# ZULTYS
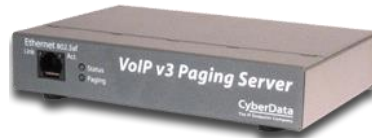
INNOVATE | COMMUNICATE | COLLABORATE

# CyberData SIP Page Server V3 Integration with Zultys MX – Serial Numbers 1461x

## Author: Zultys Technical Support Department

This document covers the integration of CyberData's SIP Page Server V3 with the Zultys MX. This document was written for MX Version 11.0 and the following CyberData Products

- 011146C SERVER,V3 VoIP PAGING (Ver. 11.3.0)
- For Serial numbers starting with 1461

All support and supporting documentation for CyberData should be obtained from CyberData itself. This document assumes the reader is at least a Zultys Certified Systems Expert (ZCSE), and is familiar with creating Users, Devices, and Paging (both SIP based and Multicast based) in general. This document also assumes the reader is familiar with setting up CyberData Paging equipment and/or has access to the Manuals for the CyberData equipment, as several sections are left out of this manual such as setting up the network configuration of the CyberData Equipment and pin outs for relay, and audio out usage.

For more information on the integration process see integration section.

# 1 Contents

# 2   Integration

CyberData SIP Paging Server can be integrated in multiple ways with the Zultys MX, each integration option has its unique benefits and draw backs. For the best integration between all types of phones (Polycom, Zultys, and other 3rd party devices) as well as routing and remote devices Zultys recommends SIP Page and Converted to Multicast.

Starting with CyberData firmware 7.2.0 you can integrate Polycom Group Paging with traditional Multicast paging services. This is accomplished via CyberData firmware enhancements to provide Multicast and Group Paging features at the same time, for more information see CyberData's website.

## 2.1   SIP Page and Converted to Multicast

When integrating the Zultys MX with the CyberData SIP Paging Server and Ceiling Speakers, Zultys recommends to integrate the CyberData Paging server into the existing paging functions of the MX. This will afford the possibility to integrate the ZIP2, ZIP3, ZIP5, Polycom and other 3rd party equipment along with the CyberData Paging equipment. Following this method of integration, the ZIP2 and Polycom phones can be integrated using the traditional SIP Paging methods used by the MX, but with the integration of the CyberData the SIP page can automatically be converted to Multicast

Paging which is used by the CyberData paging equipment, and can be integrated with the ZIP3 and ZIP5 line of phones. This will increase you paging capability from the 32 phones in a standard page zone of the MX to virtually unlimited ZIP2 (which uses unicast), ZIP3 (using multicast), ZIP5 (using multicast) and CyberData paging equipment.

Traditional paging equipment can be integrated into this solution using CyberData SIP Paging Server's Audio Out port and Relays.

Users will simply dial the page server on the MX select the proper zone, and make their page. A SIP call will be placed to the CyberData Paging Server (and any other device in the page group). The CyberData Page Server will convert the SIP page to Multicast to stream to all ZIP5 and ZIP3 devices on the network. A maximum of 32 devices on a MX250 and 16 devices on a MX30 can be added to the MX page group, ZIP5 and ZIP3 devices local to the CyberData Page Server do not need to be included in the MX Page Server as they will receive the page via multicast.

## 2.2  Pure Multicast

When using CyberData paging equipment you can integrate as a pure multicast solution, in that you will no longer use the paging services of the MX, and rely purely on Multicast capabilities of the ZIP5, ZIP3 and CyberData equipment. When using CyberData's SIP Paging server you may either dedicate a unique paging button on the phone per page zone, or you may use the DTMF zone selection capability of the CyberData SIP Paging Server to select from the 25 paging zones offered by the CyberData SIP Paging Server. The ZIP5 and ZIP3 phones only support listening to 5 multicast paging zones.

Traditional paging equipment can be integrated into this solution using CyberData SIP Paging Server's Audio Out and Relays.

Users will press a predefined paging button on the ZIP5 and ZIP3 devices to initiate the page, this will start a multicast from the device to all other devices listening to the same multicast IP address and Port pair. ZIP2 and Polycom phones cannot be part of a multicast page.

## 2.3  Traditional Paging Equipment

Traditional Paging equipment can be integrated into either integration option (SIP or Multicast) by either the MX or CyberData SIP Paging Server. It is recommended to use the CyberData SIP Paging Server to integrate with traditional paging equipment input and offers the ability to include relays, where the MX output is line out and does not offer relay capability. The CyberData Paging Server supports a 600 Ohms at 5 VPP output referred to as Page Port and a 10K Ohms at 2 VPP output referred to as Line Out.

If integrating multiple locations with traditional paging equipment it is recommended to use the CyberData Paging Adapter to integrate additional locations using SIP paging

from the MX, and the CyberData Paging Adapter to integrate to the traditional paging equipment.

## 2.4  Including Ceiling Speakers

When integrating Ceiling speakers, you may use traditional paging equipment, or it is recommended to use CyberData Ceiling Speakers that are fully integrated to the CyberData SIP Paging Server.

# 3  Multicast Paging

## 3.1  How Multicast Paging Works

After a user presses a configured "Paging" key on the phone, the phone sends a page message (which is an RTP stream, hereinafter referred to as a "page") to a preconfigured multicast address. Any device in the local network listens for the page on the preconfigured multicast address. The device will display the multicast page sent/received address to the user. You can define multiple multicast zones by using a different multicast IP or port number, a single device can listen to multiple IP:Port combinations.

The device uses G711 uLaw CODEC for multicast paging.

The recipient can drop the incoming page if required. The recipient can also press Do Not Disturb (DND) or other "ignore" options on the device to ignore/reject any incoming pages.

## 3.2  Caveats of Multicast Paging

Multicast paging is designed for ZIP5/ZIP3 phones only. There is no guaranteed interoperability with any other Zultys-supported phones.  CyberData Paging Equipment is an exception, as it has been tested and certified to work properly with the ZIP5/ZIP3 phones. The ZIP2xN phones and MXIE Softphone does not support multicast paging. The 57iCT cordless handset cannot initiate a multicast page.

This service is typically non-routable, and cannot be used to page across the MXnetwork or to remote devices.

**Note**: The Group Paging Settings are dependent on the setting for the "Allow Barge In" parameter.

**Note**: Multicast page is one-way only - from sender to the receiver.

**Note**: For outgoing pages, all other existing calls on the phone are put on hold.

For incoming pages, the ringing display is dependent on the "Allow Barge In" parameter. If this parameter is disabled, and there is no other call on the phone, then the paging is automatically played via the preferred audio device.

If there is an existing call on the phone, the call initially displays in the ringing state. The user has the option to accept/ignore the call. If the "Allow Barge In" parameter is enabled, the page call barges in, and any existing calls are put on hold.

If a page session already exists on the phone, and the phone receives another incoming page, the priority is given to the first multicast session and the second multicast session is ignored. The behavior for the incoming calls in this case is also based on the setting for the "Allow Barge In" parameter. The incoming call is handled as if there were an existing call already on the phone.

## 3.3   Advantages of Multicast Paging
Multicast paging allows for virtually unlimited paging capability in a local network, does not require a session license to operate, and is almost instantaneous, as it does not require the phones to acknowledge the page request.

Multicast paging is a certified option to increase the number of devices in a page zone from 32 to a virtually unlimited number.

## 3.4   Cloud Services
Multicast Paging is suggested for Cloud Services as this will reduce the bandwidth requirements during paging, and with the CyberData Paging server you can place a single call to the MX Page Zone which includes the CyberData Paging Server, and allow it to convert the page to a multicast page for all ZIP3, ZIP5 and Polycom Devices using a much smaller bandwidth requirement (2 SIP calls).

