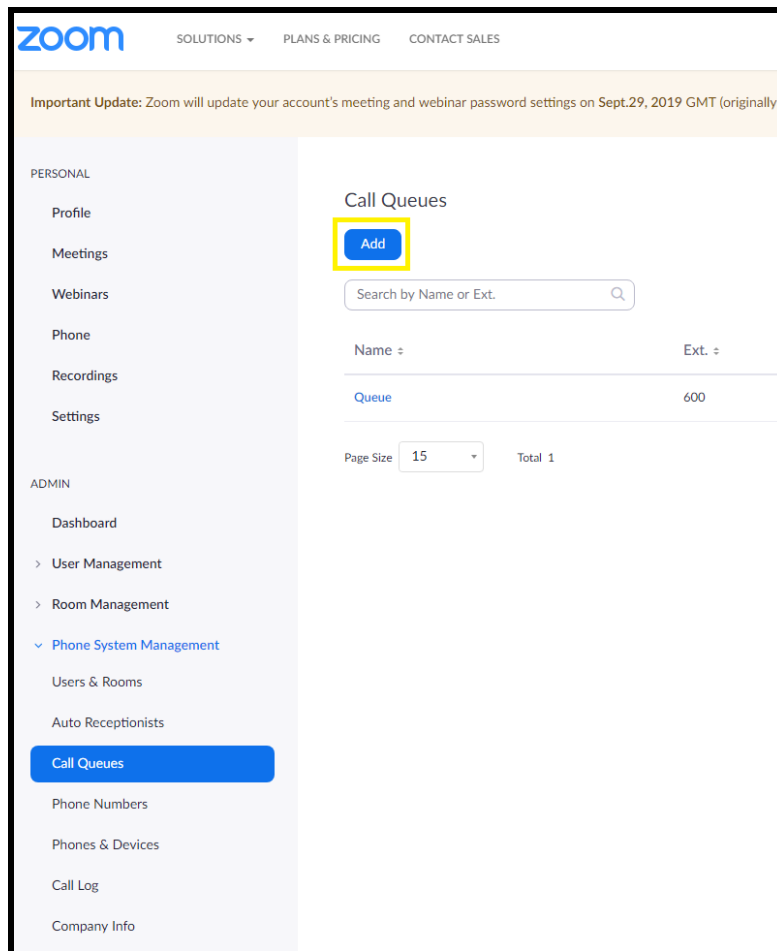
Note: If the amplifier used in your system is not on our list please reach out to our [Support department](#) to see if it is compatible. If so, a connection diagram will be created.

7.1 Creating a Call queue

CyberData recommends using the Nightringer extension as part of a call queue, allowing the paging server to also serve as an additional notification for incoming calls.

1. From the Phone System Management page select call queues and press the Add button to create a new queue.

Figure 7-1: Add call queue



2. After clicking 'Add' a pop-up will appear that allows naming and assigning a number to the call queue.

Figure 7-2: Name the queue

Call Queues > Add

Name

Description (Optional)

Extension Number

Member(s) [Add](#)

3. Name the queue, set a description and change the extension number if necessary.

Figure 7-3: Add users

Call Queues > Add

Name

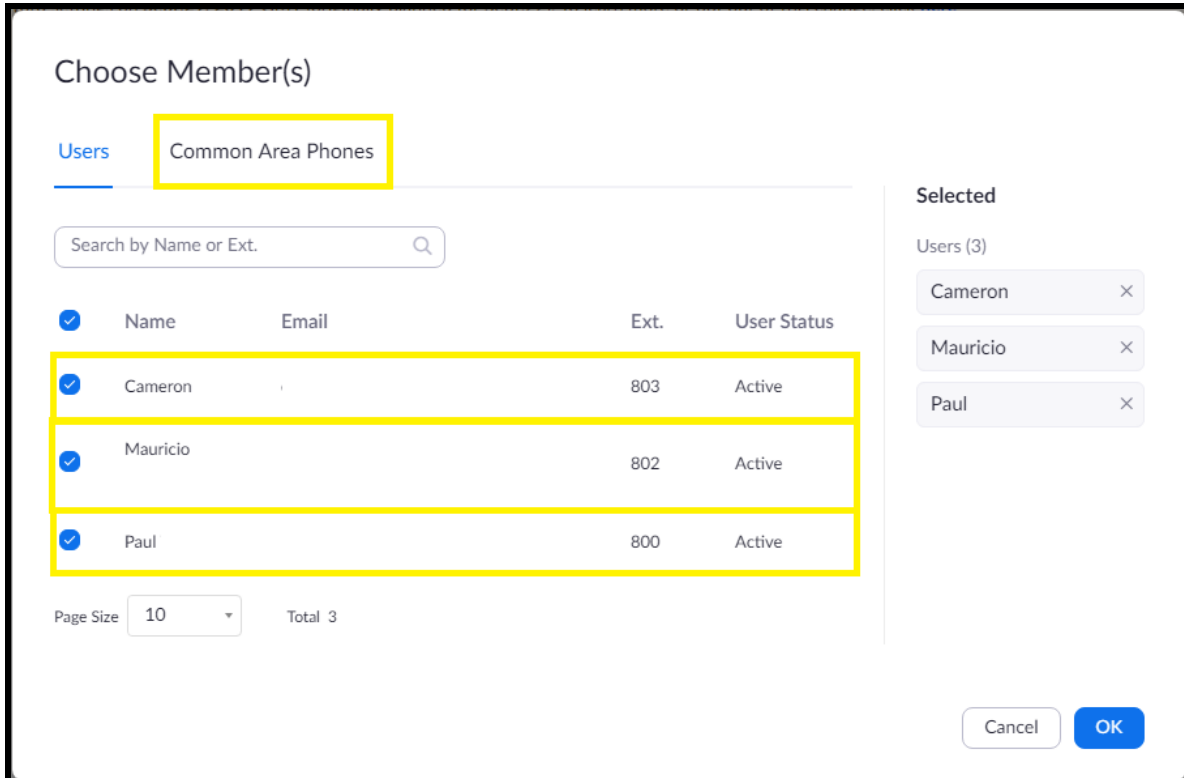
Description (Optional)