# 4   SIP Paging

## 4.1   How SIP Paging Works
SIP paging works as follows: the MX places a SIP call to the device with an auto answer flag if the device is a ZIP5, ZIP3 or a Polycom device (other device types must be specifically configured to answer pages automatically, but will not receive the auto answer flag), once all devices have answered the call, the page is made to these devices. The Cyber Data Paging Server may also be included in this paging group when properly configured for auto answer, and DTMF zone selection is disabled.

## 4.2   Caveats of SIP Paging
- SIP paging is limited to 32 devices on a MX250 and 16 devices on an MX30.
- Session License is required.
- SBC Licenses are required if SIP paging is used with Remote phone(s).
- Dependent on an answer and acknowledgement from all devices before the page can be made

## 4.3   Advantages of SIP Paging
- Works with remote devices.
- Works with the entire ZIP product line with no exceptions.

- Works with Polycom devices.
- Works with MXIE Softphone.

# 5 Creating a Generic SIP Device on the MX for night ring capabilities

If using the night ring capabilities of the SIP Page Server, a generic SIP device and a user is required to be created on the MX. For basic operation a Generic SIP device is created on the MX and assigned to a user. The CyberData equipment will register as this Generic SIP Device, this device is then invited by the MX when the extension is rang triggering the night ring capabilities of the CyberData equipment. If not using the Night Ring capabilities of the CyberData equipment this section can be skipped.

## 5.1 Create Generic SIP Profile

In order to create a Generic SIP Device, it is recommended to create a unique Generic SIP Device Profile to control the codecs, functions and number of lines used by CyberData Equipment, this device profile should be the same profile used with the paging device.

Make sure that the following options are selected.

**Sends SIP Register**: Checked.

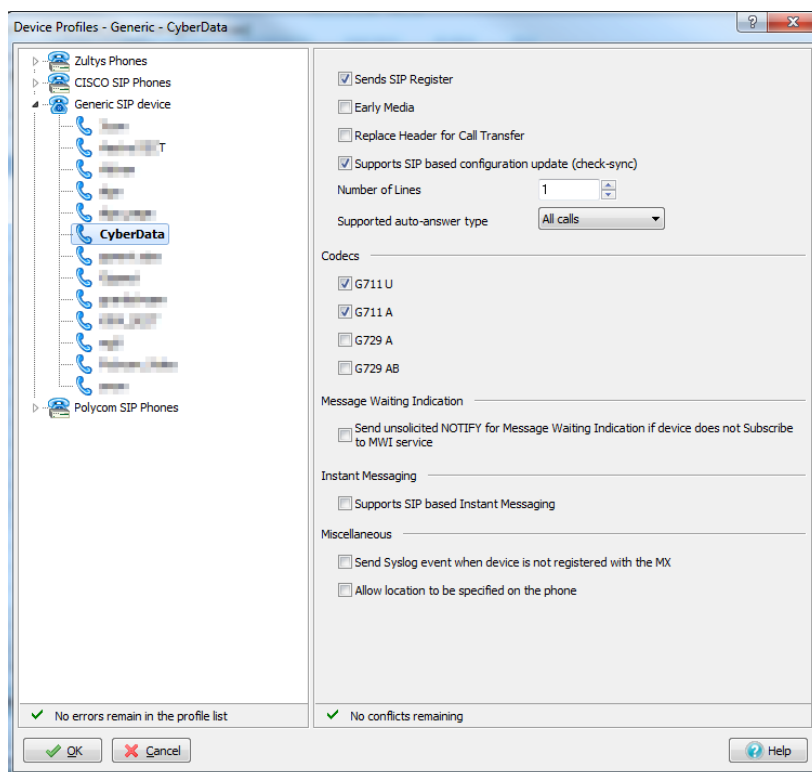**Supports SIP based configuration**: Checked.

**Number of Lines**: 1.

**Supported auto-answer type**: All Calls.

**Codecs**: G711U and G711A.

**Send unsolicited NOTIFY for messages**: Unchecked.

**Send Syslog event when device is not registered..:** This is an optional selection that is recommended to allow the MX to generate a syslog notification if the

paging equipment is off
line

The remaining options are
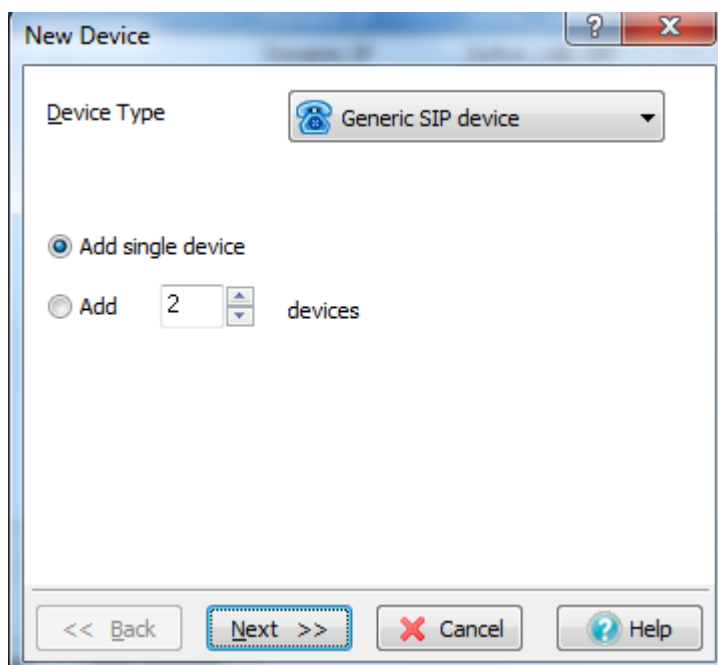unchecked.

## 5.2  Create Generic SIP Device

Create a generic SIP device on the MX for the MX to integrate with CyberData
Equipment. The CyberData equipment will register with the MX using this Generic SIP
Device.

Make sure that the following options are selected.

**Device Type:** Generic SIP
device.

**Add Single Device**:
Selected.

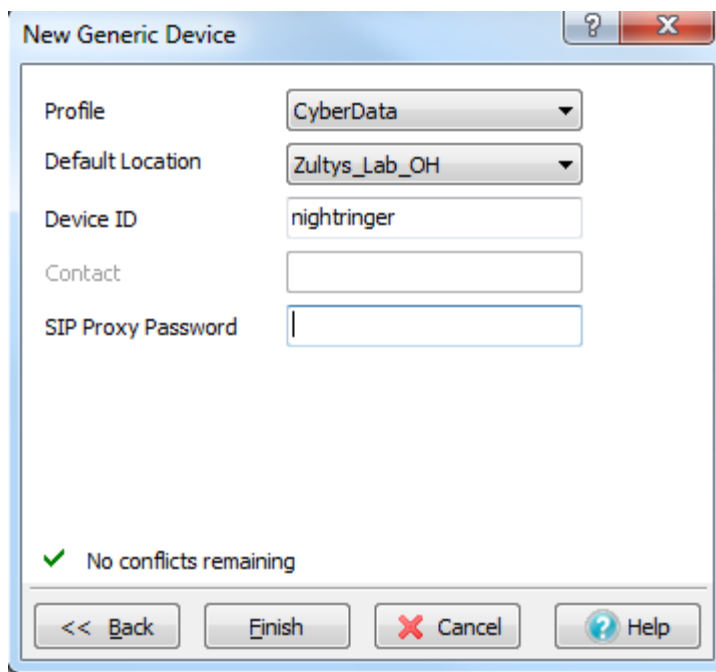Click *Next* to proceed to
the next screen.

**Profile**: Select the Generic SIP Device Profile created in section 5.1.

**Default Location**: Select the proper location from the drop-down.

**Device ID**: Type the ID to register CyberData Equipment Ringing extension.

**Contact**: Not used.

**SIP Proxy Password**: Type the password if required.

## 5.3 Create User and Assign User to the Device

After creating the device that will interface with CyberData Equipment, create a user and assign the user to this device. This document assumes the reader is a ZCSE trained and a certified technician. Since this process is covered by ZCSE training, it is considered to be outside the scope of this document.

# 6 Creating a Generic SIP Device on the MX for paging capabilities

When using the CyberData SIP Paging Server for paging capabilities, Zultys recommends creating a Generic SIP Device and a user for the CyberData Paging equipment. Only a single device and User is required for paging purposes only, the Night Ringer will require its own user and device. The Paging features of the CyberData Equipment interfaces with the MX system through a preconfigured MX user. A single user / device will interface with the MX for paging purposes. To initiate a paging message over CyberData Paging Equipment, place a call to this user / device combination to start the paging process. This same user can be included in the MX's standard page groups. If not using the SIP paging capabilities of the CyberData equipment, this section may be skipped.

## 6.1 Create Generic SIP Profile

In order to create a Generic SIP Device, it is recommended to create a unique Generic SIP Device Profile to control the codecs, functions and number of lines used by

CyberData Equipment, this device profile should be the same profile used with the night ring device.

Make sure that the following options are selected.

**Sends SIP Register**: Checked.

**Supports SIP based configuration**: Checked.
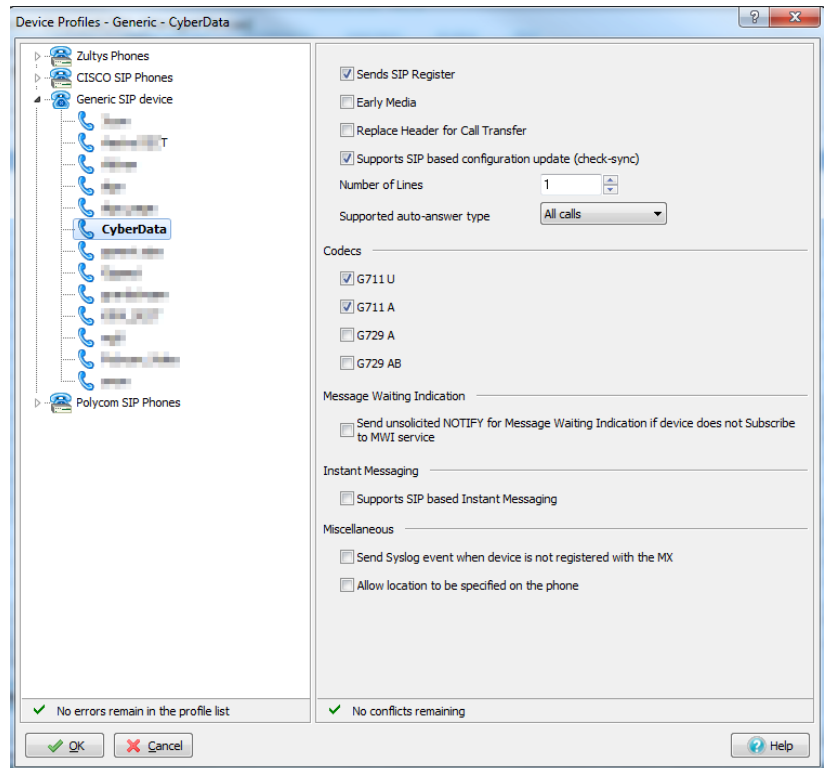
**Number of Lines**: 1.

**Supported auto-answer type**: All Calls.

**Codecs**: G711U and G711A.

**Send unsolicited NOTIFY for messages**: Checked.

**Send Syslog event when device is not registered..:** This is an optional selection that is recommended to allow the MX to generate a syslog notification if the paging equipment is off line

The remaining options are unchecked.
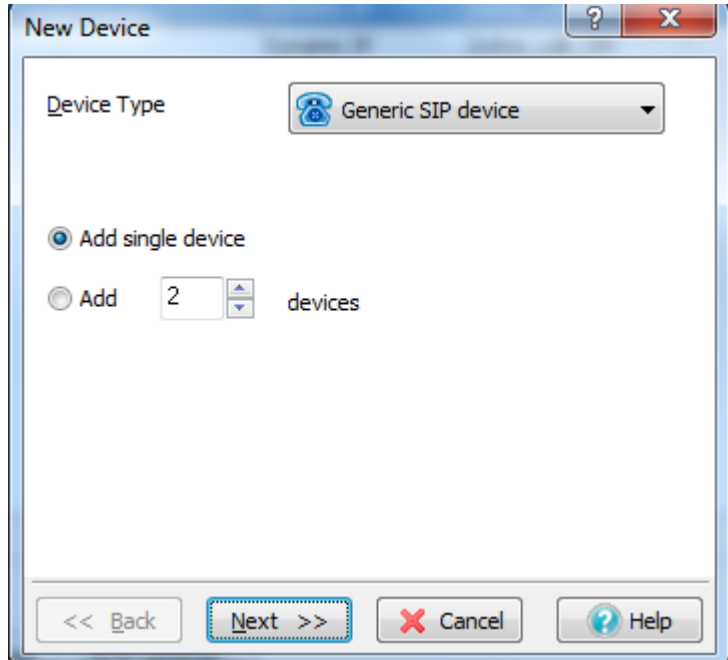
## 6.2  Create Generic SIP Device
Create a generic SIP device on the MX for the MX to integrate with CyberData Equipment.

Make sure that the following options are selected.

**Device Type:** Generic SIP
device.

**Add Single Device**:
Selected.

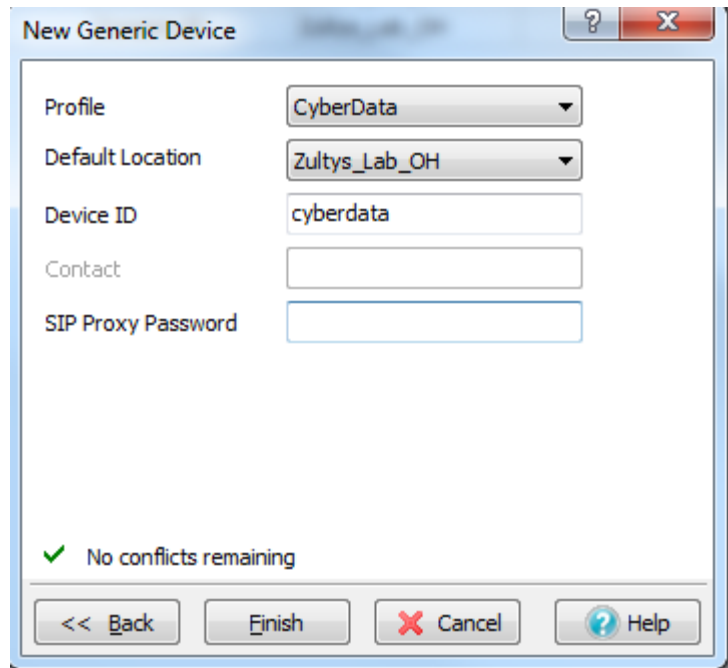Click *Next* to proceed to
the next screen.