Extension Number

Member(s) [Add](#)

4. Press the Add button to add Users and Common Area Phones to the queue.

Figure 7-4: Add Users



5. Select the users who will participate in the call group, then select "Common Area Phones."
6. In the "Common Area Phones" section, select the phones you wish to add to the queue.

Figure 7-5: Add Common Area Phones

Choose Member(s)

Users Common Area Phones

Search by Display Name or Ext.

| <input type="checkbox"/> | Display Name | Ext. |
|-------------------------------------|-----------------------------|------|
| <input checked="" type="checkbox"/> | SIP Paging Server | 506 |
| <input type="checkbox"/> | Intercom | 812 |
| <input type="checkbox"/> | CyberData SIP Paging Server | 828 |
| <input type="checkbox"/> | Yealink T49G | 817 |
| <input type="checkbox"/> | Paul's Intercom | 822 |
| <input type="checkbox"/> | Nathans Intercom | 827 |
| <input type="checkbox"/> | Nathan's Paging Server | 825 |
| <input type="checkbox"/> | Nathan's Snom | 826 |
| <input type="checkbox"/> | Paul's SIP Speaker | 824 |
| <input type="checkbox"/> | Paul's Paging Amp | 823 |

Selected

SIP Paging Server

Page 1 of 2 Page Size 10 Total 14

7. Click “OK” to confirm your selections.
8. Finally, press ‘Save’ to complete the queue.

Figure 7-6: Call queue complete

Call Queues > Add

Name

Description (Optional)

Extension Number

Member(s) Selected 6 Member(s) [Add](#)

7.2 Multicast Paging

The CyberData SIP Paging Server is a SIP to Multicast out device that is very useful for paging. Multicast allows for a nearly unlimited number of devices to receive a page if they are on the same local network. This makes the paging server a powerful product in any paging solution.

Complete this process after registering the paging server with Zoom. This setup will require making a call to the paging server to send multicast, so registration is necessary.

1. Navigate to the PGroups tab of the SIP Paging Server web interface.
2. Press the **Edit** button on the page group that will be changed.

Figure 7-7. Edit PGroup

The screenshot shows the 'Paging Groups' section of the CyberData v3.1 Paging Server web interface. It features a table with columns for '#', 'Address', 'Port Name', 'Code', 'TTL', and 'Lineout'. Each row represents a paging group, and an 'Edit' button is visible at the end of each row. The 'Edit' button for the first group (index 0) is highlighted with a yellow border.

| # | Address | Port Name | Code | TTL | Lineout | |
|---|-----------|--------------------|------|-----|---------|------|
| 0 | 234.2.1.1 | 2000 PagingGroup00 | | 255 | Yes | Edit |
| 1 | 234.2.1.2 | 2002 PagingGroup01 | | 255 | Yes | Edit |
| 2 | 234.2.1.3 | 2004 PagingGroup02 | | 255 | Yes | Edit |
| 3 | 234.2.1.4 | 2006 PagingGroup03 | | 255 | Yes | Edit |
| 4 | 234.2.1.5 | 2008 PagingGroup04 | | 255 | Yes | Edit |
| 5 | 234.2.1.6 | 2010 PagingGroup05 | | 255 | Yes | Edit |

3. In the configure PGroup Popup change all necessary fields.
 - a. The **Address** field is the multicast IP Address that will be used.
 - b. The **Port** field is the port used in conjunction with the Multicast IP Address.
 - c. The **Name** field has no impact on operation and is solely used for identification.
 - d. The **Security Code** field is an optional field that will require a security code before paging to that group.
 - e. **TTL** or Time To Live is the number of 'hops' the traffic can make before it is delivered to the endpoints, most users do not change this field.
 - f. The **Line Out** check box allows the page to play to both Multicast and the paging servers analog outputs.