**Profile**: Select the Generic
SIP Device Profile created
in section 6.1.

**Default Location**: Select
the proper location from
the drop-down.

**Device ID**: Type the ID to
register CyberData Paging
extension.

**Contact**: Not used.

**SIP Proxy Password**:
Type the password if
required.

## 6.3  Create User and Assign User to the Device

After creating the device that will interface with CyberData Paging Equipment, create a
user and assign the user to this device. This document assumes the reader is a ZCSE
trained and a certified technician. Since this process is covered by ZCSE training, it is

considered to be outside the scope of this document. Note that you need to create and assign a paging profile to the user if they will be using SIP paging.

# 7 MX Paging Server and User Configuration

This section is only used if you are integrating the CyberData SIP Paging Server with the MX Page Server, if you are using the pure multicast implementation, this section should be skipped.

## 7.1 Create MX Paging Groups

In the MX Administrator under Configure | Phone Services on the Paging Groups tab create the Paging Group. Analog Port should not be checked as any traditional paging equipment will be integrated to the CyberData SIP Paging Server itself.

| Name | Group | ▲ Prompt | Analog Port |
|---|---|---|---|
| Paging_Internal | 01 | ☑ | ☐ |
| | 02 | ☑ | ☐ |

Tabs: Auto Attendants | **Paging Groups** | Servers | Group Pickup | Conference | Voice.Mixer
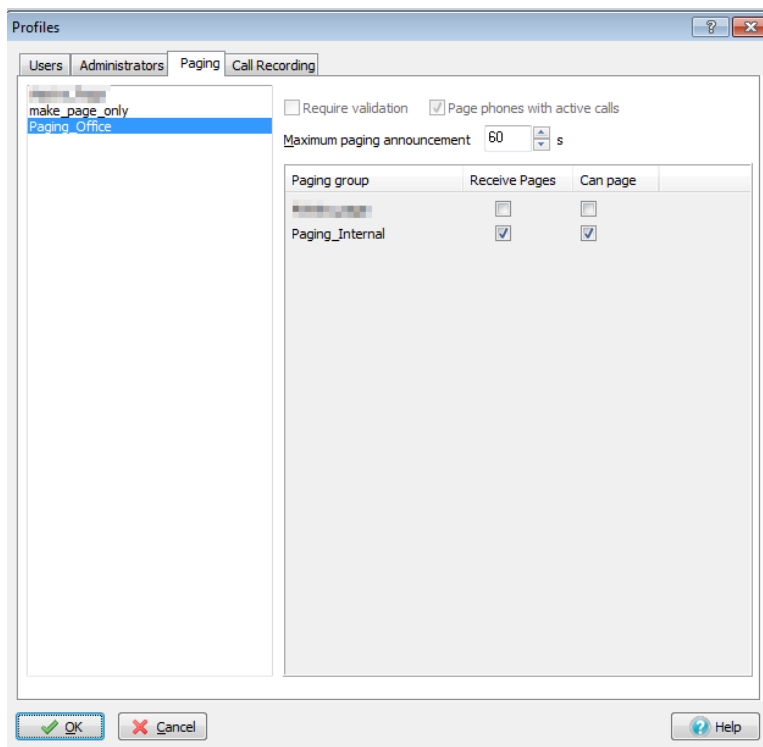
## 7.2 MX User Configuration for Paging User

In the MX Administrator under Configure | Users. Click on Profiles and create a new paging profile as indicated below, then assign this profiles to the paging server user by right clicking a single user and selecting "Edit User".

Select the appropriate Paging Profile and Paging Group.

**Receive Pages**: Checked

**Can Page**: Checked



Assign the paging Profile created above to the Paging User created.

From this same screen you can assign the paging device created in section 6 to this user

## 7.3 Configure all other users to be allowed to make pages

For users using ZIP3 and ZIP5 devices to be allowed to make a page, they must be a member of a paging profile that allows them to make a page, but not receive it, as they will be receiving the page as a multicast page.

Select the appropriate Paging Profile and Paging Group.
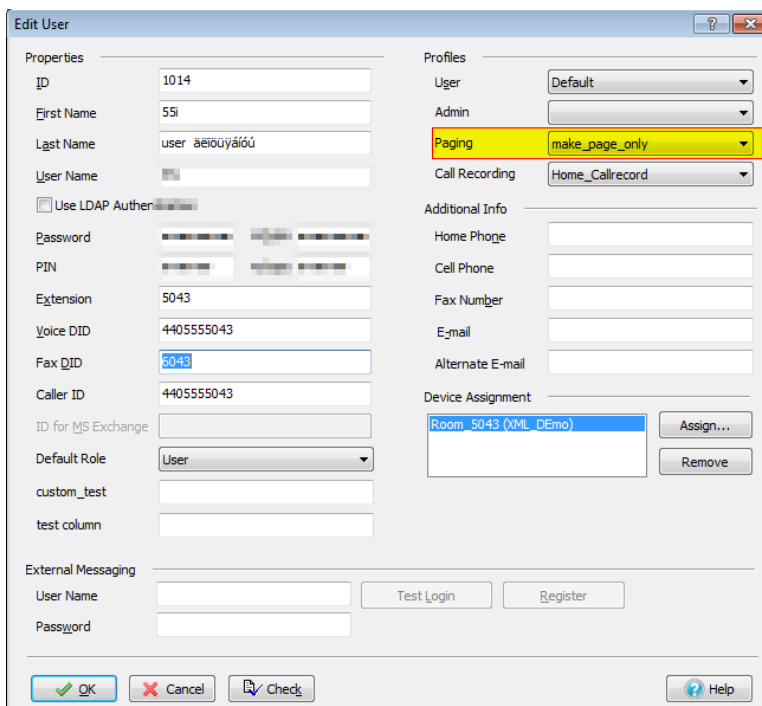
**Receive Pages**: Unchecked

**Can Page**: Checked

Assign the paging Profile created above to the Paging User created.

# 8 CyberData SIP Paging Server Setup

When deploying the CyberData SIP Paging server it is recommended to use DHCP. CyberData provides a "Discovery Utility" that can be downloaded from their website (http://www.cyberdata.net/support/voip/discovery_utility.html) to initially discover the IP address of the SIP Paging Server, once configured to register with the Zultys MX, the IP address can be found using the MX's device status screen in the MXAdministrator UI. Using the CyberData Discovery Utility to obtain the current IP address of the CyberData SIP Paging Server login using a web browser using the default username of "**admin**" and the default of "**admin**". For more information on using the discovery utility and basic setup of the CyberData equipment, please refer to the operating manuals from CyberData. If using the pure multicast integration option, the CyberData equipment will not be registering with the MX, and it is suggested to set static IPs to all CyberData equipment, or use the "Discover Utility" to identify the IP addresses assigned to the CyberData Equipment for future administration.

## 8.1 Connecting to the CyberData SIP Page Server

The CyberData SIP Paging Server now uses HTTPS to provision the device. When connecting to the CyberData Paging Server you will be required to accept the Self Signed certificate by clicking on "I understand the risks" link
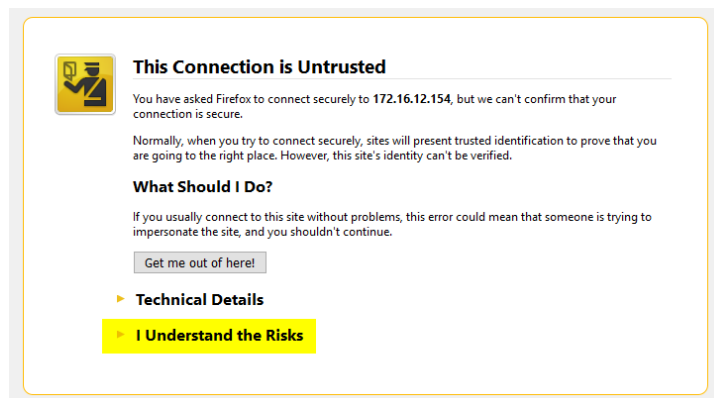


Then click "Add Exception"
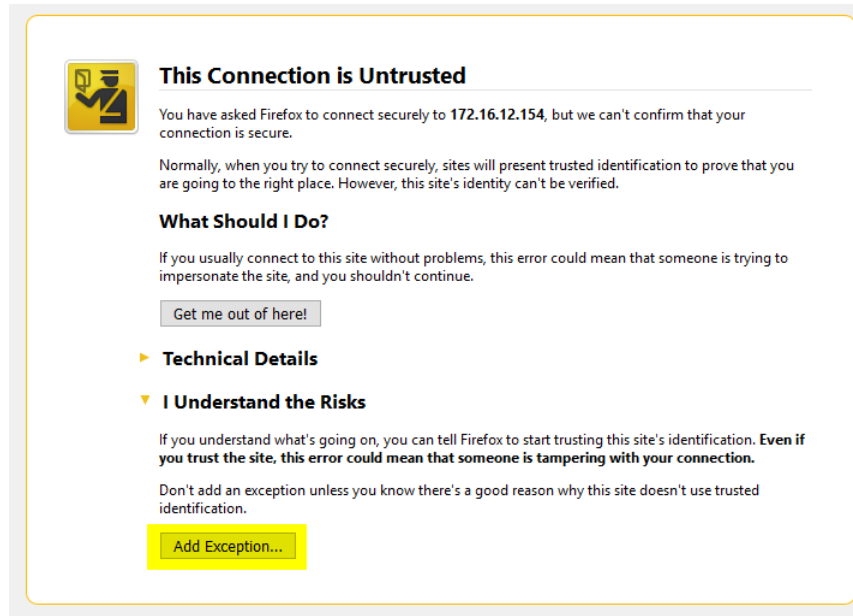
And then click Confirm Security Exception
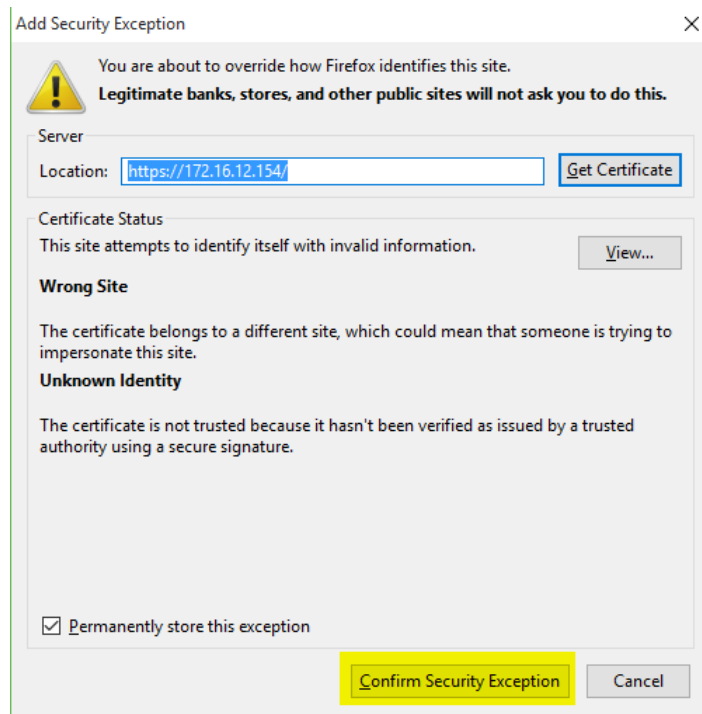


## 8.2 Home Screen

After loging into the CyberData SIP Paging server using your favorite browser you are immediately taken to the Home Screen which will display the following information

On the Left side you will find your navigation options,

**Change Username**: Type in this field to change the username (25 character limit).

- Default: **admin**

**Change Password**: Type in this field to change the password (19 character limit).

- Default: **admin**

**Confirm Password**: Type the password again in this field to confirm the new password (19 character limit).

**Current Status**:

Provides you with the current IP addressing of the device, Mac address and serial number.

The home screen will also show the current registration status, and features enabled on the CyberData SIP Paging Server.

Click on the Save button to save your configuration settings.

**Note**: You need to reboot for changes to take effect.

Click on the Reboot button to reboot the system.

## 8.3 Device Configuration

On the device configuration screen you can configure several default options for the paging server, and perform basic operation tests. The IP addresses and Port Numbers used in this document are example IP and port number, you may select the appropriate multicast IP address range and ports for your deployment.

**Note**: Multicast Address used on this screen cannot be a multicast address used for your paging groups.

**Note**: The below configuration assumes the installer is NOT use the line/line out options. If you are using Line and Line out options you will want to make required adjustments for Line In/Line Out configuration options.

**Device Name**: Shows the device name (25 character limit). If using multiple paging servers, please provide a unique name for each server.

**DTMF Duration:** The duration, in milliseconds, of DTMF tones played out of the device's analog audio ports (0-65535). :500

**Disable HTTPS (NOT recommended):** Disables the encrypted connection to the webpage. We do not recommend disabling HTTPS for security reasons. :Unchecked

**Beep on Initialization**: Checked

**Beep on page**: Checked

**Enable line-in to line-out loop back**: Unchecked
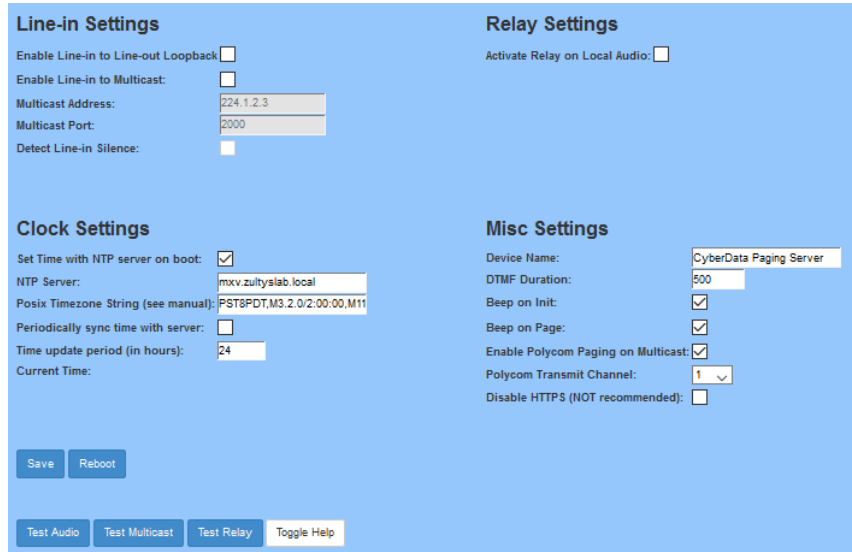
**Enable line-in to multicast**: Unchecked

**Multicast Address**: IP of your choice

**Multicast Port**: port of your choice

**Detect line-in silence**: Not Checked
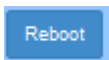
**Activate relay on local audio**: Not Checked

**Line-in Settings**

Enable Line-in to Line-out Loopback ☐
Enable Line-in to Multicast: ☐
Multicast Address: 224.1.2.3
Multicast Port: 2000
Detect Line-in Silence: ☐