- g. The **Play Stored Message** check box changes the group from a 'Live Page' group to a stored message playback group, which is very useful for playing pre-recorded audio files.
 - h. IF Play Stored Message is enabled, make sure to select the desired audio file.
 - i. IF Play Stored Message is enabled, set the number of times to play.
4. Save changes after making all necessary adjustments.

Figure 7-8. Configure PGroup Pop Up.

The screenshot shows a configuration window titled "Configure PGROUP". The fields and their values are as follows:

| | |
|---------------------|-------------------------------------|
| PGROUP | 0 |
| Address | 234.2.1.1 |
| Port | 2000 |
| Name | All Page |
| Security Code | ***** |
| TTL | 255 |
| Line-out | <input checked="" type="checkbox"/> |
| Play Stored Message | <input type="checkbox"/> |
| Audio File | [Dropdown menu] |
| Times to Play | 1 |

At the bottom of the window, there are two buttons: "Save Changes" and "Cancel".

- 5. Repeat this process for all necessary groups.
- 6. Save and reboot for the changes to take effect.

7.2.1 Setting up Multicast Receive on other CyberData Products

After configuring PGroups on the paging server, the receiving devices need to be configured to receive that multicast. The process is shared across the CyberData product lines, but for the purposes of this guide a SIP Speaker's configuration process will be shown.

1. Log into CyberData product that will receive the Multicast from the SIP Paging Server.
2. Navigate to the Multicast Tab.

Figure 7-9. Speaker Home tab



3. Check the box to Enable Multicast and pick a priority for the Multicast group.

Note: The Multicast feature uses a Priority system to rank groups in order of importance. Group 9 is the highest priority and 0 is the lowest priority. SIP Calls made to the speakers are treated as Priority 4.5, so they will play over Multicast groups 0-4 and will be superseded by Multicast groups 5-9.

Note: Multicast priority 9 is treated as 'Emergency' and will always play at max volume.

4. Set the Multicast Address and Port to match the PGroup on the Paging Server.
5. If desired check Buffered, Beep, or Relay depending on the requirements.
6. Save and Reboot for the changes to take effect.

Figure 7-10. Multicast Tab

CyberData SIP Speaker

Multicast Settings

Enable Multicast Operation:

| Priority | Address | Port | Name | Buffer | Beep | Relay |
|----------|--------------|-------|------------------|-------------------------------------|-------------------------------------|--------------------------|
| 9 | 239.168.3.10 | 11000 | Emergency | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 8 | 234.2.1.1 | 2000 | All Page | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| 7 | 239.168.3.8 | 9000 | MG7 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 6 | 239.168.3.7 | 8000 | MG6 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 5 | 239.168.3.6 | 7000 | MG5 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 4 | 239.168.3.5 | 6000 | MG4 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 3 | 239.168.3.4 | 5000 | MG3 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 2 | 239.168.3.3 | 4000 | MG2 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 1 | 239.168.3.2 | 3000 | MG1 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 0 | 239.168.3.1 | 2000 | Background Music | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

The **Buffer** setting will have the speaker record the Multicast page and play it when it has completed. This will prevent any feedback from the speaker if the page is being made in an area with a speaker.

The **Beep** setting will have the speaker play a beep tone when a multicast is received. This beep plays at the start of the multicast, so it is possible to have overlap with the beep tone and the multicast stream.

The **Relay** setting will have the speaker's onboard relay during the multicast page. This is useful if the onboard relay is connected to another device.

8.0 Contact CyberData Corporation

Sales

For sales-related questions, please visit our [Contact CyberData Sales](#) web page for more information.

Technical Support

For CyberData Technical Support, please submit a [Contact CyberData VoIP Technical Support](#) form on our website.

The CyberData VoIP Technical Support Contact form initiates a troubleshooting ticket which CyberData uses for quality assurance purposes.

Additionally, the Contact VoIP Tech Support form tells us which phone system you are using, the make and model of the network switch, and other essential troubleshooting information we need to efficiently assist with a resolution. Please also include as much detail as possible in the Describe Problem section of the form. Your installation is extremely important to us.

Documentation Feedback

We realize changes to the software or hardware of the Zoom PBX solution may render this document obsolete. We welcome and encourage documentation feedback to ensure continued applicability.