**Relay Settings**

Activate Relay on Local Audio: ☐

**Clock Settings**

Set Time with NTP server on boot: ☑
NTP Server: mxv.zultyslab.local
Posix Timezone String (see manual): PST8PDT,M3.2.0/2:00:00,M11
Periodically sync time with server: ☐
Time update period (in hours): 24
Current Time:

**Misc Settings**

Device Name: CyberData Paging Server
DTMF Duration: 500
Beep on Init: ☑
Beep on Page: ☑
Enable Polycom Paging on Multicast: ☑
Polycom Transmit Channel: 1 ⌄
Disable HTTPS (NOT recommended): ☐

Save   Reboot

Test Audio   Test Multicast   Test Relay   Toggle Help

**CyberData SIP Paging Server Integration with MX SN 1461x (0000000522)**
**Revision 8 -- November 20, 2015**
**Page 18 of 31**

**Enable Polycom Paging on Multicast****

- Check if you wish to enable Polycom Multicast paging
- Enabling Polycom Paging will result in a standard RTP multicast being sent to the specified address and port and a Polycom PTT Page multicast being sent to the specified address and port+1

**Polycom Transmit Channel**:

- The channel used to submit the multicast page for Polycom Devices

**Save** Click on the Save button to save your configuration settings.

⚠️ **Note**: You need to reboot for changes to take effect.

**Test Audio** When the Test Audio button is pressed, you will hear a voice message for testing the device audio quality and volume.
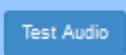
**Test Multicast** When the Test Multicast button is pressed, the Paging Server will send a five second canned ULAW message to a predetermined multicast address and port.

**Test Relay** Click on the Test Relay button to do a relay test.

**Reboot** Click on the Reboot button to reboot the system.

**ZULTYS**
INNOVATE | COMMUNICATE | COLLABORATE

Toggle Help    Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark ( ? ) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

### 8.4    Network Configuration

**Addressing Node** Select either DHCP IP Addressing or Static Addressing by marking the appropriate radio button. DHCP Addressing mode is enabled on

default and the device will attempt to resolve network addressing with the local DHCP server upon boot. If DHCP Addressing fails, the device will revert to the last known IP address or the factory default address if no prior DHCP lease was established.

**"Restore the Factory Default Settings"** for factory default settings. Be sure to click Save and Reboot to store changes when configuring a Static address.

**Hostname** This is the hostname provided by the DHCP server. See the DHCP/ DNS server documentation for more information. Enter up to 64 characters.

**IP Address** Enter the Static IPv4 network address in dotted decimal notation.

**Subnet Mask** Enter the Subnet Mask in dotted decimal notation.

**Default Gateway** Enter the Default Gateway IPv4 address in dotted decimal notation.

**DNS Server 1** Enter the primary DNS Server IPv4 address in dotted decimal notation.

**Stored Network Settings**

| | |
|---|---|
| Addressing Mode: | ○ Static ● DHCP |
| Hostname: | SipDevice033b7e |
| IP Address: | 10.10.10.10 |
| Subnet Mask: | 255.0.0.0 |
| Default Gateway: | 10.0.0.1 |
| DNS Server 1: | 10.0.0.1 |
| DNS Server 2: | 10.0.0.1 |
| DHCP Timeout in seconds*: | 60 |

*A value of -1 will retry forever*

**VLAN Settings**

| | |
|---|---|
| VLAN ID (0-4095): | 0 |
| VLAN Priority (0-7): | 0 |

Save   Reboot   Toggle Help

**Current Network Settings**

| | |
|---|---|
| IP Address: | 172.16.12.154 |
| Subnet Mask: | 255.255.255.0 |
| Default Gateway: | 172.16.12.1 |
| DNS Server 1: | 172.16.12.11 |
| DNS Server 2: | |

**DNS Server 2** Enter the secondary DNS Server IPv4 address in dotted decimal notation.

**DHCP Timeout in seconds** Specify the desired time-out duration (in seconds) that the device will wait for a response from the DHCP server before reverting back to the stored static IP address. The stored static IP address may be the last known IP address or the factory default address if no prior DHCP lease was established. Enter up to 8 characters. A value of -1 will retry forever.

Click on the Save button to save your configuration settings.

**Note**: You need to reboot for changes to take effect.

Click on the Reboot button to reboot the system.

Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark ( ? ) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

**Stored Network Settings**

| | |
|---|---|
| Addressing Mode: | ○ Static ● DHCP |
| Hostname: | SipDevice033b7e |
| IP Address: | 10.10.10.10 |
| Subnet Mask: | 255.0.0.0 |
| Default Gateway: | 10.0.0.1 |
| DNS Server 1: | 10.0.0.1 |
| DNS Server 2: | 10.0.0.1 |
| DHCP Timeout in seconds*: | 60 |

* A value of -1 will retry forever

**VLAN Settings**

| | |
|---|---|
| VLAN ID (0-4095): | 0 |
| VLAN Priority (0-7): | 0 |

Save  Reboot  Toggle Help

**Current Network Settings**

| | |
|---|---|
| IP Address: | 172.16.12.154 |
| Subnet Mask: | 255.255.255.0 |
| Default Gateway: | 172.16.12.1 |
| DNS Server 1: | 172.16.12.11 |
| DNS Server 2: | |

### 8.5 SIP Configuration

SIP configuration screen is used to configure the SIP registration parameters used by the CyberData SIP Page Server to register with the MX for paging purposes. The SIP User ID and Authentication ID are the same values which is the Device ID created in the MX in section 6 and assigned to the user created in section 6. Authentication Password is only used if a SIP Proxy Password is required by the Generic SIP Device created in the MX.

If using MXNetwork with Redundancy it is suggested to add the redundant node to the backup SIP server of the CyberData Paging Server, this way in a failover situation the paging equipment will continue to function with no intervention.

**Enable SIP Operation**: Checked

**SIP Server**: IP or FQDN of the MX

**Backup SIP Server 1**: Only Used if using MXNetwork with failover, then will be the IP address or FQDN of the failover node. Will dual register with the MXNetwork Node

**Backup SIP Server 2**: Not Used

**Remote SIP Port:** 5060

**Local SIP Port**: 5060

**Outbound Proxy**: must be left blank

**Outbound Proxy Port**: 0

**SIP User ID**: the Device ID created on the MX in Section 6

**Authentication ID**: Same as User ID

**Authentication Password**: the SIP Proxy Password for the Device ID created in section 6 (if required)

**Register with a SIP Server**: Checked

**Re-registration Interval**: 3600

**Unregister on Reboot**: Unchecked

⚠ **Note**: if checked will create an issue on registration, and the device will fail to register.

**Buffer SIP Calls**: Optional, if checked the CyberData SIP Server will buffer the page, and once the call is disconnected, it will make the page.

**RTP Port (even):** 20000

**SIP Settings**

| | |
|---|---|
| Enable SIP operation: | ☑ |
| Register with a SIP Server: | ☑ |
| Use Cisco SRST: | ☐ |
| Primary SIP Server: | 172.16.12.250 |
| Primary SIP User ID: | cyberdata |
| Primary SIP Auth ID: | cyberdata |
| 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: | |
| Outbound Proxy Port: | 0 |
| 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: | 172.16.12.250 |
| Remote SIP Port: | 5060 |
| Local SIP Port: | 5061 |
| Outbound Proxy: | |
| Outbound Proxy Port: | 0 |
| User ID: | nightringer |
| Authenticate ID: | nightringer |
| Authenticate Password: | ●●●●●● |
| Re-registration Interval (in seconds): | 360 |
| Relay rings to multicast: | ☐ |
| Multicast Address: | 234.2.1.1 |
| Multicast Port: | 10002 |

**Call Disconnection**

| | |
|---|---|
| Terminate Call after delay: | 0 |

**RTP Settings**                Save  Reboot  Toggle Help

| | |
|---|---|
| RTP Port (even): | 20000 |

## 8.6 Nightringer Configuration

Nightringer configuration screen is used to configure the SIP registration parameters used by the CyberData SIP Page Server to register with the MX for Night Bell or Nightringer purposes. The SIP User ID and Authentication ID are the same values which is the Device ID created in the MX in section 5 and assigned to the user created in section 5. Authentication Password is only used if a SIP Proxy Password is required by the Generic SIP Device created in the MX.

**Enable Nightringer**: Checked

**SIP Server**: IP or FQDN of the MX

**Remote SIP Port:** 5060

**Local SIP Port**: 5061, must be Port 5061

**User ID**: the Device ID created on the MX in Section 5

**Authentication ID**: Same as User ID

**Authentication Password**: the SIP Proxy Password for the Device ID created in section 5(if required)

**Re-registration Interval**: 3600

**Relay rings to multicast**: If you wish all multicast devices to receive the ringer page, CHECK this check box

**Multicast Address**: the IP Address to send the nightringer page to

**Multicast Port**: the Port Address to send the nightringer page to

Click on the Save button to save your configuration settings.

| SIP Settings | | Nightringer Settings | |
|---|---|---|---|
| Enable SIP operation: | ☑ | Enable Nightringer: | ☑ |
| Register with a SIP Server: | ☑ | SIP Server: | 172.16.12.250 |
| Use Cisco SRST: | ☐ | Remote SIP Port: | 5060 |
| Primary SIP Server: | 172.16.12.250 | Local SIP Port: | 5061 |
| Primary SIP User ID: | cyberdata | Outbound Proxy: | |
| Primary SIP Auth ID: | cyberdata | Outbound Proxy Port: | 0 |
| Primary SIP Auth Password: | •••••• | User ID: | nightringer |
| | | Authenticate ID: | nightringer |
| Backup SIP Server 1: | | Authenticate Password: | •••••• |
| Backup SIP User ID 1: | | Re-registration Interval (in seconds): | 360 |
| Backup SIP Auth ID 1: | | Relay rings to multicast: | ☐ |
| Backup SIP Auth Password 1: | | Multicast Address: | 234.2.1.1 |
| | | Multicast Port: | 10002 |
| Backup SIP Server 2: | | | |
| Backup SIP User ID 2: | | **Call Disconnection** | |
| Backup SIP Auth ID 2: | | Terminate Call after delay: | 0 |
| Backup SIP Auth Password 2: | | | |
| Remote SIP Port: | 5060 | | |
| Local SIP Port: | 5060 | | |
| Outbound Proxy: | | | |
| Outbound Proxy Port: | 0 | | |
| Disable rport Discovery: | ☐ | | |
| Buffer SIP Calls: | ☐ | | |
| Re-registration Interval (in seconds): | 360 | | |
| Unregister on Boot: | ☑ | | |
| Keep Alive Period: | 10000 | | |

**Note**: You need to reboot for changes to take effect.

Click on the Reboot button to reboot the system.

Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark ( ? ) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

### 8.7   PGROUPS (Paging Groups)

A PGROUP is a way of assigning multicast IP addresses and port numbers when configuring CyberData multicast paging. To assign a multicast address, you must first configure the ZIP3, ZIP5 and CyberData VoIP speakers that you want to put into a paging zone by entering a particular multicast address and port number combination in the Advanced Tab of the ZIP3 and ZIP5 device profiles, and web configuration for CyberData VoIP speakers. Each zone must have a unique IP address and Port number. The Port number must be even. The PGROUPS Configuration page consists of four pages. Each page must be saved independently.

To edit a paging group, click on the Edit button for the particular group you wish to edit. In the popup windows enter your configuration options for that paging group.

**Bypass DTMF**:

- When integrating with the MX's built in paging server, this option should be CHECKED. This will allow the CyberData SIP Page Server to automatically answer the paging SIP Call and relay the page through PGROUP 00.
- When not integrating with the MX's paging server and the CyberData SIP Page Server will control the zones(s) this options should be left UNCHECKED.

**Address**: Enter the IP address of the PGROUP.

- **Note**: To disable a relay on a group, use an IP address of 0.0.0.0.

**Port**: Enter the port number of the PGROUP.

- **Note**: The port range can be from 2000 to 65534 and must be even.

**Name**: Enter a name for the PGROUP.

**TTL**: The TTL field allows you to adjust the TTL. TTL is "time to live" and it describes how many networks (routers) a packet will go through before it is discarded. For more information, Zultys does not support or recommend routing Multicast Paging

**Line-out**: The Lineout field determines whether or not the V3 Paging Server will play audio out of the line-out port in addition to forwarding it to the PGROUP.

**Security Code**: This field allows the user to add a security code to prevent unauthorized paging to the PGROUP. Code must be between two to five numeric digits (0 through 9). Leave the field empty for no security code. Any security code

**Paging Groups**

Bypass DTMF ☑

| # | Address | Port | Name | Code | TTL | Lineout | |
|---|---------|------|------|------|-----|---------|---|
| 0 | 234.2.1.1 | 10002 | 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 |
| 6 | 234.2.1.7 | 2012 | PagingGroup06 | | 255 | Yes | Edit |

**Configure PGROUP**

| | | |
|---|---|---|
| PGROUP | 0 | Save Changes |
| Address | 234.2.1.1 | Cancel |
| Port | 10002 | |
| Name | PagingGroup00 | |
| Security Code | | |
| TTL | 255 | |
| Line-out | ☑ | |

entered for PGROUP 0 will be ignored if DTMF is bypassed.

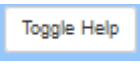Click on the Save button to save your configuration settings.
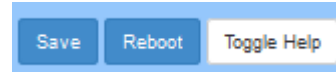
⚠️ **Note**: You need to reboot for changes to take effect.
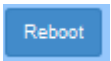
Click on the Reboot button to reboot the system.
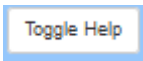
Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark ( ? ) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

### 8.8  Audio Files

CyberData SIP Paging Server allows you replace all the prompts used by the paging server with your own custom paging prompts. Custom prompts must be saved as

```
WAVE audio, Microsoft PCM, 16 bit, mono 8000 Hz
```

Zultys Technical Support can provide prompts matching the Zultys voice prompts upon request.

Custom files may be uploaded for all prompts played by the CyberData SIP Paging Server
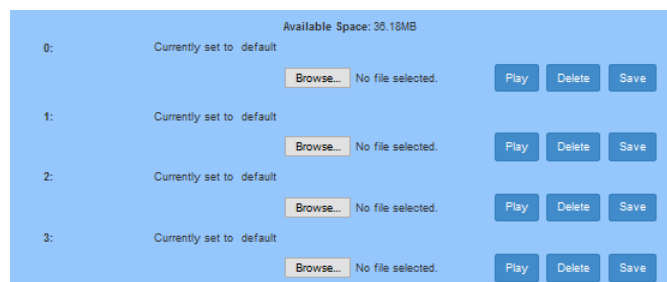
The Save button will download a new user audio file to the board once you've selected the file by using the Browse button.

Delete   The Delete button will delete any user uploaded audio and restore the stock audio file.

Play   The Play button will play that audio file

Browse...   The Browse button will allow you to navigate to and select an audio file

## 9  Polycom Devices

### 9.1  To Listen for Multicast paging

In MX Administrator Navigate to the Polycom profile and select the Advanced tab of the device profile to enable the Polycom to listen to a Multicast page. Add the following lines to the advanced tab. It is important to remember the listening port is +1 from the ZIP3 and ZIP5 devices from the CyberData Paging Server.

```
<ptt ptt.address="234.2.1.1" ptt.allowOffHookPages="0"
ptt.codec="G.711mu" ptt.compatibilityMode="1"
ptt.defaultChannel="1" ptt.displayName=""
ptt.emergencyChannel="25" ptt.payloadSize="20" ptt.port="10003"
ptt.priorityChannel="24">
    <ptt.callWaiting ptt.callWaiting.enable="0">
    </ptt.callWaiting>
    <ptt.emergencyChannel ptt.emergencyChannel.volume="-10">
    </ptt.emergencyChannel>
    <ptt.pageMode ptt.pageMode.allowOffHookPages="0"
ptt.pageMode.codec="G.711mu" ptt.pageMode.defaultGroup="1"
ptt.pageMode.displayName="" ptt.pageMode.emergencyGroup="25"
ptt.pageMode.enable="1" ptt.pageMode.payloadSize="20"
ptt.pageMode.priorityGroup="24">
        <ptt.pageMode.transmit>
          <ptt.pageMode.transmit.timeout
ptt.pageMode.transmit.timeout.continuation="60"
ptt.pageMode.transmit.timeout.initial="0">
          </ptt.pageMode.transmit.timeout>
        </ptt.pageMode.transmit>
    </ptt.pageMode>
    <ptt.pttMode ptt.pttMode.enable="1">
    </ptt.pttMode>
  </ptt>
```

# 10 Configuration for ZIP5 devices

An Administrator can add the following parameters in the Advanced Tab of the device profile to create Paging Groups or Zones that the phones will listen to.

For incoming RTP multicasts, the ringing display is dependent on the "Allow Barge-In" parameter. If this parameter is disabled, and there is no other call on the phone, then the paging is automatically played via the preferred audio device (see the model-specific IP Phone User Guide for setting Audio Mode on the phone).

If there is an existing call on the phone, the call initially displays in the ringing state. The user has the option to accept/ignore the call. If the "Allow Barge-In" parameter is enabled, the RTP multicast call barges in, and any existing calls are put on hold.

If an RTP multicast session already exists on the phone, and the phone receives another incoming RTP multicast session, the priority is given to the first multicast session and the second multicast session is ignored. The behavior for the incoming calls in this case is also based on the setting for the "Allow Barge-in" parameter. The incoming call is handled as if there were an existing call already on the phone.

## 10.1 Phone Configuration from the Advance Tab of the ZIP5 profile

For ZIP5 devices, you will only need to define the multicast IP and Port combination(s) the phone will be listening to. To make the page the user will simple call the paging extension/or MX Page Server depending on the integration process used.

- **paging group listening**: Allows you to specify up to 5 listening multicast addresses to send/receive a Real Time Transport Protocol (RTP) stream to/from these pre-configured multicast address(es). Each multicast IP and port combination is separated by a comma.

### 10.1.1 Example 1

In the below example we are creating a single page zone which this phone will receive pages from.

```
paging group listening : 234.2.1.1:10002
```

### 10.1.2 Example 2

In the below example we are creating a multiple page zones which this phone will receive pages from. This device will listen to 2 different paging groups as defined in the paging group listening entry.

```
paging group listening : 234.2.1.1:10002, 234.2.1.1:10004
```

## 10.2 Multiple Zones or Groups

If using multiple page groups or zones, for proper integration with ZIP3 and CyberData devices you must assign a unique IP address and unique port for each zone.

To configure the device to listen to multiple paging groups, add each additional unique IP and port pair to the "`page group listening :`" entry separated by a comma.


# 11 Configuration for ZIP3 Devices

You can configure a specific key on the phone from MX Administrator that will allow you to send or receive a page to or from pre-configured multicast address(es). The ZIP3 may listen to up to 10 different page groups.

## 11.1 To Listen for Multicast paging

In MX Administrator Navigate to the ZIP3 profile and select the Advanced tab of the device profile to enable the ZIP3xi to listen to a Multicast page. Add the following lines to the advanced tab:

11.1.1   ZIP33i, 35i and 37G
```
[ cfg:/phone/config/vpPhone/MulticastPage.cfg,reboot=0 ]
ListenAddress1.Label = Page_MC
ListenAddress1.IPAddress = 234.2.1.1:10002
ReceivePriority.Active = 1
ReceivePriority.Priority = 0
```


11.1.2   ZIP36G

```
ListenAddress1.Label = Cyber_MC
multicast.listen_address.1.label = Cyber_MC
multicast.listen_address.1.ip_address = 234.2.1.1:10002
multicast.receive_priority.enable =1
multicast.receive_priority.priority = 0
```

## 11.2 Configuring Page Button

In MX Administrator Navigate to the ZIP3 profile and select the advanced tab of the device profile to enable the ZIP3xi to make a Multicast page. Add the following lines to the advanced tab. In the below example, the "Page" key is the 6$^{th}$ key (or the last/bottom key).

11.2.1   ZIP33i, 35i and 37G

```
[ cfg:/phone/config/vpPhone/vpPhone.ini,reboot=1 ]
memory6.DKtype = 24
memory6.Line = 0
memory6.Value = 234.2.1.1:10002
memory6.PickupValue =
```

### 11.2.2  ZIP36G

```
linekey.6.type = 24
linekey.6.line = 0
linekey.6.value = 234.2.1.1:10002
linekey.6.pickup_value =
```

## 11.3 Multiple Zones or Groups

Each new zone or group requires a unique IP address and Port. If you use the same port for all zones but a unique IP paging will not work.

To add multiple listening groups, change the N value to a value between 1 and 10, and assign a unique IP and port for each page group.

```
ListenAddressN.Label = Page_MC
ListenAddressN.IPAddress = [Unique IP]:[Unique Port]
```

# 12 MXNetwork Integration

## 12.1 Paging Between Nodes

Integrating the CyberData SIP Page Server with MXNetwork allows for quick and easy integration of paging between the nodes. Use of the CyberData SIP Paging server allows the users to dial the extension of the CyberData SIP Paging Server at the remote node to use the CyberData SIP Paging Server's Multicast capability to page users local to the CyberData SIP Paging Server.

### 12.1.1  Paging Between Nodes Using CyberData Paging Extension

When using the CyberData SIP Paging Server with MXNetwork, the remote nodes (nodes that the CyberData Paging Server is NOT registered on) may call the SIP Paging Extension number directly.

### 12.1.2  Paging Between Nodes Using MX Page Server

The paging system needs to be designed in such a way that any node may page users on any other node. The MXnetwork is connected via a fully functional VPN network. Each node is running 6.0.10+ firmware, and the users are using ZIP2x2 phones using 1.2.30 firmware, Polycom Phones running 3.2.x firmware, and ZIP5 phones running 3.2.2.x firmware.

The user will dial an access/routing code to be routed to the appropriate node in the MXnetwork, with the appropriate page group ID. (Example: *5101) The page server on that MX Node will require the users voicemail password/PIN number to complete the page. For more details see MXNetwork Documentation available from Zultys Technical Support.

## 12.2 Failover Situation

In a failover situation users will have to dial the extension of the CyberData Paging Server itself, as Paging Information is not included in the fail over process currently.